

PRIFYSGOL CYMRU

Y Drindod Dewi Sant

UNIVERSITY OF WALES

Trinity Saint David

Wales Institute of Science and Art (WISA)

**The novel Proof of Efficiency (PoEf) Consensus
Mechanism: improved efficiency and cybersecurity for
Blockchain-based Supply Chain Management Systems.**

by

Odayne R. Haughton

Director of Studies: Professor (Associate) Carlene Campbell

Supervisors: Dr Irina Neaga & Dr Terry Walcott

Submitted in part fulfilment of the requirements for the degree of Doctor of
Philosophy in Computing at the University of Wales Trinity Saint David

October 2024

Declaration

This work has not previously been accepted in substance for any degree and is not being concurrently submitted as a candidature for any degree.

Signed (candidate)

Date

STATEMENT 1

This thesis results from my own investigations, except where otherwise stated. Where correction services have been used, the extent and nature of the correction are clearly marked in footnote(s). Other sources are acknowledged by footnotes giving explicit references. A bibliography is appended.

Signed (candidate)

Date

STATEMENT 2

I hereby consent to my thesis being available for deposit in the University's digital repository if accepted.

Signed (candidate)

Date

Abstract

The rapid growth of blockchain technology in Supply Chain Management (SCM) since 2016 has highlighted the need for faster, more reliable, and transparent data exchanges. However, current blockchain consensus mechanisms struggle to meet the efficiency and scalability requirements of modern SCM systems while remaining vulnerable to attacks. This thesis explores the optimisation of consensus mechanisms, particularly focusing on improving scalability, security, and performance. The research makes three key contributions. First, a Systematic Literature Review (SLR) of 108 peer-reviewed articles was conducted, identifying major blockchain vulnerabilities in consensus mechanisms, smart contracts, network-level attacks, and cryptographic challenges. Second, the thesis introduces the novel Proof of Efficiency (PoEf) consensus mechanism, an improvement over the traditional Practical Byzantine Fault Tolerance (PBFT) system. PoEf integrates sharding and a reputation-level score to enhance scalability and security. This mechanism dynamically adjusts the reputation of nodes based on the performance, ensuring high throughput, low latency, and scalability. Simulation results using BlockSim confirm that PoEf delivers higher throughput, lower latency, and greater scalability, making it more suitable for supply chain operations. Third, a Decision Matrix compares the performance and security of various consensus mechanisms, offering guidance for selecting the best fit for specific SCM requirements. Overall, PoEf represents a significant advancement in blockchain consensus mechanisms, demonstrating its potential to improve performance and handle large-scale SCM operations efficiently.

Keywords: Blockchain Technology, Supply Chain Management (SCM), Consensus Mechanisms, Proof of Efficiency (PoEf), Efficiency Evaluation, Blockchain Cybersecurity Issues

Acknowledgements

My deepest gratitude is extended to my supervisory team, with a special acknowledgement to Professor Carlene Campbell, my director of studies. Her enthusiasm, insight, and unwavering support have been the compass throughout my doctoral journey. Carlene's dedication to research excellence and her genuine concern for the well-being of her students have left an indelible mark on me, both academically and personally. Her mentorship has been a source of inspiration and strength, for which I am immensely thankful.

I am equally grateful to Dr Terry Walcott and Dr Irena Neaga, whose guidance and technical expertise have been fundamental in shaping and realising this project. The encouragement and enthusiasm have been instrumental in highlighting the uniqueness and potential of this work.

Special thanks are due to Graham Howe for his interest in and support of my research and for providing essential funding through MADE Cymru. His insights into the manufacturing aspect of this project have been invaluable, adding a practical dimension that transcended theoretical boundaries. I would also like to thank Professor Stephen Hole, my examination chair, for his constructive feedback, support, and consistent encouragement. I thank the School of Applied Computing and WISA staff at UWTSD for creating an enriching and motivational study environment. I am also thankful to the team at Blockchain Connected for the initial grant, which laid the groundwork for developing the blockchain facility that was crucial in the early stages of my research.

My heartfelt appreciation goes to my family for the endless support and patience. To my wife, Maisha, I owe a special debt of gratitude. Your love, sacrifices, unwavering encouragement, and belief in me, even during moments of doubt, have been my bedrock. To my darling daughter Naqeebah, you are absolute magic, the love and light of my life. I hope I can make you proud. To my dearest mother, Herma, I am forever indebted to you for everything you have done to fulfil my dreams; I continue to lean on your unbreakable strength, a light source in my life. Your presence and support have been my constant motivation, and I am eternally grateful for this.

Finally, my warmest regards to brother Andre, my friends Camir and Aubrey and everyone else who supported me in any capacity during the completion of this thesis. Your support has been a cornerstone of my success, and I am forever grateful.

Allahumma a'inni ala dhikrika, wa shukrika, wa husni 'ibadatika

Table of Contents

| | | |
|----------|--|-----------|
| 1 | INTRODUCTION | 1 |
| 1.1 | BACKGROUND & CONTEXT: BLOCKCHAIN-BASED SUPPLY CHAIN MANAGEMENT | 1 |
| 1.2 | PRIOR WORK: THE MODERN SUPPLY CHAIN | 2 |
| 1.3 | PROBLEM STATEMENT: THE NEED TO EXAMINE BLOCKCHAIN USE IN SCM..... | 3 |
| 1.4 | MOTIVATIONS FOR THE STUDY | 4 |
| 1.4.1 | IMPROVES EFFICIENCY AND CYBERSECURITY: PREDOMINANT CONCERNS IN DIGITAL SCM..... | 5 |
| 1.4.2 | PRACTICAL, ECONOMIC AND SOCIAL SIGNIFICANCE | 5 |
| 1.4.3 | INNOVATION AND PROGRESS | 6 |
| 1.5 | RESEARCH AIM AND OBJECTIVES | 6 |
| 1.5.1 | AIM | 6 |
| 1.5.2 | OBJECTIVES | 6 |
| 1.6 | SCOPE AND LIMITATIONS | 7 |
| 1.6.1 | SCOPE | 7 |
| 1.6.2 | LIMITATIONS | 7 |
| 1.7 | KEY CONTRIBUTIONS TO KNOWLEDGE | 8 |
| 1.7.1 | SLR: TAXONOMY OF CYBERSECURITY-RELATED EFFICIENCY ISSUES (MAIN CONTRIBUTION) | 8 |
| 1.7.2 | SIMULATION EVALUATION (MINOR CONTRIBUTION)..... | 8 |
| 1.7.3 | PROPOSITION OF A NOVEL CONSENSUS MECHANISM (MAIN CONTRIBUTION) | 9 |
| 1.7.4 | BLOCKCHAIN SELECTION MATRIX FOR EFFICIENT SCM SYSTEMS (MAIN CONTRIBUTION)..... | 9 |
| 1.8 | THESIS STRUCTURE | 10 |
| 1.9 | LIST OF PUBLICATIONS | 11 |
| 2 | BLOCKCHAIN AND ITS ROLE IN SUPPLY CHAIN MANAGEMENT..... | 12 |
| 2.1 | OVERVIEW | 12 |
| 2.2 | FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY..... | 12 |
| 2.2.1 | CATEGORIES OF BLOCKCHAINS | 12 |
| 2.2.2 | HOW DO BLOCKCHAINS WORK? | 14 |
| 2.2.3 | A BLOCK STRUCTURE | 16 |
| 2.3 | BLOCKCHAIN ARCHITECTURE | 17 |
| 2.3.1 | THE APPLICATION AND PRESENTATION LAYER | 18 |
| 2.3.2 | THE CONSENSUS LAYER..... | 19 |
| 2.3.3 | THE NETWORK LAYER | 23 |
| 2.4 | BLOCKCHAIN-BASED SUPPLY CHAINS..... | 24 |
| 2.5 | BLOCKCHAIN USE CASES IN SCM | 28 |
| 2.5.1 | PROVENANCE TRACKING AND TRACEABILITY | 28 |
| 2.5.2 | CIRCULAR ECONOMY AND SUSTAINABILITY..... | 29 |
| 2.5.3 | SUPPLY CHAIN FINANCE AND RISK MANAGEMENT | 30 |
| 2.6 | CHAPTER SUMMARY | 31 |
| 3 | RESEARCH DESIGN & METHODOLOGY | 33 |
| 3.1 | OVERVIEW | 33 |
| 3.2 | BACKGROUND..... | 33 |
| 3.3 | OVERVIEW OF THE RESEARCH METHODOLOGY EMPLOYED IN THIS STUDY..... | 35 |
| 3.3.1 | RESEARCH STRUCTURE..... | 35 |
| 3.3.2 | RESEARCH PHILOSOPHY | 35 |
| 3.3.3 | RESEARCH APPROACH..... | 36 |
| 3.4 | DATA COLLECTION METHODS | 36 |

| | | |
|----------|---|-----------|
| 3.4.1 | SYSTEMATIC REVIEW OF LITERATURE | 37 |
| 3.4.2 | EXPERIMENTAL COMPUTER SCIENCE | 41 |
| 3.4.3 | MEASURING PERFORMANCE OF CONSENSUS MECHANISM | 42 |
| 3.5 | CHAPTER SUMMARY | 43 |
| | | |
| 4 | SYSTEMATIC LITERATURE REVIEW: CYBERSECURITY VULNERABILITIES THAT AFFECT BLOCKCHAIN EFFICIENCY IN SCM SYSTEMS. | 44 |
| | | |
| 4.1 | OVERVIEW | 44 |
| 4.2 | INTRODUCTION | 44 |
| 4.2.1 | JUSTIFICATION FOR THE SYSTEMATIC REVIEW | 45 |
| 4.2.2 | RELATED WORK | 45 |
| 4.3 | SEARCH RESULTS | 47 |
| 4.3.1 | THE INCLUSION PARAMETERS | 48 |
| 4.4 | FINDINGS | 49 |
| 4.4.1 | PUBLICATIONS OVER TIME | 49 |
| 4.4.2 | PAPER CLASSIFICATION | 50 |
| 4.4.3 | BLOCKCHAIN-BASED SUPPLY CHAIN MANAGEMENT CYBERSECURITY TAXONOMY | 51 |
| 4.5 | DISCUSSION | 63 |
| 4.5.2 | CONSENSUS MECHANISM FAILURES (PRIORITY LEVEL: HIGH) | 65 |
| 4.5.3 | SMART CONTRACT VULNERABILITIES (PRIORITY LEVEL: MEDIUM-HIGH) | 65 |
| 4.5.4 | NETWORK-LEVEL ATTACKS (PRIORITY LEVEL: MEDIUM) | 66 |
| 4.5.5 | CRYPTOGRAPHIC CHALLENGES (PRIORITY LEVEL: MEDIUM-LOW) | 66 |
| 4.5.6 | SEQUENTIAL ORDER OF INVESTIGATION | 66 |
| 4.6 | CHAPTER SUMMARY | 67 |
| | | |
| 5 | TRADITIONAL CONSENSUS MECHANISMS IN SCM | 68 |
| | | |
| 5.1 | OVERVIEW | 68 |
| 5.2 | INTRODUCTION | 68 |
| 5.3 | EXPERIMENTAL SET-UP | 70 |
| 5.3.1 | BLOCKSIM | 70 |
| 5.3.2 | PERFORMANCE METRICS | 74 |
| 5.3.3 | SIMULATION PARAMETERS | 76 |
| 5.4 | SIMULATION RESULTS | 77 |
| 5.5 | RESULTS ANALYSIS | 79 |
| 5.5.1 | POW CONSENSUS MECHANISM | 79 |
| 5.5.2 | DPOS CONSENSUS MECHANISM | 80 |
| 5.5.3 | PBFT CONSENSUS MECHANISM | 80 |
| 5.5.4 | STELLAR CONSENSUS MECHANISM | 81 |
| 5.6 | CHAPTER SUMMARY | 82 |
| | | |
| 6 | NOVEL POEF, AN ENHANCED CONSENSUS FOR SCM | 84 |
| | | |
| 6.1 | OVERVIEW | 84 |
| 6.2 | BACKGROUND AND CONTEXT | 85 |
| 6.3 | PBFT CONSENSUS | 85 |
| 6.4 | POEF'S METHODOLOGY | 87 |
| 6.4.1 | OVERVIEW OF THE POEF CONSENSUS: | 87 |
| 6.4.2 | POEF'S NOVELTY | 89 |
| 6.4.3 | IMPLEMENTATION PHASES | 90 |
| 6.5 | THE EFFICIENCY OF POEF | 90 |
| 6.5.1 | POEF'S DESIGN | 90 |

| | | |
|----------|---|------------|
| 6.5.2 | POEF OPERATIONS | 97 |
| 6.6 | POEF, EFFICIENCY EXPERIMENTATION RESULTS | 104 |
| 6.6.1 | POEF'S THROUGHPUT | 105 |
| 6.6.2 | POEF'S LATENCY | 106 |
| 6.6.3 | SCALABILITY | 107 |
| 6.6.4 | PERFORMANCE GAP BETWEEN PBFT AND POEF | 110 |
| 6.7 | THE SECURITY OF POEF..... | 114 |
| 6.7.1 | POEF NODE'S NETWORK MODEL | 115 |
| 6.7.2 | POEF NODE'S AUTHENTICITY MODEL..... | 115 |
| 6.7.3 | POEF'S NODE TRUTHFUL-NESS MODEL BASED ON REPUTATION-LEVEL | 117 |
| 6.7.4 | POEF ENCRYPTION MODEL | 118 |
| 6.7.5 | VULNERABILITY THREAT MODELLING | 119 |
| 6.7.6 | CONSENSUS MECHANISM SIMULATIONS (WITH MALICIOUS NODES) | 123 |
| 6.8 | CHAPTER SUMMARY | 124 |
| 7 | EVALUATION AND DISCUSSION | 126 |
| 7.1 | OVERVIEW | 126 |
| 7.2 | A COMPARISON OF THROUGHPUT | 127 |
| 7.3 | AN EVALUATION OF LATENCY | 130 |
| 7.4 | AN EVALUATION OF SCALABILITY. | 132 |
| 7.4.1 | SCALABILITY THROUGHPUT..... | 132 |
| 7.4.2 | SCALABILITY LATENCY | 134 |
| 7.4.3 | OVERALL SCALABILITY ASSESSMENT | 135 |
| 7.5 | POEF'S COMPARISON WITH STELLAR | 136 |
| 7.6 | ADDITIONAL COMPARISON OF THE POEF MODEL WITH SIMILAR MODELS | 138 |
| 7.7 | DECISION MATRIX..... | 140 |
| 7.7.1 | PROOF OF WORK (POW)..... | 140 |
| 7.7.2 | DELEGATED PROOF OF STAKE (DPOS) | 141 |
| 7.7.3 | PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)..... | 141 |
| 7.7.4 | STELLAR..... | 142 |
| 7.7.5 | PROOF OF IMPORTANCE (POI) | 142 |
| 7.7.6 | PROOF OF CAPACITY (POC)..... | 143 |
| 7.7.7 | PROOF OF EFFICIENCY (POEF) | 144 |
| 7.8 | DECISION TREE MATRIX (THROUGHPUT, LATENCY, SCALABILITY)..... | 144 |
| 7.8.1 | KEY TAKEAWAYS FROM THE MATRIX:..... | 145 |
| 7.9 | CONSENSUS MECHANISM SELECTION | 145 |
| 7.9.1 | RECOMMENDATIONS FOR CONSENSUS MECHANISMS IN SCM:..... | 146 |
| 7.10 | CHAPTER SUMMARY | 148 |
| 8 | CONCLUSION AND FUTURE DIRECTIONS | 150 |
| 8.1 | INTRODUCTION | 150 |
| 8.2 | RESOLUTION OF THE AIM AND OBJECTIVES | 151 |
| 8.2.1 | AIM | 151 |
| 8.2.2 | OBJECTIVES | 151 |
| 8.3 | KEY CONTRIBUTIONS | 153 |
| 8.4 | CHALLENGES AND ETHICAL CONSIDERATIONS | 153 |
| 8.4.1 | CHALLENGES | 153 |
| 8.4.2 | ETHICAL CONSIDERATIONS..... | 154 |
| 8.5 | FUTURE WORK | 154 |
| 8.5.1 | ADDITIONAL LAYERS WITHIN THE BLOCKCHAIN | 154 |
| 8.5.2 | EXPANDING POEF'S SECURITY FEATURES | 155 |
| 8.5.3 | APPLYING POEF BEYOND SCM | 155 |

| | | |
|--------------|---|------------|
| 8.5.4 | REAL-WORLD DEPLOYMENT OF POEF..... | 155 |
| 9 | REFERENCES..... | 156 |
| 10 | APPENDICES | 168 |

List of Figures

| FIGURE | TITLE | PAGE NO. |
|--|---|----------|
| FIGURE 1.1 | Summary of the Chapters in thesis | 10 |
| FIGURE 2.1 | The blockchain architecture categories | 13 |
| FIGURE 2.2 | Illustrating how a transaction is initiated on the blockchain. | 14 |
| FIGURE 2.3 | The structure of blocks in a blockchain | 16 |
| FIGURE 2.4 | The various layers of the blockchain. | 18 |
| FIGURE 2.5 | Blockchain Consensus Mechanisms used in SCM | 21 |
| FIGURE 2.6 | Novel blockchain architecture framework from a SCM perspective | 25 |
| FIGURE 3.1 | The structure of the thesis by chapters | 34 |
| FIGURE 3.2 | Thesis research approach. | 35 |
| FIGURE 3.3 | Steps of the Systematic Review | 36 |
| FIGURE 4.1 | PRISMA flow diagram illustrating the SLR paper gathering process | 47 |
| FIGURE 4.2 | Graph illustrating the primary studies distribution by year of publication | 48 |
| FIGURE 4.3 | World bubble the main thematic areas in the primary studies. | 49 |
| FIGURE 4.4 | The main thematic areas of the Systematic Review | 50 |
| FIGURE 4.5 | Vulnerabilities that affect SCM-related blockchain systems. | 63 |
| FIGURE 5.1 | Blockchain Consensus Mechanisms model selection in BlockSim | 70 |
| FIGURE 5.2 | Illustrating the propagation protocol between two nodes (stakeholders) | 70 |
| FIGURE 5.3 | Simulation parameters in BlockSim | 71 |
| FIGURE 5.4 | The node input parameters to configure stakeholders and workers in BlockSim. | 72 |
| FIGURE 5.5 | BlockSim Simulation run result: executing the DPoS Consensus with 10 nodes for 10,000 transactions. | 73 |
| FIGURE 5.6 (a,b) - FIGURE 5.12(a,b) | Figures illustrating the throughput and latency simulation results for the PoW, DPoS, PoC, PoL, PBFT and SCP consensus mechanisms over multiple nodes and transactions. | 76-78 |
| FIGURE 6.1 | PBFT Consensus Mechanism Node Operation | 85 |
| FIGURE 6.2 | PoEf Consensus Mechanism Node Operation | 87 |
| FIGURE 6.3 | Key Features of PoEf Consensus Mechanism | 88 |
| FIGURE 6.4 | PoEf implementation phases | 89 |
| FIGURE 6.5 | Flowchart of the Consensus Mechanism, PoEf | 90 |
| FIGURE 6.6 | Flow diagram for Authorisation Network for PoEf. | 91 |
| FIGURE 6.7 | Registration Contract in the Authorisation Network for PoEf | 93 |
| FIGURE 6.8 | Flow diagram for the Stakeholder Network | 94 |
| FIGURE 6.9 | Authentication Contract in the Authorisation Network for PoEf | 96 |
| FIGURE 6.10 | The node operations across networks in PoEf | 97 |
| FIGURE 6.11 | The PoEf Consensus “Node Selection” procedure | 99-100 |
| FIGURE 6.12 | Transaction Contract inside the Stakeholder’s Network of PoEf | 101 |
| FIGURE 6.13 | Figure illustrating PoEf’s “Reach Consensus” procedure in BlockSim | 103 |
| FIGURE 6.14 | PoEf’s consensus “throughput” results from BlockSim simulation runs | 104 |
| FIGURE 6.15 | PoEf’s consensus “latency” results from BlockSim simulation runs | 105 |
| FIGURE 6.16 | PoEf’s Scalability (throughput)results with two network size (1,000 and 10,000) | 106 |
| FIGURE 6.17 | PoEf’s Scalability (latency) results with two network size (1,000 and 10,000) | 107 |
| FIGURE 6.18 | PoEf’s Throughput compared to PBFT (@10, 100, 200 nodes) | 110 |

| | | |
|-----------------|---|---------|
| FIGURE 6.19 | PoEf's Latency compared to PBFT (@10, 100, 200 nodes) | 112 |
| FIGURE 6.20 | Snippet of PoEf's threat model | 119 |
| FIGURE 6.21 | Block creation with 30% Malicious nodes | 112 |
| FIGURE 6.22 | Block creation with 45% Malicious nodes | 123 |
| FIGURE 7.1(a-h) | Consensus throughput comparison at scaling network sizes | 126-127 |
| FIGURE 7.2(a-h) | Figure illustrating consensus latency comparison at scaling network sizes | 129-130 |
| FIGURE 7.3 | Consensus Mechanisms Scalability (throughput) comparison | 131 |
| FIGURE 7.4 | Consensus Mechanisms Scalability (latency) comparison | 133 |
| FIGURE 7.5 | Stellar Consensus mechanism Node Operation | 135 |
| FIGURE 7.6 | Consensus Selection matrix for Blockchain-based SCM. | 145 |

List of Tables

| TABLE | TITLE | PAGE NO. |
|-----------------|---|----------|
| TABLE 2.1 | Highlighting approaches each consensus mechanism takes to achieve agreement within the network. | 21 |
| TABLE 4.1 | The principal vulnerabilities that affect SCM-related blockchain systems | 51-53 |
| TABLE 4.2 | Attack resilience of difference consensus mechanisms. | 57 |
| TABLE 5.1 | BlockSim Simulation input parameters and descriptions executed | 75 |
| TABLE 6.1 | Key responsibilities of Validator (S_H) and Subordinate (S_l) nodes in PoEf | 98 |
| TABLE 6.2 | the Scalability score for PoEf and PBFT (@10, 100, 200 nodes) | 112 |
| TABLE 7.1 | Throughput comparison for Reputation-based consensus. | 137 |
| TABLE 7.2 | Illustrating throughput, latency and scalability into different categories | 139 |
| TABLE 7.3 (a,b) | Decision matrix table for (Medium-Large scale SCM) | 143 |
| TABLE 8.1 | Recommended areas for future research | 154 |

List of Abbreviations *(in alphabetical order)*

| ABBREVIATION | FULL FORM |
|---------------------|--|
| BBSCM | Blockchain-based supply chain management |
| BFT | Byzantine Fault Tolerance |
| BWE | Bullwhip Effect |
| CPFR | Collaborative planning forecasting and restocking |
| CRM | Customer relationship management |
| DDoS | Distributed Denial of Service |
| DIFOT | Delivery In-Full On-Time |
| DLT | Distributed Ledger Technology |
| DoS | Denial-of-Service |
| DPoS | Delegated Proof of Stake |
| DSCSA | Drug Supply Chain Security Act |
| eDP | Estimated Delivery Performance |
| ERP | Enterprise resource planning |
| eSCM | e-Supply Chain Management |
| FBA | Federated Byzantine Agreement |
| GHOST | Greedy Heaviest Observed Subtree |
| ICT | Information and Communications Technology |
| IoT | Internet of Things |
| IT | Information Technology |
| OTIF | On-Time In-Full |
| PBFT | Practical Byzantine Fault Tolerance |
| PICOS | Population, Intervention, Comparison, Outcome, and Study |
| PKI | Public key infrastructure |
| PoC | Proof of Capacity |
| PoEf | Proof of Efficiency |
| Pol | Proof of Importance |
| PoPT | Proof of Previous Transaction |
| PoR | Proof of Reputation |
| PoS | Proof of Stake |
| PoS _{CS} | Proof-of-supply-chain-share |
| PoW | Proof of Work |
| PRISMA | Preferred Reporting Items for Systematic Reviews and Meta-Analyses |
| PoXR | Proof-of-X-Repute |
| RFID | Radiofrequency identification |
| RPoC | Reputation Proof of Cooperation |
| RQ | Research Question |
| SC | Supply Chain |
| SCM | Supply Chain Management |
| SCP | Stellar Consensus Protocol |
| SLR | Systematic Literature Review |
| TPS | Transactions Per Second |

Glossary of Terms

| Terms | Meaning in context of this thesis |
|--|--|
| Authenticity Model | Authenticity Model ensures that transactions and blocks are securely validated and added to the blockchain within an SCM network, maintaining integrity and consistency even in the presence of Byzantine nodes, by leveraging authenticated stakeholders, cross-verification of transactions, and a mechanism that guarantees the inclusion of valid transactions while preventing network forks. |
| BlockSim | A complete software tool and framework for creating and simulating discrete-event dynamic systems models for blockchain systems, supporting the investigation of numerous blockchain implementations and blockchains. |
| Bullwhip Effect (BWE) | The Bullwhip Effect is a supply chain phenomenon describing how small changes in consumer demand become more pronounced as they move up the supply chain from retailers to manufacturers. This demand data distortion may result in inefficiencies, higher expenses, and surplus inventory. |
| Byzantine Fault Tolerance | This is the ability of a computer system to continue operating even if some of its node's malfunction or act maliciously. |
| Collaborative planning forecasting and restocking (CPFR) | Describes a collection of procedures used by Supply Chain (SC) partners to schedule and convey important SC tasks, such as business planning, sales forecasting, and raw material and finished goods replenishment, to satisfy customer demand at the lowest possible cost. |
| Consensus layer | The consensus layer is the component in a blockchain architecture that has a role in ensuring the integrity, security, through the consensus mechanism with controls agreement among nodes within a blockchain network. |
| Consensus mechanism | Sits within the consensus layer. It refers to the entire stack of protocols, algorithms, incentives and rules that allow a network of nodes to agree on the state of a blockchain. |
| Delivery In-Full On-Time | An evaluation of the effectiveness of a SC's delivery process and quantifies the frequency with which customers receive what they want when they want it, paying particular attention to deliveries made from the customer's perspective. |
| Delegated Proof of Stake (DPoS) | An enhanced version of Proof of Stake that introduces a democratic voting system where stakeholders vote for a small number of delegates, who then validate transactions and create blocks on their behalf. |
| Deterministic models | Computational model that functions without relying on chance and future occurrences or outcomes may be precisely estimated based on known inputs and relationships. |
| Denial of Service (DoS) | DoS is an attack that disrupts network functions by overwhelming it with illegitimate requests, thereby impeding legitimate transactions and processes. |

| | |
|--|---|
| | Such attacks can cripple the efficiency of blockchain-based systems, causing significant delays and undermining the trust and operational continuity of supply chains. |
| Distributed Denial of Service (DDoS) | DDoS is a massive attack where the attacker disrupts the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic preventing users from accessing connected online services and sites. |
| Distributed Ledger Technology | A platform for decentralised record-keeping that securely stores data to ensure that it is accurate, synced, transparent, and unchanged (e.g. blockchain) DLTs give users the ability to safely execute, record, and verify the transactions without using an intermediary. |
| Double-spending attacks | Spending the same cryptocurrency or digital currency more than once, essentially duplicating money. |
| e-Supply Chain Management | Electronic-based SCM systems supported by Internet of Things technologies. |
| Enterprise resource planning | Enterprise Resource Planning (ERP) is a software system that enables organisations to manage and streamline the key business processes efficiently. ERP systems integrate various functions and departments within a company, facilitating real-time communication and data sharing among different areas such as accounting, human resources, procurement, inventory management. |
| Encryption model | The encryption model uses Elliptic Curve Cryptography (ECC) for secure communication between stakeholders, leveraging efficient key management with private and public keys, ensuring robust security and low resource usage suitable for SCM blockchain applications. |
| Estimated delivery performance | A commonly used Key Performance Indicator (KPI) in SCM. In measuring, the equation determines an organisation's capacity to provide goods and services in accordance with the criteria set by its clients, while considering the organisation's ability to satisfy client expectations in terms of both cost and turnaround time. |
| Federated Byzantine Agreement | A relatively new consensus mechanism where each node does not have to be known and verified ahead of time. Federated Byzantine Agreement (FBA) is a consensus mechanism used in blockchain and distributed network systems to achieve Byzantine Fault Tolerance (BFT) in a decentralised manner. |
| Greedy Heaviest Observed Subtree | Greedy Heaviest Observed Subtree (GHOST) is a chain selection protocol used in blockchain technology. It was originally proposed as a protocol modification to improve the security and efficiency of blockchain networks. |
| Hyperledger Fabric Lightning Networks | An open-source, permissioned blockchain framework for enterprise use. The Lightning Network is a secondary network for Bitcoin designed to address the issue of sluggish transaction speeds and exorbitant fees on the Bitcoin blockchain by implementing off-chain transactions. |

| | |
|--|---|
| Metadata | Data that offers details about other data is known as metadata, and it helps with information management, organisation, and comprehension. |
| Network Model | PoEfi node’s Network Model ensures secure communication between nodes in a partially synchronous blockchain network, using PBFT-based mechanisms to maintain consensus and fault tolerance, even in the presence of potentially malicious nodes. |
| Network partitioning attacks | Malicious actions intended to break up or split a computer network into disparate, frequently isolated sections. |
| On-Time In-Full | A supplier's capacity to deliver goods at full order quantities and within specified delivery windows is measured by this SC metric, which is used to evaluate performance in SCM. |
| Parallel transaction processing | The process that happens through sharding. It allows multiple transactions to be executed simultaneously, improving the system's throughput and scalability. By dividing transactions into smaller, independent groups (shards) and processing them in parallel, PoEfi ensures faster validation and block creation without the need for sequential execution. |
| Proof of Work (PoW) | A consensus mechanism that requires participants to perform computationally intensive tasks to validate new transactions and create new blocks, ensuring security through the physical cost of effort. |
| Proof of Stake (PoS) | A consensus mechanism where validators are chosen to create new blocks based on the amount of cryptocurrency they hold and are willing to “stake” or some as collateral, emphasising wealth or stake rather than computational power. |
| Practical Byzantine Fault Tolerance (PBFT) | A consensus mechanism designed to withstand system failures including malicious attacks, by employing a collective decision-making process that requires a supermajority of nodes to agree on any new entry in the ledger. PBFT is commonly tailored for distributed networks and ensures consensus amidst untrustworthy nodes offering a high level of security for SCM environments with moderate trust. |
| Proof of Importance (Pol) | A consensus mechanism used by the NEM blockchain network, which not only rewards participants with a high balance but also takes into consideration one's activity in transactions to incentivize active participation rather than merely holding wealth. |
| Reputation Proof of Cooperation (RPoC) | A consensus algorithm that uses a layered approach, segmenting nodes into groups (like Stellar) based on their reputation and past cooperative behaviour. |
| Proof-of-X-Repute (PoXR) | A consensus mechanism that integrates a reputation-based system with existing Proof-of-X protocols (like Proof-of-Stake or Proof-of-Authority). This technique influences nodes' consensus participation based on their reputation scores, which are created over time based on their conduct, reliability, and network contribution. High-reputation nodes are more likely to be chosen for block validation, encouraging trustworthy behaviour. |

| | |
|-------------------------|---|
| Re-entrancy attacks | Happens when a contract calls another contract before it resolves its state. This allows a function to be called numerous times in a single transaction when it is externally triggered while its being executed. |
| Scalability | Scalability refers to a system's ability to handle increased workload, transaction volume, or user demand without compromising performance. |
| Scalability score | The scalability score is a quantitative measure that combines throughput and latency to assess a system's ability to maintain optimal performance as workloads increase, balancing high transaction processing rates and low delays, crucial for efficient blockchain-based SCM operations. |
| Sharding | Sharding is a database partitioning technique that involves splitting a large dataset into smaller, more manageable pieces, called shards. In PoE refers to dividing the blockchain network into smaller groups of nodes (shards) that each handle a subset of transactions. |
| Smart contract | Smart contracts a series of program codes. Self-executing contract with buyer-seller terms placed directly into code. In the blockchain context, when predetermined circumstances are met, blockchain-stored programs execute automated agreements for irreversible but trackable transactions. |
| Snowballing | Refers to a method of finding more publications for a systematic literature review by looking through a paper's reference list or citations. |
| Supply Chain | An interconnected network of individuals, organisations, resources, activities, and technologies involved in the production and distribution of a product or service from supplier to customer. It encompasses all processes that transform raw materials into final products, ensuring that goods and services are produced efficiently and reach consumers effectively. |
| Supply Chain Management | The management of a product's or service's entire production process, from obtaining raw materials to shipping the final product to the client. |
| Transaction latency | The interval of time that passes between starting a transaction or making a payment and getting confirmation that it is authorised. This is a crucial efficiency metric. |
| Transaction throughput | The total number of transactions per second that the system can process in a set amount of time. This is a crucial efficiency metric. |
| Truthfulness Model | Truthfulness Model relies on assigning reputation scores to nodes, ensuring that only trusted nodes can add blocks without competition, thereby maintaining blockchain integrity and preventing attacks by limiting the influence of low-reputation nodes. |

1 Introduction

1.1 Background & Context: blockchain-based Supply Chain Management

There has been a growing interest in emerging technologies, like blockchain, among business communities as the technology has attracted significant attention as a viable technique for improving company operations [1]. Experts postulate 62% of Supply Chains (SC) will use blockchains by 2035, up from the 15% it is today [2]. The experts also expect at least 72% of technical challenges like efficiency and scalability to be fixed by then [3]. So, this research is timely as manufacturers strive to understand the architecture (i.e. consensus mechanisms) and operational features of blockchain-based SCMs. A blockchain can be described as a distributed and decentralised database. It stores all confirmed transactions¹ when data is sent and stored on the blockchain ledger in a sequential chain of blocks. These confirmed transactions are then copied across multiple nodes within a network [4]. The technology was initially introduced in 2008 and adopted in 2009 [4]. The adoption of technology in 2009, Blockchain 1.0, started with a cryptocurrency, Bitcoin, but has been progressively transforming business models that involve operations and communication of industrial enterprises. 2015, Blockchain 2.0 emerged, which enhanced 1.0's infrastructure with smart contracts. Smart contracts are programmable scripts capable of initiating transactions [5]. Lastly, Blockchain 3.0 encompasses various applications spanning multiple industries such as government, health, insurance, education, the arts, and manufacturing [5], [6].

Blockchain technology has received widespread commendation for its ability to drive the electronic information era [7]. It has been recognised as a catalyst that can enhance the performance of business processes in the previously mentioned industries and organisations that face challenges related to governance, transparency, infrastructure, and coordination inefficiencies [8]. However, scholars propose that additional investigations are necessary to more precisely describe, evaluate, and acknowledge the suitability of blockchain technology in these different industries [9] like finance [10], and Supply Chain Management (SCM) [11].

¹ Confirmed transactions refer to transactions that have been verified, processed, and permanently added to the blockchain ledger, ensuring their validity and irreversibility within the network [201].

As per the Council of Supply Chain Management Professionals, SCM encompasses two primary areas:

- (i) strategic planning, efficient execution, and operations management in creating and delivering value to end consumers. This includes procurement, manufacturing, and logistics.
- (ii) the integration and coordination of pertinent business operations within and across organisations. A Supply Chain encompasses physical and informational flows and distribution networks (i.e. the stakeholders) [12].

The Fourth Industrial Revolution (Industry 4.0) highlights how new technologies, like blockchain, have impacted supply chain innovation. SCM industries, including manufacturing and logistics, have advanced under Industry 4.0. [13]. These developments involve deploying intelligent and interconnected physical assets and equipment capable of autonomous operations and have led to self-coordinating systems, such as smart factories or smart supply chains [14]. Blockchain adds a new dimension to the advancement of smarter supply chains. Despite the technology being widely recognised as a catalyst for innovation and economic growth [15], it still faces obstacles such as scalability, security, privacy breaches, and high energy consumption due to inefficiencies [16], [17]. This can be seen in the technology's implementation across different SCM industries; for example, numerous blockchain-based healthcare supply chains are still experiencing various obstacles relating to security, privacy, scalability and interoperability [18], [19], [20]. In agriculture supply chains, the utilisation of blockchain technology presents multiple hurdles, such as the requirement for scalability to process extensive data volumes originating from diverse inputs and the necessity to safeguard confidential data against breaches [21], [22], [23]. Hence, it is essential to acknowledge that this technology is not without its own set of efficiency [24] and security concerns [25], [26] further explored in Chapter 4.

1.2 Prior Work: The modern supply chain

Organisations that implement e-Supply Chain Management (eSCM) systems, which utilise the internet to enhance the coordination of supply chain connections and increase performance, experience several operational and strategic advantages [12], [27]. They invest in these technologies to facilitate more efficient operations than the traditional states. Radiofrequency identification (RFID), enterprise resource planning (ERP), customer relationship management (CRM), collaborative planning forecasting and restocking (CPFR), and e-procurement systems represent a

few examples of eSCM that have been used to enhance the efficiency of traditional supply chains. RFID technologies have transformed inventory tracking by offering immediate insight into product movements, significantly enhancing operational efficiency in SCM [28]. ERP systems have facilitated the integration of diverse enterprise procedures, resulting in the smooth transmission of information among multiple departments, leading to enhanced operational efficiency and improved decision-making capabilities [29]. According to Ngai, Xiu, and Chau [30], implementing CRM systems has enhanced the management of customer relationships by enabling the analysis of customer data and behaviour. Hill et. al [31] reported that implementing CPFR initiatives has enhanced collaboration between suppliers and retailers, leading to improved inventory levels. Hung et al. [32] have found that e-procurement systems have simplified the procurement process, resulting in increased efficiency and reduced costs [31], [32], [33]

Notwithstanding the advancement of SCM facilitated by these technologies, blockchain presents unique benefits that rectify several deficiencies intrinsic to these eSCM solutions. Blockchain technology promotes trust among all supply chain participants by maintaining an immutable and transparent ledger of transactions, a characteristic that RFID and ERP fail to achieve completely as they do not offer comprehensive end-to-end transparency [21]. By incorporating smart contracts into blockchain technology, contractual agreements between parties are automated, resulting in increased process efficiency and decreased reliance on intermediaries compared to conventional electronic data interchange and e-procurement systems [33]. In addition, the decentralised characteristics of blockchain provide heightened levels of security and resilience in the face of system malfunctions and data tampering. This effectively addresses the weaknesses inherent in centralised systems such as ERP, CRM, and CPFR [34]. Blockchain has the potential to build on the advantages of these different technologies into a unified, transparent, and secure platform for SCM, offering a more comprehensive resolution to the existing obstacles in SCM. The technology is widely regarded as a viable remedy for addressing traceability challenges in SCM [35] and is recognised for its potential to foster stronger and more reliable connections [36], [37], not only between firms and suppliers but across the entire SCM ecosystem.

1.3 Problem Statement: the need to examine blockchain use in SCM

Blockchain technology presents a transformative potential for supply chain management (SCM) by enhancing transparency, traceability, and security. However, its integration into SCM faces significant challenges, particularly concerning scalability, efficiency, and security [38], [39]. As

global supply chains expand and grow in complexity, blockchain-based systems must adapt to handle larger networks and increased transaction volumes [40]. Current limitations, such as the inefficiency of transaction verification processes in blockchains, create performance bottlenecks, preventing blockchain from fully optimising SCM systems [41].

Thus, there is a pressing need to look for blockchain solutions that can meet the demands of modern, growing supply chains, ensuring they can handle increased volumes of transactions without compromising performance [33] while maintaining security [42]. Although blockchain inherently provides security features that safeguard against tampering and fraud activities [43], [44], vulnerabilities remain, exposing SCM systems to potential cyber threats exploit [45], [46], [47]. Additionally, there is limited scholarly inquiry into how cybersecurity vulnerabilities impact the efficiency of blockchain-based SCM systems. Moreover, the consensus mechanism, which is the part of the blockchain that ensures transaction validation, plays a pivotal role in determining both security and efficiency in blockchain-based SCM. This research, therefore, intends to conduct further empirical research to assess the impact different consensus mechanisms, like Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT), have on SCM system performance and efficiency.

1.4 Motivations for the study

While blockchain has become a disruptive application for traditional business models, providing decentralised and unchangeable ledger systems, its implementation in SCM is still complex and challenging [48], [49]. Supply chains are the fundamental support system of the worldwide economy, and ensuring effectiveness and protection is of utmost importance [50]. Blockchain technology has the potential to revolutionise the domain of SCM, but to utilise its potential fully, it is crucial to have a comprehensive grasp of the consensus processes that regulate blockchain efficiency [51]. This highlights the need to examine blockchain consensus in supply chain management. The broad analysis is motivated by the rapid convergence of blockchain technology, cybersecurity, and SCM and the Welsh Government's interest in investing more in applications for manufacturers in Wales. The study provided in this thesis is highly significant considering SCM's rapidly evolving digital landscape. The importance of this is emphasised by three (3) strong factors mentioned in sections 1.4.1, 1.4.2 and 1.4.3 respectively.

1.4.1 Improves Efficiency and Cybersecurity: Predominant Concerns in Digital SCM

Given that SCM systems usually contain sensitive data, including transactional and confidential information, the digital side of SCM is filled with varying cyber threats [21] and ensuring the security and privacy of supply chain data has become a crucial concern [52]. The secure ledger function of blockchain technology offers a promising solution to protect vital data. So, as SCM systems become more integrated into the digital economy, they face increased risks from cyber threats that can halt production [53]. On the other end, the efficiency of SCM systems is a growing concern due to the increasingly complex nature of global trade and logistics. According to a study by Kovács and Béla [54], efficiency drives the optimisation of resources, time, and costs, directly impacting the competitiveness and profitability of businesses. There is also the issue of energy consumption; according to a survey by the German Energy Agency (dena) and research centre Fraunhofer FIT, blockchain, which is one of the biggest consumers of electricity globally, has the potential to decrease significantly its power requirements and become more efficient by implementing a deliberate network design [55]. Since 2018, there has been a growing global need for more transparent and effective supply chain management, which blockchain technology has been identified to address [56]. This demand got worse after the COVID-19 pandemic when there became a need for industries to monitor food supply chains in real-time [57].

Current consensus mechanisms lack efficiency and direct applicability to SCMs [58]; therefore, there is a need for more efficient, scalable solutions to handle growing transaction volumes. Each type of blockchain handles these aspects differently, with implications for the security and operational efficiency of the entire supply chain [59]. Cai et al. [59]. recently proved this by highlighting how three different blockchain consensus (PoW, PoS and PoDaS (Proof of Data Sharing)) affect SCM performance differently. Exploring the implications of different types of blockchains is needed to develop secure, efficient and scalable blockchain solutions in SCM systems. This research direction also aligns with the call for innovation in SCM cyber-physical systems by Kshetri [21] and the need for more resilient SCM frameworks, as outlined in recent reviews by Saberi et al. [60] and Min [61].

1.4.2 Practical, Economic and Social Significance

Preserving SCM systems is economically and socially valuable due to the fundamental role in global economies and international trade [62]. The research contributions indicate the possibility of mitigating risks and vulnerabilities and maintaining a scalable, uninterrupted supply chain flow,

especially for businesses whose SC is crucial for maintaining society and the economy. The suggested solution can benefit different parties, including manufacturers, retailers, and consumers, as it could reform efficiency security measures in supply chain management [33].

1.4.3 Innovation and Progress

Recognising blockchain technology's potential impact on SCM and the urgent necessity to address its cybersecurity vulnerabilities was an early motivation this research, as its contribution would contribute to safer and more effective blockchain uses in SCM. Supply chain ecosystems are scalable [63]; therefore, consensus approaches must be expandable without compromising security or efficiency. This thesis could provide evidence-based advice to professionals and researchers seeking to improve supply chain security, efficiency, and resilience in a globalised environment.

1.5 Research Aim and Objectives

1.5.1 Aim

This research aims to investigate the efficiency and security capabilities of blockchain-based SCM. The thesis will evaluate performance (throughput and latency) across different consensus mechanisms, examining the capacity to handle larger workloads over different network sizes. It also proposes a novel consensus method for scaling SCM operations.

1.5.2 Objectives

This research intends to achieve the following:

- (i) To undertake a thorough appraisal of literature within the domains Blockchain, Supply Chain Management and Cybersecurity.
- (ii) To identify and prioritise the architecture area that most influences efficiency.
- (iii) To evaluate the efficiency parameters of different consensus mechanisms (PoW, DPoS, PoC, PoI, PBFT and Stellar) used in SCM.
- (iv) To design a novel consensus mechanism and execute a series of simulation experiments to test the efficiency of the new consensus mechanism.
- (v) To assess the results from the experimental findings (from existing and novel mechanisms) and propose a decision matrix for practitioners and scholars to select consensus mechanisms that align with SCM systems' specific efficiency and cybersecurity needs.

Manufacturers are becoming more aware of the benefits of using blockchain technology in the operational processes [64]. Many businesses have benefited from implementing and integrating blockchain technology [65]. The goals are to assess blockchain-based supply chain efficiency capabilities and cybersecurity risks, improve understanding of the technology's technical foundations, and guide selection of the exemplary technical aspects to lead to better blockchain infrastructures, offering valuable insights for academic researchers, industry practitioners, and policymakers.

1.6 Scope and Limitations

1.6.1 Scope

This research examines the intersection of blockchain technology, cybersecurity, and SCM. The scope of this thesis encompasses the following four areas:

- **Blockchain in SCM:** This research focuses on applying blockchain technology in supply chain management, particularly improving the consensus layer.
- **Cybersecurity Challenges:** The thesis delves into the cybersecurity challenges that emerge in blockchain-based SCM systems, assessing various attacks in deployed blockchains.
- **Efficiency improvement:** The thesis will assess current blockchain consensus methods and propose an improved consensus model tailored to the unique demands of SCM efficiency.
- **Cybersecurity Vulnerability Resistance:** The novel proposed consensus mechanism addresses the identified cybersecurity challenges in blockchain-based SCMs.

1.6.2 Limitations

While this research aims to provide valuable insights into the dynamic landscape of blockchain technology, cybersecurity, and SCM, it is essential to acknowledge certain limitations:

- **Generalisability:** This thesis's findings are based on a specific set of simulations representing part of the spectrum of a simulated network to represent a blockchain-based SCMs. Consequently, the generalisability of the results compared to all contexts of a fully developed blockchain system may be limited.
- **Scope Limitation:** The research has been restricted to certain types of blockchain applications (highlighted in Section 1.52) within SCM, covering only some blockchain types.
- **Methodological Constraints:** Using simulations to evaluate blockchain performance may not have captured the full complexity of real-world operations. This means that running

simulations in a controlled, virtual setting may miss certain factors that happen in real life, such as unpredictable network issues, hardware failures, or human errors.

- **Dynamic Nature:** The fields of blockchain and cybersecurity are highly dynamic, with continuous technological advancements and evolving threats. Given the rapid advancement in blockchain technologies, the research is limited by the current state of technology at the time of the study. This research captures a snapshot of the state of these fields as of 2024.
- **Access Constraints:** Access and availability constrained the extent of the research, including the type of simulations and blockchains.
- **Legal and Ethical Considerations:** As this research is partially funded by the European Union and the Welsh Government, ethical and legal considerations influence the extent to which certain data can be accessed and used in research.

Acknowledging these limitations is essential for appropriately interpreting the findings and considering any possible constraints in the research process. Notwithstanding these limitations, this thesis significantly contributes to the studied areas.

1.7 Key Contributions to Knowledge

This thesis contributes to the burgeoning field of blockchain in SCM through several key areas. The thesis has three main contributions and one minor contribution.

1.7.1 SLR: Taxonomy of cybersecurity-related efficiency issues (Main Contribution)

The thesis systematically explores literature to uncover and categorise technological flaws and inefficiencies into explorative areas in blockchain-based SCM systems in Chapter 4. Over time, several novel consensus mechanisms have been introduced to improve blockchain adoption across SCM over time, but technological gaps that expose current consensus mechanisms to cybersecurity vulnerabilities still exist. This thesis analyses literature to highlight security issues that affect the efficiency of blockchains in SCM, then it designs a taxonomy that highlights future research exploration in overcoming these gaps.

1.7.2 Simulation Evaluation (Minor Contribution)

BlockSim is used to model blockchain consensus mechanisms and the efficiency capabilities. Different consensus mechanisms used in SCM are simulated and evaluated over scaling network settings. BlockSim's results (throughput and latency) are then used to calculate scalability and

compare consensus approaches and the effect on the blockchain's efficiency. While many studies compare blockchain consensus, this thesis introduces a unique “Scalability Score” to assess consensus across network sizes.

1.7.3 Proposition of a Novel Consensus Mechanism (Main Contribution)

Chapter 6 design and testing of the Proof of Efficiency (PoEf), an optimised consensus mechanism architecture that, for the first time, combines sharding with reputation-level scoring to improve blockchain-based supply chain efficiency and safety. This consensus is tailored to SCM systems, addressing consensus difficulties like sluggish transaction speeds and security risks. The mechanism selects the most optimal nodes to confirm transactions based on history and participation; it switches between nodes to maintain performance and avoid cyber threats. Blockchain consensus procedures for supply chain management could be revolutionised by the PoEf, which has improved efficiency and attack resilience.

1.7.4 Blockchain Selection Matrix for Efficient SCM Systems (Main Contribution)

Chapter 7 discusses a customised decision matrix created to select an efficient consensus for different sizes of SCM systems. It emphasises the efficiency criteria of each consensus tailored for SCM’s growth requirements. The matrix serves as a benchmark for future developments in blockchain-based supply chains.

These contributions represent a noteworthy advancement in understanding and applying blockchain technology in SCM. They also offer a foundation for future research and development, aiming to enhance the security and efficiency of blockchain systems in this complex and dynamic space.

1.8 Thesis Structure

Chapter 2: Understanding Blockchain and its Use in SCM space

Chapter 2 breaks down the blockchain architecture, layers, and operation. It explains how the blockchain works and analyses how its performance is assessed. The goal is to set the scene of the research and explain the basic concepts of blockchain and supply chain management to the average reader.

Chapter 4: Blockchain-Based SCM Systems: A Systematic Literature Study of Academic Research

Chapter 4 presents a systematic mapping of literature that covers the domains cybersecurity + blockchain + SCM + efficiency. It covers prior research, paper screening processes, classification and data extraction. The findings

based SCM and a discussion on consensus mechanism failures, smart contract vulnerabilities, network-level attacks, and cryptographic challenges.

Chapter 6: PoEf, an Enhanced Blockchain Consensus Architecture SCM

Chapter 6 presents the Proof of Efficiency (PoEf) consensus mechanism, which optimises throughput efficiency,

processes.

Chapter 7: Discussion and Analysis of Findings

Chapter 7 analyses and compares the findings. It combines

Chapter 1: Introduction

Chapter 1 establishes the thesis by explaining blockchain's role in SCM, making traditional systems more efficient, secure and transparent. The chapter also highlights that blockchain, a "security application," has flaws that can limit its usefulness. The chapter then sets research goals, objectives, and motivations for cybersecurity, blockchain, digital SCM, and efficiency. The chapter also specifies the research's scope, limits, and approach to constructing a novel consensus mechanism that would digital SCM sidestep

based consensus mechanism SCM selection matrix.

Chapter 3: Research Methodology

Chapter 3 describes the thesis's research strategy and

Chapter 5: Consensus Mechanism, Data Collection

Chapter 6 simulates consensus processes to illuminate their

Chapter 8: Conclusion

Chapter 8 combines and summarises the study findings and contributions. The thesis encompasses a systematic literature review, an in-depth understanding of blockchain technology, simulation modelling, analysis of obtained data, evaluation of the data, proposal of a novel consensus mechanism, PoEf, and a summary of the significant contributions made. The chapter also emphasises the difficulties faced throughout the research. It proposes future approaches involving further assessment, evaluation, and development stages for secure SCM systems based on blockchain technology.

FIGURE 1.1: Illustrating a summary of the Chapters in this thesis

1.9 List of publications

- O. Haughton, C. Campbell and T. H. Walcott "PoEf, an enhanced Blockchain-Coordinated Supply Chain Management Architecture" *International Journal of Blockchains and Cryptocurrencies*, 2024. (Pending)
- O. Haughton, C. Campbell, T. H. Walcott and I. Neaga, "Blockchain-based Supply Chain Management Systems: A Systematic Mapping Study of Academic Research," 2023 International Conference on Computing, Networking, Telecommunications & Engineering Sciences Applications (CoNTESA), Zagreb, Croatia, 2023, pp. 32-38, doi: 10.1109/CoNTESA61248.2023.10384965.
- O. Haughton, C. Campbell, G. Howe and T. H. Walcott, "Evaluating the integration of Blockchain Technologies in Supply Chain Management: a case study of sustainable fishing," 2022 International Conference on Computing, Networking, Telecommunications & Engineering Sciences Applications (CoNTESA), Skopje, North Macedonia, 2022, pp. 51-56, doi: 10.1109/CoNTESA57046.2022.10011252.
- O. Haughton, G. Howe "Evaluating the integration of Blockchain Technologies in Supply Chain Management: Designing a Hybrid Blockchain," CILT's 26th Annual Logistics Research Network (LRN) Conference, Aston University, Birmingham, United Kingdom, 2022 (Conference Proceedings).

2 Blockchain and its Role in Supply Chain Management

2.1 Overview

Incorporating blockchain into SCM signifies a substantial evolution in SC transaction tracking, recording, and fostering confidence among stakeholders within a blockchain. This chapter analyses the fundamental architecture of blockchain, emphasising categories such as public, private, consortium, and hybrid models. The chapter introduces blockchain processes from transaction initiation to block formation while explicitly highlighting the essential function of the consensus layer in maintaining blockchain efficacy. An analysis of various categories of consensus mechanisms (proof-based, capability-based, voting-based, etc.) and the effects on the efficiency of SCM. Understanding these mechanisms is important in identifying the most suitable and efficient consensus mechanism for SCM applications. Thus, ensuring both the reliability and scalability of blockchain-based SCM systems.

The chapter examines the increasing significance of blockchain in supply chain management, propelled by digitisation and Industry 4.0. It emphasises the layers in blockchain architecture and how they individually influence efficiency and security, especially via the consensus layer that authenticates transactions and preserves network integrity. The chapter also discusses practical use case applications of blockchain in supply chain management, such as provenance tracking, sustainability, and supply chain finance, illustrating its revolutionary effects on transparency, risk mitigation, and global supply chain resilience.

2.2 Fundamentals of Blockchain Technology

2.2.1 Categories of blockchains

Supply chain management (SCM) has experienced a notable increase in interest in blockchain technology. This can primarily be linked to the growing trend of digitisation and the widespread adoption of Industry 4.0 principles in various industries. As highlighted in prior chapters, the introduction of Bitcoin Nakamoto and Bitcoin in 2008 has dramatically increased interest in applying this technology. The technology has evolved to accommodate many uses, resulting in the creation of three unique types of blockchains: public, private, and consortium. The categories are depicted in Figure 2.1 below.

- Public blockchains are distinguished by the inclusive nature since they enable the involvement and membership of any individual in the blockchain network [66], [67].
- Private blockchains are characterised by a restriction of transaction participation to authorised parties. In this type of blockchain, the administrator can override, modify, or eliminate any recorded entries[66], [68].
- Consortium blockchains are characterised by a governance structure, which involves several organisations rather than a single entity [69]. One such instance is Hyperledger Fabric [70].
- A hybrid blockchain is a type of blockchain network that combines private and public blockchain features. It merges the public blockchain's transparency with the private blockchain's confidentiality features [67].

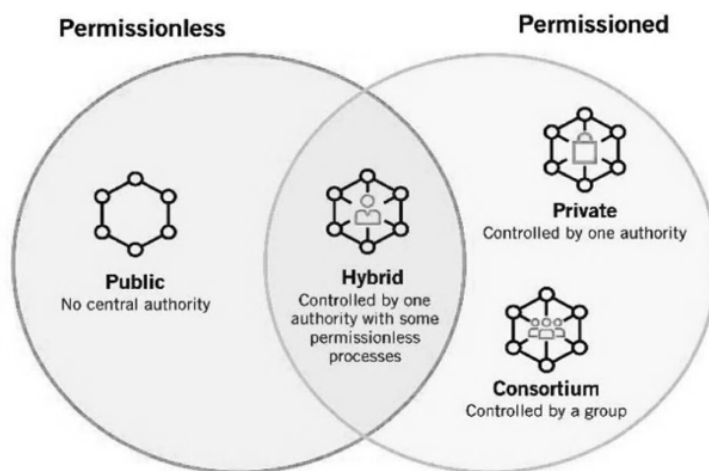


FIGURE 2.1: The blockchain architecture categories [71].

While blockchain technology has gained significant recognition for its association with cryptocurrencies, several scholars have also acknowledged its potential implementation in other supply chain applications like Longo et al. [59], Sarfaraz et al. [60] and Saberi et al. [33]. The inherent characteristics make private blockchains well-suited for implementation inside supply chain systems [61]. Incorporating blockchain technology into conventional SCM poses a notable obstacle due to the lack of customised consensus mechanisms that can effectively integrate with and address supply chain issues [72]. Information validation in the blockchain architecture is achieved using a consensus method involving network nodes, eliminating the requirement for intermediaries. According to Du et al. [73], the consensus mechanism establishes a tamper-proof environment and ensures the reliability and validity of stored information.

2.2.2 How do blockchains work?

Blockchain technology represents an intricate amalgamation of peer-to-peer networking, cryptographic security, mathematical algorithms, consensus protocols, and executable scripts known as smart contracts [74], [75], [76]. A blockchain is a decentralised ledger system connecting data blocks chronologically without centralised supervision. This system relies on a peer-to-peer network structure in which each participating node, sometimes referred to as a miner in the context of public blockchains, has equal authority and carries out many crucial responsibilities to maintain the network's integrity [77]. As illustrated in Fig. 2.2, transactions within a blockchain commence with nodes (user), which could be individuals or entities, creating data packets known as transactions ((e.g., Tx1, Tx2, ..., Txn)). These transactions are temporarily stored in a pool, waiting for selection. The blockchain network then selects a set of transactions from this pool, processes them, and groups them into a block (e.g., Bn). These transactions are broadcast to the network and await validation. In a public blockchain environment, any node can assume the role of a miner, unlike in private or permissioned blockchains where the mining capabilities are restricted [63]. Miners oversee collating pending transactions from a pool of unconfirmed transactions and crafting them into a new block by engaging in a consensus mechanism, like PoW or PoS, to compete for the right to append this block to the ledger [78].

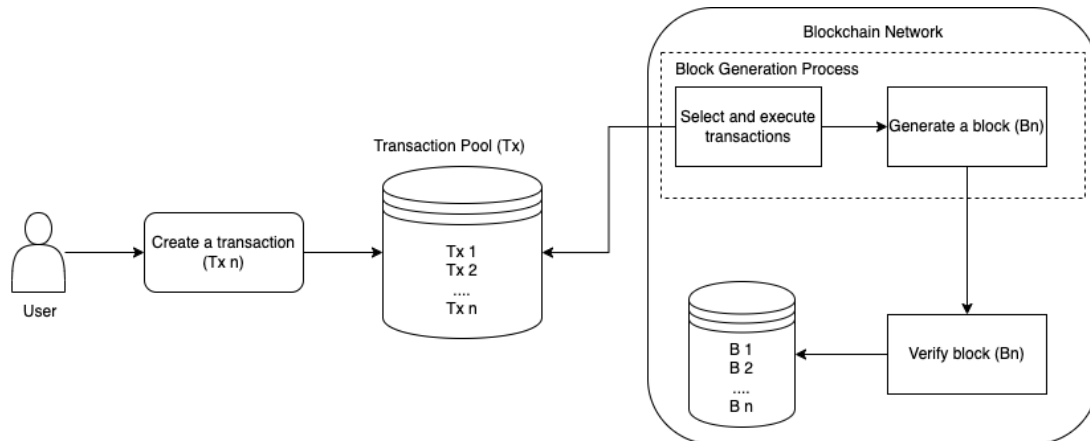


FIGURE 2.2: Illustrating how a transaction is initiated on the blockchain.

Once the block is generated, the network verifies its validity to ensure all transactions comply with the consensus mechanism's rules and protocols. The freshly assembled block is broadcasted to the network for validation, a process where other nodes verify the block's integrity and the validity of the transactions within the blockchain [79]. This verification step includes confirming transaction signatures in the case of private blockchains and upholding the network's rules. Post-verification, the block is added to the blockchain (e.g., B1, B2, ..., Bn), providing an unalterable and transparent record of all transactions [80]. From an efficiency standpoint, the operational process of blockchain

may be broadly categorised into three distinct phases: block creation, consensus validation, and ledger verification.

- The **block creation phase**: nodes within the blockchain network gather transaction data and engage in a competitive process to choose nodes to verify the transaction and confirm the block, contingent upon the computational capabilities. Nodes with accounting privileges can compile transaction information into blocks and receive rewards predetermined by the blockchain protocol's reward mechanism. In applications like Bitcoin, the rewards frequently yield economic advantages and incentivise nodes to contribute computational power to the blockchain network consistently.
- The **consensus verification stage**: worker nodes broadcast the packed block (with transaction information) to the blockchain network. All nodes within the network collectively process a significant quantity of blocks and authenticate the content of these blocks based on the consensus method. They assess the accuracy of the block content and then document the outcome inside the blockchain ledger.
- The **verification ledger maintenance phase**: nodes can store the data that has been verified during the consensus verification phase for an extended duration. This allows for retrospective data verification based on the timestamp and hash value present in the block. Consequently, the node can offer an access interface to the application layer of the blockchain (see *Fig. 2.3*), facilitating queries for ledger information. The computer power provided by the nodes within the blockchain network contributes to the decentralised, open, stable, honest, and credible nature of the blockchain system.

The consensus verification stage is central to blockchain's operational ethos and efficiency, where consensus mechanisms sustain transactional integrity and foster trust across the blockchain network. The repercussions of consensus vulnerabilities in blockchain-based SCMs, as delineated by seminal researchers such as Eyal and Sirer [81], extend to the potential destabilisation of entire SCM systems. This means that a shift towards mechanisms that synergise energy efficiency with fortified security, as explored by Saleh [82], is instrumental in optimising transaction throughput, a quintessential element for SCM processes that demand efficiency and dependability.

2.2.3 A Block Structure

Blockchain is a form of Distributed Ledger Technology (DLT) that facilitates the safe, transparent, and immutable storing of data [83]. The system comprises a network of computers, called nodes, which maintain a collective and synchronised ledger of transactions into blocks. As seen in Fig. 2.2, each block within this chain has a date and a reference to the preceding block, and the transactions confirmed in the blocks are subsequently interconnected in a sequential chain. This structure of interconnected blocks facilitates the establishment of a distributed database (called a blockchain) that exhibits resistance to unauthorised manipulation and alteration. The blockchain is designed with the objective of decentralisation among nodes (stakeholders), meaning that it operates without the oversight or control of a singular central authority, as the nodes oversee adding and confirming data and preservation of the blockchain network is achieved by a collective arrangement of interconnected nodes, which collaborate to verify and log transactions. The decentralised nature of this framework enables the transfer of digital assets, such as Bitcoin, without the involvement of intermediaries, such as banks or other financial institutions [83], [84]. Fig. 2.2 shows the sequential data structure of blocks, where distinct data blocks are interconnected chronologically based on the creation times. In the case of SCM, the data structure facilitates value transfer among nodes through immutable digitally signed operations into blocks. Blocks compile transactional data and comprise a block header and a block content.

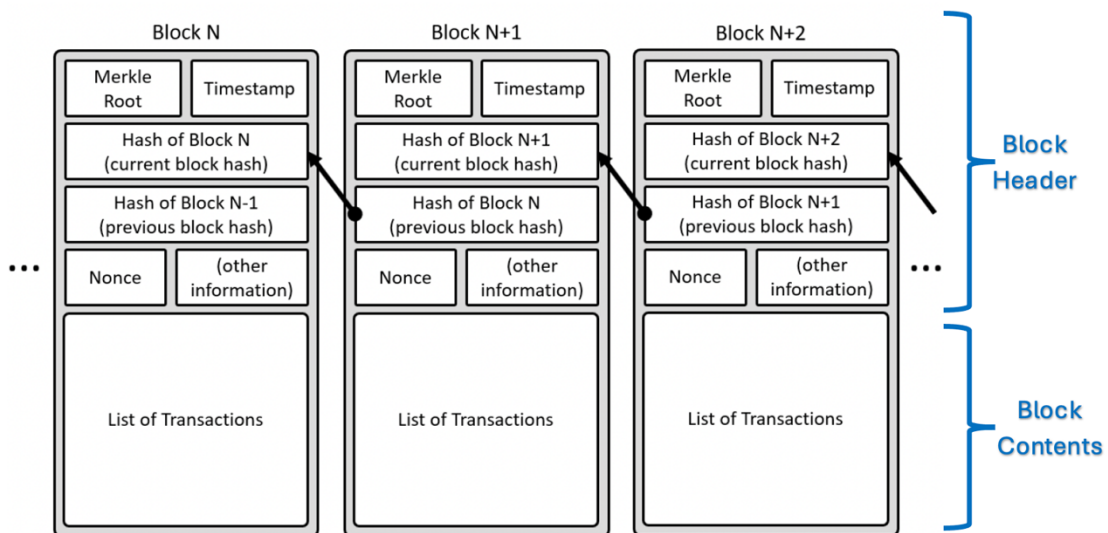


FIGURE 2.3: illustrating the structure of blocks in a blockchain [85]

The block header consists of the following components:

- The *preceding block hash* is recorded in the current block. The block generates a distinct hash value by irreversibly processing the block information. The hash value, which possesses a

concise and unchanging length, uniquely identifies the block. The hash value of the prior block is saved within the current block to establish a connection between the current block and its preceding block.

- The *Merkle Root* stores the hash value of the root node of the Merkle tree associated with the current block.
- A *timestamp* guarantees the chronological storage of data inside blocks, enabling the traceability of data sources based on the timestamp associated with each block.
- The *Difficulty Target* is the coefficient of difficulty that needs to be determined for the present block.
- The *nonce* can be described as a value computed by a node using its computational capability, often with a value lower than the difficulty target.

The block body is responsible for storing the content of transactions and any associated metadata. Every transaction record is associated with a digital signature. The digital signature process is employed to guarantee the security of the block data. The block body typically consists of the following components:

- The number of *TransactionsBytes*, a metric that quantifies the amount of storage space used by the *NumTransactions*.
- *NumTransactions*, a metric used to document the total number of *transactions* in each block.
- The *Transactions*, the recording of the amount of transaction data within a block.

2.3 Blockchain Architecture

Figure 2.4 illustrates the architecture of blockchain systems, which is dissected among five principal layers, each with distinct functions and entities: the Application and Presentation layer, the Consensus layer, the network layer, the Data layer, and the Hardware/Infrastructure layer. These layers are integral to the operation of the blockchain and determine a blockchain's efficiency and security.

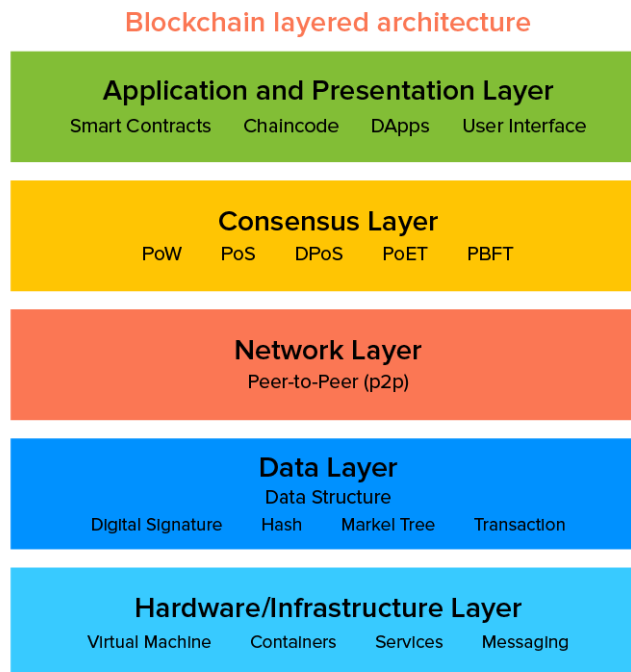


FIGURE 2.4: illustrating the various layers of the blockchain.

2.3.1 The Application and Presentation Layer

The uppermost layer in the blockchain architecture is called the Application Layer. This layer focuses on the economic structures that motivate nodes to contribute to the ongoing operation and growth of the blockchain. The fundamental nature of this layer is encompassed within the incentive model of the blockchain, which outlines the reward systems and the underlying rules that dictate the distribution [86]. It denotes the collection of economic incentives developed to provide fair remuneration for nodes that enable the operational integrity of the blockchain network. In applications like Bitcoin, this layer utilises the inherent cryptocurrency of the blockchain to establish a profitable structure, thereby incentivising miners to maintain the blockchain ledger. The incentive scheme plays a crucial role in ensuring the resilience and effectiveness of a permissionless blockchain ecosystem [81], [87]. Furthermore, these incentives function as a protective measure against a wide range of hostile risks, including DDoS attacks, as observed in networks such as Ethereum [88], and detrimental behaviours exhibited by nodes, such as selfish mining strategies [89]. In non-cryptocurrency blockchain systems, it is common practice to associate rewards with creating blocks and handling transactions. The incentive mechanisms differ in intricacy across different blockchain networks.

2.3.2 The Consensus Layer

The Consensus Layer sits above the Network Layer, holding the consensus mechanism (Fig 2.3) that manages the blockchain's operation. It contains code and rules to establish collective agreement among the nodes (participants) and verify the actual status of the blockchain ledger. This layer synchronises the entire network by enabling consensus and enforcing protocols that guarantee the accuracy and orderliness of the ledger [90]. This means that the consensus layer through the consensus mechanism is responsible for the efficiency and security of a blockchain by executing protocols that mandate nodes in the network to get an agreement (i.e. reach consensus) on the ledger's state within a specific timeframe. On the efficiency side of things, according to Nakamoto [4], the mechanisms:

- (i) define the criteria for selecting nodes that are allowed to conform transactions and add the following block,
- (ii) how fast these transactions are confirmed,
- (iii) the schedule for block generation and
- (iv) offer solutions for resolving conflicts when different versions of transactions exist among nodes.

As an example of a complete blockchain system, Bitcoin was created with the PoW consensus mechanism, and Ethereum was made with the PoS mechanism. Consensus mechanisms like PoW and PoS were devised to oversee the node's consensus process in the blockchains. However, the rules that govern each consensus mechanism to reach consensus are executed differently. In the PoW architecture, nodes (commonly called miners) allocate computational resources to expand the ledger by appending new blocks. The PoS consensus necessitates that nodes possess financial stakes, so a connection between ledger upkeep and financial investment must be established. The concept behind PoS is to enforce a monetary expense on ledger upkeep, discouraging nodes from engaging in destructive actions while incentivising adherence to specified regulations and the integrity of the ledger [91]. The efficiency of these consensus mechanisms can be assessed from the rate at which nodes confirm transactions and generate blocks. These varying operations allow a blockchain to reach consensus at different times.

Regarding security, the latency in propagating blocks among nodes can sometimes result in malicious forks, where malicious nodes spread multiple blocks simultaneously from the original ledger, resulting in different representations of the ledger. The Consensus Layer is responsible for

resolving conflicts and determining the official transactions. For example, the PoW protocol used in Bitcoin follows the longest chain rule, where nodes consider the longest valid chain to be the true blockchain. Following this rule can lead to deviations in the blockchain from malicious nodes, weakening the network’s resistance to attacks like selfish mining as throughput increases. However, PoS uses GHOST (Greedy Heaviest Observed Subtree), proposed by Sompolinsky & Zohar [92] enhanced from the longest chain rule. If there are deviations, instead of selecting the chain with the most blocks, GHOST selects the heaviest chain, where “heaviest” refers to the subtree with the most accumulated work and chains with the highest workload is accepted as the genuine ledger. Stale or orphan blocks, which are blocks omitted from the main chain, are discarded and do not affect the ledger’s state, lessening the chance of shellfish mining. Nodes play a crucial role in enhancing the transaction queue, updating the ledger with new transactions or blocks when they are added to the system, and maintaining security.

2.3.2.1 Consensus Mechanisms used in SCM

Literature has highlighted that blockchains still suffer from efficiency-related issues caused by the technology’s architecture, including the consensus mechanism. Implementing consensus mechanisms in blockchain networks is pivotal for SCM's performance and research, particularly in addressing security challenges and is essential for efficient solutions. The taxonomy, as proposed by Bodkhe et al. [47] in Fig. 2.5, highlights 17 consensus mechanisms used for SCM, and they categorise these mechanisms with four criteria: proof-based, capability-based, voting-based, compute-intensive, and miscellaneous mechanism, each bearing distinct operational implications. Understanding the fundamentals and operational features of these consensus mechanisms used in blockchain-based supply chains is needed to resolve research Gap 3, designing a decision matrix for Manufacturers to assess which consensus would be best for a rapidly scaling supply chain.

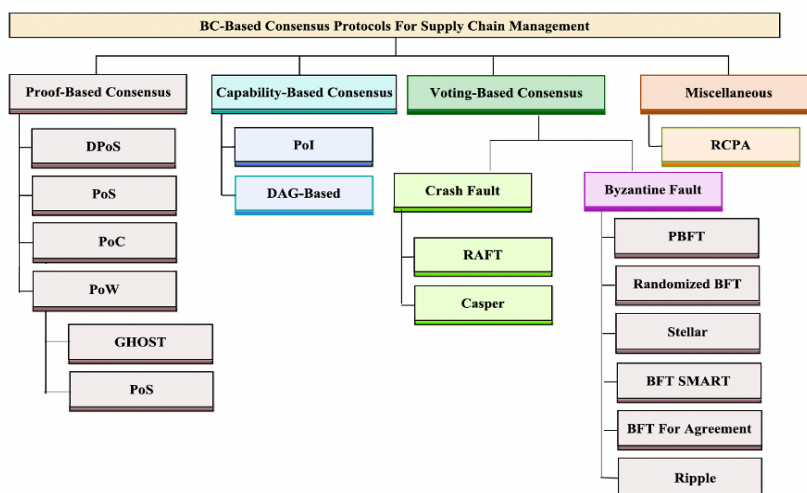


FIGURE 2.5: Blockchain Consensus Mechanisms used in SCM [47].

Each group of consensus mechanisms identified by Bodkhe et al. [47] have operational characteristics that allow manufacturers to use them in SCM, but they all are designed and handle transactions differently. From an operational standpoint, the differences between proof-based, capability-based, and voting-based consensus mechanisms in blockchain technology are defined by the approach to security, efficiency and governance. Proof-based mechanisms like PoW are resource-intensive, requiring significant computational power, ensuring high security at the cost of scalability and speed. Capability-based mechanisms like Proof-of-Importance (PoI) enhance the proof-based PoS mechanism but distinguish itself by evaluating the value of nodes through a scoring system. Nodes are assigned an “importance score” based on metrics like net transfers, quantity of vested currency, and the degree of activity [93]. Unlike PoS, where the probability of creating a block may correlate directly with the stake of a node, PoI incorporates additional factors such as transaction stakeholders, frequency, and size to assess a node’s contribution to the network [94]. PoI incentivises active participation and faster throughput, potentially leading to more transaction-rich networks.

Voting-based mechanisms employ a democratic process to influence block confirmations. This election-based approach conserves energy and avoids the competition-based miner selection characteristic of proof-based consensus mechanisms like PoS, thereby reducing the associated computational expenditures that affect efficiency [95]. Although capability-based consensus mechanisms are more efficient than Proof-Based mechanisms, they skew miner selection toward wealthier nodes, potentially leading to centralisation. Voting-based mechanisms counteract this by decoupling mining rights from wealth instead of relying on stakeholder votes to determine mining privileges, fostering a more balanced power distribution across the network [96]. Even though the DPoS mechanism improved the scalability of PoS, it inherently compromised the decentralised principle by concentrating authority within a select user base [97]. This centralisation of control would pose a higher risk of network attacks in an SCM environment due to the smaller number of actors involved in network maintenance. Similarly, other consensus methodologies like PoC and PoI grapple with centralisation challenges, rendering them less than ideal for SCM applications. Conversely, the PBFT model is constrained by its non-scalable nature, with communication overheads that increase exponentially with the network size, impeding efficient scalability. While PoC, a protocol within the proof-based consensus category, presents a resource-efficient alternative by negating the need for monetary investment, it remains susceptible to disruptions from malicious software attacks.

Therefore, selecting a suitable consensus mechanism is crucial in deciding the validation of transactions and achieving agreement among nodes regarding the ledger's state (how efficient and secure it is) inside a blockchain system. The choice of a consensus protocol holds significance in SCM, considering the importance on the data integrity and system efficiency in this field. The consensus mechanism is crucial in deciding the validation of transactions and achieving agreement among nodes regarding the ledger's state inside a blockchain system. Owing to the objective to investigate and compare the performance of several consensus protocols and determine which ones are better from efficiency and security perspective for blockchain applications for SCM.

Specific consensus mechanisms (Proof of Work (PoW), Delegated Proof of Stake (DPoS), Proof of Capacity (PoC), Proof of Importance (PoI), Practical Byzantine Fault Tolerance (PBFT), and Stellar) were selected from the three consensus categories (proof-based, capability-based, and voting-based) due to several factors. PoW, DPoS [98], and PBFT [99], [100] are widely recognised for their strong performance records, with PoW powering Bitcoin and PBFT and Stellar offering robust fault tolerance. Investigating these established protocols provides a reliable baseline for understanding their potential adaptations for SCM. As illustrated in Table 2.1, each mechanism also represents a diverse approach to consensus: PoW relies on computational effort, DPoS and PoS depend on stakeholder voting [101], and PoC [102] leverages storage capacity, while PoI integrates the importance of stakeholders, similar to what this thesis proposes. This diversity allows for thoroughly examining performance and scalability across different approaches [103]. Additionally, SCM requires high throughput and low latency, and mechanisms like Stellar and PBFT are known for their efficiency in environments where quick consensus is needed with minimal overhead (further explored in Chapter 7) [104]. BFT protocols such as PBFT and Stellar also offer strong fault tolerance, which is essential for decentralised SCM systems to remain secure even in adversarial conditions. Thus, by selecting a combination of mechanisms that excel in scalability, efficiency, and fault tolerance, this research effectively addresses the performance and security challenges in SCM.

TABLE 2.1: Highlighting approaches each consensus mechanism takes to achieve agreement within the network.

| Consensus Mechanism | Approach to Consensus |
|---|---|
| Proof of Work (PoW) | PoW relies on computational effort, where miners solve complex mathematical puzzles to validate transactions and create blocks. The one who solves the puzzle first is rewarded, and the block is added to the chain. |
| Delegated Proof of Stake (DPoS) | In DPoS, network users vote and elect delegates who are responsible for validating transactions and creating blocks. This creates a more efficient and scalable consensus mechanism compared to PoW. |
| Proof of Capacity (PoC) | PoC uses storage capacity as the deciding factor for miners. The more disk space a miner has, the more likely they are to validate transactions and create new blocks. |
| Proof of Importance (Pol) | Pol assigns importance scores to users based on factors like their activity and stake in the network. The higher the importance, the more likely the user is to validate transactions and create blocks. |
| Practical Byzantine Fault Tolerance (PBFT) | PBFT focuses on consensus through voting by a fixed set of validators. Each validator votes to agree on the next block, ensuring consistency and fault tolerance, even in the presence of malicious actors. |
| Stellar Consensus Protocol (SCP) | SCP is based on quorum slices, where each participant agrees on a block based on a subset of nodes they trust. This method is efficient and scalable, suitable for networks requiring fast and low-cost consensus. |

2.3.3 The Network Layer

The Network Layer encompasses an array of nodes and incorporates a broadcast protocol for inter-node communication. This layer is tasked with cataloguing the diverse node entities within the network infrastructure and facilitating the data interchange by implementing an underlying broadcast protocol. Nodes are the essential agents within the blockchain environment, undertaking transaction generation, dissemination, execution and endorsing and annexing blocks to perpetuate the ledger's continuum [105]. Conversely, the broadcast protocol is instrumental in orchestrating the distribution of data constructs, such as transactions and blocks throughout the network, as explained by Eyal and Sirer [81]. The network layer portrays the nodal constituents, respective locational attributes, and interconnectedness, thus defining the typology of information to be propagated and the methodologies employed therein. The principal entity within the network layer, denoted as a node, may represent either a standard stakeholder, whose aim is to engender and transmit transactions for execution and ledger inclusion, or a specialised variant, known as a 'miner', charged with augmenting the ledger via block appendages. Each node is characterised by a

unique identifier that manages its ledger balance, a localised version of the blockchain ledger, and, in the miner's case, an exclusive transaction pool that aggregates pending transactions from the network [106].

Inter-nodal communication is predicated upon the principle that when a node introduces a new transaction, it secures it with cryptographic endorsement and dispatches it to peer nodes for affirmation and ledger integration. Upon formulating a new block, Miner nodes engage the network in a verification and acceptance process to synchronise this new block with the ledger instances. The transmission of such information within blockchain networks is governed by numerous protocols, including relay networks and advertisement-based protocols, as identified by Nakamoto [4] and further investigated by Decker and Wattenhofer [107]. Within the domain of advertisement-based protocols, a node announces its newly acquired data to its peers; contingent upon the peers' lack of said data, as indicated by a data request, the node proceeds with the data transfer. Conversely, the data transfer is deemed redundant without a request, presuming the peer's pre-existing data possession.

2.4 Blockchain-based Supply Chains

The Council of Supply Chain Management Professionals (CSCMP) [108] define Supply Chain Management (SCM) as the comprehensive planning and management of all sourcing and procurement, conversion, and logistics management activities. Additionally, it involves synchronisation and cooperation with channel partners, suppliers, intermediaries, third-party service providers, and customers. Supply chain management encompasses the coordination of supply and demand management both inside individual firms and between several companies. Stock and Boyer [109] define it as managing a network of relationships within a firm and between interdependent organisations and business units. This network includes material suppliers, purchasing, production facilities, logistics, marketing, and related systems. The purpose of this network is to facilitate the forward and reverse flow of materials, services, finances, and information from the original producer to the final customer [109]. The goal is to add value, maximise profitability through efficiencies, and achieve customer satisfaction.

Mentzer et al. [110] provided an additional definition of SCM, stating that it involves the organised and strategic coordination of the various traditional business functions and tactics within a specific company and across different businesses within the supply chain. The goal is to enhance the long-

term performance of both individual companies and the entire supply chain [110]. This definition implies that improved performance is achieved through accumulated experience over time. Considering all these concepts, as they are concurrent and complementary, is essential while creating a supply chain management system based on blockchain technology. The CSCMP emphasises collaboration, integration, and coordination requirements throughout the supply chain. Stock and Boyer [109] define the significance of network ties among stakeholders, while Mentzer et al. [110] describe how these interactions contribute to long-term performance enhancement for stakeholders in the network. This research adopts an approach of converging these concepts to comprehend the relationship between SCM and the possible integration of blockchain technology. Modern supply chains still face a challenging business landscape of complexity, competition, and uncertainty as manufacturers call for more efficiency. Customers' fluctuating and unexpected demands primarily cause these challenges as the world economy grows [111].

SC operations still experience inefficiencies among stakeholders. One such inefficiency is the Bullwhip Effect (BWE), which describes how small demand fluctuations create bigger wholesale, distributor, manufacturer, and raw material supplier fluctuations [112]. The primary drivers of the BWE include demand forecast updating based on downstream orders rather than direct consumer demand, order batching to reduce shipping costs or exploit pricing strategies, price fluctuation leading to bulk purchases, and rationing coupled with shortage gaming where retailers may overstate needs to secure adequate supplies. As posited by Kshetri [21], an efficient blockchain consensus mechanism can mitigate the BWE due to the potential of enhanced transparency, speed, and reliability of information flows in supply chain networks. An efficient consensus mechanism can improve the performance of blockchain-based supply chain networks by facilitating fast and accurate data sharing across the supply chain and thus addressing the root causes of the Bullwhip Effect.

Blockchain helps organisations save time, money, and administrative effort via stakeholder consensus, to boost productivity further, blockchain technology must work efficiently [113], [114]. Through transparency, authenticity, trust, security and efficient operations, the technology transforms SCM [115], [116]. Blockchain makes transactions more efficient, secure, cost-effective, and transparent [117]. An efficient SCM indicator is real-time settlements, and Manufacturing companies have been adopting smart contracts to make the processes more efficient, instantly settle transactions, and automate processes [118]. Note that real-time settlements suggest

optimum efficiency. Blockchain technology also mitigates supply chain disruptions induced by global market paradigm shifts [119].

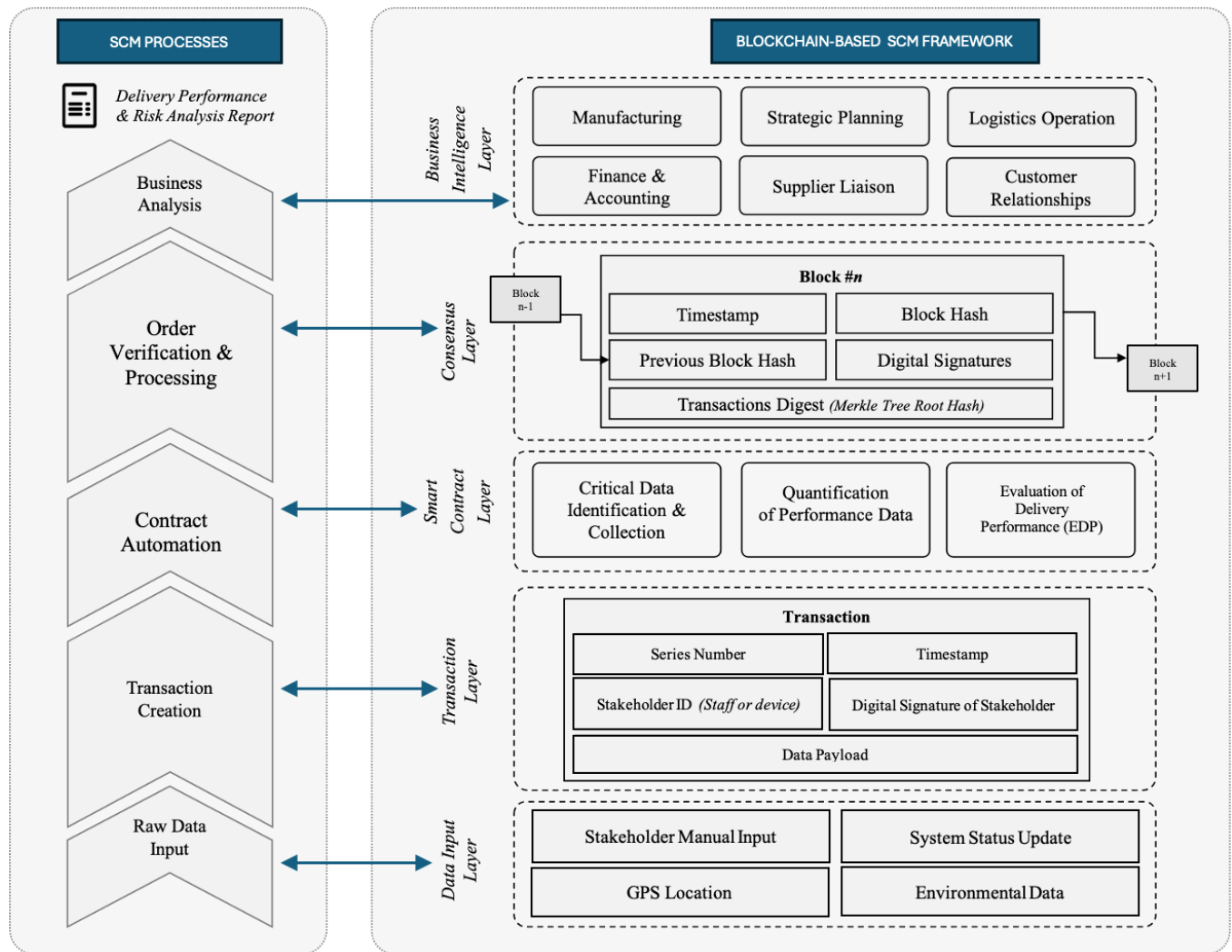


FIGURE 2.6: illustrating a novel blockchain architecture framework from a SCM perspective

Supply chain management uses blockchains to improve efficiency, record supply chain data, and turn raw data into business insights. Figure 2.6 shows a novel layered blockchain-supply chain design. The blockchain system in the figure defines the data model, gathers raw data, records it in an immutable ledger, executes smart contracts, and validates them through the consensus layer to improve efficiency and business intelligence. The diagram presents a detailed visualisation of blockchain technology's integration into SCM. It highlights a structured, multi-layered approach that extends from the initial data input to supply chain process outputs. The integration enhances supply chain efficiency, ensures data transparency, and facilitates business intelligence.

The figure presents the structure for understanding how blockchain integrates into SCM by linking key processes to the five distinct layers/operations of the blockchain architecture. The diagram is broken down into two aspects (the SCM processes and the SCM-Framework):

- **SCM Processes:** The left panel provides a streamlined flow of core SCM processes, starting from raw data input, progressing through transaction creation, contract automation², order verification and processing³, and culminating in delivery performance and risk analysis. This linear progression reflects how blockchain can improve each supply chain step by ensuring traceability, transparency, and automated verification through smart contracts.
- **Blockchain-Based SCM Framework:** The right panel breaks down the blockchain architecture into five distinct layers:
 - **Data Input Layer:** This layer captures raw data from stakeholders, including manual inputs, system updates, GPS locations, and environmental data. This is crucial for ensuring accurate, real-time information is fed into the blockchain system.
 - **Transaction Layer:** Transactions are created using stakeholder identifiers, timestamps, and digital signatures, emphasising blockchain's role in securing data integrity and non-repudiation.
 - **Smart Contract Layer:** Here, data is identified and collected, performance data is quantified, and delivery performance is evaluated. This demonstrates the automation and efficiency brought about by smart contracts.
 - **Consensus Layer:** Block creation and validation occur at this layer, which focuses on ensuring data immutability and network security.
 - **Business Intelligence Layer:** This top layer highlights how blockchain can support higher-level SCM functions like strategic planning, finance, logistics, and customer relationships through enhanced data visibility and reporting.

Figure 2.6 serves as an example of how blockchain can strengthen SCMs by decentralising data management, improving transparency, and automating functions like order verification and real-time performance evaluation. It also intuitively links the technical blockchain layers with practical SCM applications, providing a clear roadmap for how these technologies can be integrated effectively. Integrating these blockchain layers directly supports supply chain processes such as

² **Automated contracts** between suppliers, manufacturers, and distributors. Contracts ensure that all conditions in transaction requests are met before triggering actions like releasing payments or transferring ownership of goods.

³ **Order verification** is checking whether all conditions (e.g., product quantity, quality checks) are fulfilled before processing then proceeding to the next step in the supply chain.

delivery performance and supply chain stakeholder participation, illustrating how blockchain can provide a foundation for analysing performance in SCM. However, the implementation of such systems is challenging. The complexity of deploying blockchain across various SCM stages presents potential scalability issues, especially given supply chains' diverse sizes and operational scopes. Additionally, blockchain technology must seamlessly integrate with existing SCM systems, which may require significant technological and financial investments. The cost and the expected return on investment also need careful consideration, as the benefits of blockchain integration may not be immediately apparent. But blockchain still plays a role in facilitating smooth and uninterrupted supply chain networks [120], [121], [122], enhancing transparency [123] and ensuring real-time access to information for all parties involved [124].

Nevertheless, numerous blockchains experience cyber challenges related to efficiency, characterised by reduced transaction rates and increased transaction times [5]. Consequently, integrating a “non-ideal” blockchain into the supply chain may lead to a decrease in the number of transactions and an increase in transaction durations [125]. As such, additional progress is required, so prioritising and selecting a specific area within the blockchain architecture that influences blockchain performance (latency and throughput) is the next logical step of this thesis.

2.5 Blockchain use cases in SCM

2.5.1 Provenance Tracking and Traceability

One of the primary uses of blockchain technology in supply chain management is provenance tracking and traceability [21], [126]. By providing a secure and immutable record of each product's journey through the supply chain, blockchain technology enhances visibility, reduces fraud, and enables more efficient recalls when necessary [127]. Companies can create a tamper-evident and immutable ledger of product movements from origin to consumer. This application has been transformative in industries where authenticity and origin are important, such as agri-food [128], pharmaceuticals [129], and luxury goods [130]. Current consensus mechanisms struggle to keep up with these industries, e.g., Blockchain-based SCM, IBM Food Trust [131], is one of the most referenced blockchain systems in the food supply chain industry. It focuses on tracking food from farm to table, offering insights into throughput and real-time tracking needs in a global network. Their case studies provide a qualitative understanding of the network that collaborates with retailers,

farmers, and logistics providers, if scaled to track every item in detail across many global participants need to handle tens of thousands of transactions per second.

Tsang et al. [94] introduced BC-based food traceability systems and devised an innovative proof-of-supply-chain-share (PoSCS) consensus protocol. Validators, stakeholders in SCM, and mine blocks in this consensus mechanism instead of miners. PoSCS employs a probabilistic method to choose the stakeholders (validators) responsible for validating and forging the blockchain. PoSCS emphasises 'volume', 'stakeholder analysis', 'transit time', and 'shipment' rather than prioritising computational power and income. In addition, they conducted a comparison analysis of the proposed PoSCS consensus mechanism with existing consensus mechanisms. The research focused on many aspects, including the function of block generation, selection of validator/miner, and processing capacity. They demonstrated and validated the performance by doing a case study for a retail e-commerce company, but such an application would not work with a network like IBM and it was not scalable. PoSCS throughput would drop drastically to 20 transactions per second for up to 1000 transactions [132]. Interestingly, Tsang et al. [94] also proposed that PoW and PoS necessitate significant processing power, resources, and energy for decentralised networks and that the primary considerations for why PoW and PoS not being ideal to be incorporated into blockchain-based SCM food traceability systems are because of the lack of the scalability and energy efficiency, reiterating the focus that blockchains need to become more efficient.

2.5.2 Circular Economy and Sustainability

Integrating blockchain technology into supply chain management can facilitate the shift towards a circular economy and improve sustainability. Utilising blockchain technology, traceability may be enhanced to effectively monitor the movement of items and materials from production to disposal. This promotes ethical sourcing, minimises waste, and encourages resource reuse [133]. Furthermore, the implementation of blockchain technology has the potential to facilitate the establishment of decentralised energy and resource markets, hence promoting a more effective and environmentally friendly distribution of resources [134]. The traceability capabilities of blockchain allow consumers and companies to authenticate assertions regarding sustainability and ethical sourcing [60]. In the 2023 paper, Yusuf et al., [135] conducted a study to investigate using a distributed ledger technology to tackle the difficulties encountered by a vegetable provider. The authors highlighted that vegetable supply companies frequently face a restricted timeline to finalise the ledger due to the perishable nature of the items. As a result, the team established a private

blockchain network utilising, Kafka⁴, they enhanced the network layer of the blockchain to resolve supplier problems by rewriting the rules within the network layer to guarantee crash fault tolerance. The proposed Kafka blockchain network is verified using the crash fault-tolerant consensus mechanism helped to resolve the misunderstandings of information between the client and the supplier. This blockchain network is tested up to 40 rounds with 3000 transactions and getting the highest throughput of 34.1 transactions per second (TPS) and the lowest of 25.3 TPS. Similarly, Haughton et al. [66] proposed an Ethereum PoS-based consensus blockchain to evaluate the fishing industry and propose a solution for tracing the entire seafood lifecycle. This involved capturing, recording, and tracking all relevant activities and data (such as video, photos, and documents) from the initial bait stage to the final plate stage. The aim was to facilitate secure and transparent collaboration among stakeholders, including suppliers, manufacturers, distributors, and retailers, but the latency of the application lagged at (~2-3 seconds) per transaction. These platforms while solved the reason why they were designed, improving coordination and information sharing among stakeholders in the supply chain, they would not work well for large supply chains like IBM [131] or Walmart [136], that requires tens of thousands of transactions per second. Walmart implemented blockchain technology for tracking leafy greens and other perishable items to track products from farm to store shelf within milliseconds for food safety.

2.5.3 Supply Chain Finance and Risk Management

Blockchain technology can enhance supply chain finance and risk management. Blockchain technology can facilitate expedited and highly secure trade financing solutions, such as invoice factoring and supply chain credit, by establishing an unchangeable and transparent record of transactions [137]. Blockchain's ability to provide a secure and unalterable record of transactions aids in counterfeit prevention [138]. As each transaction along the supply chain is recorded on a blockchain, it becomes exceedingly difficult to introduce counterfeit goods without detection. Additionally, the increased visibility provided by blockchain technology can help stakeholders identify and mitigate potential risks, such as supplier disruptions or market volatility, more effectively [139]. A notable implementation is in the pharmaceutical industry, where the Drug Supply Chain Security Act (DSCSA) in the United States mandates track-and-trace systems to prevent the distribution of counterfeit medications [140]. In 2018, Qian and Meng [141] created a new framework for supply chain management called “DelivChain” based on a combination of aspects of PoS and

⁴ Apache Kafka is a distributed event store and stream-processing platform. It is an open-source system developed by the Apache Software Foundation written in Java and Scala languages.

PoI. It is built on a consortium-based blockchain, which allows access only to authenticated users from all participating organisations. DelivChain is a secure platform that allows users who lack trust in each other to engage in transactions with a high level of security [141]. A hybrid consensus mechanism combining PoS and PoI elements could provide DelviChain with the benefits of both mechanisms. PoS could provide network security and scalability, while PoI could provide efficiency and fairness. So, combining fragments from different consensus mechanisms can help to create a superior mechanism.

These use case examples illustrated above, represent a transformative potential for blockchain in SCM, underlining the technology's role in catalysing operational efficiencies and strategic value creation for the sector. By leveraging blockchain technology's features, stakeholders can achieve increased transparency, efficiency, and sustainability in supply chains, ultimately enhancing competitiveness in a rapidly evolving global market.

2.6 Chapter Summary

Chapter 2 has explored the foundational aspects of blockchain technology, especially its application within supply chain management (SCM). The classification of blockchain types (public, private, consortium, and hybrid) has shed light on how different governance and accessibility levels influence blockchain's effectiveness in SCM. This chapter underscored blockchain's ability to enhance transparency, data integrity, and operational efficiency, which is managed by individual layers in the blockchain. Additionally, the chapter dissected the technical processes of blockchain, focusing on block generation, consensus validation, and ledger authentication, highlighting the consensus mechanism's role in maintaining both network security and efficiency.

An essential contribution of this chapter is introducing a novel blockchain-based SCM framework that links SCM processes to the five principal layers of blockchain. This framework showcases how blockchain technology can enhance supply chain activities such as data input, transaction processing, smart contract execution, and performance evaluation. Figure 2.4 demonstrates how blockchain layers interconnect with supply chain functions to improve efficiency, resilience, and transparency.

Furthermore, it touched on various consensus mechanisms (like PoW, PoS, and PBFT) used in SCM. Subsequent chapters will simulate the performance to capture insights into how each consensus

impacts blockchain networks' efficiency, performance, and scalability in real-world SCM settings. Finally, the chapter finishes by highlighting key challenges in implementing blockchain for SCM, such as scalability and integration with existing systems. These were also highlighted alongside some practical examples of blockchain's potential to improve the supply chain. This chapter sets the foundation for the upcoming chapter on research methodology, which involves an analysis of the method that will be used to identify the security challenges in blockchains (a systematic literature review) and the process that will be used to do a deeper analysis of blockchain consensus in SCM (experimental simulations) and the impact on network performance in real-world SCM settings.

3 Research Design & Methodology

3.1 Overview

Chapter 3 focuses on the research methodology employed to assess the efficiency and security of blockchain-based supply chain management (SCM), systems. It begins by highlighting the relevance of the research in the evolving landscape of supply chain management, especially as businesses increasingly integrate blockchain technology to address challenges in transparency, efficiency, and security. The research adopts a mixed-methods approach, combining qualitative and quantitative analysis to explore the research topic thoroughly. The methodology follows a triangulation approach, which includes a systematic literature review (SLR), qualitative case study analysis, and experimental simulations using the BlockSim tool. This multifaceted method ensures a comprehensive understanding of the subject areas and verifies the research findings. The SML prioritises identifying cybersecurity vulnerabilities in blockchain-based SCM systems, aiming to map them to specific areas in blockchain architecture that manage efficiency. Building on the theoretical foundation, the research deep-dives into specific architecture areas, simulating them to propose an improved, secure, and efficient blockchain. The chapter details the positivist research philosophy guiding the methodology and the systematic investigation used to categorise and evaluate existing literature. The chapter sets the stage for practical experiments and the analysis of proposed solutions, ultimately contributing to SCM's operational security and efficiency.

3.2 Background

The relevance of this research lies in the rapidly evolving landscape of SCM, which is increasingly integrating blockchain technology to address challenges related to transparency, efficiency, and security. As businesses worldwide shift toward more digitised and secure operational models, understanding the underlying security vulnerabilities in blockchain-based SCM infrastructures becomes paramount. This is particularly relevant to stakeholders in industries relying heavily on safe, efficient supply chains, such as manufacturing, logistics, and finance.

This research will employ a mixed methods design through a triangulation approach. Turner et al. [142] highlighted that the limitations of the different research methodologies can be minimised using

mixed methods research. Mixed methods involve integrating multiple techniques to provide more thorough and robust findings. Turner et al. introduced a framework that includes (i) theory formulation and (ii) testing the practical purpose of theory while focusing on generalisability, accuracy in control and measurements, and creating an authentic context. This research will take a similar approach to examine blockchain-based SCM infrastructures' efficiency capabilities and security vulnerabilities. This thesis uses the triangulation method⁵ to include a mixture of qualitative analysis through a Systematic Literature Review and quantitative analysis through experimental computer science. The triangulation method facilitates a general understanding of the subject areas, Blockchain Efficiency + Supply Chain Management + Cybersecurity, and verifies the conclusions of this thesis.

To analyse these distinct fields of knowledge, the research begins with a Systematic Review of Literature on the cybersecurity vulnerabilities inherent in blockchain-based supply chain management systems. The SML prioritises research that explores the connection between (i) cybersecurity vulnerabilities in current blockchain systems and (ii) the blockchain architecture highlighted in Chapter 2. Chapter 2 mentions that the efficiency of blockchain-based SCM systems is determined by the blockchain architecture and how this architecture handles workload in the supply chain. The SML will highlight whether blockchain vulnerabilities can be mapped to specific areas in the blockchain's architecture that manage efficiency. The hope is that an examination of the existing cybersecurity vulnerabilities of current blockchain deployments will showcase the security gaps linked to efficiency associated with these deployments and then create and propose a solution, Proof of Efficiency (PoEf), which can adapt to the changing dynamics of blockchain technologies and cybersecurity threats.

Building on this theoretical foundation, the research will then deep-dive into one of the architecture areas by simulating it through experimental computer science. The simulations are being done to assess current infrastructures and propose an improved, secure, and efficient blockchain. The simulation tool, BlockSim, and other blockchain resources are based on the availability and proven effectiveness in simulating efficiency parameters in blockchain deployments. This research method draws on recognised methodological precedents in information systems, blockchain technologies, and cybersecurity [143]. The triangulation research methodology ensures the research is positioned to explore the challenges and contribute to the existing knowledge.

⁵ Triangulation is a research method that involves multiple approaches to studying a single phenomenon. It helps increase the reliability and validity of results by combining various data sources, methods, or theoretical perspectives.

3.3 Overview of the research methodology employed in this study

3.3.1 Research Structure

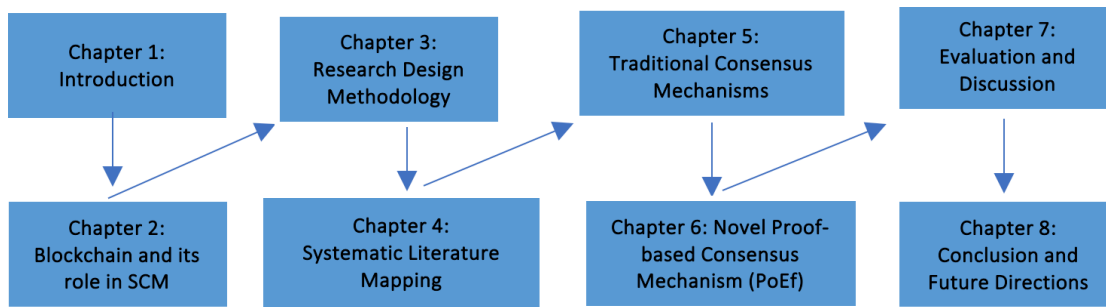


FIGURE 3.1: illustrating the structure of this thesis by chapters.

As depicted in Figure 3.1, the research structure is divided into 8 Chapters and follows a stepwise approach to accomplish the research objectives. Identifying and addressing cybersecurity challenges and technological security gaps within blockchain deployment in SCM requires a systematic approach. Following the recommendations of Yetton et al. [144], Leukel [145] and Edgar and Manz [146] on doing cybersecurity technology-related research mixed with supply chain research and developing new systems, this thesis uses a step-by-step approach to enhance existing models in blockchain-based SCMs to test and evaluate the findings.

3.3.2 Research Philosophy

The research methodology is grounded in the Pragmatism philosophy, as it employs theories and applications of a relatively new technology, blockchain, pulling relevant data from existing studies to produce, test, and derive findings that fill the current gap in the literature. The pragmatism philosophy is one of the most common foundations for triangulation. Pragmatism focuses on practical outcomes and solutions, suggesting that the best method or combination of methods is the one that solves the research problem effectively. It allows flexibility in the choice of qualitative, quantitative, or mixed methods approaches based on what works best for the study [147]. This philosophy assures that the findings are unbiased, capable of being reproduced, and applicable to a wide range of situations [147]. The thesis's objectives will be addressed from the pragmatic perspective using the exploratory sequential mixed methods design, integrating quantitative and qualitative data collection. Plano Clark [148] have recommended this mixed method for studying complex phenomena. Integrating blockchain technology in SCM and its implications for cybersecurity is one such phenomenon that would benefit from the philosophy. The data collection procedure entails simulating and looking into current Blockchain implementations to understand

the technological vulnerabilities in existing blockchain-based supply chain management systems and then simulate and test the efficiency parameters.

3.3.3 Research Approach

The research approach is broken down into four parts. The first part of the research approach is conducting an SLR. The SLR gathers and assesses existing literature using the Preferred Reporting Items for Systematic Reviews and Meta-analyses (PRISMA) framework [149] PRISMA guarantees clarity, transparency, and completeness in the research outcomes of systematic reviews and meta-analyses, especially in cases where decision-making depends on the combination of prior investigations [150]. The second stage of the research involves a quantitative experimental computer science approach using BlockSim, a blockchain simulation tool. This phase evaluates existing blockchain solutions. The third phase consists of developing a novel solution to improve efficiency and capabilities to circumvent cybersecurity challenges. The fourth phase involves creating a selection matrix.

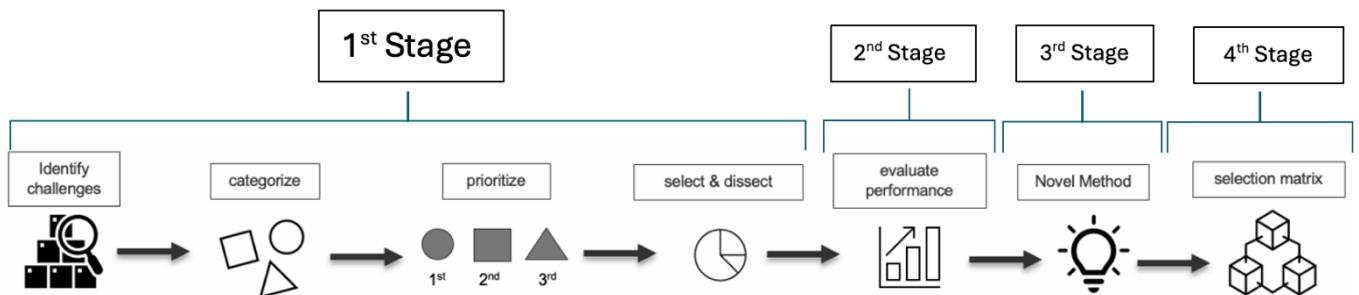


FIGURE 3.2: illustrating the thesis research approach.

As seen in Figure 3.2, the research presented follows a systematic and segmented strategy to address the knowledge gaps mentioned in the objectives. The knowledge areas found from the Systematic Literature review are categorised and examined in detail to facilitate further exploration, simulation, and testing and to aid future researchers in this relatively new field of studies integrating Blockchain and SCM.

3.4 Data collection methods

The methodology involves data from two primary sources: (i) the Systematic Literature Review and (ii) Simulation/Experimentation.

3.4.1 Systematic Review of Literature

This thesis applies systematic mapping as part of the methodology for data collection to analyse existing blockchain technology, cybersecurity, and SCM research and shape the research direction for this thesis. The review adheres to the PRISMA framework [150], ensuring a systematic, transparent, and repeatable process. The data collection involves generating research questions for the SRL, identifying relevant papers, screening and analysing data, including exclusion, and synthesising the results for further exploration. The review results are the basis for case study analysis and experimental simulations. The systematic literature review will use a similar mapping approach proposed by Petersen et al. [151], which explicitly tailors SRLs to build a classification scheme and structure of interest in software engineering. As the thesis investigates the current landscape of blockchain technology efficiency and security and proposes modifications and enhancements, this approach will help identify and categorise relevant research themes related to blockchain while highlighting gaps for potential future research. Figure 3.3 illustrates the approach of systematic review, which is segmented into five distinct phases: defining the research questions, executing the search strategy, identifying relevant papers, keyword analysis using abstracts, and the data extraction and mapping process. Choosing such an iterative approach enables an assessment of the findings from the systematic literature review. The SLR also adheres to the guidelines set forth by Kitchenham [152], ensuring a structured approach to address the research questions.

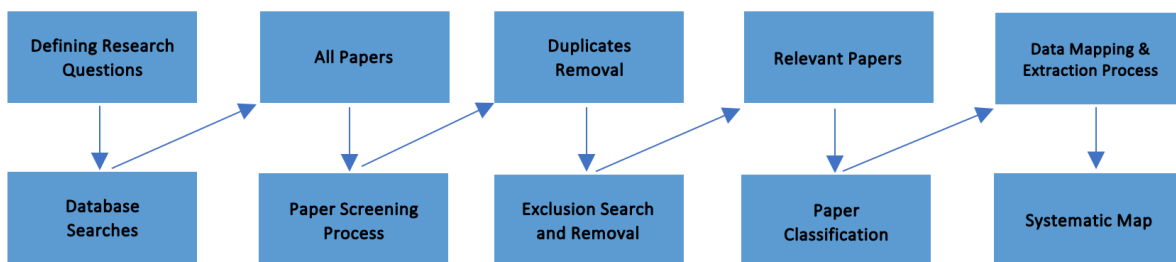


FIGURE 3.3: Illustrating steps of the Systematic Review, adopted from [151].

3.4.1.1 SRL Research Questions

The first step of the SLR involves creating research Questions.

- **RQ1:** What are the significant cybersecurity vulnerabilities in blockchain applications, and how do they impact the efficiency and performance of blockchain systems in supply chain management?

- **RQ2:** Which aspect of the blockchain plays the most critical role in mitigating cybersecurity vulnerabilities while optimising performance in blockchain-based supply chain management systems?

3.4.1.2 Selection Criteria for the Systematic Literature Review

The criteria for selecting literature and case studies were carefully defined to ensure a comprehensive targeted investigation of the research focus areas. In addition to using the PRISMA flow for the design of the SLR, the inclusion and exclusion of literature were defined according to the Population, Intervention, Comparison, Outcome and Study (PICOS) context, which is widely used in literature evidence-based research. In the context of this research:

- ‘Population’ refers to supply chain management manufacturers who use or are interested in using blockchain technologies,
- ‘Intervention’ to implementing blockchain technology,
- ‘Comparison’ of different blockchain deployments,
- ‘Outcome’ to improve efficiency and mitigate cybersecurity challenges, and
- ‘Study design’ to empirical studies providing evidence on the topic.

Literature was included in the SRL if it:

- Discussed blockchain technology with supply chain management.
- Explored cybersecurity issues associated with the implementation of blockchain.
- Was published in a peer-reviewed academic journal or conference proceedings.
- It was available in English.
- It was published between 2008 (when blockchain was first introduced) and now.

3.4.1.3 Time Horizon

This research best suits a longitudinal study examining blockchain usage in SCM over time. As this research examines how blockchain technologies have affected SCM efficiency and security from the start, a longitudinal design will allow for identifying diverse techniques and the changes over time. A longitudinal study is excellent for studying dynamic blockchain technology integration in SCM systems. This method uncovers causal links and trends that single-time-point observations overlook by gathering data at various intervals. Despite the time and resource requirements, longitudinal studies are necessary to evaluate blockchain technology's long-term effects on SCM. The time horizon will provide insights into how these technologies grow and affect SCM systems, which are hard to capture in a static research methodology.

3.4.1.4 Database searches

The second step of the SLR involves searching and compiling scholarly article using the Boolean search criteria operators:

- ("security" OR "cybersecurity") AND ("blockchain" OR "distributed ledger") AND ("Supply Chain Management" OR "Supply Chain")

Having identified the keywords for the search task, six different scientific databases were selected to search. The selected databases are Wiley Online Library, ACM Digital Library, IEEE Xplore Digital Library, ScienceDirect, SpringerLink and Taylor & Francis. Only peer-reviewed research papers published in journals, conferences and books were selected for this research.

The search queries were executed based on the title, keywords, or abstract, as per the specifications of the search platforms. The literature searches were iterated multiple times over two years during the research process. The outcomes of these Searches underwent filtration based on the inclusion/exclusion criteria outlined in Section 3.4.15 below. The specific criteria facilitated generating a collection of outcomes to the snowballing process, as described by Wohlin [153]. Successive forward and backward snowballing cycles were performed until no additional publications that met the inclusion criteria were identified.

3.4.1.5 Paper Screening process: Inclusion and exclusion criteria

The third step is to exclude all research papers irrelevant to the research questions. The criteria for inclusion and exclusion were established based on the PICOS (Population, Intervention, Comparison, Outcome, and Study) framework, a commonly employed framework in evidence-based research [154]. The term “Population” pertains to supply chain management systems, while “Intervention” denotes the type of deployment and integration of blockchain technology. “Comparison” refers to the evaluation of different kinds of blockchain deployments. The “Outcome” relates to the potential efficiency and cybersecurity concerns of implementing blockchain technology in SCM. Lastly, “Study design” encompasses empirical research studies that offer evidence and insights on this subject matter. Where there are similar publications from the same author, this SLR exclusively incorporates the most up-to-date iteration of a study.

The inclusion of literature was contingent upon the following criteria:

- Established a connection between blockchain technology, cybersecurity, and supply chain management (SCM).
- Security Context: The paper examines the cybersecurity concerns arising from adopting and utilising blockchain technology.
- Blockchain performance: The paper assessed blockchain's performance in its application environment, facilitating comparisons of different blockchain applications.
- The publication has undergone peer review and has been accepted for inclusion in a recognised academic journal or conference proceedings.
- Language: The content was accessible in the English language.
- Time period: The publication period spans from the initial introduction of blockchain technology in 2008 to 2023.

Irrelevant research publications were eliminated by assessing the titles using this method. If the pertinence of a paper could not be ascertained only from its title, an additional subsequent measure was employed to determine the study's abstract. Aside from excluding articles based on the title and abstract, additional exclusion criteria were used to eliminate certain studies. Excluded were papers lacking English text, papers lacking complete text accessibility, and papers lacking significant contributions, such as popular pieces, newsletters, or grey literature. In addition, any duplicate papers and articles not based on the technology were disqualified.

3.4.1.6 Search results

The final phase of the systematic review process involved gathering pertinent data to address this study's research questions. This step entailed collecting various data elements from each research paper, capturing the studies' core objectives and main contributions. This data collection was instrumental in ensuring a thorough and insightful analysis aligned with this review's overarching research aims.

3.4.1.7 Data extraction

This SLR relied on data extraction to ensure that every study that passed the quality evaluation provided relevant and thorough data. At first, the approach used ten random studies to enhance and validate data extraction methods. Then, studies that met quality standards were included. During this step, essential data from each document was gathered, categorised, and saved in a

spreadsheet. A systematic and detailed study was made possible by categorising the data. The systematic approach below ensures data dependability and relevance of the research based on the following type of data:

- Context data: Information about the purpose of the paper.
- Qualitative data: Findings and conclusions provided by the authors.
- Quantitative data: When applied to this research, data is observed by experimentation and research.

3.4.2 Experimental Computer Science

Experimental computer science involves formulating and constructing a practical solution to a problem by creating a prototype and then evaluating and comparing its results [155], [156]. This research employs experimental computer science to investigate blockchain systems used in SCM. The exploration is necessary to accomplish the research objectives outlined in Chapter 1, Section 1.52, and develop a new consensus mechanism with improved security and efficiency. This evaluation will be done using BlockSim, a blockchain simulation framework [157], to assess the effectiveness of Blockchain applications.

3.4.2.1 BlockSim: A Simulation Framework for Blockchain Systems

BlockSim is a simulation tool that models and facilitates the creation, imitation and assessment of the performance of discrete-event dynamic blockchain systems in various settings, such as network scenarios, consensus mechanisms, and workload instances systems [157]. Using BlockSim in this research is vital because of its Base Model functionality, which comprises essential model structures commonly seen in numerous blockchain systems. The tool allows for configuring model structures at the three primary levels of abstraction (network, consensus, and application) often seen in most blockchain implementations. The adaptability of BlockSim's Base Model to other blockchain systems is a crucial characteristic, allowing for seamless integration and adaptation to meet individual system needs or deployment standards, with a particular focus on efficiency and cybersecurity during the design.

Because the tool enables the replication of blockchain systems, it can be utilised to evaluate and experiment on the effectiveness of existing systems. BlockSim is a versatile and adaptable platform that can be customised to accurately mimic the distinct features and needs of the desired supply chain management system by facilitating the modification of current and the creation of new approaches to blockchain designs. This allows academics to evaluate the

efficiency and tackle cybersecurity constraints of existing mechanisms. To establish an experimental blockchain configuration using BlockSim, researchers must specify the simulation settings, including network topology, consensus process, transaction rate, and block size. The parameters can be adjusted to accurately represent the efficiency and limitations of the target blockchain system, ensuring that the simulation results are appropriate and meaningful for each scenario. This implies that a proposed new mechanism can be integrated into the simulation tool, and its performance and security attributes assessed and evaluated.

3.4.3 Measuring Performance of Consensus Mechanism

To evaluate the performance of the proposed new blockchain mechanism, researchers must establish a set of performance metrics and evaluation criteria [158]. For this thesis, metrics will include security-related measures of “the block creation percentage” with malicious nodes on the network and efficiency-related measures of transaction “throughput”, “latency”, and “scalability”. These metrics will be used to evaluate the new mechanism’s performance and its overall efficiency. Validating and comparing the suggested new mechanism is essential in the research process because it ensures that the developed solution properly satisfies the research aim and potentially provides suggestions for future work, such as refining the proposed method, exploring alternative techniques, or conducting further experiments under different conditions or with varying simulation parameters.

Each mechanism will be evaluated based on throughput, latency, and scalability to assist supply chain manufacturers in selecting the most suitable consensus mechanism for small, medium, and large SCM systems. The decision matrix will outline the optimal choices depending on system size and requirements. For this research evaluating “supply chain-like” networks in BlockSim, small-sized supply chains will involve a few nodes (up to 30) evaluating low transaction volumes (1 - 1000 transactions); fast processing will be required, though minor delays will be acceptable. Medium SCM systems will involve a moderate number of nodes (30 - 100) processing transaction volumes between 1000 - 10000 transactions and will need a balance between throughput and latency to ensure efficient performance. Attributing to the IBM food supply blockchain [131] or the Walmart [136] blockchain system highlighted in Section 2.3, large SCM systems will involve a large number of nodes (100 - 200 or more) and high transaction volumes (10000 - 50000 transactions). Large SCM systems demand mechanisms with high throughput and low latency to be considered efficient. These BlockSim metric settings for simulating blockchain-based SCM systems are suitable since they accurately simulate manufacturers and supply chain operators’ different real-world

circumstances. For large supply chains that manage large data volumes, including orders, payments, and shipments. The following metrics are essential for testing consensus efficiency across scaling network sizes:

- (i) Throughput, a measure that shows how the system can handle diverse workloads.
- (ii) Transaction latency, a measure testing how fast a consensus can handle transaction. SCM processes like deliveries and inventory changes require low-latency processing, enabling smooth operations among network participants
- (iii) Scalability, a measure that tests how large the network can grow. SCMs can range from modest local operations to global networks with hundreds of nodes and tens of thousands of transactions.

Simulations in Blocksim verify that the consensus mechanism can handle system growth without performance loss by assessing scalability from a few nodes to over 200. The simulation results are applicable to real-world SCM processes of various sizes and complexity due to these characteristics.

3.5 Chapter Summary

Chapter 3 established a clear and structured research approach to addressing the efficiency and security challenges in blockchain-based SCMs. This chapter outlined a triangulation approach through a mixed-methods research design that combines a SLR and experimental computer science through simulations. The methodological design ensures that both qualitative and quantitative insights are gathered to assess the security vulnerabilities and efficiency gaps in blockchain-based SCM systems. Triangulation combines qualitative and quantitative methods to improve outcome reliability. The SLR is being proposed to highlight cybersecurity vulnerabilities within blockchain architectures that affect the efficiency, which are further explored in subsequent chapters.

The combination of the PRISMA framework for systematic review and BlockSim for simulation provides a robust platform to test, validate, and improve consensus mechanisms within blockchain deployments. The integration of pragmatic philosophy in this research facilitates a solution-focused approach, ensuring that practical insights are generated to enhance both efficiency and security in SCM systems. Chapter 3 lays the foundation for the next chapter, the Systematic Literature Review (SLR), which examines the literary landscape of Supply Chain Management, Blockchain Technology and cyber security, identifying gaps, and mapping vulnerabilities to the blockchain architecture highlighted in Chapter 2 and set the stage for developing and testing a novel consensus, the Proof of Efficiency (PoEf) mechanism.

4 Systematic Literature Review: cybersecurity vulnerabilities that affect blockchain efficiency in SCM systems.

4.1 Overview

Chapter 4 systematically maps and reviews cybersecurity vulnerabilities affecting blockchain efficiency, particularly in SCM. Blockchain's potential for SCM lies in its architecture, which consists of incentive, consensus, and network layers, each contributing to overall performance and security. Although blockchain is integrated into SCM to improve transparency and efficiency, several vulnerabilities remain, requiring detailed examination. These vulnerabilities can be mapped to blockchain layers with issues with consensus mechanisms, smart contracts, network-level attacks, and cryptographic challenges. These are crucial for securing and efficiently implementing blockchain technology in SCM. A systematic literature mapping approach addresses these gaps and offers a structured understanding of the current research landscape.

The mapping identifies 108 studies that meet the inclusion criteria, categorising them into four domains: consensus mechanism failures, smart contract vulnerabilities, network-level attacks, and cryptographic challenges. The findings show a significant increase in blockchain adoption in SCM since 2016, yet further research is still needed to improve performance and security. Consensus mechanisms emerge as the most critical area for investigation due to the direct impact on blockchain efficiency. Other areas, such as smart contracts, network-level attacks, and cryptographic challenges, follow in priority but remain essential for maintaining security and operational continuity in SCM systems. The chapter establishes the foundation for further research, specifically in simulating and testing consensus mechanisms in SCM using BlockSim.

4.2 Introduction

Blockchain's unique properties have led to its study in banking [35], governmental systems [36], healthcare provisions [159], and, in this study, SCM [27], [160]. Goods are efficiently coordinated from production to consumption in SCM. This involves a complex network of manufacturing and distribution companies. From basic trade systems to sophisticated, technology-driven SCM, companies can actively detect and solve problems, meet consumer needs, and meet economic

goals. In a modern world with high consumer expectations, swiftly receiving products boosts supply chain management and execution strategy, and every layer (that is susceptible to vulnerabilities) threatens SCM's performance and security.

Despite advances, research gaps in blockchain in SCM ecosystems, particularly security ones, remain. This paper explores prior studies on how SCM blockchain infrastructure decisions expose the SC to cybersecurity vulnerabilities that can impair efficiency and shape its future.

4.2.1 Justification for the Systematic Review

A systematic approach to the literature review is needed to integrate the gains achieved through knowledge, methods employed, and the trajectory of the continuing academic discourse [161]. The SLR is essential as it offers a detailed and structured assessment of existing knowledge, which is crucial for setting up the direction for the thesis., and uncovering gaps in the existing literature, which is vital for directing towards contributing to the novel insights of this research [162]. It lays the foundation for ensuring the investigation carried out in this thesis is grounded in existing knowledge and theories relevant to blockchain and SCM. Applying the SLR guides the research decisions and influences the simulation model development. According to Okoli et al., Insights derived from the SLR can directly impact the design and implementation of experimental simulations, ensuring that research components are both relevant and practical [163].

4.2.2 Related Work

Since 2016, systematic literature reviews have been conducted in these intersecting spaces. Yli-Huumo [80] conducted an SLR in 2016 to analyse published research findings on blockchain technology. Although the review focused on technical aspects of blockchain technology, approximately 80% focused on Bitcoin and related security and privacy concerns. The review did not address blockchain applications in supply chain management. Since 2016, blockchain technology has seen broader application diversification like SCM, prompting this research to delve into blockchain developments still riddled with cybersecurity challenges and application efficiency issues.

Similarly, in late 2016, Conoscenti et al. [164] carried out an SLR examining blockchain's adaptability and usage, particularly to the Internet of Things (IoT) and peer-to-peer devices. The

research assessed whether the blockchain and peer-to-peer approaches could facilitate a decentralised and private-by-design IoT. Still, there is no mention of how different types of blockchain architectures affect the privacy of the solutions. 2017 Seebacher et al. [165] conducted another SLR, highlighting blockchain's growing influence on supply chain service systems, revolutionising how transactions are performed. In 2019, Salman et al. [166] produced a survey paper that looked at different approaches to blockchain implementation from a broad perspective and highlighted how these blockchain approaches solve cybersecurity concerns in traditional systems, with no mention of how diverse blockchains handle security differently.

In 2020, Dutta et al. [114] explored using blockchain technology in supply chain operations. They investigated challenges related to consensus mechanisms, network-level attacks, cryptographic enhancements, and smart contract improvements. The study examined how blockchain technology can enhance various functions within the supply chain and identified the current research trends in different domains of supply chain operations. Many articles in 2021 focused on specific applications that bring more efficiency to the supply chain sector, like Song et al. [167], who proposed a supply chain system framework integrating IoT with blockchain to tackle entry barriers for new businesses and enhance supply chain efficiency. In 2022, Lui et al. [168] reviewed blockchain applications in supply chain management. They briefly mentioned how blockchain consensus mechanisms could address supply inefficiencies and highlighted how smart contracts play a role in security blockchains in SCM. Last year, in 2023, the number of applications implemented in the supply chain sector increased and is still growing, but Singh et al. [169] highlighted that there is still a need to explore the performance of blockchain and that it should be evaluated in terms of privacy, security, energy efficiency, throughput, latency, and privacy.

Even though there has been a constant increase in blockchain developments with different approaches over the years due to the fast-paced development and growth of the technology, there is still a continuous scholarly need for research assessing the integration of these approaches in sectors like SCM and how these different developments affect performance. Prior research has primarily examined the broader characteristics of blockchain technology, or how the technology itself, based on its characteristics, improves the efficiency and security of traditional systems, but has not sufficiently looked at the architecture of blockchains and how different architectures/approaches affect the security posture and efficiency of SCM systems. An in-depth examination of the blockchain's architecture is essential for comprehending the potential effects of

certain blockchain implementations on the security and efficiency of SCM solutions. It also helps identify possible research, enhancement and innovation areas in this rapidly growing industry.

4.3 Search results

The search results obtained from the Boolean search criteria operators yielded 10,894 studies. After eliminating duplicate entries, the total number of studies decreased to 6,465. Upon thoroughly examining the research based on the predetermined inclusion and exclusion criteria, 703 papers met the requirements and were deemed suitable for further review. The PRISMA flow diagram in Figure 4.1 illustrates the SLR paper-gathering process over 3 main steps (identification, screening and inclusion). The diagram outlines the stages involved in identifying and selecting studies for this systematic literature review. The PRISMA flow begins with the Identification stage, where 10,894 records were retrieved from six major databases based on predefined inclusion criteria, such as “security” or “cybersecurity” and “blockchain” or “distributed ledger” in the context of supply chain management. After removing 4,429 duplicate records, 6,465 records were left for further screening. In the Screening stage, 5,762 records were excluded based on the title and abstract, leaving 703 reports for retrieval. A detailed inclusion and exclusion review excluded 631 reports, leaving 72 studies eligible for further assessment. Finally, in the Inclusion stage, additional studies were included using a snowballing technique, with 20 reports identified through forward snowballing and 16 through backward snowballing, resulting in 108 studies being included in the final review. This flow diagram provides a transparent and structured approach to the systematic review process, adhering to PRISMA guidelines.

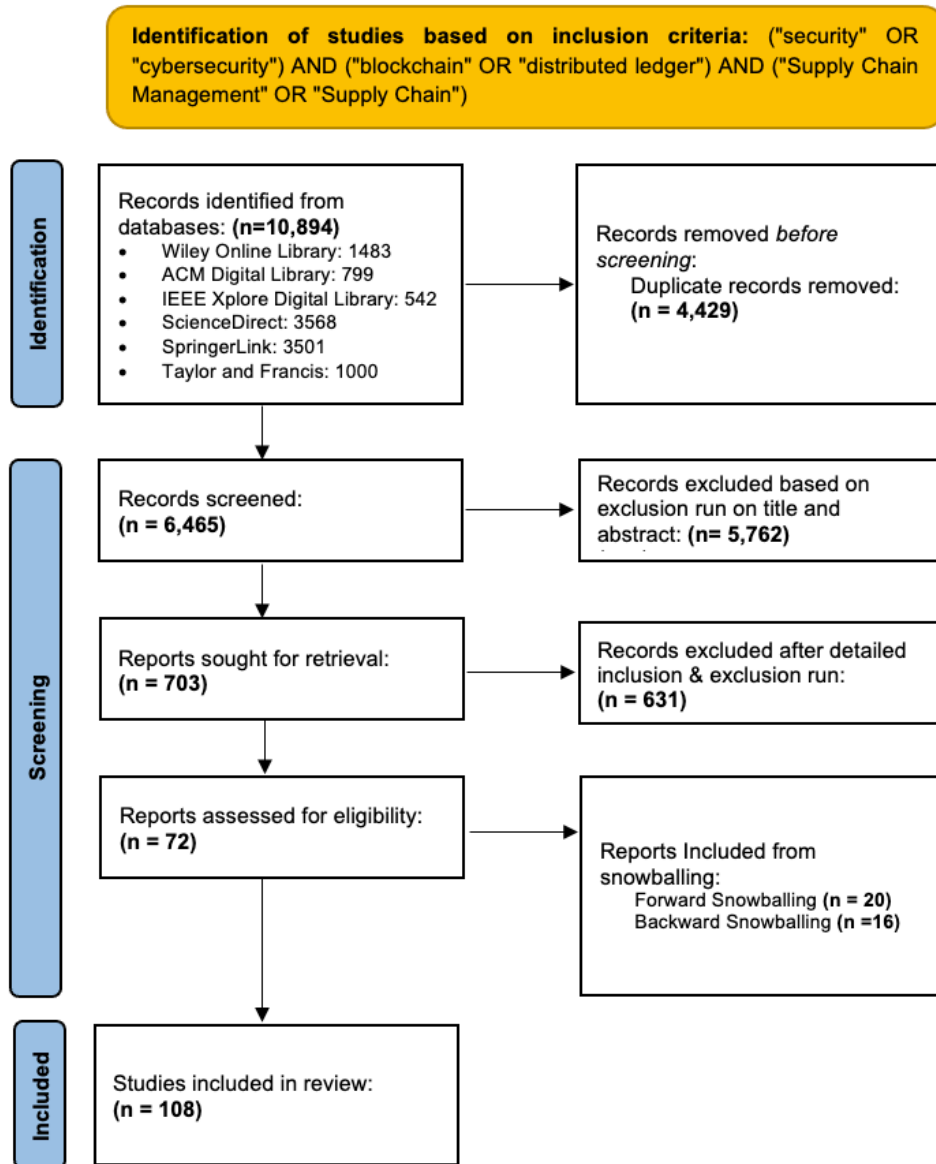


FIGURE 4.1: PRISMA flow diagram illustrating the SLR paper gathering process.

4.3.1 The Inclusion Parameters

Papers were included if they included the following elements:

- Blockchain in SCM. Each paper was required to concentrate specifically on blockchain's application in SCM or provide a technical perspective of blockchain's impact on supply chain security and efficiency.
- Blockchain application. Papers offered details on implementing blockchain technology in SCM systems, aiding in resolving research queries.
- Security context. The papers elucidated the security challenges they addressed, aligning with this SLR's research questions.

- Blockchain performance. The papers evaluated the performance of blockchain technology in the respective application environments, allowing for comparative analysis across different blockchain deployments.
- Data acquisition. The studies were assessed for the methodology in data collection, measurement, and reporting to gauge the accuracy and reliability of the data presented.

4.4 Findings

4.4.1 Publications over time

The first SCM research articles on blockchain appeared in 2016. The technical aspect of blockchain led to publications in technical forums, consulting reports, news evaluations, and comments from 2008 to 2015. Since 2016, engineers, academics, and practitioners have considered blockchain applications. Figure 4.2 shows the distribution of the selected literature sources and a continuous and annual increase in blockchain technology's SCM performance publications. Increased publications emphasise cybersecurity and operational efficiency and show the technology's supply chain possibilities. The trend shows increased interest and investment in SCM blockchain applications. Research in this field should continue to develop. The market for Blockchain-based supply chains is expected to grow from USD 0.56 billion in 2023 to USD 4.21 billion in 2028, with a compound annual growth rate (CAGR) of 49.87%, according to commercial blockchain developer Antier [170]. This may be a reason for the growing number of valuable studies on improving and optimising blockchain technology in real life.

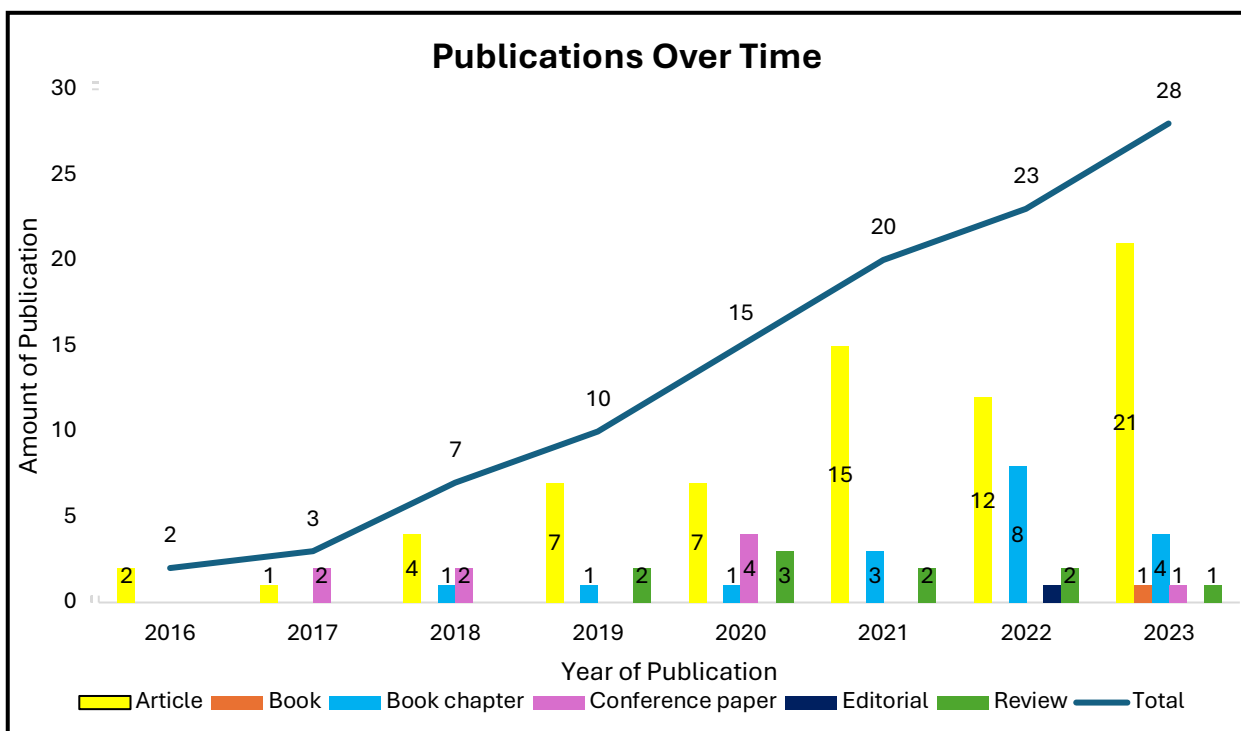


FIGURE 4.2: Graph illustrating the primary studies distribution by year of publication

4.4.2 Paper Classification

The identified research papers were categorised in the fourth stage of the systematic literature mapping procedure. The classification used the keyword strategy described in Yli-Huumo et al. [80]. An evaluation of the abstract was performed for each manuscript to identify important keywords and the main contributions of the research. The objective was to methodically categorise these documents into separate classifications for more convenient analysis and reference. If the abstract contained insufficient information for accurate classification, the document was examined briefly to determine the most suitable category. The systematic technique guaranteed the precise categorisation of each paper, enabling a better organised and cohesive study of the research environment. The chosen papers are then categorised based on performance-related supply-chain-centric subjects to address RQ1 and RQ2. It was observed that each paper may have cited multiple topics to address the range of selected papers effectively. For this research, every primary research article underwent an evaluation process, during which qualitative and quantitative data were gathered and concisely summarised in Figure 4.3 and Figure 4.4

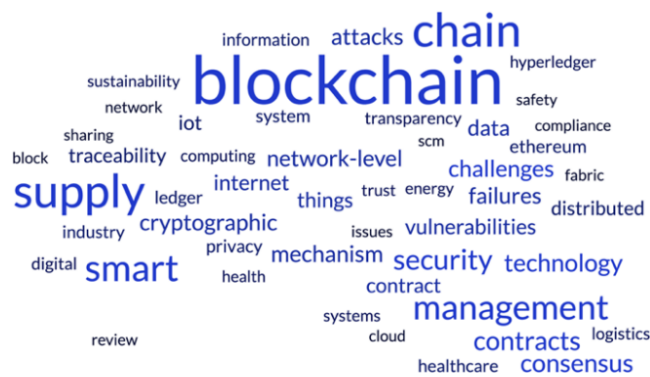


FIGURE 4.3: illustrating a word bubble of the main thematic areas in the primary studies.

Figure 4.3 uses a word bubble to classify the themes found in the 108 main studies. Figure 4.4 summarises all the papers in our data review analysis after meeting the necessary quality evaluation criteria. Appendix 1 expands Figure 4.4 into a more exhaustive list. Vulnerabilities, attacks and enhancements are outlined based on the location. The root causes and consequences are analysed, and then papers are categorised in possible areas of future research directions, proposed to enhance blockchain efficiency, drawn from the literature, and discussed. Table 4.1 highlights attacks/vulnerabilities associated with each thematic area (blockchain's layers). This was used to develop a taxonomy of the vulnerabilities/attacks and the consequences, which were consolidated in a taxonomy illustrated in Figure 4.5.

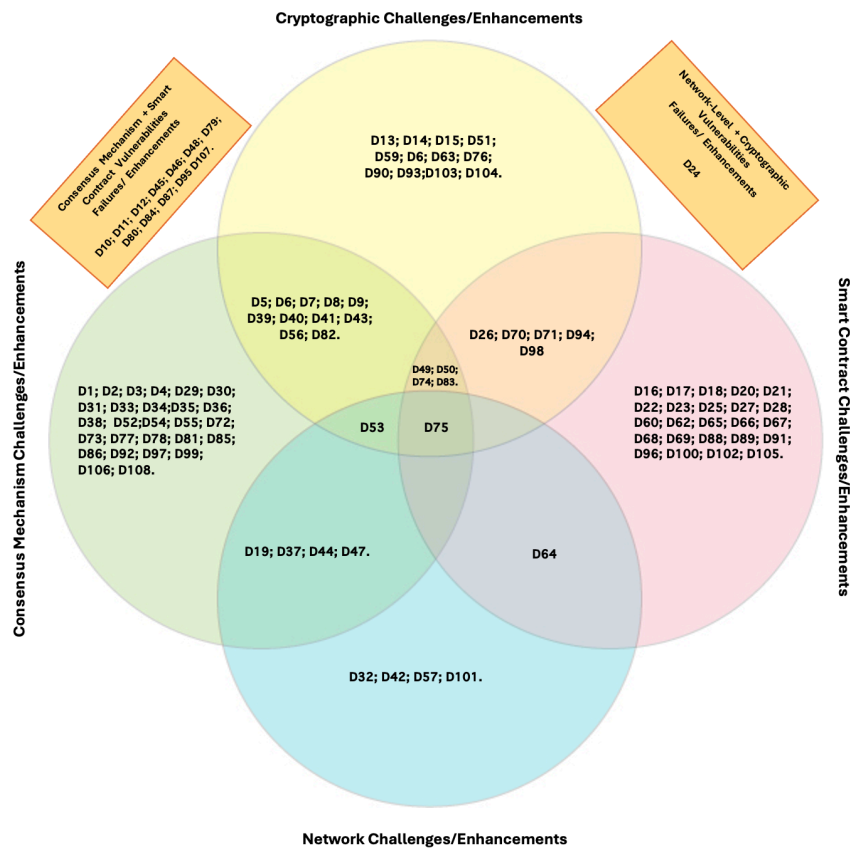


FIGURE 4.4: The main thematic areas of the Systematic Literature Mapping (complete list of papers is in Appendix 1).

4.4.3 Blockchain-Based Supply Chain Management Cybersecurity Taxonomy

Blockchain technology faces cybersecurity risks despite its strong security features. Maintaining secure and efficient blockchain-based SCM systems requires understanding these problems. Chapter 2 describes the blockchain design with five layers: hardware, data, network, consensus, and contract/application. This research will focus on blockchain technology, not hardware. Previous studies show that blockchain vulnerabilities and attacks may be classed by architecture position. A good example is Denial of Service (DoS) attacks. DoS threaten blockchain performance across its architecture. DoS attacks can overload smart contracts with transactions at the application layer, delaying them and raising computational costs. Smart contracts (self-executing contracts with coded terms) can be insecure if not constructed to prevent excessive resource consumption [171]. This hinders valid transactions and degrades blockchain application reliability and safety [172]. Thus, these attacks can damage blockchain applications' reputation and value. DoS attacks can also undermine distributed nodes' blockchain consensus in the consensus layer. An attacker can slow block formation by targeting mining or validation nodes, which delays transaction confirmation [173], reducing blockchain throughput and allowing double-spending and fraud.

The network layer is essential for blockchain node communication. This layer's DoS assaults overwhelm the network with traffic, causing congestion and packet loss. The inability of nodes to propagate transactions and blocks efficiently increases latency and network dependability [174]. Such disruptions can adversely damage blockchain network performance and security as nodes struggle to maintain consensus and synchronise with the latest blockchain state. Data layer DoS attacks can target blockchain data storage and retrieval. Blockchains maintain transaction histories and states in distributed databases. Attacks that overrun data storage might delay access to SCM information, making it harder for nodes to validate new transactions and blocks [175], compromising blockchain data integrity and availability, and reducing system trust and efficiency. DoS attacks exploit multilayered blockchain flaws. These attacks can slow performance, disrupt consensus, and jeopardise network and blockchain data dependability. This means blockchain layers can classify flaws or susceptibilities.

Between 2011 and 2019, Alkhalifah et al. [176] created a cybersecurity taxonomy affecting blockchains generally and categorised it into five vulnerability areas: two people-related and three technology-related. These domains are clients' vulnerabilities (people), consensus mechanisms vulnerabilities (technology), mining pool vulnerabilities (people), network vulnerabilities (technology), and smart contracts vulnerabilities. This research extends the technology taxonomy, explicitly focusing on blockchain-based supply chains. Using a keywording on author and index keywords, this research classified vulnerabilities into four technology areas: (i) Failures in consensus mechanisms, (ii) Vulnerabilities in smart contracts, (iii) Attacks at the network level, and (iv) Challenges related to cryptography that could affect blockchains' SCM efficiency. This SLR addresses technology flaws from 2011 to 2019 [176] and introduces a new area: cryptographic challenges. Table 4.1 illustrates the principal vulnerabilities that affect SCM-related blockchain systems; the full table is in Appendix 1.

TABLE 4.1: Illustrating the principal vulnerabilities that affect SCM-related blockchain systems.

| Vulnerabilities | Issue Category | Consequences | Connected Reference | Affect Blockchain Efficiency? | How it affects efficiency |
|-----------------|--|---|------------------------------------|-------------------------------|--|
| Double Spending | Consensus Mechanism Vulnerabilities/Enhancements | Alter blockchain network; Spend the same digital coin more than once; | D44; D53; D77; D92; D108; D53; D31 | Y | Double spending undermines trust and security, causing network nodes to expend additional resources to resolve discrepancies, thus reducing transaction processing efficiency. |

| | | | | | |
|----------------------------------|--|--|-------------------------|-----------|--|
| 51% Majority (DoS Attack) | Consensus Mechanism Vulnerabilities/Enhancements | Control Mining Process; Unfair Control of Computational Power | D99; D53; D78; D85 | Y | If attackers gain majority control, they can disrupt network operations and slow down or halt transaction processing, significantly reducing efficiency. |
| Bribery (Double Spending attack) | Consensus Mechanism Vulnerabilities/Enhancements | Obtain Majority of Computational Power; Bribe Minors to subvert the consensus agreement | D44; D108; | Sometimes | This depends on network safeguards, but successful bribery attacks could lead to inefficiencies as the network attempts to correct fraudulent transactions. |
| Selfish Mining | Consensus Mechanism Vulnerabilities/Enhancements | Waste the Computing Power of Honest Miners | D11; D44; D53; D77; D31 | Y | This manipulates the blockchain's reward system and can lead to inefficiencies in block validation times and reduced network trust. |
| Sybil Attacks | Consensus Mechanism Vulnerabilities/Enhancements | Create multiple forks; block honest nodes; reduce throughput; control block's network | D37; D53; D36 | Y | Fake identities in the network can disrupt consensus and network operations, reducing efficiency. |
| TimeJacking | Cryptographic Challenges/Enhancements | Split in the Network; Isolate Victim Node; Fake Transactions; Waste Computational Powers on stale blocks | D53 | Y | Manipulating a node's system time can affect blockchain operability and synchronisation, leading to delays and inefficiencies in transaction processing. |
| Quantum | Cryptographic Challenges/Enhancements | Access to Public/private Key; Control User Account; Hash Collision | D53; D61; D90 | N | The threat is currently theoretical but could become significant if quantum computing can break blockchain cryptography, leading to a complete overhaul of security protocols. |
| Transaction malleability | Cryptographic Challenges/Enhancements | Modify Transaction Identifier; Valid Signed transaction before it is mined | D53; D76 | Sometimes | It allows attackers to alter the unique transaction ID, potentially causing confusion and inefficiency in transaction processing. |
| Re-entrancy | Smart Contract Vulnerabilities/Enhancements | Ether loss | D65; D100 | Y | It can lead to multiple withdrawals or unintended interactions within smart contracts, draining resources and slowing down the network. |
| Parity Multi Signature Wallet | Smart Contract Vulnerabilities/Enhancements | Data Leakage; change wallet owner; drain funds | D65; D95 | Y | Specific vulnerabilities like those exposed in the Parity wallet can freeze or lose funds, directly affecting transaction efficiency. |
| Timestamp Dependence | Smart Contract Vulnerabilities/Enhancements | Adjust transaction timestamps; lock funds for a | D95; D100; | Sometimes | Manipulation can affect transaction ordering and block generation, potentially leading to performance issues. |

| | | | | | |
|----------------------------|---|---|---------------------|---|---|
| | | period; change contract's output. | | | |
| Mishandled Exceptions | Smart Contract Vulnerabilities/Enhancements | returned transactions; | D65; D95 | Y | Poor error handling can cause unexpected crashes or freezes in smart contracts, leading to inefficiencies. |
| DoS with unexpected revert | Smart Contract Vulnerabilities/Enhancements | Reverted/stopped transactions; fail payments | D88; | Y | Such attacks can make smart contracts unavailable, halt transactions and affect system performance. |
| Tx.origin | Smart Contract Vulnerabilities/Enhancements | disguise smart contract; transfer funds | D100; | Y | Exploits involving tx.origin can compromise wallet security, indirectly affecting transaction speeds and efficiency. |
| DDoS | Network-Level Attacks Failures/Enhancements | Impact on memory pool; transaction backlog; trapped users pay higher transaction fees | D47; | Y | DDoS assaults can overload network resources, reducing transaction throughput and latency. |
| DNS Ownership | Network-Level Attacks Failures/Enhancements | Change DNS seeds; Centralisation risks | D19; D57; D64; D101 | Y | Compromising DNS can redirect users to malicious sites, affect network traffic, and reduce the efficiency of legitimate transactions. |
| Eclipse Attacks | Network-Level Attacks Failures/Enhancements | Isolate victim node; control the network; waste computational power | D44; D53; | Y | These isolate a node from the rest of the network, affecting its data consistency and overall efficiency. |
| BGP Routing | Network-Level Attacks Failures/Enhancements | Re-routing traffic; create fork blockchain | D32; D53 | Y | Manipulation can lead to data interception or rerouting, affecting transaction times and reliability. |
| Replay | Network-Level Attacks Failures/Enhancements | Delay/ Intercept of data | D42; D100 | Y | Replay attacks waste computational resources and reduce efficiency by repeating transactions. |

4.4.3.1 Satisfying RQ1

What are the significant cybersecurity vulnerabilities in blockchain applications, and how do they impact the efficiency and performance of blockchain systems in supply chain management?

Table 4.1 outlines vulnerabilities that affect efficiency in blockchain systems, categorising them into issue types (expanded in Sections 4.3.3.1-4.3.3.4): consensus mechanism failures, cryptographic challenges, and smart contract vulnerabilities. The table and Sections 4.3.3.1-4.3.3.4 satisfy RQ1, highlighting each vulnerability's consequences and referencing relevant studies, indicating whether

these vulnerabilities impact blockchain efficiency. For example, double spending and Sybil attacks directly reduce efficiency by requiring nodes to expend additional resources to resolve discrepancies and manage fake identities in the network. Similarly, cryptographic challenges like TimeJacking and quantum computing threats could disrupt synchronisation and affect transaction processing efficiency. Smart contract vulnerabilities, such as re-entrancy and mishandled exceptions, lead to resource drain and slow down network performance. The table is a foundation for proposing the novel PoEf consensus model, identifying the vulnerabilities that critically impact efficiency. It offers insights into how PoEf can be designed to improve security and enhance the overall efficiency of blockchain-based SCM systems.

4.4.3.2 Consensus Mechanism Failures

Consensus mechanisms are the bedrock of blockchain technology efficiency. They guarantee unanimous consensus among network participants on the legitimacy of transactions and ensure that all participants in the network agree on a single version of the truth, serving as the foundation of transaction validation on blockchain networks. Without consensus among the stakeholders, transactions cannot be confirmed. Nevertheless, existing mechanisms are susceptible to specific vulnerabilities that have the potential to undermine the integrity and efficiency of SCM systems that employ blockchain technology. Coming out of the taxonomy for this review are:

- A **double-spending attack** is an attacker replicating a transaction to spend twice the same funds. The attacker would send a copy of the currency transaction to make it look legitimate. This malicious conduct disrupts the normal functioning of the blockchain and results in the theft of funds. This infringes the confidence within the supply-chain blockchain network and requires nodes to allocate extra resources to resolve data inconsistencies, decreasing the overall speed and efficiency of transaction processing [D53]. PoW and DPoS can be vulnerable to double-spending attacks, especially if an adversary controls a large portion of the network, while PoI, PoC and Stellar are better protected due to the reliance on different, less brute-force vulnerable consensus methods [D31] [D36].
- A **Sybil attack** occurs when one or more malicious actors gain control over the whole network. If attackers generate several fraudulent identities (Sybil identities), they can overpower the honest nodes through voting, and attackers can gain disproportionate influence over the network's consensus mechanism. This can skew the transaction validation process, allowing malicious actors to prioritise fraudulent or obstruct legitimate transactions, thereby decreasing transaction throughput and increasing the time required for

consensus. Subsequently, they can manipulate the receiving and transmission of blocks, impeding the network access of other legitimate users [D37]. A malicious pool operator can introduce many miners with no computational capability into a mining pool, so execute a Sybil attack. These miners cannot mine any blocks successfully but can propagate data on behalf of malicious users and prevent data transmission from honest users. Thus, just the block created by the attacker would be added to the network, resulting in the attacker receiving greater rewards and reducing the network's throughput [83]. This attack has the potential to result in various types of attacks, including Denial of Service (DoS), Distributed Denial of Service (DDoS), and 51% majority attacks [D53]. Sybil attacks are a risk for decentralised systems that rely on identity (DPoS, PoI, Stellar, PoW), though PBFT is more resilient due to its permissioned nature and known nodes [D36].

- In a **51% Majority Attack**, the attacker can manipulate the blockchain mining process by controlling at least 51% of the computational power [D78]. They would establish a sequence of blocks separate from the authentic version of the chain. By using the 51% majority, they expedite the processing of the blocks, establishing the isolated (fraudulent) chain as a legitimate one over time. The 51% majority is often considered double spending [D53]. If attackers achieve a position of dominance, they could interfere with network operations and impede or stop the processing of transactions, resulting in a considerable decrease in efficiency. Malicious miners could execute a Denial of Service (DoS) attack by gaining control of the bulk of the mining power. They create empty blocks and disregard other blocks [D78]. An “agreement mechanism” is developed in [D99] to serve as the foundation for a strategy to enhance resilience against 51% attacks. PoW and DPoS are particularly vulnerable to 51% attacks, where an adversary can control most resources, while mechanisms like Stellar, PoC, and PBFT have designs that reduce the risk of such attacks [D85].
- A **selfish mining attack** is a strategy where a miner or a group of miners intentionally withhold blocks they have mined from the network to gain an unfair advantage over other miners. This attack exploits how the blockchain consensus mechanism works, and Malicious miners can manipulate the blockchain to acquire more block rewards [D77]. This action exploits the incentive system of the blockchain, resulting in longer block validation delays and decreased trust in the network. An inherent limitation of previous consensus techniques, like PoW, is the potential for miners to collude and employ self-serving tactics to maximise the rewards beyond what they would achieve through individual mining efforts. Miners who engage in this

behaviour are called selfish miners, and the unauthorised mining cooperation is known as selfish mining. This is inequitable to the other conscientious miners who adhere to the rules established by the consensus mechanism [D44]. As reference [D11] suggested, the Data Highway Protocol could decrease the likelihood of selfish mining. While PoW is known to suffer from selfish mining risks, Stellar's consensus reduces the incentive for such behaviour. DPoS and PBFT show strong resilience against these types of attacks due to the node structure [D31]

- **Bribery Attacks** incentivise validators or miners to manipulate the behaviour and direct the efforts towards specific blocks or forks. Through this approach, the attacker can present arbitrary transactions as legitimate and receive compensation from dishonest nodes for verifying them. Miners are paid an amount equal to or greater than the block rewards if the network reverts the block to incentivise them to work on the attacker's blocks or chain. If the network reverts, the attacker encounters a more substantial issue. If the malicious branch is reverted for reasons such as the attacker being unable to continue bribing or dishonest nodes ceasing to work on that branch, the attacker would be obligated to pay a substantial sum of bribes. This is because the bribes will accumulate for each maliciously created block. Bribery attacks could enhance the likelihood of double spending because attackers may bribe miners to prioritise fraudulent transactions [D44]. While the efficiency of the blockchain itself may not be directly impacted, successful bribery attacks can potentially cause inefficiencies as the network works to rectify erroneous transactions. Multiple bribery methods have been suggested, each with different trust and risk characteristics [D108]. Evaluating these many bribery mechanisms is challenging because there is a lack of systematic procedures for quantification. Bonneau [D108] proposed many strategies to mitigate the impact of bribery attacks, contingent upon the existence of network safeguards. Implementing such techniques and the inherent difficulty and expense associated with bribery attacks on consensus mechanisms such as PoW and PoS lead to the conclusion that bribery assaults are not the most significant concern regarding blockchain efficiency. PoW is more vulnerable to bribery attacks since miners can be incentivised to behave maliciously. Other consensus models like PBFT and PoC have mechanisms that mitigate the risk [D97].

TABLE 4.2: illustrating attack resilience of different consensus mechanisms.

| Attacks | DPoS | Pol | Stellar | PoW | PoC | PBFT |
|--------------------------------------|-------------|------------|----------------|------------|------------|-------------|
| <i>Double-spending attack</i> | N | Y | Y | N | Y | Y |
| <i>Sybil attack</i> | N | N | N | N | N | Y |
| <i>51% Majority Attack</i> | Y | N | N | Y | N | N |
| <i>Selfish mining attack</i> | N | N | Y | Y | N | Y |
| <i>Bribery Attacks</i> | N | N | N | Y | N | N |

Each vulnerability threatens blockchain-based systems' security and operational efficiency, demanding creative solutions. These risks must be addressed to ensure blockchain applications' long-term reliability and efficiency in supply chain management and other domains. This research highlights these challenges and develops more resilient consensus techniques to be adapted to modern SCM systems' requirements. Table 4.2 summarises the resilience of various blockchain consensus mechanisms against common security attacks that would negatively impact a Blockchain-based SCM system's efficiency.

4.4.3.3 Cryptographic Challenges

The security and integrity of blockchain heavily rely on cryptographic techniques, which sit in the Data Layer of the blockchain. Li et al. [68], along with several other authors like Yu et al. [69] and Latifa et al. [177], emphasise that flaws in cryptographic techniques or the implementations can lead to systemic failures in blockchain networks. Cryptographic challenges in blockchain technology impact its operational efficiency, primarily due to the reliance on cryptographic techniques to secure and validate data across the network. Some of these vulnerabilities include:

- ***Timejacking*** occurs due to the susceptibility of timestamp processing in a blockchain. Each participating node in a blockchain network possesses a time counter that indicates the current network time. Malicious actors could introduce several Sybil nodes onto the network and simultaneously manipulate the time of these nodes. By transmitting false timestamps, this action can impede the average time of the specific node while also causing the network to fragment and isolate the targeted node from the rest of the network [D53]. This not only diverts resources towards ineffective efforts but also fragments the blockchain's continuity, leading to inefficiencies in transaction processing and increased vulnerability to fraud.

Consequently, fraudulent miners use computational resources on outdated blocks, negatively impacting the network due to fraudulent transactions [D53].

- A **quantum attack**, where attackers can employ Shor's algorithm to attack the blockchain's cryptography component, enabling them to decode the private key from the public key. According to [D61], the danger level is elevated in blockchains like Ethereum because quantum attackers can execute hash collision attacks, which gives them the ability to assume full control of an account and deplete all its funds [D61]. The potential for quantum attacks to execute hash collision attacks presents a significant risk, particularly for blockchains that do not yet employ quantum-resistant algorithms, compromising these systems' security and operational integrity. Researchers and Scientists are currently developing post-quantum cryptography techniques to safeguard blockchain systems from potential quantum attacks [D53, D90].
- The **transaction malleability attack**, which can be linked to either the network layer, the data layer, or both [D76]. Supply chain transactions contain data that is stored on the blockchain, and the blockchain employs encryption techniques to safeguard this data. Depending on the application, a transaction ID (Tx.ID) is assigned to each confirmed transaction and appended to the blockchain. Transaction malleability is an illegal modification to a transaction before that transaction is accepted in a block. During these attacks, a malicious node intercepts the transaction and generates an altered version of the signature by modifying the transaction identifier (Tx.ID), then distributes it to other nodes in the blockchain [D53]. A successful transaction malleability attack might lead to subsequent attacks, such as double spending [D76]. This vulnerability not only undermines the trust in a blockchain's transactional integrity but also burdens the network with the need to identify and rectify fraudulent entries, thereby reducing overall system efficiency.

Each of these cryptographic vulnerabilities poses a severe risk to the efficiency and reliability of blockchain networks, particularly in applications such as SCM, where data integrity and security are paramount. Continuous updates to cryptographic practices and the integration of advanced security measures are essential to mitigate these risks and enhance the operational efficiency of blockchain systems.

4.4.3.4 Vulnerabilities in Smart Contracts

Smart contracts, autonomous self-executing contracts with terms written into code, play a crucial role in automating SCM processes on the blockchain. They are integral to automating processes in blockchain SCM; however, they introduce significant cybersecurity risks. These contracts, once deployed, are immutable, and any vulnerabilities in the code can be exploited, leading to substantial losses or disruptions in SCM operations. Authors like Luu et al. [178] and Atzei et al. [179] have documented various vulnerabilities in smart contracts, highlighted below, ranging from re-entrance attacks to contract dependencies.

- **Re-entrancy vulnerability** is a security weakness that allows an attacker to repeatedly enter and execute a specific section of code before it has completed its previous execution [D100]. The attack occurs when attackers generate a contract with malicious code at an external location by utilising the fallback mechanism. Consequently, assailants would take control of this susceptible contract and repeatedly invoke the same function without the state being updated. It disrupts normal contract operations and can lead to inefficiencies in transaction processing as the system struggles to manage unintended recursive functions that sap computational resources [D65].
- A **Parity Multi-Signature Wallet**: To withdraw digital assets from a wallet, it is advisable for users to have a multi-signature wallet, which requires several signatures or private keys. This is because users' personal information and daily withdrawal restrictions are maintained in the wallets. [D65] The vulnerability of the parity multi-signature wallet lies in its reliance on a centralised public library and the unrestricted access it provides to external wallet library functions. This configuration has made the wallet an attractive target for assaults [D95]. The reliance on a single, centralised library exposes the system to risks if the library is compromised. If attackers gain control, they could manipulate transaction permissions and access, leading to transaction delays and disruptions in the supply chain operations that depend on these wallets for transaction validation and execution.
- **Time dependence**: Upon successful mining of a block, the miner must provide the timestamp for the block. After mining, the miner will examine the timestamp of a new block and perform the verification process to ensure that the timestamp of the new block is greater than the timestamp of the previous block and that the local machine's timestamp is not more than 900 seconds [D95]. When attackers manipulate timestamps, it affects conditions within smart contracts reliant on specific timings [D95, D100]. This can lead to incorrect execution

of contract terms, affecting everything from payment schedules to delivery confirmations within a supply chain, thus reducing operational efficiency and reliability.

- Some smart contracts execute an external call by utilising the “call”, “transfer”, and “send” functions to accomplish the necessary operations. The exception management mechanism of these contracts relies on the execution of callee contracts and the interplay between contracts [D65]. **Mishandling exceptions** can cause transactions to fail unexpectedly, which, in a supply chain context, could halt or delay logistical operations dependent on smart contract executions, leading to inefficiencies and increased operational costs. According to other writers, mishandling an exception potentially led to a DoS attack against smart contracts [D88].
- **DoS with Unexpected Revert** is a problem that arises when a transaction is reverted because of inadequate handling of an unfinished transaction [D88]. This can interrupt the execution of the caller contract and potentially lead to a DoS state in the caller contract [D88]. If smart contracts unexpectedly revert because of unhandled conditions, it can stall all linked transactions. In supply chain scenarios, this could freeze operations requiring contractual execution, such as payments or order processing, severely affecting operational efficiency.
- **Tx.origin** refers to the original sender of a transaction in a blockchain network. Tx.origin is a Solidity global variable that provides the account address that initiated the call or transaction. Utilising the tx.origin variable for authentication exposes the smart contract to the risk of phishing attacks [D100]. When the target submits a transaction to the malicious contract, it will activate the "fallback" function and execute the "withdraw" function of the vulnerable contract, so all the funds will be transferred from another address to itself [D100]. Using Tx.origin for authentication can expose contracts to phishing attacks where attackers can redirect transactions. This could mean unauthorised access to goods or funds redirection in a supply chain, causing security and efficiency concerns.

These vulnerabilities necessitate robust security protocols in smart contract development's design and testing phases to mitigate potential risks in SCM systems.

4.4.3.5 Network-Level Attacks

Despite the decentralised nature, Blockchain networks are vulnerable to various network-level attacks that can impede the availability and integrity. Apostolaki et al. [180], along with Saad,

Spaulding et al. [181], have highlighted the susceptibility of blockchain networks to attacks, some of them highlighted below:

- **Distributed denial of service (DDoS)** attacks exploits the vulnerability of the blockchain network layer, just like any other network infrastructure. These attacks affect the memory pools by overwhelming the network with redundant requests, ultimately slowing the processing of legitimate transactions and resulting in a significant backlog [D47]. This results in increased latency and may lead to network downtime. During such attacks, the system's resources are diverted to manage the flood of data, reducing the network's capacity to process genuine transactions efficiently.
- The Domain Name System (DNS): Peer-to-peer network nodes communicate with other contributors to transmit data through a node discovery protocol. This protocol works based on DNS seed addresses that distribute the addresses of other active nodes on the network [D19]. Researchers explained that the current DNS system is vulnerable to many attacks, such as eclipse attacks, DDOS attacks, cache poisoning attacks, single point of failure, and centralisation [D57]. Current DNS suffer security and privacy issues due to the poor process of node discovery protocol, a weak verification mechanism that leads to a cache poisoning attack, moving ownership and control of the authentication keys to the user's security domain and results in centralised DNS services that can act as a single point of failure, which makes legacy DNS vulnerable to DDoS attacks [D57, D64]. Vulnerabilities within the DNS can lead to misdirection of network traffic, including data and transaction requests. This misrouting can cause delays in the propagation of transaction data across the network, leading to slower confirmation times and an increased likelihood of transaction failures or inconsistencies. [D101].
- In an **eclipse attack**, the perpetrator aims to acquire many IP addresses to gain control over the connections of all legitimate nodes. The adversary node strategically isolates a targeted node and coerces it into doing unauthorised and malicious actions. These involve isolating a node and feeding it false information, effectively deceiving the node about the state of the rest of the network. Attackers commonly employ a botnet to infiltrate and isolate the node [D44]. This isolation can cause the node to work on outdated or incorrect data, wasting computational power and creating inefficient data synchronisation across the network. The target node is situated in an entirely distinct environment from the ongoing network activity.

The success of the attack is dependent upon the exploitation of the victim's adjacent nodes, thus making it highly reliant on the structure of the blockchain network [D53].

- **The Border Gateway Protocol (BGP)** is a routing protocol utilised for the transmission of routing information (IP packets) between autonomous systems (AS) over the internet [D32]. A BGP routing attack, sometimes called BGP hijacks or prefix hijacks, occurs when a malicious AS broadcasts a fraudulent IP, giving attackers a disproportionate influence over the network's consensus mechanism. This can skew the transaction validation process, allowing malicious actors to prioritise fraudulent or obstruct legitimate transactions, decreasing transaction throughput and increasing the time required for consensus. Therefore, the network can be divided into two or more separate components, which manage communication between each element and redirect traffic and blockchain forks into parallel chains [D53, D32].
- A **replay attack** occurs when the blockchain is divided into two separate chains. The attacker impersonates the conversation between two legitimate nodes and obtains the hash key [D100]. The attacker seizes a signed communication and attempts to manipulate data transmission, posing as a legitimate user, to undermine the recipient [D42]. This requires the network to expend additional resources to verify and rectify each transaction, significantly reducing operational efficiency and increasing the workload.

These delay or prevent transaction confirmations, disrupting SCM operations. Each attack disrupts the usual flow of data and consensus across the blockchain network, essential for operational efficiency and trust. Blockchain systems in supply chain management lose throughput, cost, and efficiency due to the computational and administrative overhead of managing and mitigating these interruptions. Thus, network security must be strong to prevent and minimise such assaults.

4.5 Discussion

The initial search findings indicate a substantial quantity of scholarly articles on blockchain, emphasising the rapid progress of this technology and distributed decentralised systems within a mere ten-year span. Although still in its early stages, the field showcases various experimental concepts and conceptual solutions that tackle current difficulties. Nevertheless, much of this

research needs more quantitative data and proof of practical application. A wide range of novel methodologies arise in various research studies within practical technical solutions.

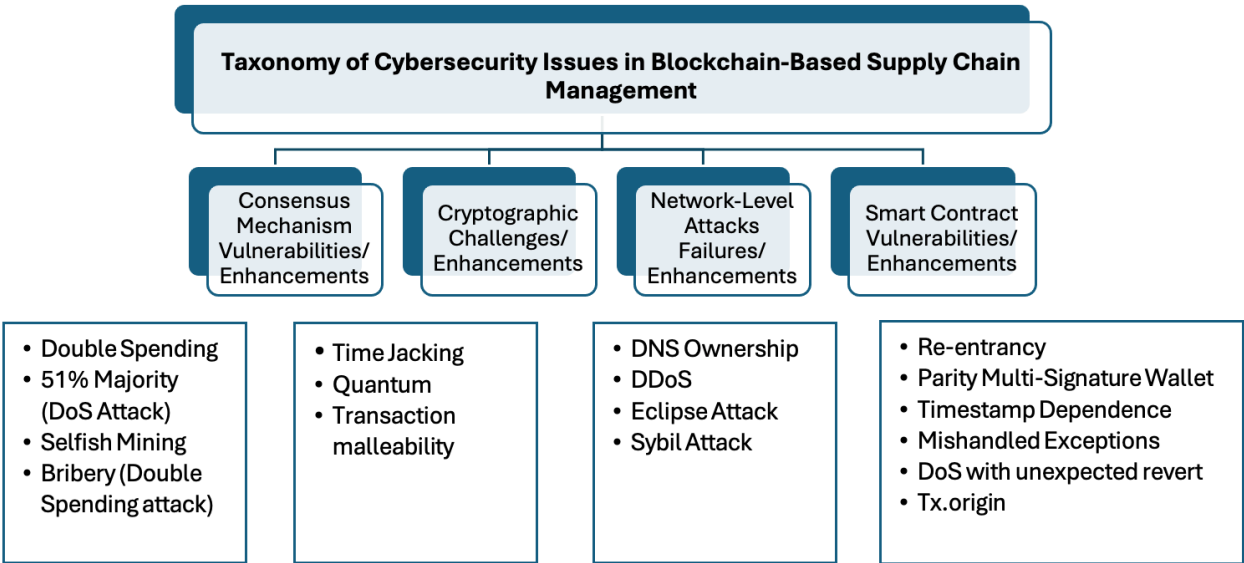


Figure 4.5: Diagram illustrating vulnerabilities that affect SCM-related blockchain systems.

4.5.1.1 Satisfying RQ2

Which aspect of the blockchain plays the most critical role in mitigating cybersecurity vulnerabilities while optimising performance in blockchain-based supply chain management systems?

Figure 4.5 illustrates the taxonomy of various cybersecurity issues that can affect the efficiency of blockchain-based SCM systems. From an efficiency standpoint, the Consensus Mechanism should be prioritised for investigation, as it is the core process that governs how transactions are validated and added to the blockchain. Suppose the consensus mechanism is compromised (through attacks like double spending, 51% majority, or selfish mining). In that case, it leads directly to inefficiencies by increasing the processing time and computational resources required to reach an agreement (consensus) across the network. This reduces overall throughput, making it a critical area for improving efficiency.

Following consensus, Smart Contract vulnerabilities should take the next level of priority. Smart contracts automate key processes in SCM systems, such as payments and product tracking. Still, if they are vulnerable to issues like re-entrancy or mishandled exceptions, they can slow down transaction processing and cause operational bottlenecks, affecting system performance. Network-level attacks should be investigated next because issues like DDoS or Eclipse attacks can isolate

parts of the network or overwhelm nodes, leading to delays in transaction processing and data synchronisation. These attacks degrade the network's performance by affecting communication between nodes, essential for maintaining blockchain functionality. Finally, Cryptographic Challenges like TimeJacking and potential future quantum attacks, though highly impactful, are theoretical or long-term threats that might compromise data security rather than immediately affect system efficiency, i.e., these are important but less urgent from an efficiency improvement perspective in blockchain-based SCM systems.

4.5.2 Consensus Mechanism Failures (Priority Level: High)

Consensus techniques are essential to blockchain transaction integrity. Eyal and Sirer [81], describe how failures or attacks might affect the SCM system. SCM activities require speed and dependability. Therefore, switching to energy-efficient and safe technologies like PoS over PoW improves security and transaction processing [82]. A secure and efficient consensus mechanism keeps SCM processes reliable and unbroken for real-time decision-making and operational continuity. The consensus method underpins blockchain security and efficiency. It validates transactions and maintains network integrity as the initial protection against attackers. Thus, safeguarding the consensus layer can affect SCM system robustness. This region establishes the blockchain's operational integrity, which should be addressed first. Smart contracts and cryptography protect specific transactions or data, but the consensus mechanism affects the entire network. Its efficiency and security affect network security and cryptography.

4.5.3 Smart Contract Vulnerabilities (Priority Level: Medium-High)

Smart contracts are essential for automating SCM procedures [178], [179]; however, these weaknesses pose serious security hazards. Not only does addressing these concerns prevent data breaches and financial losses, but it also ensures that contemporary SCM's automated operations are trustworthy. Smart contract security mitigates errors and delays in automated procedures, making SCM operations more reliable and efficient. After consensus layer security, smart contract vulnerabilities must be addressed. Smart contracts automate SCM processes, making security crucial. These vulnerabilities can impair SCM operations. Consensus processes assure blockchain authenticity, but smart contracts verify individual actions. Though secondary to consensus, the vulnerabilities can affect finances and operations, making this issue a concern.

4.5.4 Network-Level Attacks (Priority Level: Medium)

Apostolaki et al. [180] and Saad et al. [181] explore blockchain networks' attack vulnerability, which affects availability and integrity. Such assaults can interrupt SCM, where data delivery is priority. More robust network security protocols and sophisticated methods like decentralised node distribution can reduce these threats and make SCM systems secure, efficient, and data-tamper-free. Blockchain network availability and integrity depend on network layer security. After consensus methods and smart contracts are secure, attackers may use network flaws, making this issue more significant. Network security strengthens consensus and smart contracts. Although not the initial line of defence, it protects against external attacks, making it an important area to handle after the Consensus and Smart Contract.

4.5.5 Cryptographic Challenges (Priority Level: Medium-Low)

Blockchains depend on cryptography for integrity. Cryptographic approach or implementation defects can cause systemic failures, as by Li et al. [68], Yu et al. [69], and Latifa et al. [177]; cryptographic approaches must evolve to advance blockchain SCM. Promoting cryptographic security protects SCM data and ensures supply chain transaction confidentiality and integrity. Every blockchain operation uses cryptography. Cryptographic issues like quantum computing include more advanced and developing dangers. Cryptographic issues must be addressed for long-term sustainability, but they can be prioritised after more immediate issues. Cryptographic difficulties often demand a long-term strategy for data integrity and security. While damaging, they differ from direct attacks on consensus mechanisms or smart contracts.

4.5.6 Sequential Order of Investigation

- 1st: Consensus Mechanism Failures: Establish a secure and efficient foundation for the blockchain.
- 2nd: Smart Contract Vulnerabilities: Ensure that the crucial automation for SCM is reliable and secure.
- 3rd: Network-Level Attacks: Protect the network infrastructure supporting the blockchain.
- 4th: Cryptographic Challenges: Future-proof the blockchain against emerging and evolving threats.

Addressing these areas in the proposed order ensures a holistic approach to enhancing the security and efficiency of blockchain-based SCM systems. Starting with the consensus mechanism establishes a strong foundation, followed by securing the operational elements (smart contracts),

fortifying the network infrastructure, and finally, focusing on long-term cryptographic sustainability. This sequential approach ensures that each layer of security supports and enhances the next, leading to a robust and efficient SCM system. Addressing these cybersecurity challenges is about fortifying the blockchain against attacks and integrating security measures to improve operational efficiency. Efficient consensus mechanisms, secure and reliable smart contracts, robust network defences, and advanced cryptographic techniques can reduce transaction times, minimise errors and streamline SCM processes. This integration of security and efficiency is vital for SCM systems operating at scale and handling complex, multi-faceted operations.

4.6 Chapter Summary

This chapter carried out a longitudinal systematic literature mapping of peer-reviewed, technology-oriented research to identify and analyse the current knowledge regarding blockchain technology and its cybersecurity challenges in supply chain SCM systems, focusing on consensus mechanism failures, smart contract vulnerabilities, network-level attacks, and cryptographic challenges. The review highlighted the importance of the varying layers of the blockchain architecture in enhancing blockchain efficiency, given the role in managing resolving transactions among nodes. Among the identified vulnerabilities, **the Consensus Mechanism Failures** emerged as the area that should be prioritised for research, as it directly manages the efficiency of the entire blockchain network. Failures within consensus mechanisms significantly affect transaction processing speed, scalability, and overall network performance, making it a key focus for ensuring secure and efficient SCM operations. The systematic literature mapping and analysis of peer-reviewed research emphasised the urgency of addressing consensus-related inefficiencies. As cyberattacks on blockchain systems continue to rise, enhancing these mechanisms is crucial to maintaining security and operational efficiency within SCM networks. This sets the foundation for the following research stage, which seeks to propose novel solutions that enhance consensus mechanisms and address the identified vulnerabilities. The chapter provides a foundation for understanding and managing the intricate relationships between blockchain technology in SCM, cybersecurity, and efficiency, allowing for innovative solutions and system performance. The next chapter will delve deeper into existing consensus mechanisms, investigating the strengths and weaknesses in supply chain management. Using the BlockSim simulation tool, this research will test and compare the performance and efficiency of various consensus mechanisms, ultimately identifying the most suitable and secure options for blockchain-based SCM systems. The simulation results will inform the design of a more secure, efficient consensus model tailored for SCM applications.

5 Traditional Consensus Mechanisms in SCM

5.1 Overview

Chapter 5 focuses on the data collection process and experimental setup for assessing the efficiency of various consensus mechanisms in SCM systems. As blockchain technology continues to be a pivotal tool in optimising supply chains, consensus mechanisms remain the foundation of transaction validation and security. However, challenges like high transaction latency, low throughput, and limited scalability persist due to the inefficiencies in popular consensus mechanisms. To help address these limitations, the chapter evaluates multiple consensus mechanisms, including proof-based methods (PoW, DPoS, PoC), voting-based mechanisms (PBFT, Stellar), and capability-based mechanisms (Pol), with a particular focus on how they support SCM's varying transactional and operational demands. The experimental setup is conducted using the BlockSim simulation framework. BlockSim allows for detailed modelling of blockchain consensus mechanisms, providing insights into performance metrics like throughput, latency, and scalability across small, medium, and large SCM networks. The simulation experiments assess the performance of each consensus mechanism under different conditions, such as transaction volume and network size, which range from small networks of up to 30 nodes to larger systems involving 200 nodes and 50,000 transactions.

The chapter also outlines the parameters configured in BlockSim, including block size, number of nodes, transaction size, and consensus mechanism type. The experiments aim to identify the scalability and efficiency trade-offs associated with each consensus method, with results measured against real-time processing scenarios. Through simulations, Chapter 5 provides valuable data on how these mechanisms perform in blockchain-based SCM systems. It offers an analysis of the throughput, latency, and scalability in varying network sizes and conditions, which determine where in the decision matrix (to come in a subsequent Chapter) will fall.

5.2 Introduction

Chapter 4 discussed consensus mechanisms as the basis for information validation, reliability and efficiency in the blockchain space [73]. However, Zheng et al. [182] highlighted that the technology still faces limitations such as low transactions per second (TPS), high transaction latency, and

issues with decentralisation because of inefficient consensus mechanisms. For example, inefficient consensus mechanisms like the Proof-of-Work (PoW) mechanisms stem from an energy-intensive and time-consuming consensus process [183]. Introducing the Practical Byzantine Fault Tolerance (PBFT) eliminates the POW mechanism's performance barrier, increasing throughput and lowering latency. However, PBFT's high communication complexity and limited scalability still plague the PBFT mechanism [184]. As modern SCM software seeks to incorporate industry best practices and technology to optimise delivery [44], they require adaptable and coherent communication techniques to prevent things like BWE as supply chains scale. Therefore, consensus mechanisms used in SCM must improve, from throughput to latency and scalability, to handle big or complicated high-efficiency needs. Chapter 3, section 3.3 mentions that supply chain manufacturers can choose a consensus mechanism for small, medium, and large SCM systems based on throughput, latency, and scalability. This research will focus on small SCM systems with up to 30 nodes and 1-1000 transactions. Fast processing is needed, but minor delays are acceptable. Medium SCM systems (30-100 nodes, 1000-10000 transactions) require a balance between throughput and latency. Large SCM systems with 100-200 nodes and 10,000-50,000 transactions need high throughput and low latency to scale efficiently and effectively.

Operational choices in consensus mechanisms supporting large SC must balance transaction speed, security and scalability depending on the blockchain's application needs. Supply chains might favour the efficiency of voting-based mechanisms to handle large volumes of transactions swiftly, whereas systems managing high-value transactions might prioritise the robust security offered by proof-based mechanisms despite higher costs and energy demands. To ensure the strength of blockchain-based supply chain operations, it is crucial to analyse different consensus mechanisms from a security and performance standpoint [21]. In addition to this, enhancing transaction efficiency is essential for achieving a competitive advantage in SCM, so guidance in selecting an optimal consensus mechanism that facilitates efficiency in a large supply chain is needed [185]. Owing to the intrinsically scalable characteristics of supply chain ecosystems, a selected consensus mechanism must be capable of accommodating growth while maintaining the integrity of security and efficiency [63]. Zheng et al. [182] emphasise that there are inherent trade-offs to using different consensus approaches from a throughput and transaction latency perspective.

5.3 Experimental Set-up

To collect “efficiency data” from consensus mechanisms used in SCM, BlockSim simulator was executed with Python 3.9 in Visual Studio Code on a MacBook Pro Machine with an Intel Core i7 CPU at 2.21 GHz and 16GB of RAM. This thesis designs and implements simulation experiments to evaluate SCM-based consensus mechanisms, including proof-based mechanisms (PoW, Delegated Proof of Stake (DPoS), Proof of Capacity (PoC)), capability-based mechanisms (PoI), and voting-based mechanisms (PBFT, Stellar), within the blockchain simulator. The result from the simulator is used to evaluate efficiency and security characteristics. To assess the efficiency and security, parameters including the transaction speed (latency and throughput), system scalability, and tamper resistance are collected for each mechanism over different real-time processing scenarios.

5.3.1 BlockSim

BlockSim is an open-source simulation framework initially developed by Faria and Correia [186] and further expanded by Alharby and van Moorsel [187] to facilitate blockchain network research. BlockSim can simulate supply chain networks by modelling the components of a blockchain-based supply chain, such as transactions, nodes, and consensus mechanisms. Since BlockSim is a discrete-event simulation tool, it allows for creating a dynamic and detailed model of a blockchain system that can capture the flow of transactions across different nodes within the supply chain. Users can simulate how different consensus mechanisms impact the performance of the supply chain network in terms of throughput, latency, and scalability. Additionally, it enables the modelling of various network conditions, transaction validation, and block propagation, making it a valuable tool for studying the effectiveness of blockchain in enhancing transparency, security, and traceability in supply chain systems. BlockSim was chosen above other simulation tools because it is extensible and easy to customise for different blockchain systems. Adjusting the modular components lets users mimic blockchain protocols for consensus mechanism research. BlockSim hides needless complexity and provides straightforward simulation instructions, making it easier for researchers to use without understanding the system design. Python, which researchers are familiar with, makes the simulator straightforward to modify, integrate, and experiment with. The original frameworks simulate the peer-to-peer network of a public blockchain, including Bitcoin (PoW consensus), Ethereum (DPoS consensus) and an appendable module for other consensus, which consists of thousands of nodes to simulate additional mechanisms. As seen in Figure 5.1, the core of BlockSim is a Base Model, which contains several functional blocks (e.g., blocks, transactions

and nodes) common across blockchains that can be extended and configured as suited for the system and study of interest.

```

1
2 class InputsConfig:
3
4     """ Select the model to be simulated.
5     0 : The base model
6     1 : Bitcoin model
7     2 : Ethereum model
8     3 : AppendableBlock model
9     """
10    model = 2
11
12    ''' Input configurations for the base model '''
13    if model == 0:
14
15    ''' Block Parameters '''

```

FIGURE 5.1: illustrating Blockchain Consensus Mechanisms model selection in BlockSim [47].

Other developers, such as Basile et al. [188], enhanced the tool to simulate different types of consensus mechanisms. This is done by changing block generation-related parameters to allow other mechanisms to be simulated. The enhancement is designed as an event-driven simulator, wherein each participating node behaves according to generated events, e.g., block generation and message exchange, as shown in Figure 5.2.

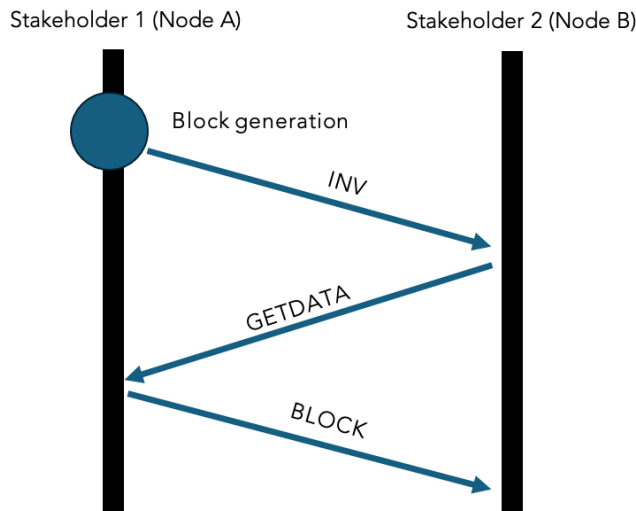


FIGURE 5.2: illustrating the propagation protocol between two nodes (stakeholders)

Key configurable parameters include:

- **Block size (MB):** The maximum amount of data that can be included in a block. Larger block sizes can accommodate more transactions but may increase the time needed for block propagation.

- **Number of nodes (Count):** Representing The number of participants or validators in the blockchain network
- **Rate (Tx):** The number of transactions in each block propagation
- **Transaction Size (MB):** The size of each transaction. Larger transaction sizes may limit the number of transactions per block, impacting throughput.
- **Consensus Mechanism:** The protocol used to validate transactions, such as PoW, DPoS, or PBFT. Different consensus mechanisms affect performance in terms of throughput and scalability.

The default block settings are generated using probability in assuming PoW and propagated along the simulated blockchain network. To evaluate whether BlockSim appropriately simulates blockchain networks, developers such as (Alharby and van Moorsel [187] & Basile et al. [188]) compared BlockSim's simulated environments with actual environments regarding public blockchain networks. Specifically, they compared the median number of block propagation times and the ratio of fork occurrences. BlockSim, metrics can be adjusted from Simulation settings and Node Parameters.

```

86
87
88     ''' Node Parameters '''
89     Nn = 8912 # the total number of nodes in the network
90     NODES = []
91     from Models.Bitcoin.Node import Node
92     # We define network nodes by assigning to each node: i)a unique id; ii)the hash (computing) power; and iii)a boolean value specifying wheth
93     NODES = [Node(id=0, hashPower=0, isSegwitNode=False), Node(id=1, hashPower=0, isSegwitNode=False), Node(id=2, hashPower=0, isSegwitNode=Fal
94
95     ''' Simulation Parameters '''
96     simTime = 86400 # the simulation length (in seconds)
97     Runs = 1 # Number of simulation runs
98
99     ''' Input configurations for Ethereum model '''
100    if model == 2:
101
102        ''' Simulation Parameters '''
103        sim_params = {
104            'nodes': 4,
105            'workers': 1,
106            'rate': 50_000,
107            'tx_size': 512,
108            'faults': 0,
109            'duration': 300,
110            'mem_profiling': False
111        }
112        simTime = 500 # the simulation length (in seconds)
113        Runs = 2 # Number of simulation runs
114
115    ''' Block Parameters '''
116    Binterval = 12.42 # Average time (in seconds)for creating a block in the blockchain
117    Bsize = 1.0 # The block size in MB
118    Blimit = 8000000 # The block gas limit
119    Bdelay = 6 # average block propogation delay in seconds, #Ref: https://bitslog.wordpress.com/2016/04/28/uncle-mining-an-ethereum-consensus-
120    Breward = 2 # Reward for mining a block

```

FIGURE 5.3: Figure illustrating simulation parameters in BlockSim

In Figure 5.3, the metrics specify the number of stakeholders (nodes) and workers per stakeholder (workers) to deploy, the input (transactions) at which the initiator stakeholder submits transactions to the system (input) with the size of each transaction in bytes (tx_size), the number of faulty nodes in the case of PBFT consensus (faults), and the duration of the simulation run in seconds (simTime). The minimum transaction size is 9 bytes; this ensures the transactions of a stakeholder

are all different. The configuration script deploys as many stakeholders as workers and divides the input rate equally amongst each stakeholder. For instance, in Fig. 5.3, when configuring the testbed with two hundred nodes, five workers per node, and an input of 10,000 tx, the scripts deploy five worker stakeholders, each submitting transactions to two hundred nodes at a rate of 10,000 tx. When the parameter faults are set to $f > 0$ for PBFT, the last f nodes and stakeholders are not booted; the system will thus run with $n-f$ nodes (and $n-f$ stakeholders).

Fig. 5.4 illustrates how nodes are configured to handle transactions and create blocks based on various parameters within the blockchain simulation environment. The Node Parameter's class code configures a blockchain node's performance characteristics, including latency, transaction generation, roles (Stakeholder, Worker), and the handling of transaction requests and conflicts, helping to simulate a blockchain network for benchmarking or testing purposes.

```

167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199

Ttechnique = "Full"

''' Node Parameters '''
node_params = {
    header_size = 1_000, # The preferred header size.
    max_header_delay = '100ms', # The maximum delay that the Stakeholder waits between generating two headers, even if the header did not reach
    gc_depth = 50, # The depth of the garbage collection. Denominated in number of rounds
    sync_retry_delay = '10000ms', # The delay after which the synchronizer retries to send sync requests. Denominated in ms
    sync_retry_nodes = 3, # How many nodes to sync when re-trying to send sync-request. These nodes are picked at random from the committee.
    batch_size = 500_000, # The preferred batch size. The workers seal a batch of transactions when it reaches this size.
    max_batch_delay = '100ms', # The delay after which the workers seal a batch of transactions
}
block_synchronize = {
    range_synchronize_timeout = '30s', #The timeout configuration when synchronizing a range of certificates from peers
    certificates_synchronize_timeout = '30s', #The timeout configuration when requesting certificates from peers
    payload_synchronize_timeout = '30s', # Timeout when has requested the payload for a certificate and is waiting to receive them
    payload_availability_timeout = '30s', # The timeout configuration when for when we ask the other peers to discover who has the payload
    handler_certificate_deliver_timeout = '30s'
},
consensus_api_grpc = {
    socket_addr = "/ip4/127.0.0.1/tcp/0/http",
    get_collections_timeout = "5_000ms", # The timeout configuration when requesting batches from workers
    remove_collections_timeout = "5_000ms" #The timeout configuration when removing batches from workers
},
max_concurrent_requests = 500_000 #The maximum number of concurrent requests for Stakeholder-to-Stakeholder and worker-to-worker messages.

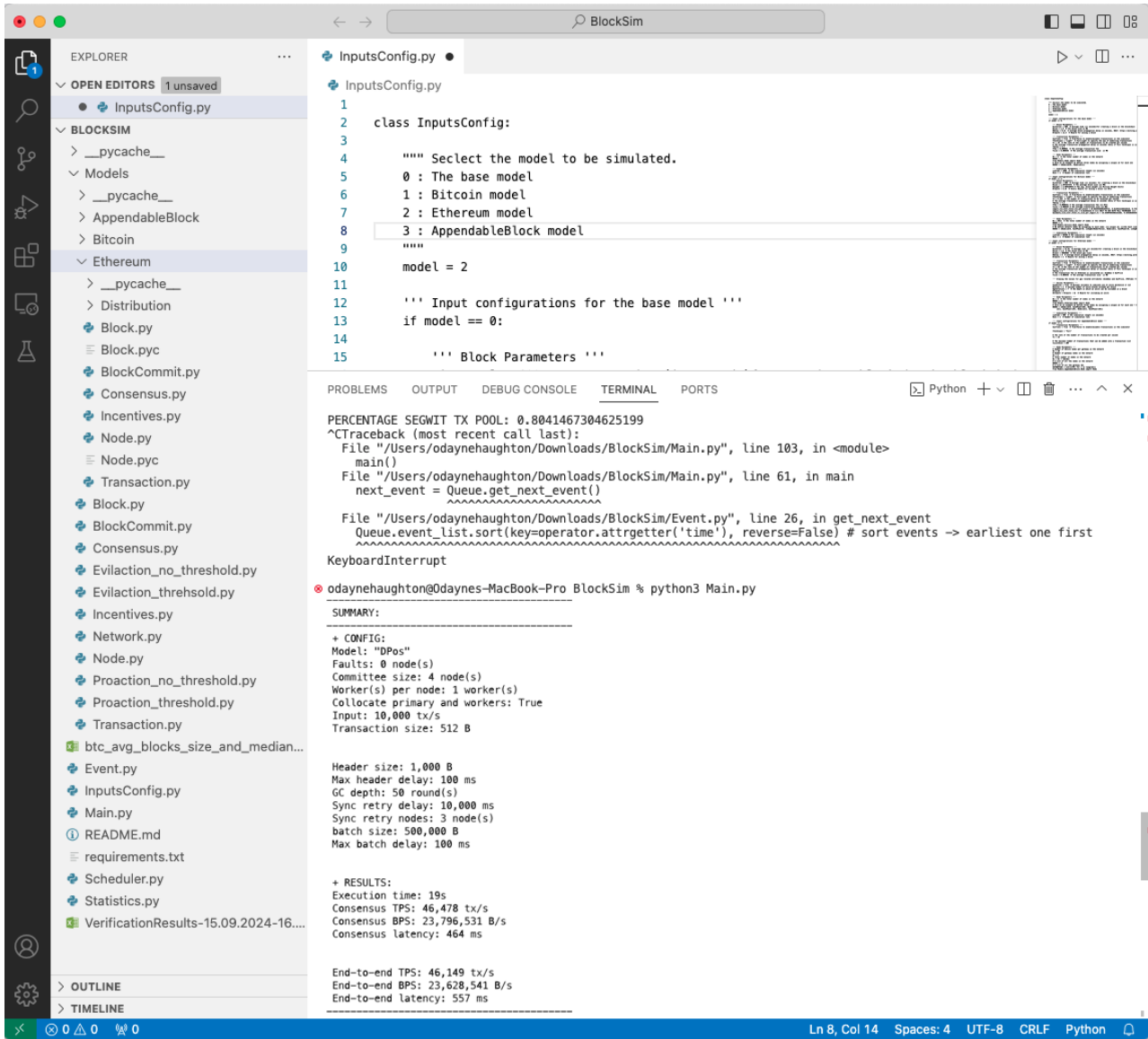
# The rate of the number of transactions to be created per second
Tn = 10

# The maximum number of transactions that can be added into a transaction list
txListSize = 100

```

Figure 5.4: illustrating the node input parameters to configure stakeholders and workers in BlockSim.

5.3.2 Performance Metrics



```
1
2 class InputsConfig:
3
4     """ Select the model to be simulated.
5     0 : The base model
6     1 : Bitcoin model
7     2 : Ethereum model
8     3 : AppendableBlock model
9     """
10    model = 2
11
12    ''' Input configurations for the base model '''
13    if model == 0:
14
15        ''' Block Parameters '''
```

```
PERCENTAGE SEGWIT TX POOL: 0.8041467304625199
^CTraceback (most recent call last):
  File "/Users/odaynehaughton/Downloads/BlockSim/Main.py", line 103, in <module>
    main()
  File "/Users/odaynehaughton/Downloads/BlockSim/Main.py", line 61, in main
    next_event = Queue.get_next_event()
                 ~~~~~
  File "/Users/odaynehaughton/Downloads/BlockSim/Event.py", line 26, in get_next_event
    Queue.event_list.sort(key=operator.attrgetter('time'), reverse=False) # sort events -> earliest one first
KeyboardInterrupt

odaynehaughton@Odaynes-MacBook-Pro BlockSim % python3 Main.py

SUMMARY:
-----
+ CONFIG:
Model: "DPos"
Faults: 0 node(s)
Committee size: 4 node(s)
Worker(s) per node: 1 worker(s)
Collocate primary and workers: True
Input: 10,000 tx/s
Transaction size: 512 B

Header size: 1,000 B
Max header delay: 100 ms
GC depth: 50 round(s)
Sync retry delay: 10,000 ms
Sync retry nodes: 3 node(s)
batch size: 500,000 B
Max batch delay: 100 ms

+ RESULTS:
Execution time: 19s
Consensus TPS: 46,478 tx/s
Consensus BPS: 23,796,531 B/s
Consensus latency: 464 ms

End-to-end TPS: 46,149 tx/s
End-to-end BPS: 23,628,541 B/s
End-to-end latency: 557 ms
```

FIGURE 5.5: illustrating BlockSim Simulation run result: executing the DPos Consensus with 10 nodes for 10,000 transactions.

5.3.2.1 Throughput

Throughput is measured by the total number of transactions processed within a predetermined period in seconds, i.e. the transactions per second (TPS). TPS is an essential measure of the operational efficiency of a blockchain network as the metric functions as both an assessment of the blockchain's present computing capabilities (i.e. how efficient the consensus mechanism is) and as a predicted gauge of its future scalability.

$$\text{Throughput (TPS)} = \frac{\text{Number of transactions processed}}{\text{Total time taken (seconds)}} \quad (5.1)$$

Examining TPS across different consensus mechanisms used in SCM helps formulate the decision tree matrix on the resilience and effectiveness of the investigated consensus mechanisms. Starting from the blockchain's initiation time, throughput provides the system's processing capacity to be assessed and evaluated for blockchain-based SCM system's efficiency. This is important for blockchain supply chains where increasing numbers of transactions (from orders, shipments, and communications among suppliers, distributors, and retailers) must be processed swiftly to maintain operational efficiency. Simulating environments with different numbers of transactions (as shown in Fig 5.5) helps determine when the network is experiencing bottlenecks. High throughput results suggest that the blockchain can scale up to handle high transaction volumes of up to about 50,000 without degradation in performance. This is a critical aspect of expansive supply chain networks, which might involve thousands of transactions simultaneously.

5.3.2.2 Latency

Consensus latency, sometimes called block time or block delay, is the amount of time it takes for a transaction to be approved and recorded on the blockchain. The metric is calculated by comparing the time transactions taken from when they are submitted to when they are validated and stored using the time stamps.

$$\text{Latency (seconds)} = \text{Time for block confirmation (seconds)} \quad (5.2)$$

In BlockSim, latency can be observed by measuring the time difference between the initiation and final confirmation of transactions across different node parameters. Lower latency under heavy transaction loads indicates a robust consensus mechanism and network architecture that can handle rapid scaling. This is important for supply chains, particularly in time-sensitive environments where delays in transaction confirmations could lead to disruptions in logistical operations or inventory management.

5.3.2.3 Scalability

Scalability evaluates how well the consensus mechanisms maintain a high rate of confirmed transactions as the network grows.

$$\text{Scalability} \propto \frac{\text{Throughput}}{\text{Latency}} \quad (5.3)$$

This formula expresses that scalability improves as throughput increases and/or latency decreases. In practical terms, scalability is essential for SCM systems anticipating high transaction volumes. The ability to process numerous transactions rapidly is a benchmark of efficiency.

5.3.3 Simulation Parameters

Section 5.2 mentioned data being collated across all three SCM consensus categories (proof-based, capability-based and voting-based procedures), namely; PoW, DPoS, PoC, PoI, PBFT, SCP, and RCPA. Scalability and operational efficiency were measured by eight throughput simulations for different transaction amounts. The reason for conducting eight throughput simulations across different transaction amounts and network sizes is to ensure comprehensive coverage of how each consensus mechanism manage different workloads (small, medium and large). Running multiple simulations over these different network sizes ensures that the mechanisms can be assessed for the peak performance and how they handle smaller or intermediary transaction loads, making the findings more robust and applicable to different network settings. Table 5.1 shows block input parameters for each consensus technique at 1, 50, 100, 500, 1000, 5000, 10000, and 50000 transactions at various network sizes (10, 15, 30, 50, 80, 120 and 200) nodes. Simulations of the seven consensus mechanisms show the efficiency, scalability, and applicability as workloads increase (as they would in real-world blockchain-based SCMs). The simulations examined each mechanism’s performance parameters scaled with load to assess the mechanism’s real-world applicability.

TABLE: 5.1: BlockSim Simulation input parameters and descriptions executed.

| Parameter | Description | Value |
|--------------------------------|--|---|
| Consensus Mechanism | <i>The consensus module being simulated</i> | {PoW, DPoS, PoC, PoI, PBFT and SCP} |
| Number of transactions (input) | <i>The number of transactions in a block</i> | {1, 10, 50, 100, 500, 1000, 5000, 10000, 50000} transitions |
| Workers | <i>Minimum number of nodes that try to help transactions reach consensus</i> | 5 |
| Stakeholder Nodes (input) | <i>the network size</i> | {10, 15, 30, 50, 80, 120, 200} nodes |
| Tx Size | <i>the size of each transaction in bytes</i> | 512 MB |
| Faults | <i>the number of faulty nodes</i> | 0 |
| Mem_profiling | <i>optimise memory allocation</i> | False |
| simTime | <i>maximum time the simulation will run for before timing out</i> | 1500 sec |
| Runs | <i>TryCatch: simulation will try to run “x” times if it fails</i> | 2 |

5.4 Simulation Results

Data from traditional consensus mechanisms, PoW, DPoS, PoC, Pol, PBFT and SCP, have been compiled across all three consensus categories (proof capability and voting-based mechanisms) utilised for SCM, as outlined in Section 5.1.1. These assessed the efficiency of consensus protocols by:

- (i) increasing the network size,
- (ii) increasing the transaction size, and
- (iii) constraining the transaction simulation duration.

The maximum limit for the network size at 200 nodes was established, the upper limit for the number of transactions at 50,000 transactions, and the simulation duration at 1500 seconds, as this will provide a comprehensive assessment of the blockchain’s scalability and performance under high-load conditions, ensuring that the simulation reflects real-world demands and stress tests the system's efficiency and security. Each transaction was considered as a distinct block to maintain simplicity and generality. The transaction throughput was assessed for each mechanism by counting the number of transactions handled before the completion of the simulated period. Figures 5.6 (a,b)- 5.12 (a,b) show the outcomes derived from the experiments. To mimic real-world activity as much as possible, as outlined in Section 3.3, one hundred twenty-eight simulation run was done to assess throughput and latency across different transaction volumes and nodes, evaluating operational efficiency.

PoW:

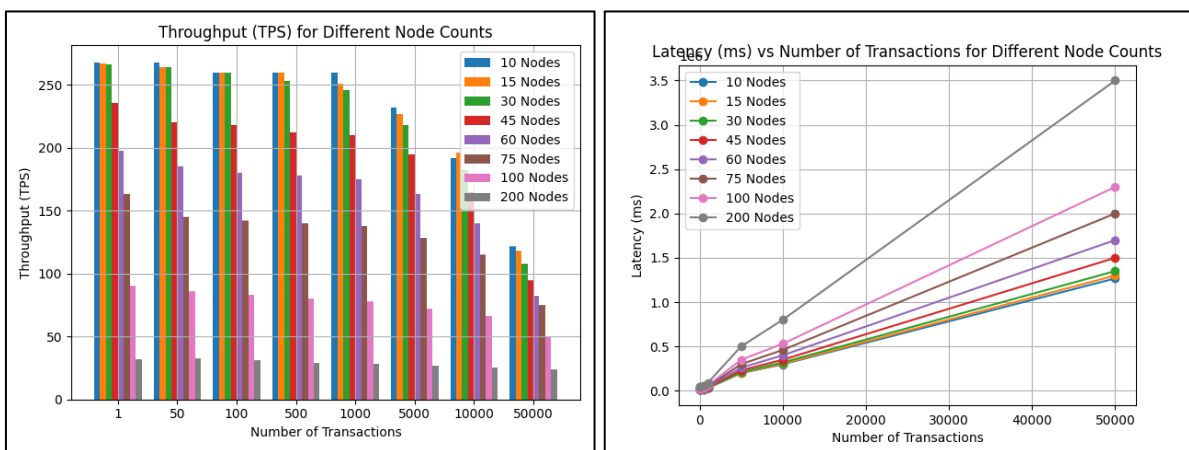


FIGURE 5.6 (a, b): Figures illustrating PoW consensus throughput and latency simulation results over several nodes and transactions.

DPoS:

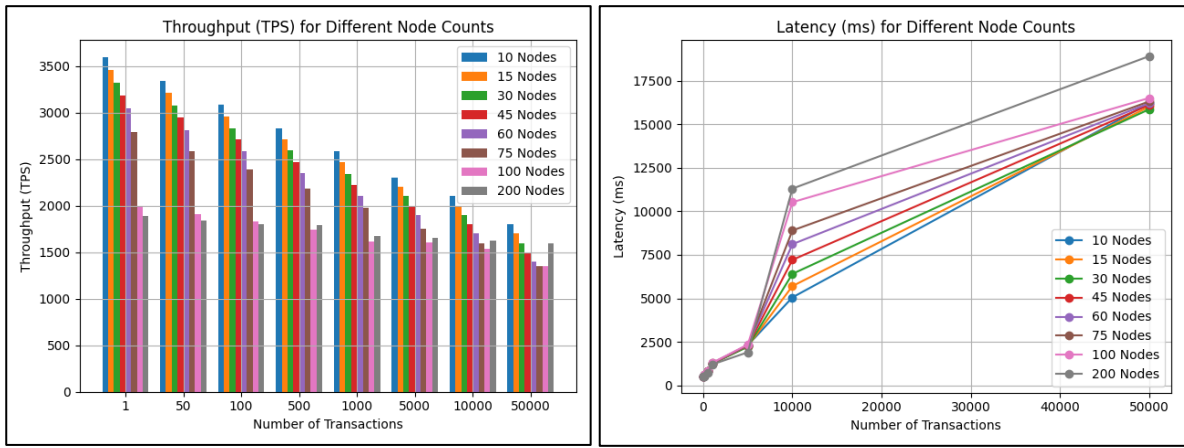


FIGURE 5.8 (a, b): Figures illustrating the throughput and latency simulation results for the DPoS consensus over multiple nodes and transactions.

PBFT:

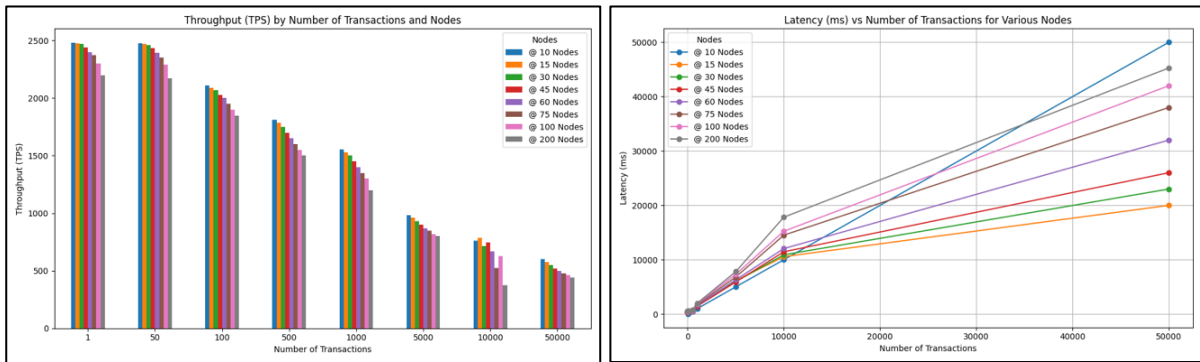


FIGURE 5.9 (a, b): Figures illustrating the throughput and latency simulation results for the PBFT consensus over multiple nodes and transactions.

Stellar:

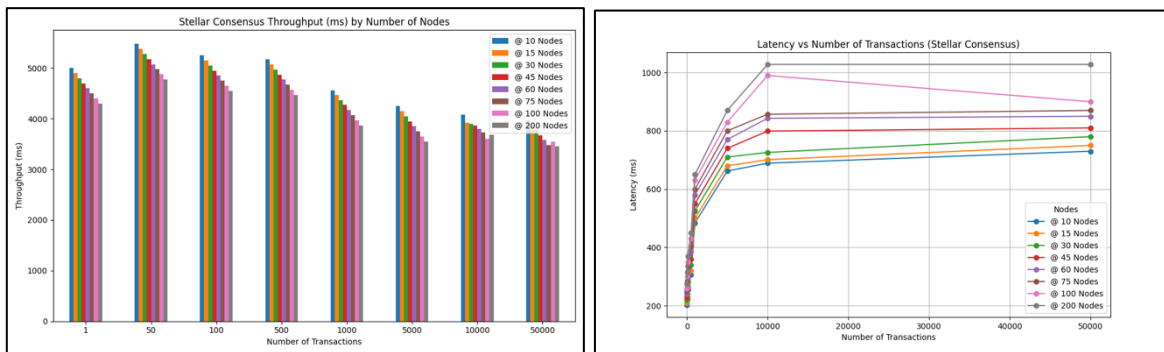


FIGURE 5.10 (a, b): Figures illustrating the throughput and latency simulation results for the Stellar consensus over multiple nodes and transactions.

Pol:

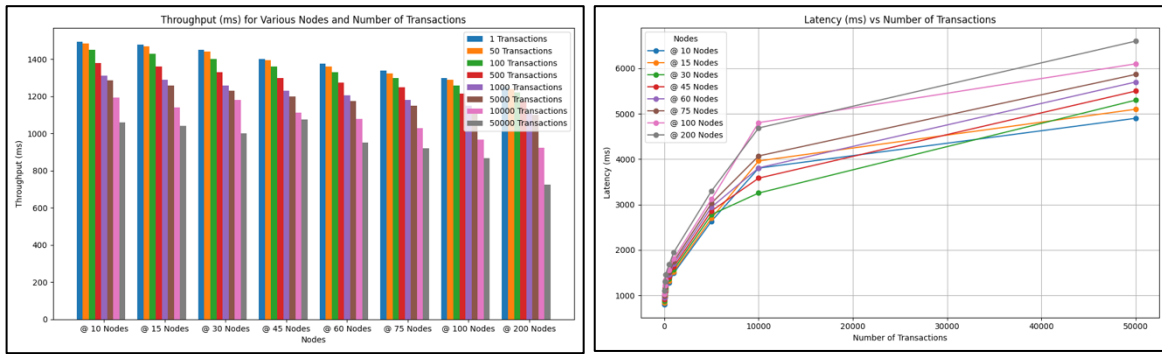


FIGURE 5.11 (a, b): Figures illustrating the throughput and latency simulation results for the Pol consensus over multiple nodes and transactions.

PoC:

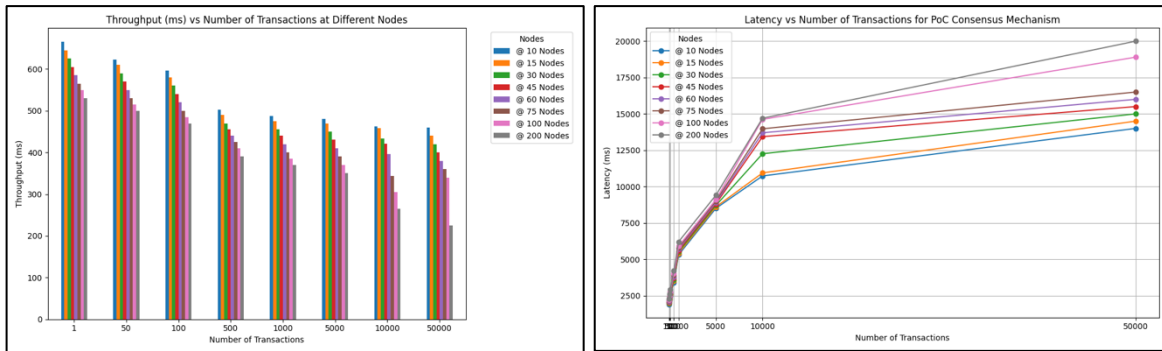


FIGURE 5.12 (a, b): Figures illustrating the throughput and latency simulation results for the PoC consensus over multiple nodes and transactions.

5.5 Results Analysis

5.5.1 PoW Consensus Mechanism

In a PoW system, throughput is limited by:

- Block size: The maximum number of transactions that can be included in a block.
- Block time: The average time it takes to mine a new block.

Fig. 5.7a shows that adding more nodes to the network does not directly increase throughput. This is because the block size and time stay the same during the simulation even though the number of nodes changes. Figure 5.7b shows the increase in transmission times as nodes increased. This is because, in PoW, every new block that is mined needs to be sent to all the other nodes for verification. As illustrated in 5.7b, this process takes longer time in larger networks (with more nodes) because blocks have more Nodes to go through, which also increases the delay.

5.5.2 DPoS Consensus Mechanism

DPoS, a modification of the Proof of Stake (PoS) mechanism, is a consensus method that makes transaction processing and block generation faster than PoW and PoS. In DPoS, people who own tokens choose a small group of stakeholders (witnesses) who will verify transactions and add new blocks to the blockchain [189]. DPoS reduces the number of people involved in creating blocks compared to PoW. This results in lower latency and higher throughput, as figures 5.8a and 5.8b show that there is a direct correlation between network size and efficiency data. As the network size increase throughput decreases by approximately 8.38% and latency increases by approximately 80.98%. DPoS can handle more data than PoW and the traditional PoS systems because:

- DPoS do not need as many people to validate blocks, therefore making blocks faster with less communication overhead.
- Most DPoS systems make blocks every few milliseconds, which increases throughput. However, as transactions increase, the system gets backed up and slows down, potentially creating a bottleneck.

5.5.3 PBFT Consensus Mechanism

PBFT is a consensus mechanism designed to handle Byzantine failures (where nodes can fail or behave maliciously, and the system still works normally in distributed systems. The mechanism confirms consensus among nodes through a series of message exchanges; unlike PoW or DPoS, PBFT is a leader-based consensus mechanism, where one node proposes a block, and others (called replicas) validate the block through a voting process [190]. The PBFT protocol can tolerate up to f faulty nodes in a network of $3f + 1$ total node. PBFT is particularly used for private and consortium blockchains, where nodes are known and trusted, and the consensus process optimises high throughput and low latency under certain conditions, such as networks with relatively low node counts and where trust assumptions are established, making it ideal for environments that require fast finality, like financial systems, supply chain management, or permissioned enterprise blockchains. However, the simulation results in Fig. 5.9(a,b) shows the performance of PBFT degrades as the number of nodes or transactions increases. This is due to communication overhead. PBFT requires multiple sets of communication (prepare, pre-prepare, and commit) between all nodes, which means that as the number of transactions and nodes increases, the communication overhead expands, as shown in figure 5.9(a,b) the throughput decreases at a rate of up to approximately 18.90% and the latency at a rate of 105.81%. Increasing network size and

transactions cause the system to experience significant slowdowns and decreased efficiency in environments with high transaction volumes and larger networks. The communication overhead becomes a limiting factor for scalability in high-demand, larger network deployments and similar outcome would occur if applied to supply chain management systems.

PBFT improve throughput over the previous approaches by batching transactions into blocks [190]. However, as illustrated in Figure 5.9(a,b), the consensus overhead eventually limits the system's ability to execute more transactions. This is why throughput increased slightly by 0.2% between 1 and 50 transactions but decreased when the network reached 100 transactions. As more transactions are added to PBFT, each transaction takes many communication sets between nodes, increasing latency. When there are fewer nodes (10-15), the network quickly reaches consensus (3 ms), leading to higher throughput and lower latency. As the number of nodes increases, latency increases due to the need for more communication and coordination between nodes. Similar occurrences would be experienced if applied to a blockchain-based SCM system.

5.5.4 Stellar Consensus Mechanism

The Stellar Consensus Protocol (SCP), being a federated Byzantine agreement (FBA) mechanism, is an ideal consensus method for scalable decentralized networks, particularly in SCM. Unlike PBFT, SCP does not rely on mining or a central group of validators but instead uses a flexible voting process where nodes select trusted peers (quorum slices). This structure is highly beneficial for SCM, where transparency, speed, and security are priority. In the context of SCM, SCP ensures fast processing of transactions such as tracking goods, verifying deliveries, and processing payments. The simulations show that SCP's communication efficiency allows for excellent throughput, especially in smaller networks, which is essential for smaller supply chains. As the network grows, throughput decreases marginally but remains highly efficient, unlike in PBFT, making it a scalable option for larger, more complex supply chains.

The protocol's flexibility also allows SCP nodes to communicate only with the quorum slices rather than every node in the network, significantly reducing communication overhead. This is crucial in supply chains where rapid decision-making and trust are necessary to keep operations running smoothly. For large SCM systems, the scalability of SCP, where throughput decreases by only 4.62% and latency by 20.90%, ensures that even with increased complexity and node count, the system

maintains a high performance. This makes SCP particularly suitable for supply chains with high throughput and low latency demands, ensuring operational efficiency and trust within the network.

5.5.4.1 PoI Consensus Mechanism

The PoI consensus mechanism enhances the PoS mechanism. Still, it is designed to reward active network participants based on the contribution and activity rather than wealth (in PoS) or computational power (like PoW). PoI assigns an “importance score” to each node based on factors like (i) the number of tokens held, (ii) the number and frequency of transactions and the node’s network activity and contribution [191]. As shown in Figure 5.11(a,b), similarly to the previously discussed consensus mechanisms, PoI’s throughput declines as more nodes participate in the consensus process due to the added complexity and communication overhead. The latency also increases as the number of nodes and transactions grows, reflecting the additional communication and consensus overhead. Notably, with higher transactions (of up to approximately 50000), the throughput decreases at a rate of about 5.15%, and the latency increases at a rate of about 30.85%, illustrating that the mechanism does not scale well, as seen in the figure 5.22 (a,b).

5.5.4.2 PoC Consensus Mechanism

To reach consensus, the PoC consensus mechanism employs disc space instead of processing power (like PoW) or token ownership (like PoS and PoI). Miners allocate storage by “plotting” pre-computed hashes in PoC. More storage means a miner’s chances of adding a block to the network increase. This approach improves the PoW mechanism and is more efficient because miners store cryptographic puzzle solutions (nonces) in advance when plotting [192]. This innovation requires miners to search the precomputed plots for the nearest challenge answer, with the best solution getting the block reward. The simulations show that PoC throughput decreases as nodes and transactions increase because miners must scan the storage to locate the best solution, potentially generating bottlenecks and delays, as shown in Fig. 5.12a,b. As nodes and transactions increase, network latency also increases due to the requirement for additional communication between nodes and the time needed to search stored graphs, which potentially delay consensus.

5.6 Chapter Summary

From an efficiency perspective, increasing throughput while preserving low latency generally enhances the efficacy and scalability of blockchain-based systems. Nonetheless, attempts to improve throughput in current consensus processes frequently result in increased latency, reducing

overall scalability. Numerous blockchain scaling solutions seek to enhance throughput while maintaining latency, thus assuring optimal system performance. This thesis utilised BlockSim to simulate and study the efficiency metrics of several consensus techniques to evaluate the effectiveness across different circumstances. Efficiency is assessed against throughput, latency, and scalability, with the scalability of a blockchain system being key factor for accommodating the intricate, dynamic, and frequently geographically dispersed components of contemporary supply chains. Consensus mechanisms characterised by high throughput, low latency, and robust scalability guarantee that as the supply chain expands and transaction volumes rise, the blockchain system can uphold its integrity and service standards, ensuring uninterrupted supply chain operations. This chapter assessed the efficacy of current blockchain-based supply chain management consensus mechanisms utilise six protocols: PoW, DPoS, PBFT, Stellar, Pol, and PoC. A testbed experiment was setup in BlockSim using blockchain network of 200 nodes, and the consensus protocols for each system were executed. The efficacy of each methodology utilising identical transaction volumes and network dimensions was also assessed.

Based on simulation results, each consensus mechanism has varied strengths and limitations in handling throughput and latency as nodes and transactions expand. Due to its cryptographic puzzle-solving, PoW has high latency and low throughput, especially as network traffic increases. DPoS reduces the number of participants needed to validate blocks, improving throughput and latency, but congestion persists as transactions increase. While capable of handling Byzantine failures, PBFT degrades with additional nodes and transactions owing to communication costs, as multiple messaging sets cause delays. Stellar operated better than PBFT by limiting communication to trusted nodes and maintaining good throughput as the number of nodes increased. Complex quorum management reduces throughput at higher scales. Pol determines node importance with rising delay, and PoC has storage scanning bottlenecks. As technology improves and changes, these mechanisms must evolve to keep up with industry demands. Stellar's design shows promise in retaining efficiency with an extensive network. However, the mechanism is prone to manipulation and bias in an SCM system because the nodes choose a set of trusted peers with mutual relationships to reach consensus, making the consensus process exclusive. Therefore, the PoEf is being introduced in the next chapter. The PoEf uses a reputation-based selection protocol to improve the potential bias gap and a sharding method that increases scalability and reduces latency even in high-transaction volumes and many nodes. PoEf manages node participation and workload distribution more efficiently than existing techniques, which is suitable for blockchain-based supply chains of any size.

6 Novel PoEf, an enhanced Consensus for SCM

6.1 Overview

Chapter 6 introduces a novel consensus mechanism, Proof of Efficiency (PoEf), specifically designed to address the limitations of existing blockchain consensus mechanisms, particularly Practical Byzantine Fault Tolerance (PBFT), in Supply Chain Management (SCM) environments. PoEf leverages multilevel sharding techniques and a reputation-based node selection system to improve throughput, scalability, and security, overcoming the communication overhead and scalability issues present in PBFT. The chapter starts by exploring the background and context of PoEf, discussing how it evolved from PBFT to meet the efficiency needs of modern SCM systems. Unlike PBFT, which struggles with high transaction volumes and large networks, PoEf optimises the consensus process by selecting a subset of nodes based on the reputation to reach consensus more quickly and securely. It also divides the network workload into smaller shards, allowing parallel processing of transactions and improving throughput and latency. This makes PoEf suited for large-scale SCM networks that require rapid transaction processing and real-time data validation.

The core innovation of PoEf lies in its hybrid node structure, where nodes are categorised into different tiers (authentication nodes, validator nodes, and subordinate nodes). This hierarchical approach reduces the communication burden on the network and ensures that only trusted nodes participate in the consensus process. By introducing a reputation-based scoring system, PoEf rewards trustworthy nodes with greater decision-making authority, enhancing the network's security and reliability. The chapter also details PoEf's operational phases, including the node selection process, sharding, and the consensus-reaching mechanism. PoEf's design includes advanced features like its Authorisation Network, which verifies supply chain participants before allowing them to join the network, and its Stakeholder Network, where validated transactions are processed. This layered approach ensures both operational efficiency and robust security in SCM systems. In summary, Chapter 6 positions PoEf as a scalable and efficient consensus mechanism designed to meet the high transaction volumes and security demands of modern blockchain-based SCM systems. PoEf's superior performance compared to PBFT in terms of throughput and latency, as demonstrated through multiple simulation runs, makes it a suitable alternative for large-scale supply chain operations.

6.2 Background and Context

Using a multilevel sharding technique proposed by Luu et al. [193], a novel consensus mechanism, the Proof-of-Efficiency (PoEf), is proposed. The PoEf addresses weaknesses in existing consensus mechanisms and is more efficient. PoEf is an evolution of PBFT designed to reduce communication overhead by incorporating reputation-based node selection and sharding techniques. It operates by selecting a subset of nodes for consensus based on the reputation scores and dividing the workload into separate shards, reducing the time required to reach consensus. These features improve the system's throughput, scalability, and security.

As illustrated in Chapter 4's taxonomy, four different areas (the consensus mechanism, the cryptographic/data layer, the network layer and the smart contracts) of the blockchain could be explored for efficiency improvement, with consensus mechanisms being the most prevalent. In consensus mechanisms, the idea behind efficiency is to have nodes on the blockchain to reach consensus and confirm transactions in the fastest possible time. The PBFT consensus was chosen as the basis for the PoEf because it is very good at keeping the system's functionality and always aims to reach consensus even when some nodes are broken or hostile. PBFT ensures there is consensus by having multiple rounds of communication between nodes. This means the system can handle when some nodes act hard to predict or even dishonestly and still reach an agreement. So PBFT is perfect for situations that need to be safe and efficient, like supply chain management systems, but it is not scalable. Based on this thesis's experiments and prior literature, PBFT has low latency and high throughput. Experiments show that bandwidth consumption and latency significantly increase when the system's nodes exceed 100.

6.3 PBFT Consensus

PBFT consensus improved transaction speed, performance, and security compared to its predecessors. In PBFT, there are three types of nodes: (i) master, (ii) slave, and (iii) clients. The method starts by randomly selecting a master node to resolve transactions; then, in subsequent requests, the slave nodes are elected master nodes if there is view-switching (which is a protocol that changes the primary node when it fails, allowing the network to select a new leader and continue processing transactions without interruption). Fig. 6.1 illustrates the classic PBFT mechanism consensus protocol that brings transactions through a 'request', 'pre-prepare', 'prepare', 'commit', and 'reply' phase before reaching consensus. In the request phase, the client sends a transaction to

master node 0. Then, in preparation, master node 0 sends the request to slave nodes 1, 2, and 3. The preparation step involves slave nodes sending the messages they receive to all others. Each node broadcasts a commit message and executes the transaction request. Upon validating the requests in the transaction list and view, during the final response phase, the node transmits the outcome of addressing the client's request to the client. When all nodes in a blockchain receive $f + 1$ identical responses (where f representing the maximum number of fault-tolerant nodes in PBFT), and then consensus is reached. The PBFT key features include quick finality (confirm and finalise transactions immediately once consensus is reached) leading to low latency in smaller networks (increasing speed), its improved performance is also attributed to the low latency in smaller networks and it's security is attributed the fact the consensus can still validate transactions with to up to one-third faulty nodes on the network.

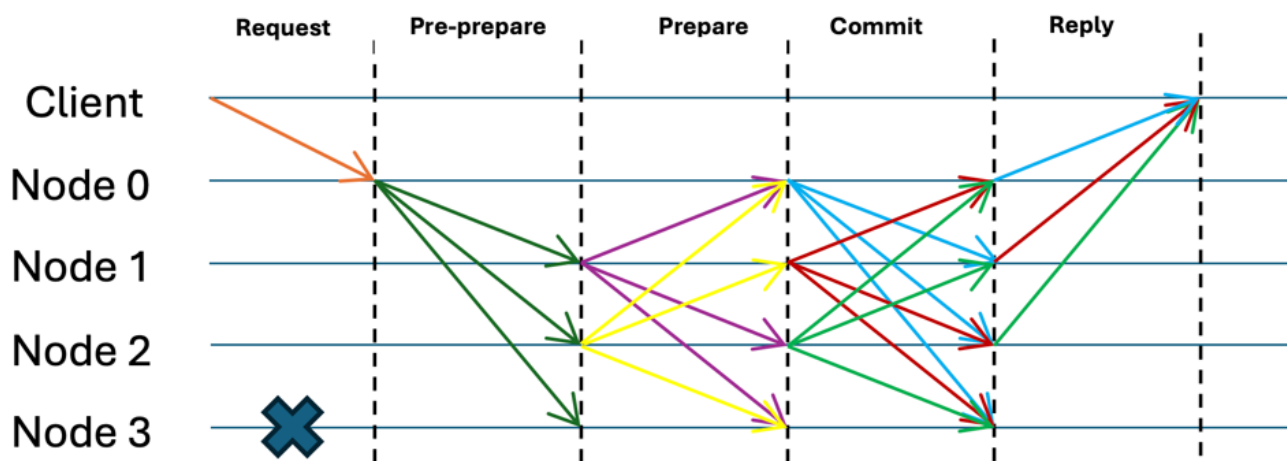


FIGURE 6.1: PBFT Consensus Mechanism Node Operation

As seen in Chapter 5's simulation results, the PBFT consensus is not scalable as there is an inverse correlation between throughput and number of transactions, (i.e. as throughput decreases as the number of transactions increase). For example, at a network size of 10 nodes with 100 Tx to process, PBFT is processing transactions at a rate of 2109 TPS. When the number of transactions to process increases to 1000 Tx, it is processing at a rate of 1552 TPS (dropping by 557 TPS). With 5000 Tx to process, the throughput decreases by 826 TPS to 981 TPS. So, in the case of an SCM, as the number of transactions requested from stakeholders increases, the throughput significantly declines. Interestingly, increasing the network size, at 100 nodes for the same 100, 1000 and 5000 transactions, the throughputs are 1920 TPS (falling by 189 TPS), 1328 (falling by 224 TPS) and 821 (falling by 160 TPS), respectively, as compared to when the network only had 10 nodes. This means the effect on the throughput performance is minor, even with more nodes.

Similarly, PBFT's latency significantly increases when the number of transactions or nodes grows, making it unsuitable for medium to large SCM systems. For example, with just 10 nodes, the latency for processing 1,000 transactions is 1,294ms. However, when the network expands to 200 nodes, this changes to 2,062ms, representing a significant increase in latency. Even for smaller transaction loads, such as 100 transactions, the latency increases from 362ms at 10 nodes to 610ms at 200 nodes. PBFT's inherent characteristics, such as its reliance on frequent communication among all nodes to reach consensus, become a bottleneck as network size and transaction volume grow. For instance, processing 50,000 transactions with 100 nodes results in a latency of 42,092ms, which becomes even more pronounced at 200 nodes with a latency of 45,265ms. This shows how PBFT struggles to scale efficiently, making it less effective for large-scale SCM systems requiring timely and high-throughput processing. For medium to large supply chain networks, PBFT's latency is inadequate to handle the high throughput and fast transaction speeds needed in dynamic and distributed SCM environments. Nonetheless, the consensus is still commonly used in the SCM space for smaller SCMs as the consensus does not handle an increasing number of transactions well.

6.4 PoEf's Methodology

6.4.1 Overview of the PoEf consensus:

PoEf is an evolution of PBFT designed to reduce communication overhead by incorporating reputation-based node selection and sharding techniques. It operates by selecting a subset of nodes based on the reputation scores to help the blockchain reach consensus. As seen in Fig. 6.2, the mechanism divides the workload into separate shards and works on them in parallel, reducing the time required to reach a consensus. These features improve the system's throughput, scalability, and security because the approach reduces the burden on network communication, which causes the throughput to decrease in the other mechanisms explored in Chapter 5. PoEf aims to provide a more efficient and secure consensus mechanism for large-scale supply chain management transactions while ensuring real-time responsiveness and system adaptability.

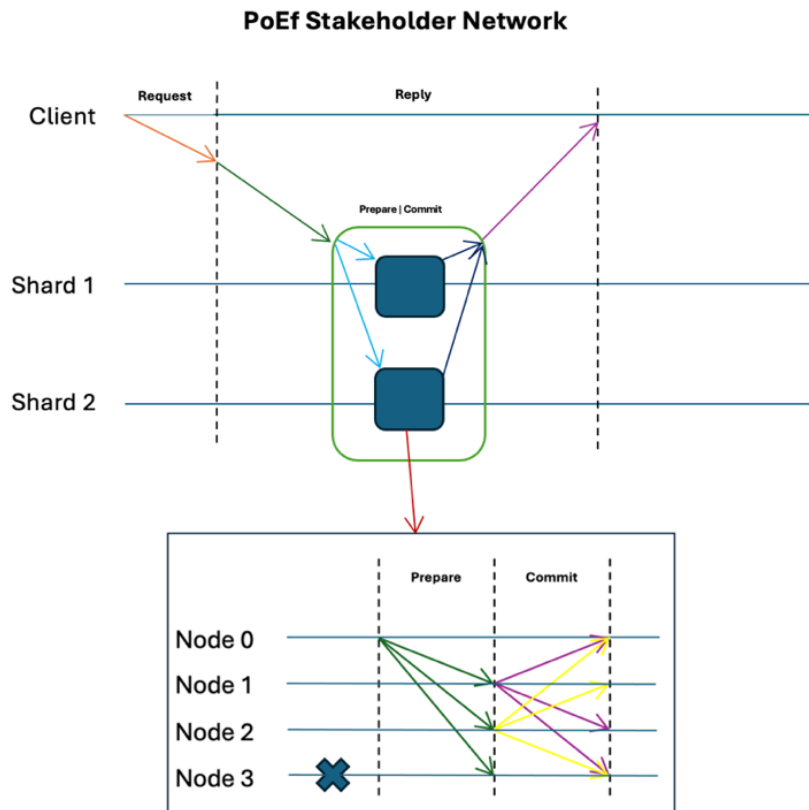


FIGURE 6.2: PoEf Consensus Mechanism Node Operation

Figure 6.2 illustrates the PoEf Stakeholder Network, detailing how a transaction is handled from the moment a client submits it through the network of nodes and shards. When a client initiates a transaction (represented by an orange arrow), it is broadcast to multiple shards for validation. The network is divided into shards (Shard 1 and Shard 2), each containing validator nodes that semi-independently process subsets of the transactions, leveraging sharding to enhance scalability and efficiency. The nodes undergo two phases within each shard: the Prepare and Commit phases. During the Prepare phase, the nodes communicate and ensure consensus within the shard. If the preparation phase succeeds, they move to the Commit phase, where the transaction is confirmed, and the consensus is finalised. Even if a node (e.g., Node 3) fails or acts maliciously, the remaining nodes continue the process without disruption. The two shards communicate to ensure the transaction is validated across the network, and once consensus is reached, the validated transaction is returned to the client (purple arrow). The PoEf consensus mechanism optimises throughput and latency by combining sharding and node-level consensus, allowing the system to handle large transaction volumes efficiently. Similarly, fault tolerance as discussed previously, ensures that even with node failures, the network continues to operate efficiently, and the Prepare/Commit phases ensure reliable transaction validation before the final commitment to the blockchain.

6.4.2 PoEf's Novelty

The PoEf consensus mechanism is an improvement of PBFT (see section 6.3) with four additional features listed below and shown in figure 6.3:

- **Reputation-based Selection** - a model where nodes are ranked based on their reputation, which is determined by their past performance and contributions to the network. It uses an algorithm to evaluate the reliability of nodes and prioritise those with better scores for validating transactions. The selection consists of an authorisation and authentication protocol that uses blockchain technology to verify suppliers and manufacturers, ensuring that only trustworthy participants are in the supply chain and can verify transactions.
- **Dual Mechanism Approach** - PoEf combines reputation-based selection with random number generation feature (in-built in Python) to ensure fairness in the consensus process. It prevents the possibility of a few nodes controlling the system, making it more resistant to manipulation. The dual aspect makes it a more balanced protocol for selecting nodes during block creation.
- **Sharding for Scalability** - a technique used to split the network into smaller groups or "shards." Each shard handles a portion of the total transactions, which reduces communication overhead and enhances the blockchain's ability to scale.
- **Node Efficiency** - PoEf focuses on optimising the performance of nodes by remodelling their ability to process transactions efficiently.

| Key Features Proof of Efficiency (PoEf) | | | |
|---|---|--|---|
| <p>Reputation-based Selection</p> <p>PoEf ranks nodes by reputation based on their performance and network contributions. Transaction validation is on nodes with better reputation scores, lowering computational load.</p> | <p>Dual Mechanism Approach</p> <p>PoEf combines random number generation with the reputation based system, ensuring fairness in node selection. This prevent dominance by a few nodes and reduce the likelihood of manipulation.</p> | <p>Sharding for Scalability</p> <p>PoEf uses sharding to partition the network into smaller groups, each handling a subset of transactions. This reduces communication overhead and enhances scalability, enabling higher throughput.</p> | <p>Node Efficiency</p> <p>PoEf focuses on node efficiency and trustworthiness instead of energy intensive mining processes</p> |

FIGURE 6.3: Key Features of PoEf Consensus Mechanism

6.4.3 Implementation Phases

The PoEf mechanism goes through several development phases (see figure 6.4) to improve the current PBFT infrastructure to become more efficient and secure. For improved efficiency, the PoEf mechanism incorporates a reputation system that evaluates nodes according to criteria like transaction success rate, participation, and communication. Sharding is employed to partition the network into smaller subnetworks, with validators selected from a stakeholder validation process. The validators employ a communication process that minimises message exchanges relative to PBFT.

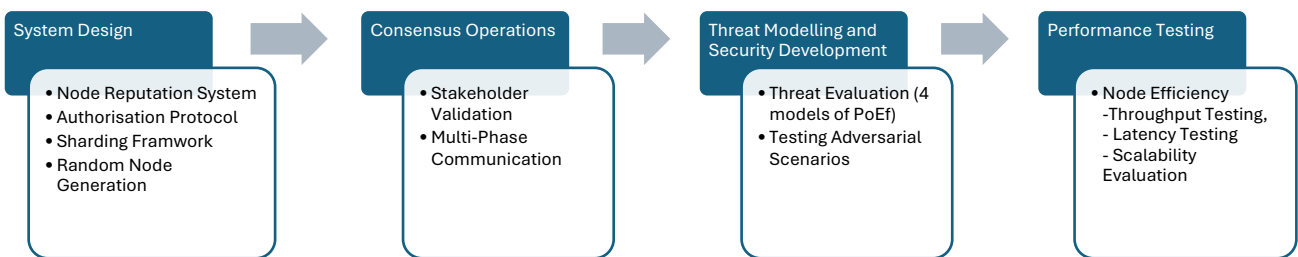


FIGURE 6.4: PoEf implementation phases

6.5 THE EFFICIENCY of PoEf

6.5.1 PoEf's Design

PoEf uses a sharding clustering process to separate the original PBFT network with a single leader-node into two networks with three types of nodes (authentication node, validator node and subordinate node), see figure 6.5 and figure 6.10. The first sub-network, the Authentication network, has one kind of node, “authentication nodes”. These nodes allow supply chain stakeholders to register and acquire a trust level score to join the Stakeholder’s network. The second sub-network, the Stakeholders Network, has a “two-node type” structure: (i) high-authority “validator nodes” selected based on trust-level scores and (ii) clusters of “subordinate nodes” led by the validator nodes. As illustrated in Figure 6.5, Stakeholders first undergo an authorisation procedure within the “Authorisation Network.” After completing the authorisation procedure, stakeholders are provided with cryptographic keys, namely a certificate containing public and private keys, enabling them to participate actively in the “Stakeholder Network”. At the same time, when individuals are issued the key pairs, they are also assigned an initial trust score based on the experience data they have supplied.

Assumption: The model assumes stakeholders (manufacturers and merchants) have been operating for a few years and are familiar with the market.

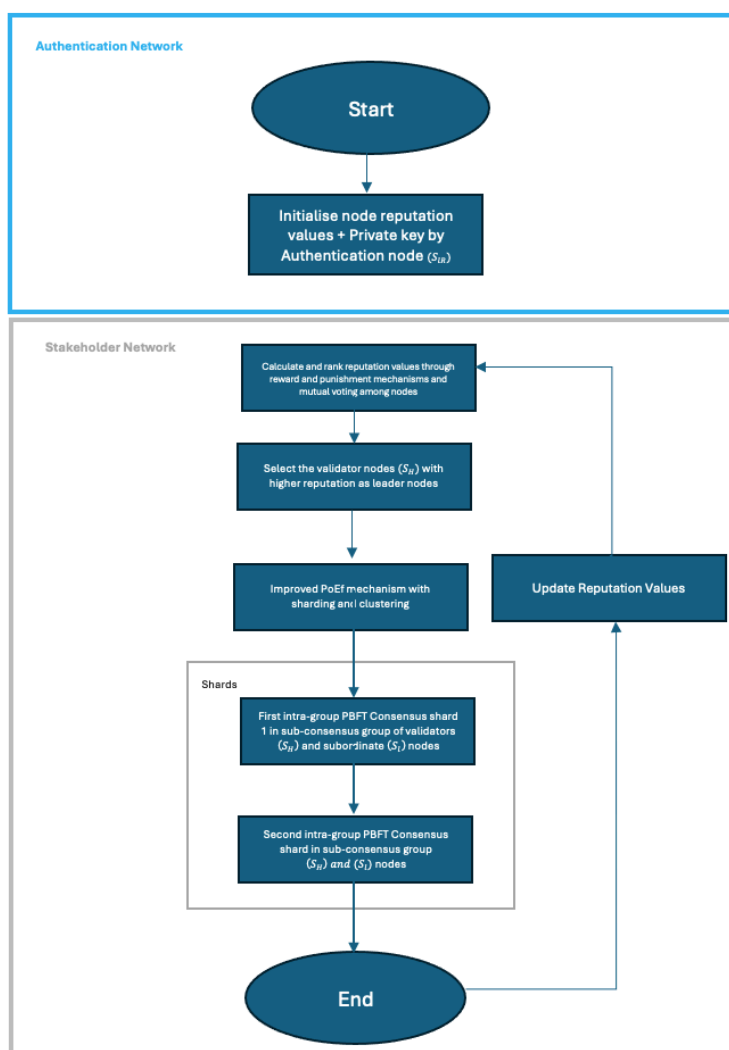


FIGURE 6.5: Figure illustrating the flowchart of the Consensus Mechanism, PoEf

6.5.1.1 Authorisation Network

The Authorisation network is the preliminary assessment stage for stakeholders seeking entry into the network. This phase entails verifying potential participants and utilising the blockchain’s inherent validation capabilities. Upon successful verification, stakeholders are granted unique cryptographic keys and assigned an initial reputation score, which is determined based on the experience data they provide.

6.5.1.2 Authorisation Network Breakdown

Underpinning the authorisation network, as illustrated in Figure 6.6, is the presumption that stakeholders, specifically manufacturers and merchants, possess established market tenure. The network’s operational characteristics are like the “DelivChain” model, a novel blockchain-based

framework for SCM developed by Y. Qian and Meng [141]. In DelivChain, trust is not a prerequisite for transactional engagement because the participants before they join the network. This means trust is established outside the transactions traded on the SCM, i.e., in blockchain terms, being on a separate network (which is what the authorisation network wrote for PoEf). DelivChain maintains a high level of security, as participants must register based on previous experience through a registration contract, as illustrated in Fig. 6.7. PoEf uses a similar process, calling it the authorisation network. It takes data from participants and converts it to a reputation score and private key that allows them to join the stakeholder network. The workflow for the Authorisation Network I illustrated in Fig. 6.6.

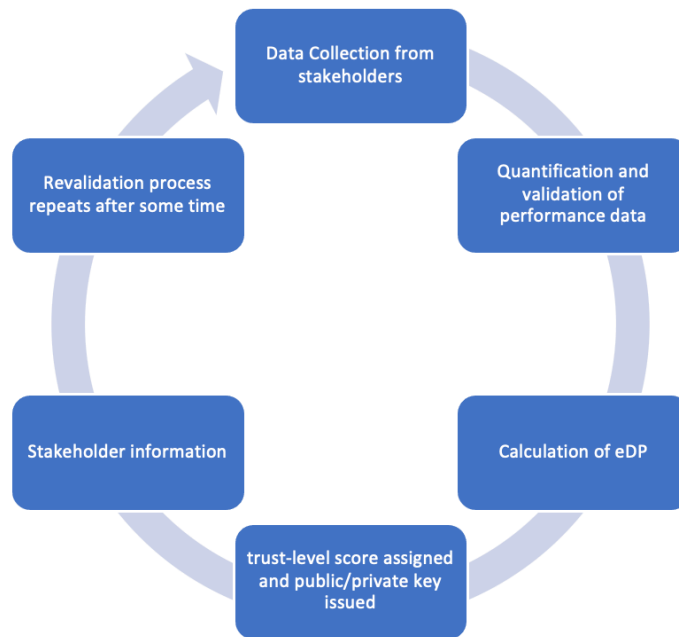


FIGURE 6.6: illustrating the flow diagram for Authorisation Network for PoEf.

6.5.1.3 Steps in the Authorisation Network

- i. Data identification and collection: Raw data is collected from potential suppliers. The raw data comes from production and delivery in the supply chain.
- ii. Quantification of performance data. Raw data collected from the previous stage is checked and validated. In this stage, the smart contract converts the data into quantitative values with different weightings based on experience, turnover, and customer base. These values benchmark an organisation’s production performance and issue a reputation-level score, R_t . For example, suppose the data implies one supplier’s manufacturing delays. In that case, this will be converted to a risk percentage value based on that supplier’s expected production capability, ultimately resulting in a lower reputation-level score.

$$R_t = \rho \times R_{t-1} + (1 - \rho) \times \sum_{j=1}^t S(j) \quad (6.1)$$

Where:

- R_t is the current reputation score of the node at time t
- R_{t-1} is the previous reputation score of the node at a time $t - 1$
- ρ is the weight or decay factor that balances the contribution of the past reputation score versus new activity. It ranges from 0 to 1.
- t is the number of transactions the node validates in the current cycle.
- $S(j)$ is the score assigned to each successfully validated transaction j , reflecting the node's contribution to consensus.

This formula gives more weight to recent activities while also considering the past performance of the node.

- iii. Calculation of estimated delivery performance (eDP). In this stage, the smart contract will use the supply chain assessment model On-Time In-Full (OTIF) to consider all the quantitative values obtained in the previous stages and calculate the overall eDP of the stakeholder applying.
- OTIF, sometimes called “DIFOT” (Delivery In-Full On-Time), is one of the most used metrics for delivery performance in supply chain management. A percentage value is used for an organisation's delivery key performance index (KPI) assessment. The formula of OTIF calculation could be presented as

$$\text{OTIF} = \frac{\text{number of deliveries OTIF}}{\text{total number of deliveries}} \times 100 \quad (6.2)$$

- iv. All applications which have passed the verification and validation are first assigned a reputation-level score (which will determine if they operate the Stakeholder Network as a ‘high-order node’ or a ‘subordinate node’) and subsequently issued a public/private key pair that will allow them to join the Stakeholder network.
- v. Stakeholder information will be encapsulated into a newly generated block and permanently stored in the blockchain ledger. The revalidation process occurs yearly.

The authorisation network is supported by the Registration contract. As illustrated in Fig. 6.7(a,b), the Registration Contract in the PoEf mechanism integrates the stakeholders into the network by validating the credentials, generating cryptographic keys, and calculating the reputation scores. The contract starts with collecting key inputs: the stakeholder's password (pw_s) for authentication, the stakeholder's data (D_s), such as the performance and operational history, and the eDP (estimated delivery performance) value, which quantifies the stakeholder's supply chain

performance. These inputs are processed using the $Register((pw_s), (P_B(D_s)))$ function to start the execution. The pending block $(P_B(D_s))$ represents the intermediate state of a transaction or block that has not yet been finalised on the blockchain. The data of the stakeholder, (D_s) , is processed in this pending state. In the execution phase, the stakeholder's private key (PK_s) is generated using the password and processed data, which is needed for signing and securing transactions in the network. The contract outputs the stakeholder a private key (PK_s) for secure interactions and a reputation score (R_l) , impacting the node's role and privileges in the PoEf system. Overall, this contract ensures that only verified and efficient stakeholders participate, maintaining security and trust in the network.

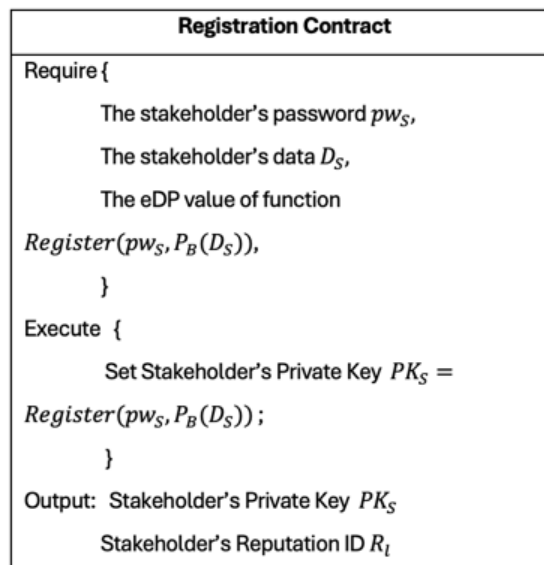


FIGURE 6.7a: illustrating the Registration Contract in the Authorisation Network for PoEf

```

53
54 # Stakeholder Registration Contract
55 class Stakeholder:
56     def __init__(self, name, password, data):
57         self.name = name
58         self.password = password
59         self.data = data
60         self.private_key = None
61         self.reputation_score = 0 #Initial Reputation Score
62
63     def register(self):
64         # Registration contract execution: generate private key and assign reputation score
65         self.private_key = generate_hash(self.password + self.name)
66         self.reputation_score = calculate_reputation(
67             previous_reputation=self.data['previous_reputation'],
68             num_transactions=self.data['total_orders'],
69             transaction_scores=[1 for _ in range(self.data['on_time_orders'])] # Simple transaction score list
70         )
71         return self.private_key, self.reputation_score
72
73 # Supply chain registration and performance evaluation function
74 def registration_and_evaluation(supplier_name):
75     supplier = suppliers_data[supplier_name]
76
77     # Create a new stakeholder
78     stakeholder = Stakeholder(
79         name=supplier_name,
80         password="password123", # Sample password, in real case it should be provided by the stakeholder
81         data=supplier
    
```

FIGURE 6.7b: illustrating the Registration Contract in the Authorisation Network for PoEf

6.5.1.4 Stakeholder Network

The stakeholder network, illustrated in Fig. 6.9, is where stakeholders confirm transactions. This phase entails two layers of participants (validator nodes and subordinate nodes) fulfilling the transaction requests. To join the stakeholder network, stakeholders would use the unique cryptographic keys, and an initial reputation score assigned by the authorisation network. The workflow for the Stakeholder Network is illustrated in Fig. 6.8.

Assumptions: The model assumes: (i) there is an infinite production capacity by the manufacturer, (ii) an order management backlog is created in lieu of lost orders, (iii) there is an unpredictability of the actual demand of products, (iv) vendors/merchants that are a part of the network is responsible for tracking the end-consumer demand and place orders using the reorder-point/order-quantity (r, Q) inventory standard. This standard is a staple in inventory control and is predicated on automatically ordering a fixed quantity Q when inventory levels hit a specified reorder point r and (v) there is an allowance for order modifications and cancellations.

6.5.1.5 Steps in the SCM Stakeholder Network.

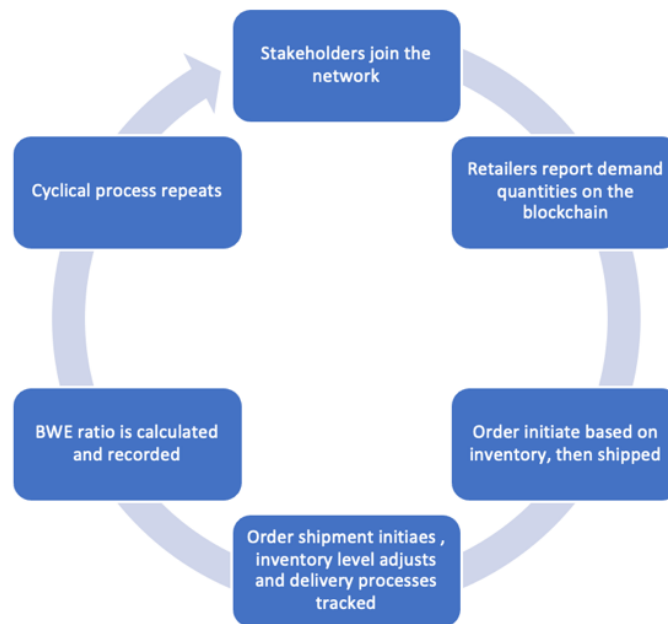


FIGURE 6.8 illustrates the flow diagram for the Stakeholder Network

- i. Authenticated stakeholders can join the network using the keys. Fig. 6.9(a,b) shows that users cannot join the network without authentication and the private key.
- ii. Vendors/merchants initiate the process by reporting demand quantities on the blockchain, triggering inventory checks and order fulfilment procedures across the supply chain tiers.

- iii. Order placement begins when inventory is available. When items are unavailable, upper-level orders are based on inventory levels relative to reorder points, with all transactional information recorded on the blockchain.
- iv. Order shipment and delivery processes are tracked, and inventory levels are adjusted accordingly. Continuous inventory analysis ensures alignment with reorder thresholds.
- v. Discrepancies in lead times are recorded and updated in the system based on the delivery times of scanned inventory as it moves along the supply chain.
- vi. The BWE ratio is calculated and recorded, offering insights into demand-order variances.
- vii. This cyclical process repeats, ensuring a streamlined SCM operation across all levels.

The Stakeholder network is supported by the Stakeholder authentication contract, designed to simulate a supply chain system where stakeholders (i.e. suppliers) can authenticate themselves, process transactions, and interact with the blockchain. First, the contract connects to a blockchain node to manage the network's participants. A function is used to verify the identity of stakeholders by checking the credentials (private key and password) obtained from the registration contract, which allows them to join the stakeholder network and conduct transactions. If authenticated, the stakeholder can perform tasks such as fulfilling product demand, placing orders, and updating inventory levels recorded on the blockchain. The contract also includes functionality for managing inventory, reordering products when stock levels fall below a specified threshold and calculating metrics like the Bullwhip Effect (BWE) ratio to track demand-order variances. It monitors stock levels, simulates transactions, and ensures smooth supply chain operations by allowing stakeholders to interact with the blockchain. The contract ensures trust and efficiency in the stakeholder network when managing transactions.

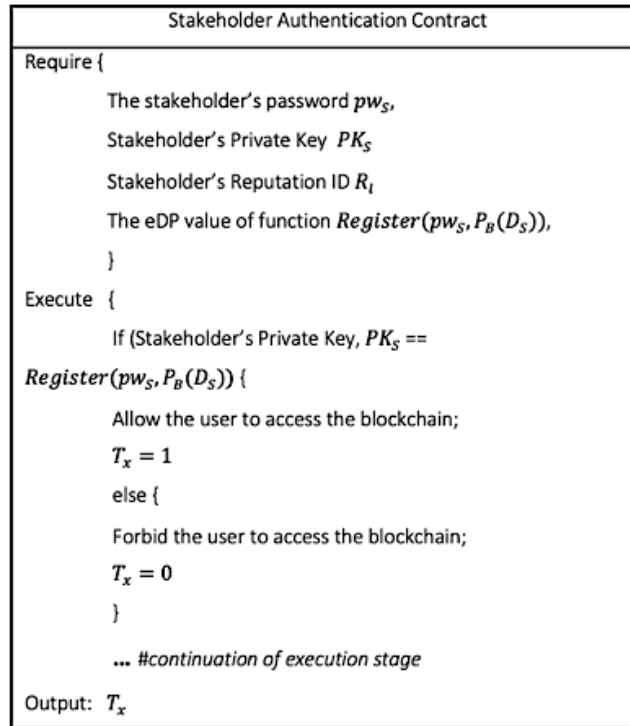


FIGURE 6.9a: illustrating the Authentication Contract in the Authorisation Network for PoEf

```

46 # Stakeholder Authentication Contract
47 def authenticate_stakeholder(stakeholder_name, password, private_key):
48     """
49     Authenticate stakeholder before joining the network.
50     Returns True if authenticated, False otherwise.
51     """
52     stakeholder = stakeholders.get(stakeholder_name)
53     if stakeholder and stakeholder['password'] == password and stakeholder['private_key'] == private_key:
54         print(f"{stakeholder_name} authenticated successfully.")
55         return True
56     else:
57         print(f"Authentication failed for {stakeholder_name}.")
58         return False
59
60 # Function to simulate the transaction
61 def process_transaction(stakeholder_name, product_name, demand_quantity):
62     """
63     Processes a transaction: checks inventory, updates levels, and records it on the blockchain.
64     """
65     # Ensure the stakeholder is authenticated
66     stakeholder = stakeholders.get(stakeholder_name)
67     if not stakeholder:
68         print(f"Stakeholder {stakeholder_name} not registered.")
69         return False
70
71     # Check if inventory is available and place order if necessary
72     product = inventory_levels.get(product_name)
73     if not product:
74         print(f"Product {product_name} not found.")

```

FIGURE 6.9b: illustrating the Authentication Contract in the Authorisation Network for PoEf (in Python)

6.5.2 PoEf Operations

Similarly to the exploration of how blockchain work in Section 2.2.2 of this thesis, highlighting the block creation phase, consensus verification stage and verification ledger stage, PoEf operations

also go through 3 related phases. To reach consensus PoE_f goes through (i) node selection, (ii) transactions broadcasting and (iii) Block confirmation.

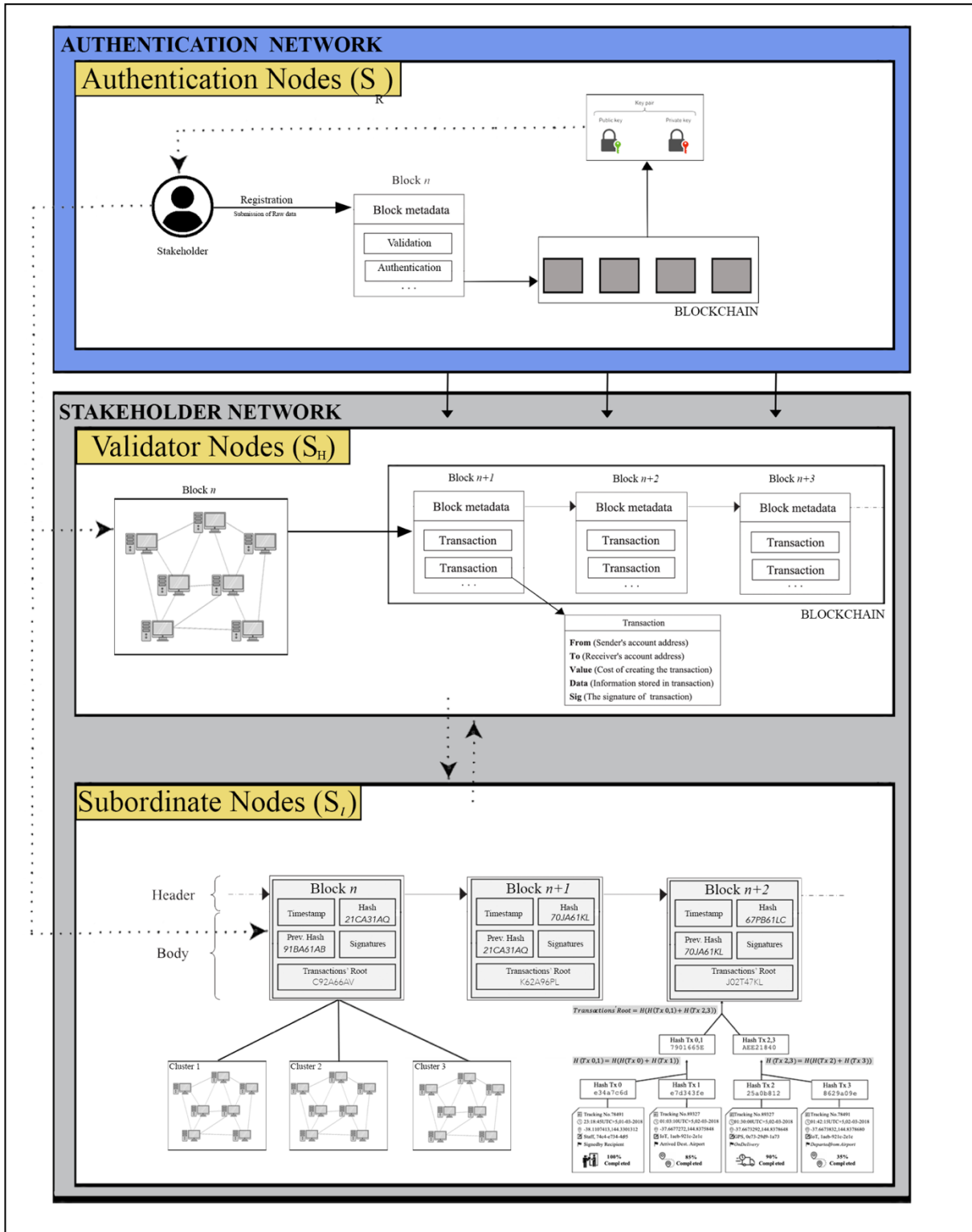


FIGURE 6.10: illustrating the node operations across networks in PoE_f

PoE_f stakeholders denoted as $S = \{S_1, S_2 \dots S_n\}$ are responsible for initiating, validating, and confirming transactions and adding them to the blockchain. Transactions represent blockchain-encoded stakeholder data, which is used to verify the authenticity of the stakeholder's information.

As illustrated in Figure 6.5, the PoEf mechanism nodes (stakeholders) operate across three primary phases: (i) registration and verification nodes (S_R) use a reputation-based process to register and verify stakeholders, (ii) the selection of high authority consensus nodes (validator nodes(S_H)) and (iii) the subsequent confirmation of transactions. To be considered a (S_H), the node must hold a reputation score. Following registration and verification, the mechanism employs a reputation system to evaluate the node’s credibility. Nodes that abstain from staking the identity or nodes with a lower trust level score are relegated to a tertiary pool of subordinate nodes, (S_L). This tiered node selection process enhances the efficiency of the block addition process, allowing for immediate block incorporation post-verification. In the structure of the mechanism, each node: (S_R), (S_H) and (S_L) operates in tandem to enable the block to reach consensus and confirm transactions.

6.5.2.1 How are high authority nodes selected?

In this thesis, ‘ n ’ signifies a set of nodes that manages the functioning of a network. The Stakeholder network categorises n into two distinct tiers: (S_H) and (S_L). The allocation of nodes into the layers of (S_H) and (S_L) are based on a dual-method approach using a random number generation mechanism and a node reputation score system. Randomisation eliminates centralisation from deterministic node selection methods, essential to blockchain technology’s decentralisation. Within this context, creating random function numbers adds stochasticity to the node selection process, reduces systemic biases that cause some vulnerabilities and ensures an eclectic network node representation. Simultaneously, the reputation score of the node assesses nodes by considering the past performance, dependability, and overall impact on the network. Nodes with better reputation scores are preferred for the (S_H) nodes and they are responsible for upholding network consensus and validating transactions. Implementing a merit-based allocation system strengthens the network’s security and fosters a sense of trust among its participants.

TABLE 6.1: illustrating key responsibilities of **Validator** (S_H) and **Subordinate** (S_L) nodes in PoEf

| Validator Nodes (S_H) | Subordinate Nodes (S_L) |
|---|--|
| Validate transactions within the network. | Assist in the validation of transactions within clusters or specific shards. |
| Maintain network security and integrity. | Process block metadata and contribute to consensus at a local (cluster) level. |
| Process and commit blocks to the blockchain. | Maintain communication with higher-level nodes (S_H) to report validation results. |
| Handle cross-shard communication and synchronisation. | Handle internal transactions within the assigned shard or cluster. |

| | |
|---|---|
| Participate in the consensus mechanism, ensuring efficiency and throughput. | Provide redundancy and ensure fault tolerance by continuing operations if other nodes fail. |
|---|---|

Integrating both randomness and reputation-based scoring mechanisms underscores a novel approach to selecting consensus nodes. The node selection approach balances the need for unpredictability to deter manipulation, rewarding reliable nodes through the (R_i) . In large blockchain-based SCM networks with high-volume transactions, node selection must be organised to ensure efficiency. PoEf’s node selection technique shows how dynamic blockchain technology is, where reorganising nodes can improve overall network stability and efficiency.

6.5.2.1.1 Consensus Node Selection Procedure

```

111 # Example list of nodes
112 nodes = [
113     {'auth_status': True, 'reputation_score': 90},
114     {'auth_status': False, 'reputation_score': 70},
115     {'auth_status': True, 'reputation_score': 85},
116     {'auth_status': True, 'reputation_score': 95},
117     {'auth_status': True, 'reputation_score': 60}
118 ]
119
120 # Threshold for reputation score to be considered as a high authority node
121 auth_threshold = 75
122
123 # Function to authenticate node
124 def authenticate_node(node):
125     """
126     Authenticates the node based on its 'auth_status'.
127     """
128     return node['auth_status']
129
130 # Function to get reputation score
131 def get_reputation_score(node):
132     """
133     Retrieves the reputation score of the node.
134     """
135     return node['reputation_score']
136
137 # Function to select a random node from a list excluding certain nodes
138 def select_random_node(nodes, exclude_list):
139     """
140     Selects a random node from the list of nodes, excluding those in the 'exclude_list'.
141     """
142     eligible_nodes = [node for node in nodes if node not in exclude_list]
143     return random.choice(eligible_nodes)
144

```

FIGURE 6.11a: illustrating the PoEf Consensus “Node Selection” procedure

```

144
145 # Main function to select consensus nodes for PoEf
146 def consensus_node_selection(nodes, auth_threshold):
147     """
148     Node selection process for PoEf consensus mechanism. High authority nodes (SH)
149     are selected based on reputation score. Other nodes are assigned to Subordinate Nodes (SL).
150     """
151     authorized_node_list = [] # High authority nodes (SH)
152     cluster_list = [] # Subordinate nodes (SL)
153     master_node_list = [] # List of master nodes in SL clusters
154
155     # Iterate over nodes to select based on reputation and authentication
156     for node in nodes:
157         if authenticate_node(node) and get_reputation_score(node) > auth_threshold:
158             authorized_node_list.append(node) # Add to SH list
159         else:
160             cluster_list.append(node) # Add to SL list
161
162     # Select master nodes from clusters (SL)
163     for cluster in cluster_list:
164         master_node = select_random_node(cluster_list, authorized_node_list)
165         master_node_list.append(master_node)
166
167     return authorized_node_list, master_node_list
168
169 # Example usage
170 high_authority_nodes, master_nodes = consensus_node_selection(nodes, auth_threshold)
171
172 # Print results
173 print("High Authority Nodes (SH):", high_authority_nodes)

```

FIGURE 6.11b: illustrating the PoEf Consensus “Node Selection” procedure

Figures 6.11(a and b) defines a procedure for selecting consensus nodes in a network based on authentication and reputation scores in PoEf. It first iterates over a list of nodes (Nodes_N) and checks if each node is authenticated (AuthStatus) and whether its reputation score exceeds a given threshold (AuthThreshold). If a node meets both conditions, it is added to the high authority nodes list (AuthorizedNodeList, representing S_H nodes). Otherwise, the node is assigned to the subordinate nodes list (ClusterList, representing S_L nodes). After evaluating all nodes, the code selects master nodes from the subordinate clusters (S_L) by randomly choosing one node from each cluster and adding them to the MasterNodeList. So, high-reputation nodes are selected for the S_H tier. Nodes not selected for S_H undergo consolidation in a group of S_L clusters. These clusters choose master nodes that verify transactions in the S_L shard. If a master node fails, a node with a better reputation score can take over, keeping the network running. The way that nodes' roles are dynamically assigned in PoEf shows how important it is to keep the network trustworthy at different levels. This makes PoEf a novel example of blockchain technology for supply chain management since it works well in a constantly changing environment, and reputation is a big part of reaching consensus on blocks.

6.5.2.2 Transactions broadcasting

Stakeholders in the dual-role process shown in Figure 6.5 are divided into “providers,” who offer services, and “raters,” who receive services. By the nature, the provider uses the private key to verify service data, which adds security to the data transfer pipeline. The rater then rates the service and

adds a reputation score, denoted by R_l to the transaction, as shown in Fig. 6.11. This score is then propagated across the network using digital signatures.

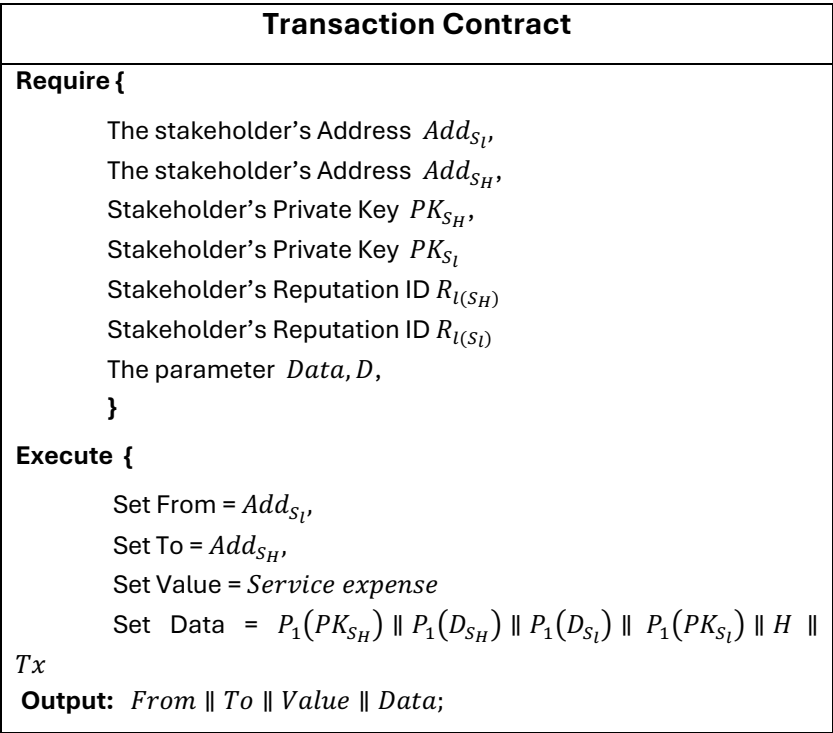


FIGURE 6.12: illustrating the Transaction Contract inside the Stakeholder's Network of PoEf

The reputation score, R_l is contained within the range of 0 to 1, with "1" indicating the highest level of happiness and a score of "0" indicating the lowest level of satisfaction. New stakeholders are added to the network with an initial score (R_0) equating 0. At the same time, an honesty parameter, H , is given the value of "1" to show original trustworthiness. This value can be lowered to "0" in the event of misconduct, such as sending contradictory messages or making transaction mistakes.

$$R(\Delta_T) = \sum_{t=0}^{t=i} R_S(T) \tag{6.3}$$

The equation, which represent a change in the reputation score, shows that a stakeholder's reputation $R(\Delta_T)$ at a certain point in time Δ_T is made up of the initial reputation $R_S(t_0)$ and the current reputation $R_S(t_i)$. This total score is constantly updated at times set by the network's leaders. This shows how important it is to keep participating honestly to improve your reputation in the network. To get/maintain a good reputation score, a stakeholder needs to be active in the system regularly and follow honest and trustworthy rules.

6.5.2.3 Consensus Block confirmation

A block cannot be validated without achieving consensus. The subsequent ten steps outline the procedure that PoEf uses to validate blocks via the subordinate nodes:

- (i) **Transaction Initiation:** A node initiates a transaction, represented as T_x, P_k, C_t where T_x is the transaction, P_k is the stakeholder's private key, and C_t is the current timestamp marking the transaction's creation. Transactions are then sent to the shard of S_l nodes.
- (ii) **Shard Cluster Verification:** Upon receiving the transaction, the shard with the cluster of S_l nodes first verify P_k and C_t . Successful verification leads to the transaction being endorsed with a private key $(T_x P_k, C_t)_{CPk}$ by the cluster and then sent to the master node in the cluster for authentication.
- (iii) **Master Node Validation:** The master node in each cluster is tasked with the authentication process so the master node checks the authenticity of the cluster node's signature and ensures the transaction is not already recorded in the blockchain. Post-verification, the transaction is signed by the master node's private key, represented as $((T_x P_k, C_t)_{CPk})_M$
- (iv) **Transaction Pooling:** Verified transactions by the Master node are then pooled in a waiting area. Once a predetermined threshold of transactions is reached in the pool (i.e. in the case of SCM whatever is requested in the original transaction by the client can now be fulfilled by stakeholders), the master node packages them into a smaller block, denoted as $((S_b)_{Tx})_M$, and broadcasts it to its peer nodes in the same clusters.
- (v) **Subordinate Node Verification:** On receiving $((S_b)_{Tx})_M$, other nodes in the cluster verify its contents. If the verification is affirmative, they send a consent signature $(Con_R(S_b)_{Tx})_M$ to the master node and S_l confirms the nodes contents.
- (vi) **Consent Broadcasting:** The master node then compiles all subordinate consents and forwards them along with the small block and its private key signature $(Con_R(S_b)_{Tx}, P_k)_M$ to the higher authority consensus group S_H .
- (vii) **Continuous Transaction Processing:** The remaining transactions in the pool that are not packed in the current small block are prioritised in the next consensus round or handled by a different shard.
- (viii) **Validation by Higher Authority Nodes:** Nodes in the higher authority layer validate the signatures and transactions within the received small block.
- (ix) **Acknowledgment or Rejection:** Post-validation, these nodes send either an acknowledgment $(Ak_{accepted}(S_b)_{Tx})_{auth}$ or a rejection $(Ak_{rejected}(S_b)_{Tx})_{auth}$ back to the subordinate nodes.
- (x) **Block Formation:** Successfully verified small blocks are sequenced chronologically. Small blocks are compiled into a larger block, which is then appended to the blockchain.

These steps are illustrated in the Reach Consensus procedure coding script in Fig. 6.13. The procedure emphasises the collective responsibility of nodes (S_n) in the network. By distributing transaction verification across different shards, the proposed protocol boosts the original PBFT mechanism throughput and alleviates the computational burden traditionally placed on miners on a single network.

```

76 # PoE Consensus Simulation
77 def ReachConsensus(transaction_list, sl_nodes, sh_nodes):
78     # Step 1: Transaction initiation
79     for tx in transaction_list:
80         random_sl_node = random.choice(sl_nodes)
81         random_sl_node.verify_transaction(tx)
82
83         if random_sl_node.is_master:
84             random_sl_node.sign_transaction(tx)
85             random_sl_node.add_transaction_to_pool(tx)
86
87     # Step 2: Master node packaging into small blocks
88     small_blocks = []
89     for node in sl_nodes:
90         if node.is_master:
91             small_block = node.create_small_block()
92             small_blocks.append(small_block)
93
94     # Step 3: Subordinate node verification and consent
95     consents = []
96     for block in small_blocks:
97         for node in sl_nodes:
98             if node.verify_transaction(block.transactions[0]): # Simulating block check
99                 consents.append(f"Consent from {node.node_id}")
100
101     # Step 4: Validation by higher authority nodes (S_n)
102     for sh_node in sh_nodes:
103         for block in small_blocks:
104             if sh_node.verify_transaction(block.transactions[0]):

```

FIGURE 6.13: Figure illustrating PoE's Reach Consensus procedure

6.6 PoE, Efficiency Experimentation Results

Similarly, to the simulations conducted in chapter 5 on different consensus mechanisms to ensure a comprehensive coverage of how each consensus mechanism manage different workloads (small, medium and large). PoE uses the same parameters for throughput, latency, and scalability to evaluate its efficiency across the 8 different network sizes, each with 8 different transaction amounts. A total of 64 simulations were conducted for PoE's throughput evaluation, and an additional 64 simulations were used to evaluate PoE's latency.

6.6.1 PoEf's Throughput

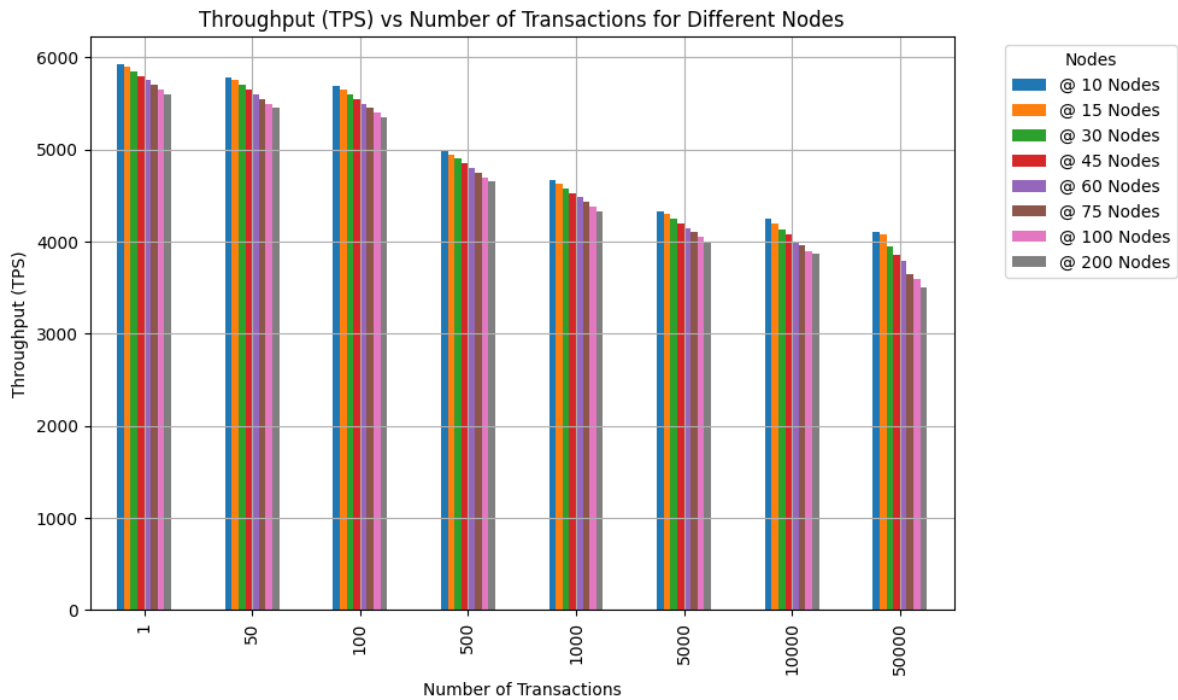


FIGURE 6.14: illustrating PoEf's consensus "throughput" results from BlockSim simulation runs.

Figure 6.14 illustrates the throughput results of the PoEf consensus mechanism across different transaction amounts. Throughput is measured in transactions per second (Tx/s) on the vertical axis, and the number of transactions is shown on the horizontal axis, growing at scale (from 1 to 50,000 transactions). Each group of bars on the chart represents the throughput of PoEf across different transaction volumes. The results show that as the number of transactions increases, PoEf's throughput incrementally decreases. The figure shows an inverse relationship between the number of transactions and the throughput. This behaviour is consistent with other consensus mechanisms evaluated in Chapter 5, wherein an increase in transaction volume generally results in decreased processing capacity. PoEf's throughput was also evaluated across different network sizes. Each single bar colour represents a particular network size. The graphs illustrate that as the network size increases (i.e. more nodes/stakeholders are on the network), PoEf's throughput decreases.

6.6.2 PoEf's Latency

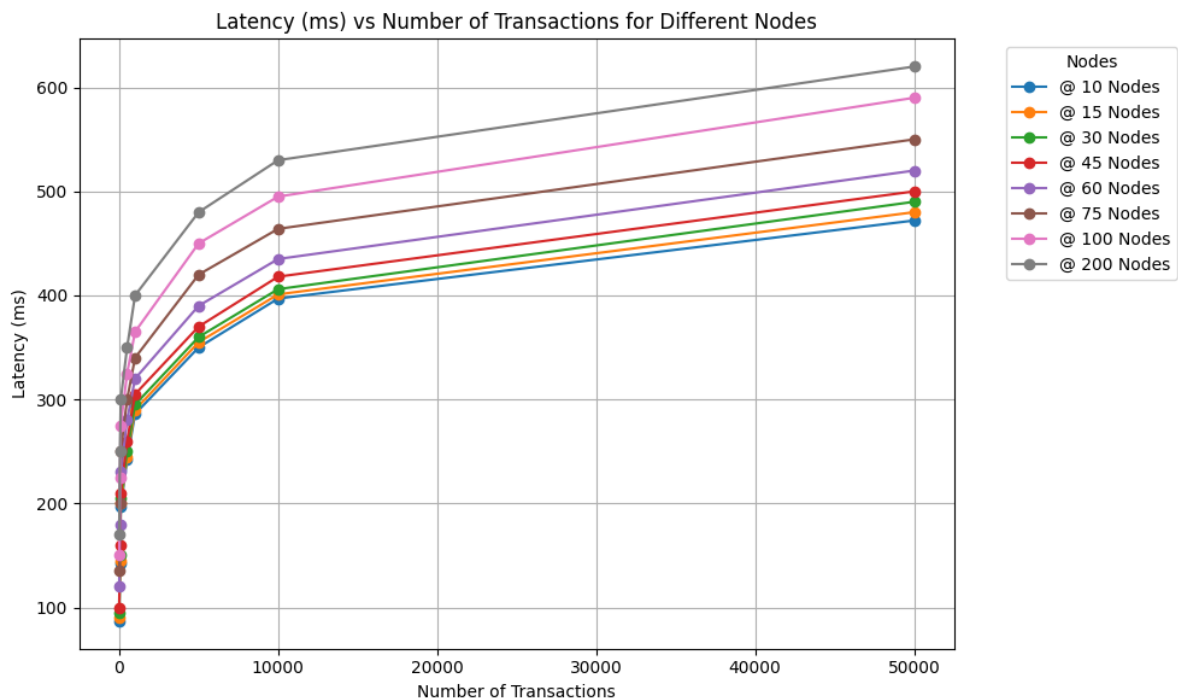


FIGURE 6.15: illustrating PoEf's consensus "latency" results from BlockSim simulation runs

Figure 6.15, depicts the consensus latency, measured in milliseconds, for the PoEf consensus mechanism as the number of transactions increases. The horizontal axis shows a scaling number of transactions, and the vertical axis represents the transaction latency. Each colour line represents the latency of PoEf at a different network size. Similarly, to measuring its throughput, PoEf's latency was evaluated across 8 different network sizes. Based on the simulations, at low transaction volumes (1 to 100 Tx) with small network sizes (up to 100 nodes), the latency remains relatively low (below 400ms) and stable at different network sizes up to 100. As the transaction volumes increase, the latency isn't affected much, e.g. up to approx. 1,000 transactions, the latency maxes at 400ms at the largest network size (200) in this experiment. Still, as the count goes from 1,000 to 5,000, there is a noticeable increase in latency, although it remains below 500ms. At a high transaction volume (10,000 Tx) and the highest number of nodes (200), PoEf latency crosses 500ms. As the number of transactions and nodes increases with growing network size, the latency of PoEf also incrementally increases, showing that the PoEf mechanism's performance degrades more significantly under high transaction loads and network loads. While the PoEf mechanism can efficiently handle low to moderate numbers of transactions with minimal impact on latency, the mechanism starts to experience higher delays at higher transaction volumes and network sizes, which are necessary factors for scalability.

6.6.3 Scalability

In the context of blockchain-based SCM systems, scalability means the capacity of a network to expand and maintain its efficiency (from a latency and throughput perspective) as the number of participants, transactions, or data volume grows. Scalability is significant because as supply chains grow (more transactions, more nodes/stakeholders), the system must still perform efficiently, processing orders and tracking shipments without delays or bottlenecks. A scalable SCM system can handle increasing complexity and transaction volume while maintaining speed and reliability. The thesis assesses PoEf scalability from both throughput and latency perspectives, then merges both metrics into a scalability score for further comparison.

6.6.3.1 PoEf's Scalability (throughput)

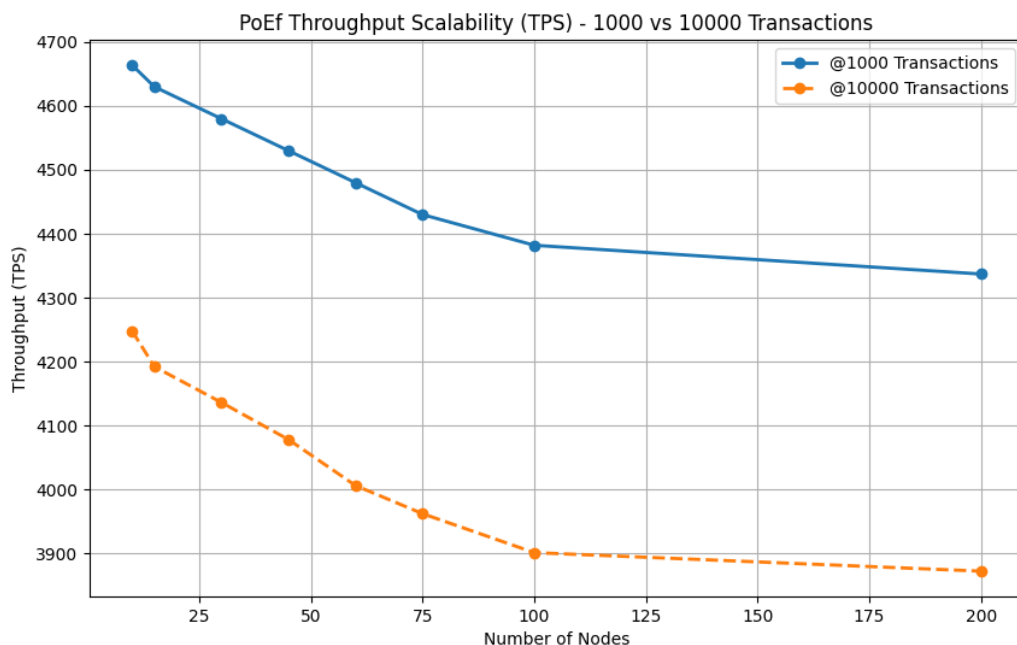


FIGURE 6.16: illustrating PoEf's Scalability (throughput) results with two network size (1,000 and 10,000)

Figure 6.16 illustrates PoEf's Scalability in terms of throughput (TPS) at two different numbers of transactions (1,000 and 10,000) are submitted to the system. The horizontal axis represents the number of nodes in the network, while the vertical axis shows the throughput. The graph provides insight into the scalability of the PoEf consensus mechanism, showcasing how it performs as the network expands (from 10 to 200 nodes). Regardless of whether PoEf is processing 1,000 or 10,000 transactions, the results indicate that PoEf's throughput does not suffer significantly as more nodes join the network. When the consensus handles 1,000 transactions with 100 nodes on the network, the throughput is 4,382 TPS, and as the network grows to 200 nodes, PoEf's throughput is 4337,

meaning the throughput would have decreased by only 50TPS when the network size doubled. A similar trend is seen when the number of transactions increases to 1,000. This stability in transaction processing speed with the increase in nodes highlights the mechanism's capability to scale efficiently, a necessary factor for blockchain-based SCMs that need to support growing user bases without compromising performance. The graph demonstrates a consistent level of performance across network sizes from 10 to 200 nodes. This consistency indicates that PoEf can handle increased demands and maintain the transaction rate without significantly degrading the performance. The minor incremental reduction (7.01% and 8.85% respectively) can be attributed to restricted bandwidth, and the work nodes must undertake when communicating on the network to reach consensus. Overall, the data reveals that PoEf's mechanism can handle a large SCM (up to 200 nodes and 50,000 transactions) effectively without too much degradation.

6.6.3.2 PoEf's Scalability (Latency)

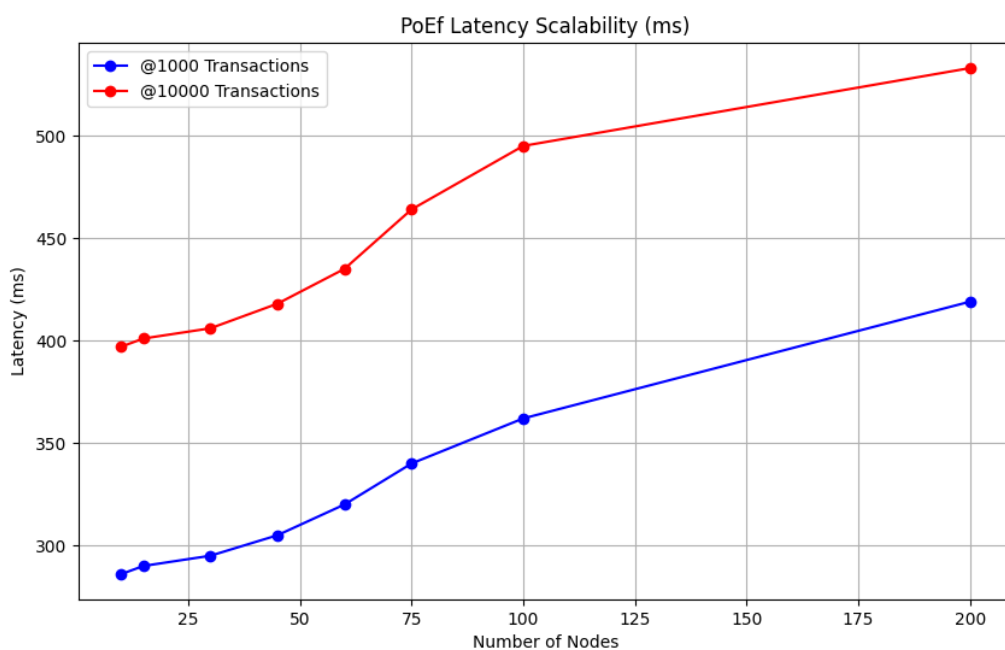


FIGURE 6.17: illustrating PoEf's Scalability (latency) results with two network size (1,000 and 10,000)

Figure 6.17 shows PoEf latency scalability for 1,000 and 10,000 transactions across 10 to 200 nodes. As nodes increase, transaction load delay increases, similar to other consensus systems examined in Chapter 5, where more nodes increase communication and consensus overhead. Transaction delay is low for smaller networks but increases as the network develops above 30 nodes. Since 10,000 transactions require more processing and communication before consensus, latency is higher than 1,000. After 100 nodes, latency growth for 10,000 transactions plateaus, showing a point

of diminishing returns where adding nodes does not significantly lower workload per node but increases communication overhead and delay. PoEf relies on multiple layers of nodes ((S_L) and (S_H)) to drive this pattern. Latency increases as layers communicate more with more nodes. PoEf remains an optimal consensus for large SCM systems because adding nodes doesn't increase latency.

6.6.3.3 The Scalability Score

This is a quantitative measure to assess how well a mechanism can handle increasing workloads or demands while maintaining optimal performance. It combines key metrics, throughput, and latency to provide a single score that reflects the system's scalability. Creating a scalability score when assessing blockchain-based SCM systems serves multiple purposes, highlighted below:

- (i) It provides a quantifiable and standardised way to evaluate how well a consensus mechanism handles increasing transaction loads and network sizes, which is needed for dynamic SCM systems that can significantly expand.
- (ii) Measuring how a system's throughput and latency scale as demand helps balance throughput and latency, allowing SCM operators to assess how well the system manages high transaction volumes without excessive delays. This balance is essential for maintaining efficiency in large, distributed SCM networks where real-time processing is necessary for tracking shipments, inventory, and order fulfilment.
- (iii) Assessing scalability ensures the system can prevent bottlenecks, transaction delays, or performance degradation under high-load conditions, which are common in large-scale SCM environments.

To develop a formula that calculates scalability based on throughput and latency, it is essential to define the interaction between these two metrics. Scalability can be interpreted as the balance between high throughput and low latency. These two factors are inversely related when evaluating scalability, meaning that higher throughput and lower latency together represent better scalability.

First, determine an upper bound for a "Very High" throughput. Since higher throughput corresponds to better scalability, throughput will positively impact the scalability score through the formula.

$$T = \frac{\text{Throughput (TPS)}}{5000} \quad (6.4)$$

where 5000 TPS represents the upper bound for very high throughput (from the experimental data collected, throughput values for different consensus mechanisms generally hover around or below

5000 TPS in most of the simulation test runs. For example, consensus mechanisms like PoEf and Stellar often show values close to or slightly exceeding 5000 TPS under optimal conditions (e.g., PoEf achieving 5780 TPS for 50 nodes). Therefore, **5,000 TPS** can be considered a realistic and representative upper bound for what is considered "very high throughput" in the context of blockchain-based SCM systems)

Then, determine an acceptable bound for latency. Since lower latency indicates better performance, a penalty for high latency is applied using an inverse relationship. The formula is expressed as:

$$L = \frac{15000}{\text{Latency (ms)}} \quad (6.5)$$

where 15,000ms is considered the upper threshold for very high latency, the average latency, derived from the peak latency value under optimal network conditions (200 nodes at 50,000 transactions) is **~15,000ms**, excluding PoW, which intrinsically exhibits exceptionally high latency (up to 3,500,000 ms)

A combination of these two can be a simple weighted average:

$$SS = \frac{w_T \cdot T + w_L \cdot L}{w_T + w_L} \quad (6.6)$$

where:

- w_T is the weight for throughput,
- w_L is the weight for latency

for the purpose of this research w_T and w_L will be 0.5 (Setting both w_T and $w_L = 0.5$ assumes that **throughput and latency** contribute equally to the overall scalability of the system. This is suitable for scenarios where both fast transaction processing (throughput) and low delays (latency) are similarly crucial for maintaining system performance, particularly in real-time or near-real-time systems like SCM. While throughput is critical to ensure the system can handle high transaction volumes, the system's ability to process each transaction quickly (i.e., low latency) is equally essential to prevent bottlenecks and ensure timely decision-making.

6.6.4 Performance Gap Between PBFT AND PoEf

6.6.4.1 Throughput Comparison over different network sizes (10, 100, 200 nodes)

Figures 6.18 (a-c) illustrate throughput comparisons that show that PoEf outperforms PBFT across all network sizes. PoEf's demonstrate significantly greater throughput than PBFT for various

transaction loads and node configurations, meaning that PoEf scales throughput better as network size increases. As transaction quantities climb (1 - 50,000), PoEf and PBFT lose throughput, but PBFT loses more performance. PoEf, on the other hand, maintains high throughput as transaction volumes increase, making it preferable for handling higher transaction loads without degradation. PoEf handles 4,000 transactions per second in a 100-node network with 500 transactions, while PBFT handles 1,000. In 200-node networks, PBFT's throughput decreases with transaction volume, but PoEf maintains excellent throughput, demonstrating the two techniques' different scalability. PBFT problems with high transaction volumes, especially in larger networks.

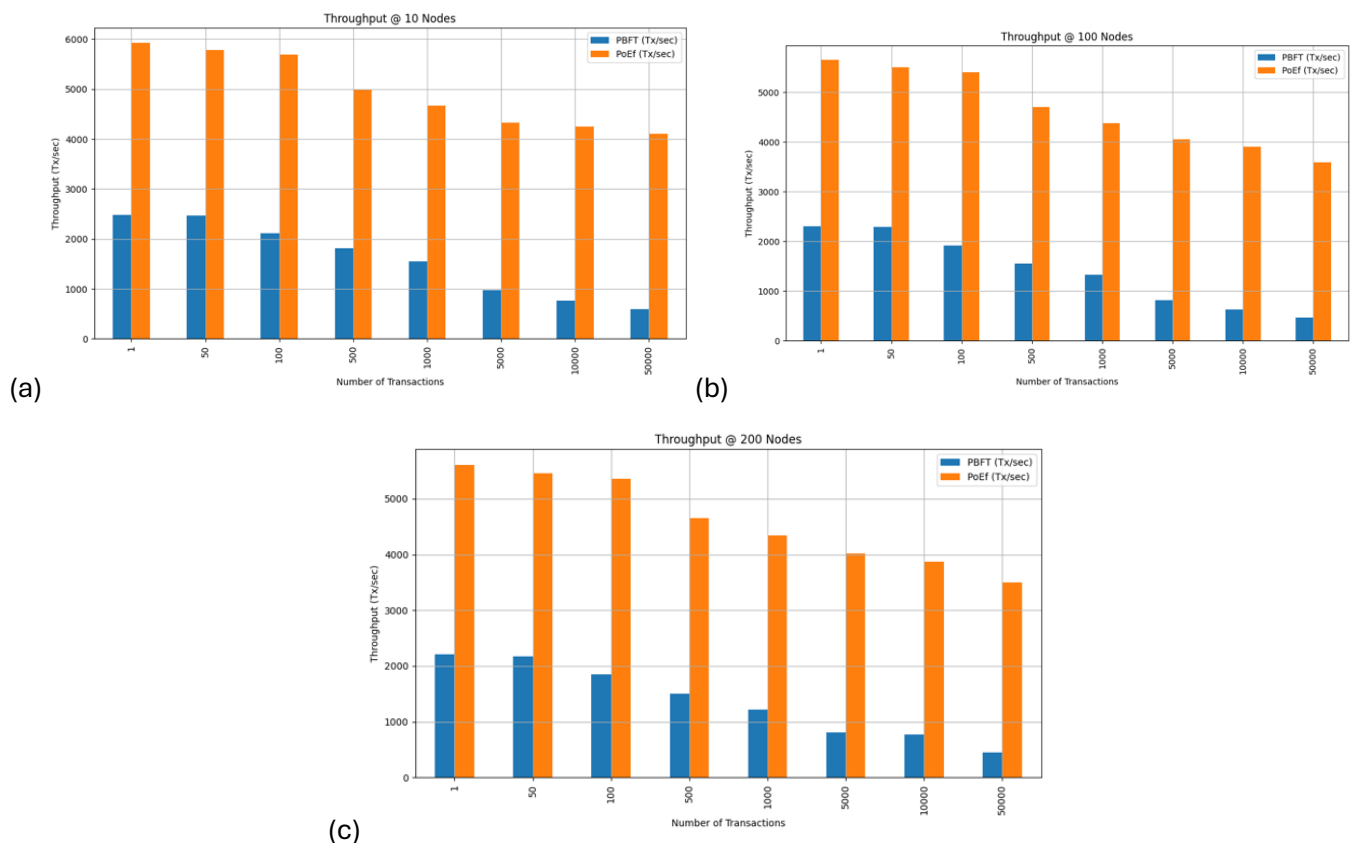
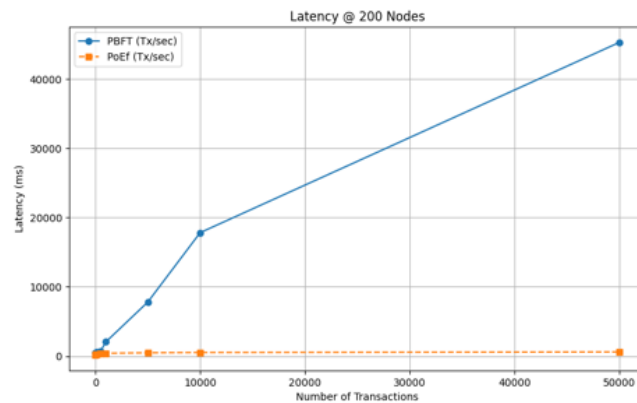


FIGURE 6.18(a-c): illustrating PoEf's Throughput compared to PBFT (@10, 100, 200 nodes)

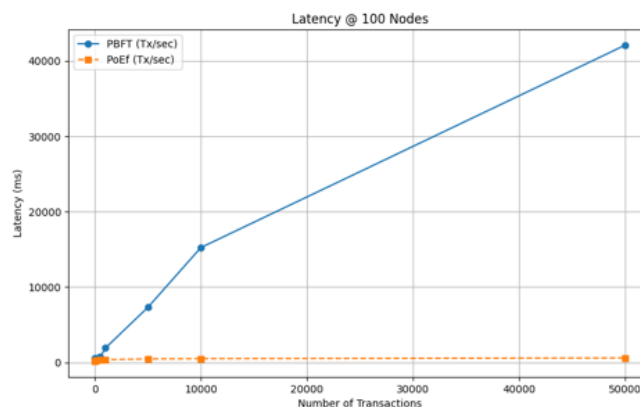
PoEf's excellent throughput across network sizes and transaction volumes makes it suited for high transaction loads and scalability in large supply chains. Performance on larger networks shows it can handle more load without sacrificing performance. However, PBFT may work for smaller or more stable supply chains with lower transaction volumes and fixed network sizes. PBFT may work for smaller networks with less performance because of its simplicity. In dynamic and large-scale supply chains, PoEf's higher scalability makes it the preferred alternative for variable loads. In contrast, PBFT may suffer in conditions of variable demand and increasing networks.

6.6.4.2 Latency Comparison over different network sizes (10, 100, 200 nodes)

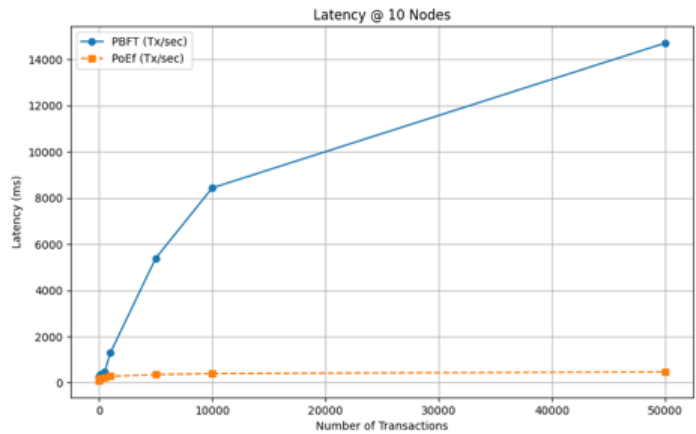
Figures 6.19 (a-c) compare PoEf and PBFT latency across 10, 100, and 200 nodes. Looking carefully at both consensus' scalability, PBFT latency increases with network size, especially as transactions increase. PoEf achieves efficiency primarily due to its hybrid design and the way it organises and utilises nodes within the network. In PoEf, the nodes are divided into two main groups: subordinate nodes (S_I) and high-authority nodes (S_H). Each group is responsible for a specific role in optimising the consensus process. PBFT's latency increases significantly in the 200-node network when transaction loads increase, and the struggle to maintain low latency is caused by communication and synchronisation difficulties. Comparatively, PoEf's latency is constant across network sizes, as its latency performance in larger networks shows its ability to handle more transactions. Increasing transaction quantities barely affect PoEf's latency, making it ideal for contexts with high variability in transaction demands. PoEf has a latency advantage in smaller network settings. However, PBFT also has low latency with modest transaction volumes, showing that PBFT may be workable for small supply chains with low transaction loads, while PoEf can process more transactions in a large SCM network.



(a)



(b)



(c)

FIGURE 6.19: illustrating PoEf’s Latency compared to PBFT (@10, 100, 200 nodes)

PoEf's latency scalability makes it better for transaction processing in medium to large-sized supply chains with higher transaction volumes. It beats PBFT in latency-sensitive applications for big supply chains, although it can work for smaller, more stable networks with fewer transactions.

6.6.4.3 Performance Gap between the two consensuses

The performance gap can be evaluated using the Scalability Score. The scalability score for the 3 network sizes (10, 100 and 200) at 1,000, 10, 000 and 50,000 transactions respectively, is illustrated in Table 6.2 , based on the sample calculation:

Sample PoEf Calculation (10 nodes @ 1000 transaction)

$$T = \frac{4664}{5000} = 0.93 \quad | \quad L = \frac{15000}{286} = 52.45 \quad | \quad SS = \frac{0.5 \cdot 0.93 + 0.5 \cdot 52.5}{1} = 26.69 \quad (6.7)$$

Table 6.2: tabulating the Scalability score for PoEf and PBFT (@10, 100, 200 nodes)

| Transactions | Nodes | PoEf Scalability score | PBFT Scalability score |
|--------------|-------|------------------------|------------------------|
| 1000 | 10 | 26.69 | 5.95 |
| 10000 | 100 | 15.54 | 0.55 |
| 50000 | 200 | 12.45 | 0.55 |

In **smaller supply chain networks** with fewer participants, **PoEf is far more scalable** than PBFT. based on the calculations, PoEf at 10 nodes is 26.69 which in the case of SCM would allow faster and more efficient transaction processing than PBFT 5.95, resulting in quicker order fulfilment and real-time inventory tracking. PBFT, while functional, may introduce bottlenecks that can slow down

these processes. For **larger SCM networks**, where multiple stakeholders (200 nodes) and 50000 thousand transactions, **PoEf is highly scalable** and capable of supporting these operations efficiently. In contrast, **PBFT's low scalability** makes it unsuitable for larger networks, as the system would likely face delays and bottlenecks, slowing down order processing, shipment tracking, and inventory management.

Although PoEf being based on PBFT, there is noticeable performance gap between both. The PoEf addresses PBFT's inherent limitations of scalability, communication overhead and resource inefficiency (where all nodes to participate in the consensus process). PBFT uses a leader-based consensus process with multiple rounds of communication, which increases overhead as the number of nodes and transactions grows. More communication among nodes leads to higher latency, lower throughput and limited scalability. In contrast, PoEf improves this by incorporating a reputation-based node selection system and sharding. The reputation system reduces the nodes involved in each consensus round, minimising communication overhead and enhancing throughput. Additionally, sharding allows the workload to be distributed across smaller subnetworks, leading to parallel transaction processing among shards and further improving scalability. As a result, PoEf achieves better performance on average of up to ~675% for both latency and throughput when compared to traditional PBFT, in large-scale and high-transaction environments. These improvements enable PoEf to handle more transactions more efficiently, making it better suited for supply chain management systems where scalability and efficiency are a priority.

6.7 THE SECURITY of PoEf

Chapter 4 elucidated various flaws that compromise the efficiency of consensus methods, specifically double Spending attack, 51% Majority (DoS Attack), Selfish Mining and Bribery. PoEf's architecture enables the mechanism to circumvent these vulnerabilities, which are common across consensus mechanisms, by integrating 4 key security-related concepts into its design.

These security-related models written in Python are:

- (i) the network model of the nodes,
- (ii) the authenticity model of the nodes,
- (iii) the truthfulness model and
- (iv) the encryption model of the nodes.

6.7.1 PoEf node's Network Model

To maintain security, nodes across the Authentication and Stakeholder networks of PoEf must be authenticated to communicate with each other in a partially synchronous manner. They work together to reach and maintain consensus on transactions on the blockchain. The networks are designed to guarantee connectivity between legitimate nodes, ensuring that all transactions are securely shared between shards. In addition, the system is designed, based on PBFT, to accommodate Byzantine faults, acknowledging the possibility that specific nodes may act maliciously or erratically, reflecting a real-world applicability of the PoEf blockchain implementation. The network's fault tolerance is quantified by designating n as the total number of nodes, with a subset f that may be faulty. In adherence to the Byzantine fault tolerance principles, the system is constructed to function correctly if the number of faulty nodes does not exceed f , where the relationship $3f + 1 \leq n$ ensures the network's resilience and ability to reach consensus, even in the presence of these potential faults. This research is complimentary to the contributions of Xiao et. Al. [194], whose analytical work provides the proposed network's design against Byzantine faults. The findings underpin the network's security model and are instrumental in the proof of concept for the PoEf's operational framework. Hence, the system adopts established theoretical models and incorporate previously simulated research to ensure a secure and efficient blockchain network tailored for contemporary SCM challenges.

6.7.2 PoEf node's Authenticity Model

The security model of the PoEf consensus mechanism is examined to establish its resilience within the context of the SCM blockchain network. This involves maintaining the system's integrity against malicious nodes and other vulnerabilities of the Consensus Layers highlighted in the taxonomy in Chapter 4. The underlying assumption of this thesis is that the PoEf mechanism ensures a state of maximum security by disallowing forks, provided that the number of Byzantine nodes remains below a certain threshold denoted as f as highlighted Network Model section. In addition to incorporating the mechanism within an SCM framework, PoEf achieves authenticity in a partly synchronous network, representing an SCM system's operating conditions. This attribute guarantees that, notwithstanding any network delays, new blocks will ultimately be added to the blockchain, hence supporting ongoing SCM operations.

In PoEf, a group of stakeholders denoted as $S = \{S_1, S_2 \cdots S_n\}$. These stakeholders are responsible for initiating, validating, and confirming transactions and adding them to the blockchain. In focusing

on transactions that are waiting to be added, known as pending transactions, and represented by T_x , and the pending blocks P_B . For such transactions and blocks, the following attributes are endorsed to ensure the security and authenticity of the blockchain. From a security and authenticity perspective:

- (i) PoE ensures integrity by checking private keys from network nodes. This means there is an assurance that a transaction (T_x) is reliable and comes from an acknowledged and authenticated stakeholder (S_n) upon its formal inclusion in the blockchain. Furthermore, every transaction is cross-checked to ensure they are recorded once on the blockchain, mitigating duplicate transactions. This is an essential feature for SCM operations where unique transactions (e.g., orders, shipments) are unchallengeable.
- (ii) There is an assurance of closure for each block. This is achieved when a potential block P_B is successfully appended to the blockchain, signifying its conclusive status. Once a block has been committed to the blockchain, it implies that the transactions encompassed inside this block are immutable and irrevocable, with no possibility of modification or reversal in the future, which is important for the immutable record-keeping required in SCM.
- (iii) If a potential block P_B is to be considered valid, it ensures that every transaction T_x within that block will be included in the same block P_B across all stakeholders' records who have accepted the block as valid. This guarantees consistency and consensus within the network concerning the transactions documented in varying blocks/shards, thus maintaining consistency and reliability in the SCM ledger.
- (iv) Central to SCM operations, the research delineates that for every transaction initiated by a stakeholder, if T_x is valid; all stakeholders will eventually commit it, assuring transaction throughput and avoiding system deadlock.

This security model is key in SCM because it ensures that the blockchain functions correctly and gives SCM stakeholders trust that the system will stay reliable and effective even if malicious actors try to break it. The model ensures that the mechanism can withstand security threats while delivering the high throughput and scalability that modern supply chain management systems need.

System integrity depends on authenticity. It requires the mechanism to work quickly and execute legitimate transactions. Despite conflicts, the network continues to operate, demonstrating its resilience and authenticity.

- **Assumption (Authenticity of PoEf):** *The authenticity of PoEf is demonstrated by its ability to operate consistently throughout a network of S nodes. This suggests that, regardless of the internal status of each node, there is a guarantee that at least one honest node will inevitably add a new block to the blockchain within a specific time limit.*

To explain the authenticity of PoEf, it is posited that transactions, T_x , originating from trustworthy nodes S , are all intended to be included in the blockchain in either the current or a later iteration, therefore earning unanimous approval from the honest participants within the network. When considering a node with a high reputation, denoted as S_H , that sends a transaction T_x , to the network, there may be two possible outcomes:

- (i) the transactions are received if all stakeholders in the network receive T_x to validate, it indicates the network's capacity to maintain authenticity within an asynchronous environment, thereby validating the operational integrity for the node, S_H .
- (ii) the transactions are not received. If there is an absence of T_x , such an event would occur under circumstances where S_H is either acting with malicious intent or experiencing a failure during the transaction's transmission phase.

The verification process relies on a dual-pathway assessment, where the receipt of a transaction by peer nodes is used for measuring the network's commitment to authenticity. This framework ensures that the PoEf consensus mechanism not only aspires to but also achieves a high degree of authenticity, which is needed to maintain the honesty and reliability of transactions within decentralised systems.

6.7.3 PoEf's Node Truthfulness Model based on Reputation-level

The fundamental premise of PoEf's architecture is that when a truthful node, denoted as S adds a block to the blockchain; no other truthful nodes in the network will attach a competing block for the same round. This design ensures network safety by preserving the trustworthiness and consistency of the blockchain. The effectiveness and reliability of the PoEf consensus mechanism are intrinsically linked to the resilience of its underlying reputation-based protocol.

- **Assumption (Node Reputation in PoEf):** *To explain the truthfulness of PoEf, consider a network of nodes $\{S_1, S_2 \dots S_n\}$ where each node S is assigned a reputation-level score R_i , reflective of its decision-making weight within the network. If in examining two arbitrary blocks*

examine two blocks, P_0 and P_B , appended to the blockchain by distinct honest nodes S_h , and S_i , from the set $[n + 1]$, in any given round Q . In such a scenario, the equality $P_0 = P_B$ holds, ensuring the integrity of the round's outcome.

The preservation of security based on reputation in PoEf is contingent upon the fulfilment of the following conditions:

- The number of validators controlled by the attacker in the network is less than f .
- The stakeholders that fall within the control of the attacker possess a cumulative reputation score, R_l , that is inadequate to disrupt the decision-making process of the network.

This means that:

$$R_l = \frac{\sum_{i=1}^{|S|} R(\Delta_T)}{3} \quad (6.8)$$

where $R(\Delta_T)$ signifies the reputation score of individual stakeholders and $|S|$ represents the total number of stakeholders (validators). Ultimately, if an attacker cannot compromise the network's safety unless the conditions are not satisfied establishes a safeguard against threats to the network's consensus integrity.

6.7.4 PoEf Encryption model

Key cryptography is essential for secure communication. PoEf uses Elliptic Curve Cryptography (ECC), which employs a pair of keys for each user: private and public keys. The public key is an elliptic curve resultant point produced by scalar multiplication of the private key with a predefined generator point P_g . The private key is a securely chosen random number. Each SCM blockchain member receives a private key, a secret random integer known only to the owner, and a public key, a publicly known point on an elliptic curve. This generator point P_g , often referred to as the base point, is a predefined parameter in the elliptic curve system. Prior to any encrypted communication, the involved stakeholders must concur on a specific elliptic curve and its associated parameters, namely, the curve coefficients a and b and base point P_g . The curve is defined by the equation $y^2 = x^3 + ax + b$ where the discriminant $4a^3 + 27b^2 \neq 0$ to ensure the curve has no singular points. ECC is often used in blockchain encryption systems because it is efficient: i.e., it needs fewer resources, lets you use smaller key sizes, and guarantees that the code will be easier to understand. The time complexity of point multiplication in ECC is approximately $O(\sqrt{X})$ where X is the size of the field.

Moreover, ECC's robustness against sophisticated attack vectors is encapsulated by its resilience measure M , which can be expressed as: $M = \frac{1}{3} \sum_{i=1}^S R(\Delta T)$, where $R(\Delta T)$ denotes the resilience factor against time-based attacks. In cryptographic systems, this is related to the time it takes for a transaction or a block to be confirmed and become part of the blockchain. Putting it all together, the formula calculates the average resilience score of all Stakeholders (validators) or nodes in the network, where the resilience score is a function of time delay. This could be used to assess the blockchain network's overall robustness, particularly under network delay or disruption conditions. The resilience score may factor in the node's ability to handle such situations without compromising the integrity and security of the blockchain. ECC is ideal for modern SCM-blockchain applications because it is an efficient and robust cryptography technique that results in low CPU, content and network usage and fast encryption processes. Sarfaraz et al. [103] discuss how ECC is useful when speed and security are prioritised needed blockchain-based SCM development.

6.7.5 Vulnerability Threat modelling

A threat model defines a system's defensive measures against malicious actors. In the case of consensus mechanisms, a threat model classifies prospective adversaries into two main categories (external and internal malicious actors). External adversaries refer to entities that are actively attempting to gain unauthorised access to a network. This can be done by illegal entrance attempts or by impersonating confirmed participants. Internal threats occur when authenticated nodes act hostilely due to vulnerabilities. Even with proper credentials, nodes can behave abnormally, as illustrated in Fig 6.20 of a threat model script written to check for a double-spend (i.e. repeating the same transaction) vulnerability. PoE_f would pick it up as an attack handling because transactions are constantly checked for validators' private keys between nodes. Hassan et al. [195] adversaries aim to introduce and distribute fake transactions in blockchain ledgers. This scenario is a blockchain assault, which seeks to compromise the transactional ledger by preventing legal transactions or ensuring fraudulent transactions.

```

110 # Example: Detecting adversarial behavior in consensus (e.g., double-spending)
111 class ThreatModel:
112     def __init__(self):
113         self.transactions = {}
114
115     def detect_double_spend(self, transaction):
116         if transaction["sender"] in self.transactions:
117             if transaction["amount"] > self.transactions[transaction["sender"]]:
118                 print("Potential double-spending detected!")
119                 return True
120             else:
121                 self.transactions[transaction["sender"]] = transaction["amount"]
122                 return False
123
124 # Example usage:
125 threat_model = ThreatModel()
126 transaction1 = {"sender": "0x123", "amount": 100}
127 transaction2 = {"sender": "0x123", "amount": 150} # Adversarial attempt
128
129 threat_model.detect_double_spend(transaction1) # No threat

```

FIGURE 6.20: illustrating snippet of PoEf’s threat model

The analysis conducted in this thesis is predicated on the use of permissioned blockchains, which are distinguished by the presence of secure communication channels that facilitate interactions exclusively among verified participants. Notwithstanding the robust nature of the environment, it is essential to acknowledge that the reputation-based processes governing these blockchains are susceptible to manipulation, as shown by Aluko and Kolonin [196].

Coming out of the systematic analysis in Chapter 4, identifying and analysing a range of potential threats that affect the consensus and other layers of the blockchain. PoEf’s design and threat model make the consensus layer resistant to the following attacks:

- **Attack 1 (Double-Spending):** An adversary conducts concurrent transactions with distinct nodes, attempting to double-spend within the network.

Defence: Sharing transaction validation across many node clusters in PoEf eliminates double-spending because there are continuous synchronising and authentication checks before block finalisation, i.e. many nodes checking transactions and signatures will catch any attempt to double-spend. The multi-layer node topology (containing subordinate and master nodes) makes network deception harder for attackers. Double-spending attacks in SCM can cause inventory tracking errors and payment fraud. PoEf uses a multi-layer node topology, transactions are confirmed by the private key across many trusted nodes before joining the chain. The consensus process synchronises the network, making double-spending efforts obvious. In comparison, PBFT lacks decentralised verification depth, making it more vulnerable to assaults.

- **Attack 2 (Sybil Attacks):** An entity fabricates multiple identities, ostensibly to enhance network resilience but with the ulterior motive of weakening the system's security posture.

Defence: PoEf's reliance on reputation scores and layered nodes (high-authority and subordinate nodes) ensures that any attempt to flood the network with fake identities will be ineffective. Only trusted nodes, based on reputation, can participate in crucial decision-making processes, and attempts to create fake nodes will be easily identified and excluded from participating in the consensus process. In SCM, Sybil attacks could undermine trust by allowing a malicious actor to flood the network with false nodes, potentially corrupting the consensus process or manipulating supply chain data. PoEf incorporates reputation scores and requires nodes to build trust over time before participating in the consensus process. This makes it resistant to Sybil attacks, as fake nodes are filtered out. PBFT lacks such reputation-based systems, making it more vulnerable to Sybil attacks.

- **Attack 3 (DDoS):** Distributed DDoS attacks are coordinated against specific nodes, inundating them with spurious transaction requests to erode the availability.

Defence: PoEf mitigates DDoS attacks by distributing transaction processing across multiple nodes. Using subordinate and master nodes ensures that the failure or overloading of a few nodes does not affect the overall network performance. The shard-based architecture ensures that DDoS attempts targeting specific nodes are less effective, as the overall network can still function with the remaining nodes. A Distributed Denial of Service (DDoS) attack could prevent some nodes from verifying transactions in the supply chain network, leading to delays in transaction processing and data flow disruptions. The shard-based architecture of PoEf distributes the workload across multiple nodes, so if some nodes are targeted in a DDoS attack, the system remains operational. PBFT's centralised structure makes it more vulnerable to DDoS attacks since fewer nodes handle the consensus process.

- **Attack 4 (51% Majority):** The consensus process is targeted by an attacker aiming to co-opt network nodes to influence decision-making.

Defence: The PoEf consensus model uses a hybrid node structure where multiple layers of nodes, both subordinate and master, participate in the validation process. This makes it difficult for any 1 attacker to gain control of more than 51% of the nodes, as the consensus is distributed across several independent layers. This decentralisation makes it harder to co-

opt the network for malicious purposes. In a 51% attack, an attacker could take over the network and rewrite the transaction history, resulting in fraudulent activities like altering shipment records or payments. PoEf’s multi-layered consensus mechanism, involving both subordinate and master nodes, makes it extremely difficult for an attacker to control 51% of the network. PBFT, with its simpler architecture, is more prone to this type of attack due to a smaller node consensus group.

- Attack 5 (Fault Tolerance):** A malicious node masquerades as a benign participant, biding its time until it accrues a sufficient reputation score before launching an attack on the system

Defence: PoEf’s emphasis on reputation scores and node behaviour ensures that a malicious node cannot accrue significant trust or influence in the system. The consensus mechanism is designed to continuously evaluate node performance and behaviour, preventing malicious actors from gaining influence over time. Even if a node initially gains a reputation, any suspicious behaviour will lead to its exclusion from the network’s core decision-making processes. A malicious node could gain trust and compromise the system, leading to incorrect decision-making or supply chain manipulations. PoEf continuously monitors and evaluates node behaviour through reputation scores, quickly identifying and isolating bad actors. PBFT lacks this continuous monitoring, making it more susceptible to long-term trust attacks.

Within the threat model, the adversary is assumed to be limited by resources that make it impossible to break encryption protocols. In addition, the method purposely leaves out terminal attacks and key theft, focussing instead on the more common threats (like DDoS) in blockchain-based supply chains. PoEf’s revised architecture, reputation-based trust, and sharding node layers make it more resilient to these common blockchain consensus vulnerabilities. Owing to this Table 4.2 in Chapter is revised below in Table 6.3 to reflect the addition of PoEf.

TABLE 6.3: illustrating attack resilience of consensus mechanisms (including PoEf.)

| Attacks | DPOS | Pol | Stellar | PoW | PoC | PBFT | PoEf |
|--------------------------------------|-------------|------------|----------------|------------|------------|-------------|-------------|
| <i>Double-spending attack</i> | N | Y | Y | N | Y | Y | N |
| <i>Sybil attack</i> | N | N | N | N | N | Y | N |
| <i>51% Majority Attack</i> | Y | N | N | Y | N | N | N |
| <i>Selfish mining attack</i> | N | N | Y | Y | N | Y | N |
| <i>Bribery Attacks</i> | N | N | N | Y | N | N | N |

6.7.6 Consensus mechanism simulations (with malicious nodes)

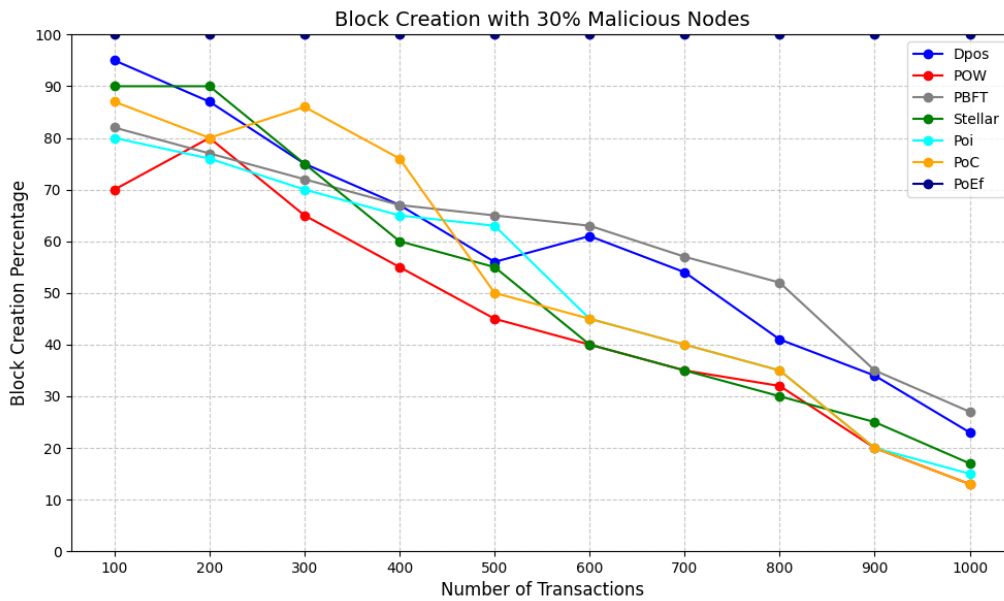


FIGURE 6.21: Block creation with 30% Malicious nodes

A series of experiments were conducted to evaluate PoEf mechanism from a security perspective and compare it to existing consensus protocols involving varying percentages of malicious nodes in the network. As illustrated in Fig. 6.21 and 6.22 these tests simulated two scenarios: one with 30% and another with 45% of the nodes behaving maliciously. The 51% threshold was not considered since in real-world scenario for permissioned blockchains, like the one used in this study, restrict node access, preventing a majority of nodes from being malicious. The experiments revealed the existence and behaviour of malicious nodes across the network.

The figures show that current consensus protocols are degrading; this is because they often focus on processing power, simple selection algorithms, or voting systems for selecting validators without factoring in the reputation of these nodes. In scenarios with a high percentage of malicious nodes, most existing consensus mechanisms show a sharp decline in the ability to create blocks as the number of transactions increases. Mechanisms such as PoW, PBFT, Stellar, and PoC particularly struggle as they rely on simpler validation methods that do not account for the reputation of nodes, making them more vulnerable to attacks by malicious actors. For example, PoC exhibits one of the steepest declines in both scenarios, indicating its inefficiency in maintaining block creation under adversarial conditions. As a result, if a malicious node is selected as a validator, it can process and generate a block, which is then shared with other nodes for validation. Despite the creator's untrustworthiness, other nodes may still validate the block-based solely on hash values and keys.

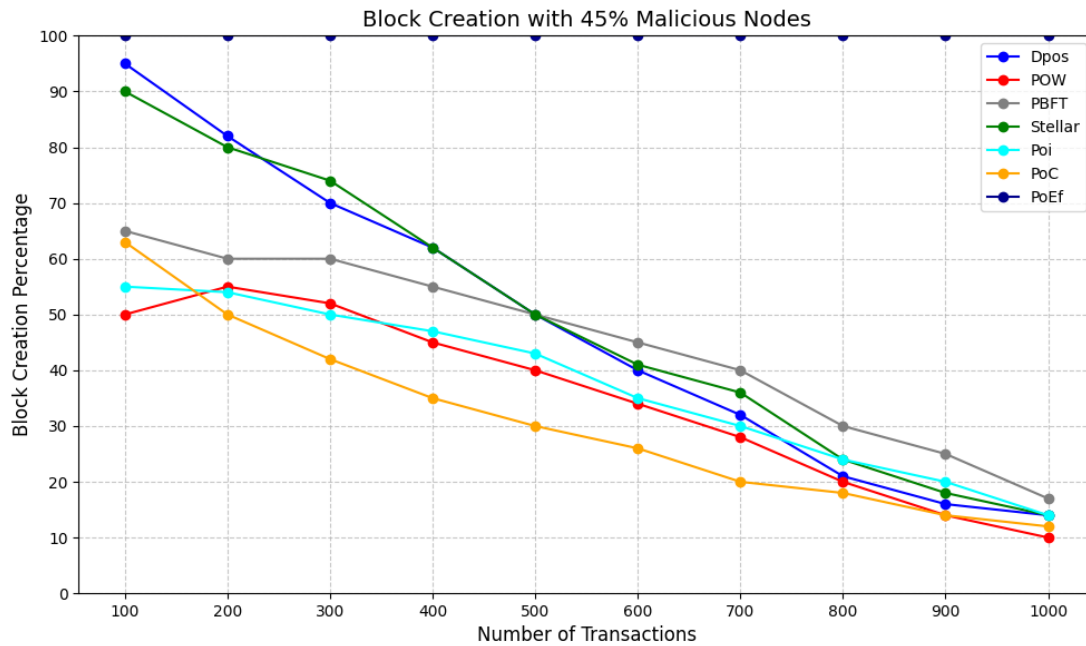


FIGURE 6.22: Block creation with 45% Malicious nodes

The results indicate that increasing the number of rogue nodes diminishes the efficacy of current consensus processes. Nonetheless, PoEf guarantees that only authentic blocks are incorporated into the ledger. PoEf integrates reputation as a fundamental criterion for selecting validators at both levels of the protocol. Moreover, block formation in PoEf is not dependent exclusively on a singular validator. Despite a previously reliable node attaining a high reputation and being elevated to a master node, if it produces fraudulent blocks, the layer of validators will intercept and obstruct the addition of these blocks to the blockchain. In contrast, PoEf has a more resilient block production rate as transaction volumes rise. This corresponds with the prior explanation of PoEf's reputation-driven validator selection, which emphasises reliable nodes for block validation. Despite the presence of numerous hostile nodes, PoEf's layered validation architecture inhibits rogue nodes from seizing control of the network. This graph clearly underscores PoEf's durability and efficiency relative to other consensus mechanisms, particularly in sustaining performance under adversarial conditions.

6.8 Chapter Summary

The PoEf consensus mechanism represents a novel advancement over its predecessor, PBFT. It addresses some of the traditional consensus mechanism's inherent scalability and efficiency limitations. While PBFT (a predominant consensus used in SCM) effectively ensures consensus in blockchain-based systems using fault tolerance, it struggles with high latency and throughput

degradation as network sizes and transaction volumes increase. PoEf introduces a more layered, structured approach (see figure 6.2), distributing responsibilities across authentication, validator, and subordinate nodes to optimise performance and security.

In PoEf, authentication nodes serve an important role to verify the legitimacy of nodes participating in the consensus process. Validator nodes then focus on validating transactions, ensuring integrity before they confirm are appended to the blockchain. Subordinate nodes handle the majority of transaction processing and consensus voting. This delegation of duties streamlines the consensus process and reduces the communication overhead seen in PBFT, leading to improved scalability and lower latency. Separating responsibilities among different node types allows PoEf to scale more effectively, even as the number of transactions and network size grows. Simulation results have shown that PoEf consistently outperforms PBFT in terms of throughput and latency, particularly in larger networks. This makes PoEf an ideal consensus mechanism for SCM systems, where the ability to process large volumes of transactions across distributed nodes is essential. In SCM, where data integrity, speed, and scalability are paramount, PoEf's efficient handling of transactions ensures that goods and services are tracked accurately and in real-time without bottlenecks or delays caused by consensus inefficiencies.

On the security side, PoEf's layered architecture is fortified by a threat model that allows the mechanism to circumvent common blockchain vulnerabilities. PoEf circumvents double-spending, Sybil attacks, DDoS attempts, 51% majority attacks, and fault tolerance exploitation through a combination of reputation-based node selection, distributed workload management, and constant node verifications. Its multi-layered consensus mechanism ensures that no single entity can compromise the system, unlike PBFT, which is more vulnerable to Sybil and 51% attacks due to its structure. By continuously evaluating node behaviour and leveraging sharding techniques, PoEf improves network security while maintaining efficiency.

Based on the experiments, PoEf is a novel, efficient consensus mechanism that builds upon the foundations of PBFT but outperform it in both efficiency and security and is applicable to high-demand SCM environment.

7 Evaluation and Discussion

7.1 Overview

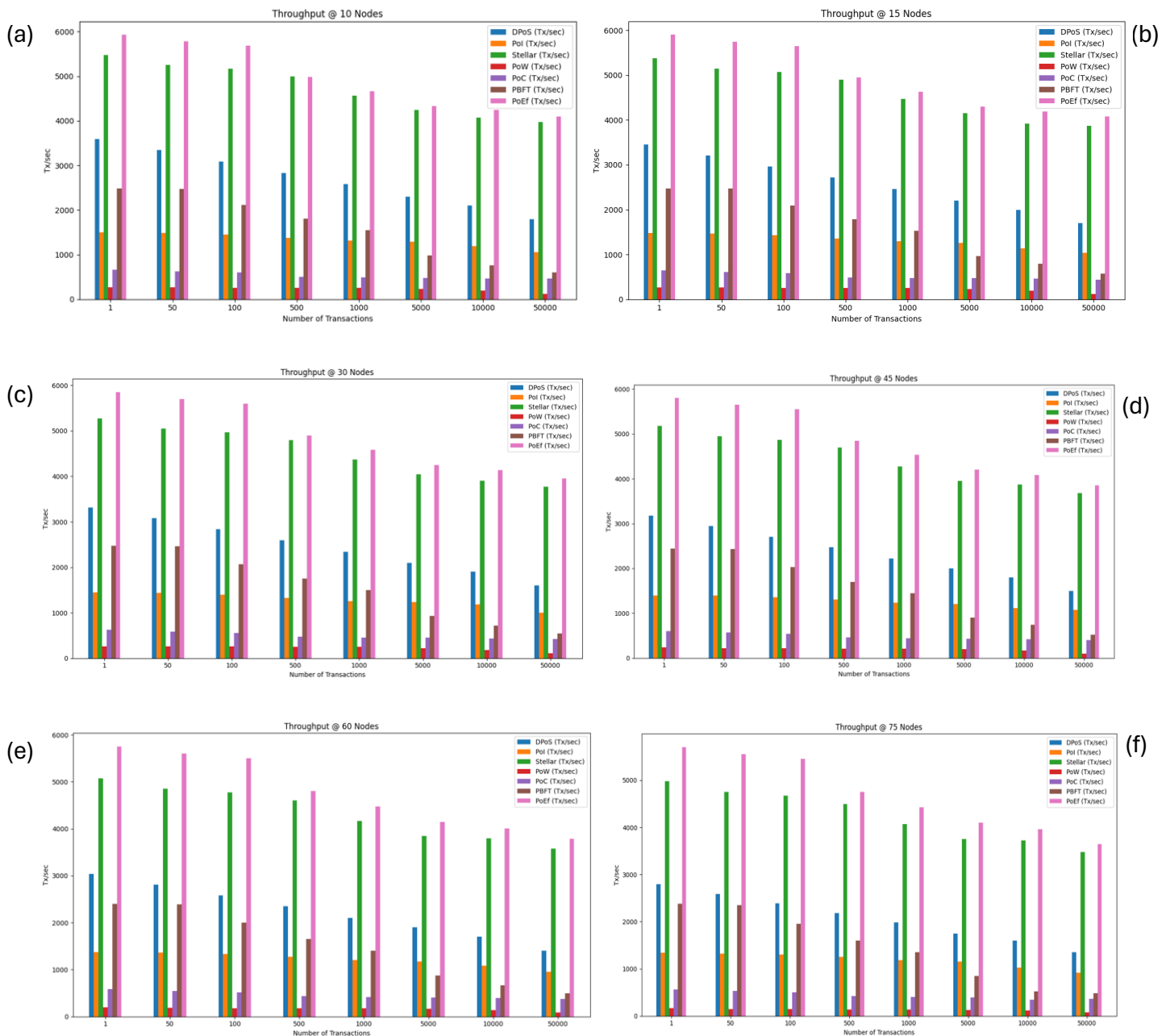
Chapter 7 presents a comparison of consensus mechanisms, including Proof of Work (PoW), Delegated Proof of Stake (DPoS), Stellar, Practical Byzantine Fault Tolerance (PBFT), Proof of Importance (PoI), and the novel Proof of Efficiency (PoEf). The experimental findings are derived from a series of 896 individual simulation runs focusing on the key performance metrics of efficiency: latency, throughput, and scalability. At the core of this analysis is the PoEf consensus mechanism, designed to outperform traditional methods, particularly in blockchain-based SCM applications. The PoEf mechanism notably improves increased throughput (data processing speed), reduced latency (time delay), enhanced scalability, and robust security. These improvements are essential for modern SCM systems, which require real-time data processing to maintain operational efficiency. The results show that PoEf consistently outperforms traditional consensus mechanisms across all performance metrics, processing transactions at a higher rate. It maintains low latency across scaling network sizes and transaction volumes, making it scalable for small and large supply chain networks. Key metrics in this chapter include:

- **Throughput:** Evaluates the transaction processing capacity of mechanisms across different network sizes (10-200 nodes) and transaction volumes (1-50,000 transactions).
- **Latency:** Assessing the system's responsiveness by comparing the time a transaction takes to be confirmed and recorded.
- **Scalability:** Demonstrating how well these mechanisms handle increasing network sizes and transaction volumes.

Subsequent sections in this chapter break down the performance of each consensus mechanism in terms of throughput, latency, and scalability. Special attention is given to the comparative performance of PoEf and Stellar, which are derived from the PBFT consensus method and show comparable simulation results. The comparison emphasises PoEf's consistently high performance across all metrics, especially in larger networks.

7.2 A Comparison of Throughput

Throughput is a key component in assessing the efficiency of blockchain-based SCM systems. The consensus mechanism selected has a major effect on the blockchain's transaction processing rates, which in turn affects the supply chain's overall capacity and ability to manage high transaction volumes. To choose a consensus mechanism that best fits the demands of the supply chain, an analysis of the SCM's blockchain architecture, the consensus mechanism used, and the throughput capacity is needed.



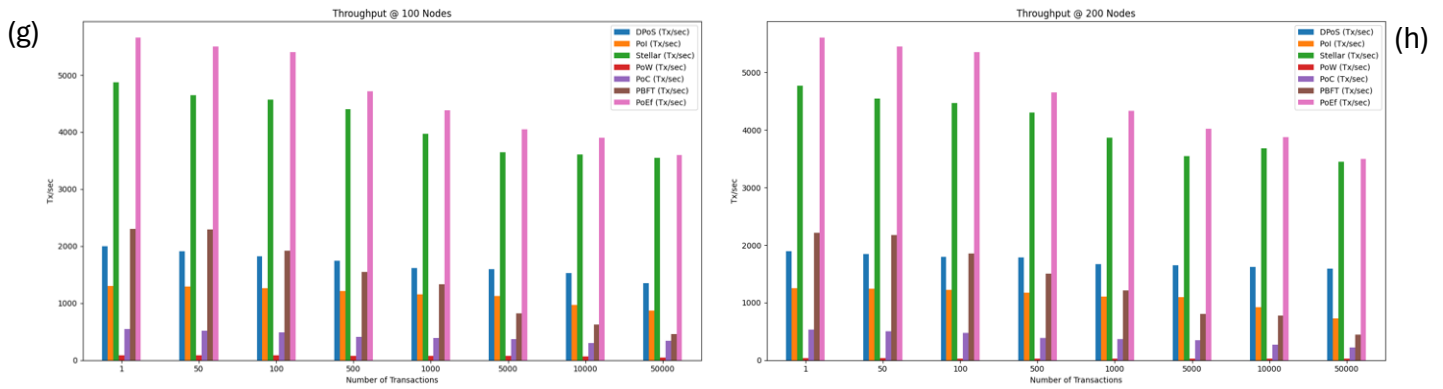


FIGURE 7.1(a-h): illustrating consensus throughput comparison at scaling network size

Figure 7.1(a-h) shows throughput changes with different consensus methods, such as DPoS, Pol, Stellar, PoW, PoC, PBFT, and PoEf, with varying network sizes (10 to 200 nodes) and transaction volumes (1 to 50,000). PoEf and Stellar, consensus methods designed from the traditional PBFT, both have the best throughput across all network sizes, which shows that they can be scaled up and down quickly, which is especially important in supply chain settings with many transactions. PoEf consistently outperforms PBFT and Stellar across all network sizes and transaction volumes.

PBFT offers decent performance, especially in smaller networks, but its throughput decreases more rapidly than PoEf and Stellar as the network scales. For example, at 10 nodes, PBFT processes ~2,500 Tx/sec with 1 transaction sent to the system, but its throughput declines more sharply as the number of transactions increases. At 50,000 transactions, PBFT's throughput is only 600 Tx/sec. PBFT's architectural limitations, particularly in communication overhead and node synchronisation, become evident in larger networks, making it less suitable for large SCM networks that require high throughput. PBFT faces significant scalability challenges with 200 nodes and 50,000 transactions as its throughput is reduced to ~450 Tx/sec. This limitation can be attributed to PBFT's reliance on a consensus process that requires multiple rounds of communication among all nodes to reach an agreement, leading to communication overhead. Its performance degradation in large, dynamic networks with high transaction volumes would pose a challenge. Stellar, on the other hand, exhibits strong performance in smaller networks as well. With 10 nodes, it processes 5,000 Tx/sec with one transaction and maintaining a higher throughput in smaller transaction ranges than PBFT. However, as the network grows, its throughput similarly declines. At 200 nodes and 50,000 transactions, Stellar manages only 3,450 Tx/sec. For SCM applications, which may involve complex and large-scale networks with a high number of participants (in this case, 200 nodes), Stellar's throughput becomes less competitive at these network sizes, especially when the transaction volume is also

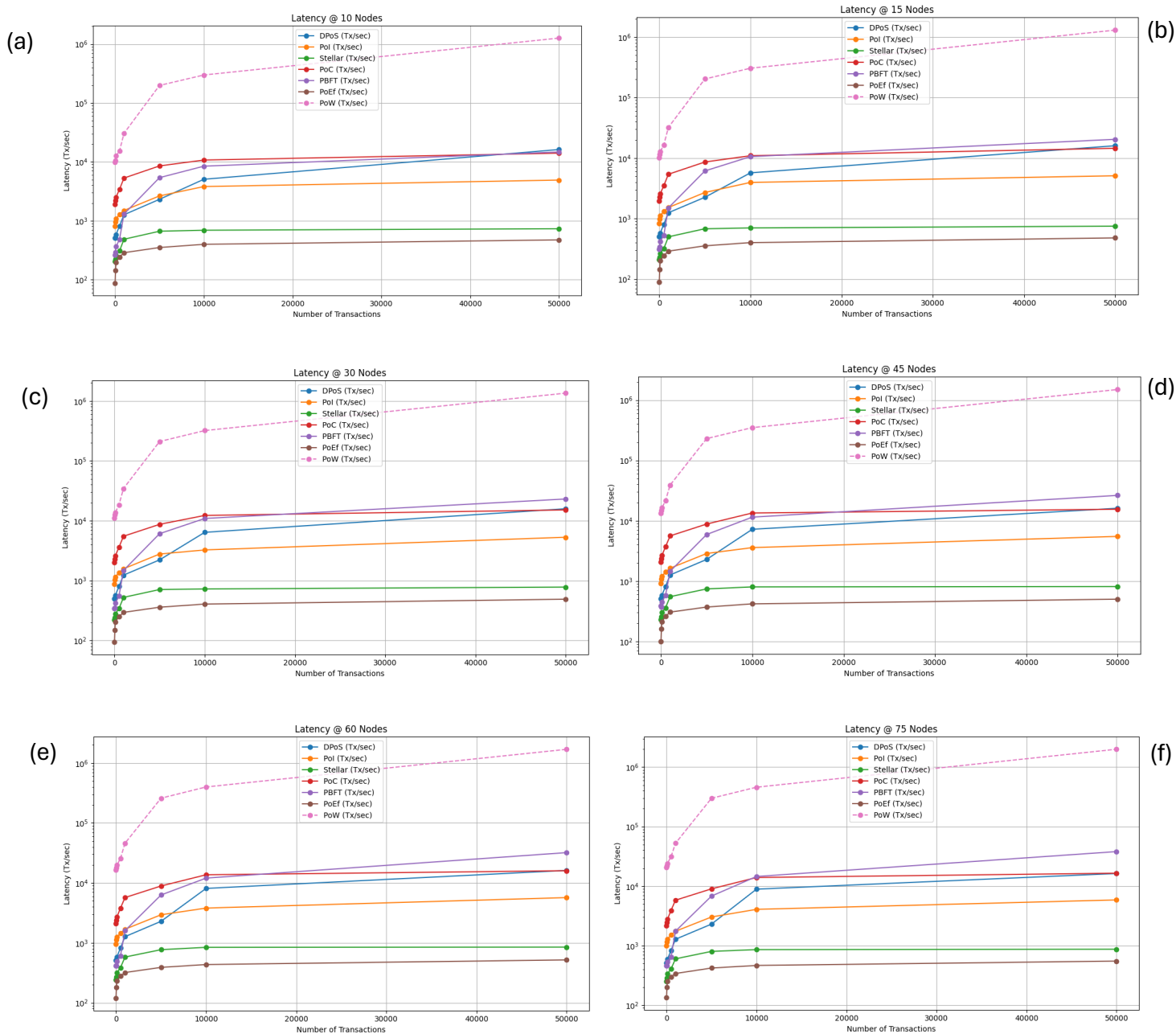
large (>10,000 transactions). Its reliance on quorum slices for consensus introduces delays as more nodes are added to the network.

PoEf stands out with consistently high throughput across all scenarios, making it highly suitable for environments like SCM, where real-time processing, scalability, and efficiency are critical. Its superior performance across varying node sizes indicates it can handle large-scale, dynamic networks without significantly dropping throughput. For instance, with 10 nodes (Fig. 8.1a) and one transaction, PoEf can process ~6,000 Tx/sec while maintaining high throughput even as the transaction volume scales. At 200 nodes and 50,000 transactions, PoEf still processes ~3,500 Tx/sec when there's more communication on the network. PoEf's efficiency in large, dynamic environments makes it the superior choice for large SCM applications. Its ability to maintain high throughput, even as the network and transaction volumes scale, ensures it can handle global supply chains' complexities and demands. Additionally, from a security perspective, PoEf's permissioned structure allows for greater control over participants, ensuring that only trusted entities participate in the consensus process, which is crucial for supply chain integrity. Each shard handles a portion of the overall workload, and consensus is reached within smaller subgroups of nodes, significantly reducing communication overhead and ensuring that the consensus process remains efficient, even in large networks.

Other consensus mechanisms, such as PoW and PoC, exhibit much lower throughput in all network configurations, significantly as the number of nodes and transactions increases. The inefficiency in handling large-scale networks and high transaction volumes limits the suitability for SCM, where real-time, high-throughput processing is vital. DPoS and Pol also perform moderately but fall short in scalability compared to PoEf and Stellar, highlighting the constraints in managing high-volume networks. PoEf's efficiency, followed by Stellar, makes these mechanisms particularly promising for supply chain management applications, where throughput and scalability are essential for maintaining smooth and reliable operations across a distributed network. The PoEf mechanism is a notably efficient solution, providing higher throughput than traditional and contemporary consensus mechanisms. Its integration into SCM systems can potentially enhance the overall efficiency and scalability, accommodating the evolving needs of modern supply chains.

7.3 An Evaluation of Latency

Latency is a metric that quantifies the duration between the commencement of a transaction and its final inclusion into the ledger. The simulations evaluated the timestamps of transactions recorded at the commencement of transactions with those at the stages of validation and integration into the ledger. This statistic's significance lies in its capacity to assess the agility (i.e., efficiency) of the blockchain network, offering an illustration of the dynamics involved in transaction processing.



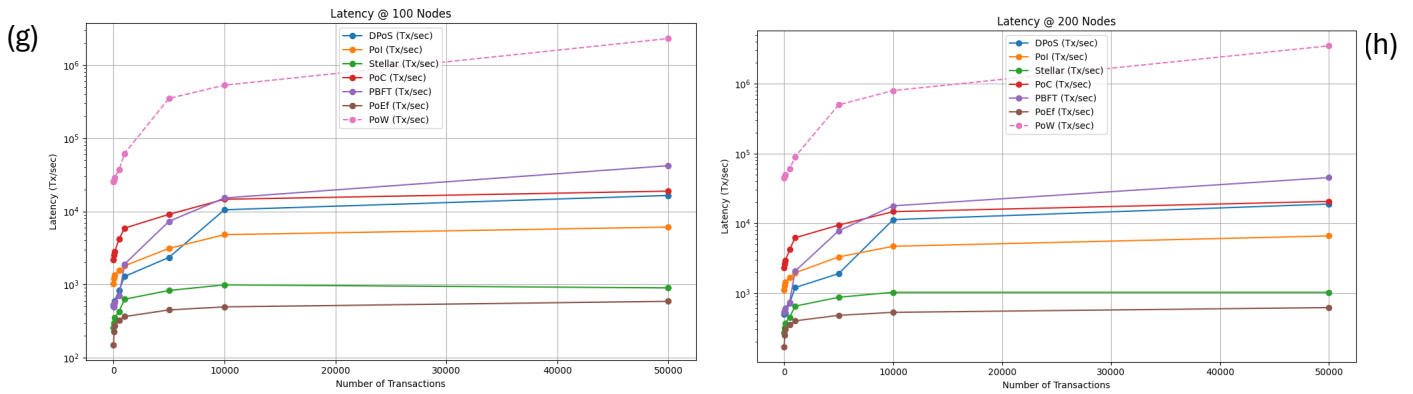


FIGURE 7.2(a-h): illustrating consensus latency comparison at scaling network sizes

FIGURE 7.2(a-h) illustrates a latency comparison across various consensus mechanisms as network sizes and transaction volumes scale. A similar comparison is made with the PoEf, Stellar, and the PBFT consensus, which are both built on. PoEf consistently demonstrates lower latencies than other consensus mechanisms, making it ideal for SCM applications requiring high throughput and quick transaction processing. Even at 200 nodes and 50,000 transactions, PoEf maintains a relatively low latency of just over 600 milliseconds, demonstrating its scalability and efficiency. This performance is needed for large and dynamic SCM systems that rely on high throughput and low latency to maintain operational efficiency and quick decision-making. The multi-layered architecture of PoEf, combined with its shard-based processing, allows it to manage large networks and high transaction volumes without experiencing significant latency degradation, making it the most suitable option for SCM compared to PBFT and Stellar. Stellar follows behind with low latencies compared to PBFT and other mechanisms in this research. For example, at 200 nodes and 50,000 transactions, Stellar's latency is still over 6,600 milliseconds, making it less ideal for large SCM applications that demand faster processing times. The PBFT mechanism, while competitive in smaller networks, performance degrades as node count and transaction volumes increase, leading to higher latencies. For instance, at 200 nodes and 50,000 transactions, PBFT's latency surges to over 45,000 milliseconds, which is problematic for large-scale SCM systems that require faster transaction finality.

Throughout Figures 7.2(a-h), PoW and PoC show extremely high latencies due to the computational requirements, making them less suitable for real-time systems. DPoS and PoI manage low latencies in smaller networks but face scalability challenges as network size grows. Overall, PoEf's maintenance of a comparatively low latency across varying scales while processing high transaction volumes makes it an ideal candidate for large-scale SCM systems, where delays could have a cascading effect on the efficiency of the supply chain.

7.4 An Evaluation of Scalability.

Scalability refers to a consensus mechanism's ability to maintain effective performance (high throughput or low latency) as the number of transactions or network size increase. It is typically evaluated through transaction throughput (Tx/sec) or latency (ms). In the context of SCM systems, scalability is important because as supply chains increase in size and complexity, the consensus mechanism must handle an increasing load without significant degradation in performance.

7.4.1 Scalability Throughput

Figure 7.3 compares throughput performance across consensus mechanisms with increasing network size and number of transactions. The chart provides a comparison of the throughput (Tx/sec) across various consensus mechanisms (DPoS, PoI, Stellar, PoW, PoC, PBFT, and PoEf) at different network sizes (30, 100, and 200 nodes) to represent how the mechanisms would operate in a small, medium and large-sized SCM-system.

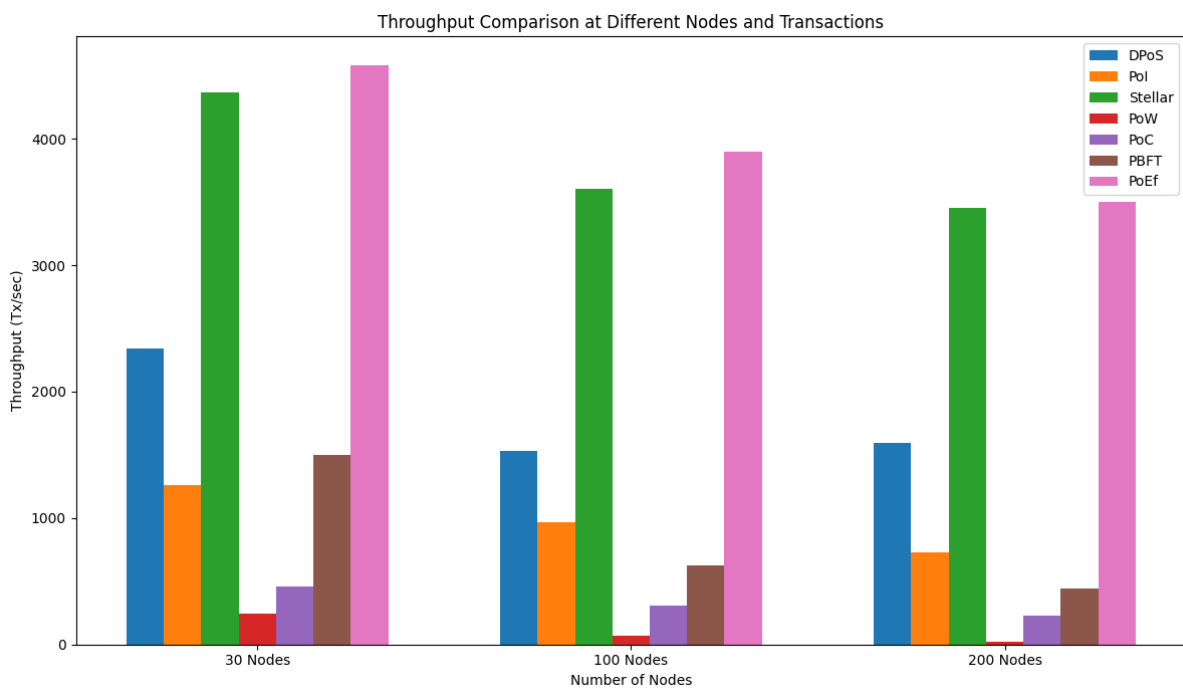


FIGURE 7.3: illustrating Consensus Mechanisms Scalability (throughput) comparison

@30 Nodes (Small Network)

Stellar and PoEf consistently stand out as the top performers in terms of throughput, both surpassing 4,000 Tx/sec. Stellar demonstrates remarkable efficiency, particularly in smaller networks, where its consensus mechanism operates with speed and reliability. However, PoEf leads with the highest

throughput overall, likely attributed to its hierarchical node structure, which streamlines communication and optimises performance across the network. In contrast, DPoS and PoW exhibit more moderate throughputs, ~2,000 Tx/sec or below. While these mechanisms show decent scalability, they cannot match the performance of Stellar or PoEf, particularly as network size increases. On the other hand, PBFT and Pol deliver comparatively lower throughput, a result of the increased communication and coordination overhead intrinsic to Byzantine fault-tolerant protocols. These protocols prioritise security and fault tolerance, which comes at the cost of performance, making them less scalable in environments that demand high throughput. This distinction becomes more important when evaluating which consensus mechanism is better suited for different scales of SCM systems, where throughput plays a key role in operational efficiency.

@100 Nodes (Medium Sized Network)

PoEf consistently delivers the highest throughput as the number of nodes increases, demonstrating its ability to handle growing transaction loads without significant performance degradation. This layered structure enables PoEf to manage transactions efficiently, making it a good choice for medium-sized SCM systems where scalability and transaction processing are essential. Stellar follows closely behind, maintaining solid throughput levels, though it does experience some decline as the network size increases. Despite this, Stellar remains highly effective in managing transactions in mid-sized supply chains. PBFT, while showing some improvement, needs to be at most 2,000 Tx/sec, highlighting its challenges in scaling effectively within larger networks. This limitation reflects the communication overhead of Byzantine fault-tolerant protocols, which affects its performance as node numbers grow. Meanwhile, PoW continues to exhibit relatively low throughput, likely due to its high computational requirements. These demands make PoW less efficient in handling the higher transaction volumes needed for SCM systems, where speed and scalability are essential. Overall, PoEf's superior scalability positions it as the ideal choice for systems requiring high throughput across expanding networks.

@200 Nodes (Large Network)

PoEf, is the leading consensus mechanism, showcasing remarkable scalability and maintaining high throughput even as the network size expands. This exceptional performance makes it a prime candidate for large SCM systems that need to process many transactions (over 10,000) quickly and efficiently. Stellar, while continuing to perform well, experience a slight decline in throughput as the network grows, likely due to the increasing complexity of maintaining consensus across a larger number of nodes. Despite this, Stellar remains a strong contender for medium-sized SCM systems.

On the other hand, PBFT and PoI struggle significantly to scale, with the throughput decreasing even more as the network expands. This performance limitation indicates that PBFT and PoI may not be ideal for large SCM systems, where speed and high transaction volume are essential for seamless operations. The differences in scalability between these mechanisms underscore the importance of selecting the right consensus mechanism based on the size and needs of the SCM system.

7.4.2 Scalability Latency

Figure 7.4 compares latency performance across consensus mechanisms with increasing network size and number of transactions. The graph provides a comparison of the throughput (Tx/sec) across various consensus mechanisms (DPoS, PoI, Stellar, PoW, PoC, PBFT, and PoEf) at different network sizes (30, 100, and 200 nodes).

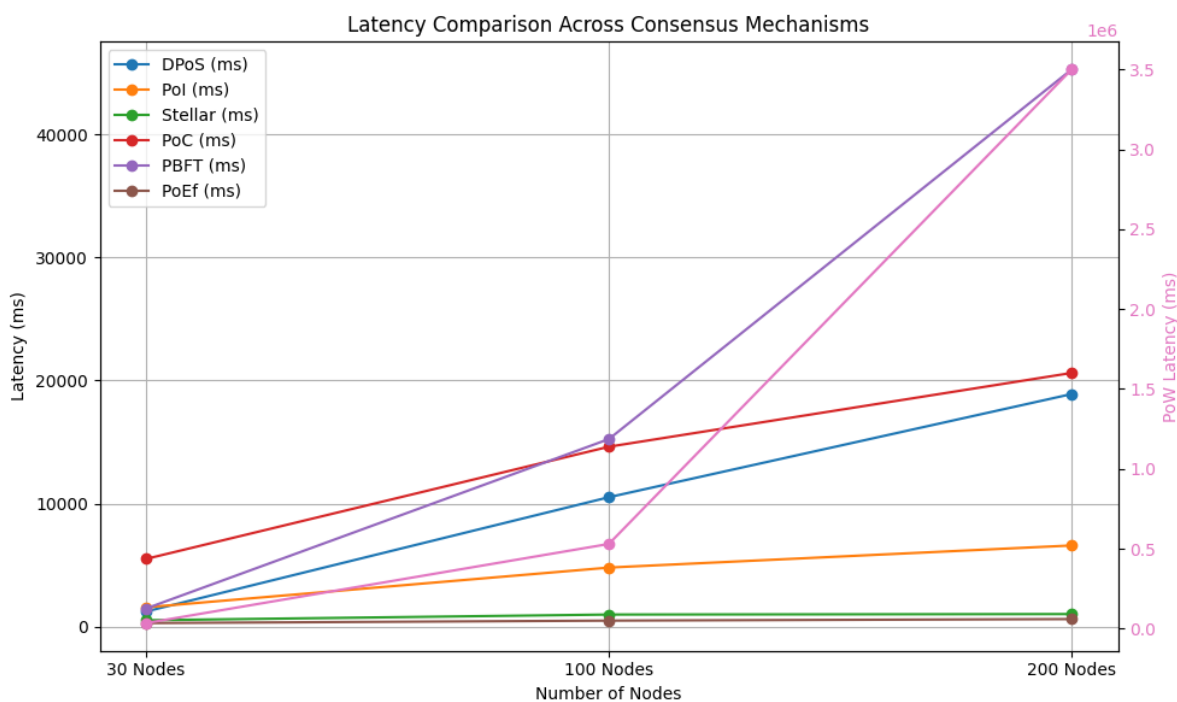


FIGURE 7.4: Figure illustrating Consensus Mechanisms Scalability (latency) comparison

The latency comparison across the consensus mechanisms in Fig.7.4 highlights significant differences in how they scale with increasing nodes. PoW exhibits the most extreme increase in latency, surpassing 1 million milliseconds by 200 nodes, largely due to its computationally heavy proof-of-work process, which demands significant resources to solve cryptographic puzzles. This results in inefficient handling of large networks, making PoW unsuitable for time-sensitive SCM operations where rapid transaction processing is crucial.

On the other hand, PoEf and Stellar maintain impressively low latencies across all network sizes. PoEf's hierarchical and layered structure, where validation is distributed across subordinate and master nodes, helps ensure that latency remains minimal even as the number of nodes grows. Stellar's federated Byzantine agreement (FBA) also performs efficiently, keeping latency low due to its use of quorum slices that allow nodes to reach consensus quickly without requiring full network coordination. At 200 nodes, Stellar manages a latency of 1,028ms, which, although higher than PoEf, still outperforms other mechanisms significantly. Both are strong mechanisms for SCM systems, particularly in large or dynamic environments where scalability and low latency are paramount. PBFT and PoC show moderate latency increases. PoC and PBFT experience further latency increases to 20,615ms and 45,265 ms, respectively, at a network size of 200 nodes, indicating the inefficiency in managing large-scale SCM networks. PBFT, while effective for smaller networks, suffers from communication overhead as nodes increase, slowing down decision-making and thus driving up latency. This makes PBFT more suitable for small- to medium-sized SCM systems where node count and transaction volume are more contained. PoC similarly sees rising latencies due to the complexity of verifying large transaction sets, making it less suitable for highly scalable or high-throughput scenarios. DPoS and PoI continue to degrade, with latencies of 18,900ms and 6,600ms, respectively, further demonstrating the limitations.

The implications for SCM are clear: in large-scale supply chain networks, consensus mechanisms like PoEf and Stellar, which can scale while maintaining low latency, are far better suited to handle the increased demand. In contrast, PoW, PBFT, and PoC may struggle to meet the performance, and scalability needs of modern supply chains, particularly as node numbers and transaction volumes grow. Efficient and fast transaction processing is crucial for keeping up with supply chains' dynamic and high-volume nature, underscoring the importance of selecting the "ideal" consensus mechanism based on these metrics.

7.4.3 Overall Scalability Assessment

The simulations identified Stellar and PoEf consensus mechanisms exhibited noteworthy performance, as they showed low-efficiency disruption despite the increase in the number of nodes. For small SCM systems, where the number of nodes is typically fewer (up to 30), and transaction volumes are low (1 - 1000 transactions), scalability is less of a pressing concern. Most consensus mechanisms can manage these relatively simple configurations without sacrificing performance. Mechanisms such as PBFT, Stellar, and PoEf all demonstrate the ability to maintain acceptable throughput and latency

for these smaller networks. However, as these systems grow, the performance gap between these mechanisms starts to widen, particularly in latency and throughput. Medium SCM systems involving 30 to 100 nodes, and 1000 to 10000 transactions start to demand more scalable solutions. The growing transaction volumes and increased node participation require a consensus mechanism that can balance throughput and latency to avoid bottlenecks in decision-making processes. In our simulations, mechanisms like PBFT begin to experience higher latency and reduced throughput at these levels, signalling scalability challenges. Stellar performs relatively better in terms of throughput but struggles with increasing latency. PoEf, however, continues to deliver consistent throughput and low latency, demonstrating that it scales more effectively for medium-sized SCM systems. Scalability becomes a defining factor for large SCM systems, where the network can consist of over 100 nodes and transaction volumes exceed 10000 transactions. These systems require a consensus mechanism to handle high transaction volumes without delays or performance degradation. As our simulations indicate, PBFT begins to struggle significantly with both throughput and latency in large configurations. However, PoEf and Stellar maintain high throughput and low latency, making them the most scalable and efficient choice for large SCM systems. Its ability to handle growing networks and transaction volumes without sacrificing performance ensures smooth and efficient operations across the supply chain, even as the system expands in size and complexity.

PoEf and Stellar demonstrate strong performance in our simulations, offering unique advantages in throughput and latency. However, factors beyond raw performance metrics should be considered when evaluating which consensus mechanism is better suited for SCM's evolving needs. In particular, the security trade-offs should be considered.

7.5 PoEf's comparison with Stellar

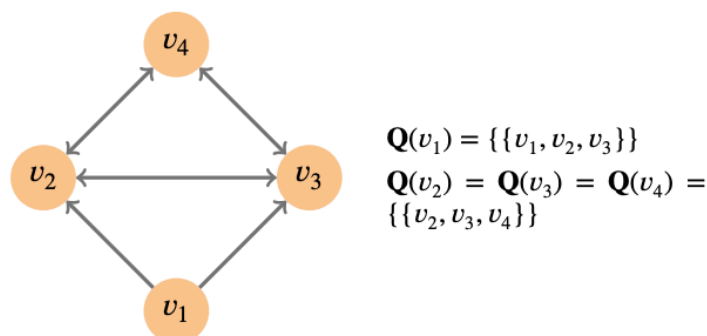


FIGURE 7.5: illustrating Stellar Consensus mechanism node operation [197].

The experimental results in this thesis show that the Stellar consensus process is a lot like PoEF in terms of efficiency. This means that the node actions in Stellar should be examined to see the trade-offs. It is emphasised in Chapter 2 that the Stellar consensus mechanism, like the PoEf, is developed from the primary PBFT consensus mechanism. Stellar also uses a tiered node setup that segregates nodes into smaller groups for consensus agreement, but the consensus method is different in both mechanisms. In Stellar, as illustrated in Fig. 7.5, the nodes are organised into groups called quorums. For there to be agreement on a decision, like approving a transaction, there must be a quorum of nodes or stakeholders who agree on it. A quorum slice is the part of a quorum that convinces one node to agree. Figure 2 illustrates a Stellar node structure of four nodes. Each node has a single slice, and the lines show how it is connected to the other parts of that slice. How it works is if Node v1, which includes {v1, v2, v3}, gets a transaction, it would only need nodes v2 and v3 to reach consensus. However, node v4 is included in the slices of nodes v2 and v3, which means that node v2 and node v3 can only approve a transaction with node v4's approval. Because of this, consensus can't happen without v4, and the only group that has v1 is made up of all five nodes: {v1, v2, v3, v4}. In a normal PBFT, all nodes must agree on the same slices, which means that $\forall v1, v2, Q(v1) = Q(v2)$. PBFT doesn't differentiate between slices, quorums (in Stellar), or shards (in PoEf) because every member agrees with every slice.

When comparing PoEf to Stellar, the fact that membership and shards in PoEf need to be approved first makes the setting more controlled and restricted. Stellar's network is open, so anyone can join without getting permission. This decentralised and open approach is essential in supply chain management because the efficiency is determined by the stakeholders (nodes) participating in consensus processes, data exchange, and transactions. PoEf permission model, where nodes must be checked and approved before joining the network and validating transactions, ensures that only trustworthy parties, like makers, suppliers, and logistics providers, can decide or reach an agreement. It creates a closed, safe space needed for managing the supply chain. Its members are already known companies with a history of doing business with each other. Stellar is a good choice for applications focusing on financial inclusion, cross-border payments, and decentralised finance (DeFi) because its open and decentralised network design lets any stakeholder join and participate in the consensus process. PoEf's slightly better performance is due to the events on its nodes. While PoEf and Stellar's FBA quorum model work well for large SCM systems to reach consensus, Stellar's model divides nodes into smaller groups and lets nodes trust each other more freely. Still, it doesn't have the hierarchical structure that PoEf does because consensus needs agreement from all nodes. PoEf's shard-based design, which considers stakeholders' reputation level score, makes

transaction handling faster by splitting up work among several nodes that can check and confirm transactions based on reputation.

7.6 Additional comparison of the PoEf Model with similar models

Building upon the comparative analyses previously presented, the PoEf mechanism can be further compared to other consensus methods based on the reputation of the nodes. The Proof-of-X-Repute (PoXR) and the Reputation Proof of Cooperation (RPoC) techniques, as described by Wang et al.[198] and Sarfaraz et. Al [103], respectively, serves as a comparative benchmark to the PoEf mechanism. Both the PoXR and the RPoC protocols employ a consensus technique predicated on the reputation scores of network nodes and streamlining the process of achieving consensus within a public blockchain context. It is important to note a significant discrepancy between the technical design and operational paradigms of PoEf, PoXR and RPoC. The foundation of PoEf is initially based on prior and ongoing experience built on the supply chain assessment model OTIF. At the same time, the PoXR comprises a conventional protocol resembling PoW, supplemented by an additional layer of reputation. The RPoC is solely based on reputation ratings during transactions in the blockchain. Similarly to PoEf, both the PoXR and RPoC protocols operate on the principle that the probability of a truthful validation of the following block is directly proportional to a node's reputation. Consequently, this process inherently exhibits an iterative nature. Furthermore, PoXR has challenges in upholding user privacy due to the capacity of users to obscure the identities, hence potentially dodging accountability for participating in hazardous behaviours.

To validate the PoEf mechanism and establish a fair comparison, Table 7.1 gives a side-by-side analysis of PoEf, PoXR, and RPoC average throughputs at 1000 transactions. PoEf throughput was averaged over eight different network sizes (10-200 nodes), but the network size for RPoc was not available and experiments with PoXR was ran with only 4 nodes (in 2020).

Table 7.1: illustrating a throughput comparison for Reputation-based consensus.

| Consensus Mechanism | Average Throughput (TPS) @1000 |
|----------------------------|---------------------------------------|
| PoXR | 4100 |
| RPoC | 5400 |
| PoEf | 4504 |

Neither PoXR nor RPoC is a widely recognised or standard consensus mechanism in the blockchain community. This means that specific data regarding the maximum throughput is not readily available. The limited publicly available data for PoXR and RPoC were evaluated in a standardised operating environment, precisely a public network context. Table 7.1 illustrates that the average throughput performance of PoXR is ~4100 TPS between 1 and 1000 transactions and ~5400 RPoC. Assessing the PoEf data for a similar number of transactions gives an average of ~4504 TPS. Each comparative throughput performance is identical. However, each has a different approach to reaching consensus. PoXR focuses on validating the efficient execution of computational tasks, where nodes compete based on how efficiently they execute tasks. The approach is similar to PoW and demands significant computational resources, leading to high energy consumption and potential delays as the network grows. PoXR achieves an average throughput of ~4100 TPS @ 1000 nodes, which would be suitable for medium to large-sized networks, though it may slow down with more transactions and nodes due to its resource-intensive competition. RPoC reaches consensus based on the reputation nodes build over time through successful contributions, such as transaction validation. While reputation incentivises good behaviour, the intertwined reputation and consensus layers create computational overhead. RPoC achieves a higher throughput of ~5400 TPS, but the need for constant reputation updates with the same node can slow down the consensus process. PoEf takes a different approach by separating tasks among different node types in a hierarchical structure. Subordinate nodes handle simpler tasks; validators ensure accuracy, and higher-authority nodes finalise the consensus. By separating reputation calculation from the consensus layer and using sharding, PoEf maintains an average throughput of ~4504 TPS, balancing scalability and efficiency. While slightly lower than RPoC, PoEf's design makes it as scalable for large networks, as it reduces computational load and improves transaction handling.

Simulating each mechanism under similar conditions, with particular emphasis on resilience, should prove notable outcomes comparing each mechanism. The research findings support the notion that the PoEf model displays a slight advantage over PoXR but underperforms compared to RPoC in terms of throughput for 1000 transactions. These values could differ as the network or number of transactions grows. Insights from a validation process could strengthen the effectiveness of PoEf in real-world scenarios and establish it as a more feasible option when both high throughput efficiency and robust security are of utmost importance.

7.7 Decision Matrix

The ideal consensus mechanism for SCM depends on specific needs, such as its ability to handle scaling transaction volumes, processing speed, growth expectations, and security requirements. The consensus mechanisms explored each imparts distinct influences on the security and efficiency of blockchain-integrated SCM systems. The experiments' upper and lower limits were categorised and tabulated across different ranges to classify and guide the performance of consensus mechanisms based on the throughput, latency, and scalability. The classification and justification of the ranges illustrated in Table 7.2 are based on the observed performance of various consensus mechanisms under increasing network sizes and transaction volumes. By categorising these ranges, manufacturers interested in the technology can understand how different mechanisms perform regarding throughput, latency, and scalability. The specific ranges were chosen to reflect realistic performance boundaries observed during simulations and experiments in SCM contexts and blockchain networks.

Table 7.2: codifying throughput, latency and scalability into different categories

| Range | Throughput (TPS) | Latency (ms) | Scalability Score |
|------------------|--------------------|--------------------|-------------------|
| Very Low | Less than 500 TPS | Less than 500 ms | 0 - 1 |
| Low | 500 – 1500 TPS | 500 - 1000 ms | 1 – 3 |
| Medium | 1501 – 3000 TPS | 1001 - 5000 ms | 3.01 – 6.0 |
| High | 3001 – 5000 TPS | 5001 - 15000 ms | 6.01 – 8.0 |
| Very High | More than 5000 TPS | More than 15000 ms | Above 8.0 |

7.7.1 Proof of Work (PoW)

PoW is famous for its robust security system, making it an essential part of the blockchain ecosystem, especially in use cases where keeping data safe is a priority. However, because it has low throughput and high latency, it is not as good for SCM systems that need to handle many transactions quickly. With a maximum throughput of only ~300 TPS and a lowest latency of ~ 9800, PoW is Very Low based on the categorisation and is unsuitable for environments with high transaction volumes. Its mining process is resource-intensive, which can lead to inefficiencies for high-throughput SCM systems, but security characteristics come from this same mining process. High delays and inefficient operations can slow down the supply chain, making it harder for SCM to do real-time tracking and inventory management. So, while PoW offers robust security, its scalability limitations make it unsuitable for large SCM systems.

7.7.2 Delegated Proof of Stake (DPoS)

DPoS scales well by delegating the consensus process to a few elected nodes, which reduces communication overhead. With a high throughput of ~3600 TPS and a latency low of ~500 at a network size of 10 nodes with 1 transaction, the mechanism performs reasonably well. In DPoS, nodes are elected to participate in the consensus process, limiting the number of nodes involved in resolving transactions and improving efficiency. An increased network size doesn't affect the performance metrics, but with an increased number of transactions (up to 50000 transactions), that throughput drops to a low of 1800 and latency a high of ~16000; this could be because of only a few elected nodes resolving transactions. So, DPoS is efficient in networks that don't have a lot of transactions. In addition, from a security perspective, DPoS faces centralisation risks [199], as a few nodes are responsible for validation, which could compromise decentralisation in large networks. Therefore, DPoS is best suited for small to medium SCM systems.

7.7.3 Practical Byzantine Fault Tolerance (PBFT)

The PBFT consensus offers a high-throughput, low-latency solution ideal for small to medium SCM systems. For small SCM systems, where the network typically consists of fewer nodes (10 to 30 nodes) and lower transaction volumes, PBFT demonstrates stable performance. With a throughput of around 2400-2500 TPS and low latency (264ms for 1 transaction and 1294ms for 1000 transactions at 10 nodes), PBFT is suitable for environments that do not require extensive scaling. This makes it a good option for smaller supply chains where fast processing is important, but network size remains limited. The system can efficiently handle low to moderate transaction volumes, ensuring operations like order tracking or inventory management run smoothly. However, as SCM systems grow to a medium scale (e.g., 60 to 100 nodes), PBFT's performance shows signs of strain. Throughput begins to decline, with drops to 2400 TPS at 60 nodes and 2306 TPS at 100 nodes, especially as the number of transactions increases. Latency also rises, with 1000 transactions at 100 nodes causing latency to reach 1906ms. For medium-sized supply chains that require handling more nodes and transaction volumes, PBFT's growing communication overhead and slower consensus times mean that while it can still function, its performance would begin to create inefficiencies, particularly during peak operational times. For large SCM systems (e.g., 100 to 200 nodes), PBFT struggles significantly. Throughput drops to just 2211 TPS at 200 nodes, and the latency spikes dramatically for large transaction volumes. For example, with 50000 transactions at 200 nodes, latency reaches an unacceptable 45265ms, which would cause severe delays in high-volume transactions. This makes PBFT unsuitable for large, complex SCM systems that require processing

high transaction volumes in real-time, such as global supply chains managing high-frequency order flows or real-time shipment tracking. PBFT's heavy communication requirements and inability to scale efficiently would result in bottlenecks and poor performance.

7.7.4 Stellar

Stellar is ideal for high-pressure SCM systems that handle transactions rapidly and efficiently due to its high throughput and low latency. The excellent scalability and productivity rankings indicate they can manage large SCM jobs. Due to its security, SCM systems must be carefully considered, especially when handling confidential data or lucrative trades [197]. Stellar functions well with small to small, medium-sized and larger networks, reaching a processing speed of ~5500 TPS. Stellar Consensus uses federated voting, which works well for trustworthy users but not in SCM, where participants don't know each other. So, from a security perspective, it would be better to use Stellar in small networks with known contexts or large networks that don't have private data. Its high throughput and low latency make it suitable for SCM systems that need to be efficient, but the consensus cannot handle complex threats because of its openness [200]. Because of this, we need either more security measures or hybrid models that combine the usefulness of these Stellar with more robust security.

7.7.5 Proof of Importance (PoI)

PoI has reasonable throughput and latency for small to medium-sized SCM systems, but it fails to scale for larger configurations. PoI achieves 1493 TPS with 10 nodes for a single transaction, which drops to 1250 TPS as the network reaches 200 nodes. This progressive drop-off in throughput shows that PoI works well for smaller networks but becomes limited as networks develop. The performance gap widens with transaction volumes. PoI's throughput declines to 1060 TPS at 10 nodes and 726 TPS at 200 nodes at 50000 transactions. This pattern implies that PoI may struggle with complicated supply chain settings' high transaction volumes and vast network sizes. In addition, PoI's latency grows with network capacity and transaction volume, limiting its scalability. PoI has a transaction latency of 803ms at 10 nodes and 1100ms at 200 nodes. Transaction volumes increase latency, with 50000 transactions resulting in 4900ms at 10 nodes and 6600ms at 200 nodes. These increased latency values, especially in larger networks and increased transaction scenarios, show that PoI may struggle to process transactions quickly in large SCM systems. Owing to these variables, PoI's performance suggests it is appropriate for small SCM systems with modest networks and

transaction volumes. Its secure identity verification mechanism makes it appropriate for contexts that require participant trust. PoI may perform well for medium SCM systems, but as transaction volumes rise, it may struggle to retain efficiency. PoI's identity verification security trades off scalability and processing speed for larger and more transaction-heavy networks.

7.7.6 Proof of Capacity (PoC)

PoC offers a unique approach in SCM systems, relying on disk space rather than computational power to mine blocks, which generally results in moderate scalability and throughput performance. The throughput tables indicate that PoC maintains a throughput of 665 TPS with 10 nodes and 530 TPS with 200 nodes for a single transaction. This drop in throughput highlights that while PoC performs well in small SCM systems, its efficiency decreases as the network scales up. For instance, with 1000 transactions, throughput falls from 487 TPS at 10 nodes to 370 TPS at 200 nodes, demonstrating that PoC may struggle in larger networks with higher transaction volumes. This pattern is consistent across all transaction sizes, suggesting that PoC is more suited to smaller SCM systems where the storage requirements can be better managed. When evaluating latency, PoC exhibits increasing delays as both the number of nodes and transactions grow. At 10 nodes, PoC maintains a latency of 1901 ms for a single transaction, which increases to 2321 ms at 200 nodes. As the transaction volume rises, latency escalates sharply, reaching 9427 ms for 5000 transactions at 200 nodes and 20615 ms for 50000 transactions at the same network size. These high latency figures indicate that PoC may not be able to meet the real-time processing requirements of larger, high-transaction SCM systems. While its use of storage instead of energy-intensive computation makes PoC efficient in terms of resource usage, its latency and throughput limitations make it better suited for small to medium SCM systems where transaction volumes are lower, and scalability needs are more manageable. From a security standpoint, PoC provides a moderate level of assurance due to its approach of using storage to reach consensus rather than computational work or stake-based systems. However, its performance suffers as data volumes increase and disk usage grows. Therefore, PoC is more suitable for small SCM systems where security needs can be addressed with additional layers of protection and where the storage capacity can be managed more effectively without causing processing delays.

7.7.7 Proof of Efficiency (PoEf)

The PoEf outperform appraised consensus mechanisms, characterised by very high throughput and efficiency. It also demonstrates excellent scalability due to its hierarchical structure and sharding techniques, allowing it to handle large transaction volumes with minimal computational overhead. Its processing speed, reaching ~6000 TPS, makes it highly suitable for environments requiring high transaction throughput. PoEf's node operations involve a layered system where subordinate, validator, and high-authority nodes perform specific roles that enhance scalability and efficiency. At the same time, its security characteristics provide the reassurance necessary for safeguarding against potential cyber threats, affirming its place as a potentially transformative solution in blockchain-based SCM systems. PoEf, characterised by high throughput and efficiency coupled with security against the identified consensus vulnerabilities, stands out as a solution that can enhance SCM efficiency and robustness. Its architecture addresses the scalability issues present in PBFT while providing a secure, efficient and scalable environment needed for large contemporary SCM systems. PoEf's node operations involve a layered system where subordinate, validator, and high-authority nodes perform specific roles that enhance scalability and efficiency.

7.8 Decision Tree Matrix (Throughput, Latency, Scalability)

Table 7.3 (a,b) simplifies and categorises the experimental findings into a decision tree matrix. SCM systems are increasingly facing demands for higher transaction volumes, real-time data processing, and robust security to protect against fraud and cyber-attacks. The throughput and latency are extracted from the simulations and the Scalability score is calculated from the formula in Chapter 6. By assessing the strengths and weaknesses of each mechanism, manufacturers can select the most suitable blockchain configuration that aligns with the specific SCM needs.

Table 7.3 (a,b): Decision matrix table for (Medium-large scale SCM)

@100 Nodes With @1000 Transactions (Medium-Sized SCM)

| Consensus Mechanism | Throughput | Latency | Scalability Score |
|---------------------|--------------------|----------------------|-------------------|
| PoEf | High (4382 TPS) | Very Low (365 ms) | Very High (20.99) |
| Stellar | High (3970 TPS) | Low (630 ms) | Very High (12.30) |
| DPoS | Medium (1617 TPS) | Medium (1290 ms) | High (5.98) |
| PoC | Very Low (370 TPS) | High (5902 ms) | Low (1.31) |
| PBFT | Low (1214 TPS) | Medium (1906 ms) | Medium (4.06) |
| PoI | Low (1110 TPS) | Medium (1805ms) | Medium (4.27) |
| PoW | Very Low (28 TPS) | Very High (62000 ms) | Very Low (0.12) |

@200 Nodes With @50000 Transactions (Large Sized-SCM)

| Consensus Mechanism | Throughput | Latency | Scalability Score |
|---------------------|--------------------|------------------------|-------------------|
| PoEf | High (3497 TPS) | Low (620 ms) | Very High (12.45) |
| Stellar | High (3450 TPS) | Medium (1028 ms) | High (7.64) |
| DPoS | Medium (1592 TPS) | Very High (18900 ms) | Very Low (0.56) |
| PoC | Very Low (225 TPS) | Very High (20615 ms) | Very Low (0.39) |
| PBFT | Low (446 TPS) | Very High (45265 ms) | Very Low (0.21) |
| Pol | Low (726 TPS) | Very High (6600ms) | Very Low (1.21) |
| PoW | Very Low (24 TPS) | Very High (3500000 ms) | Very Low (0.00) |

7.8.1 Key Takeaways from the Matrix:

The tables highlight that PoEf consistently outperforms other consensus mechanisms across medium and large-sized supply chains, demonstrating high throughput, low latency, and high scalability scores, making it the most efficient choice for real-time SCM. Stellar follows closely behind, with strong scalability in both environments, although its slightly higher latency makes it less optimal than PoEf. DPoS performs moderately in smaller networks but significantly struggles with scalability in large-scale operations due to high latency. Consensus mechanisms like PoC, PBFT, and Pol exhibit low scalability, particularly in larger SCM systems, where the performance declines sharply in both throughput and latency, making them unsuitable for handling complex, high-volume supply chains. PoW is the least scalable option, with extremely low throughput and prohibitively high latency, rendering it impractical for any real-time SCM scenario. These results underscore the importance of selecting a consensus mechanism that balances throughput and latency, especially for large, global SCM operations where transaction speed and efficiency are paramount.

7.9 Consensus Mechanism Selection

The need for a robust methodology is underpinned by the theoretical understanding that the choice of consensus mechanism directly impacts a blockchain network's scalability, efficiency, and security. As SCM systems vary in size and complexity, a one-size-fits-all approach to consensus mechanism selection is inadequate. Figure 7.6 proposes a synthesis of the experimental simulation findings from various consensus mechanisms, including PoW, DPoS, Stellar, PBFT, Pol, and the newly proposed PoEf, to incorporate the consensus throughput, latency and scalability. In

evaluating efficiency, Figure 7.6 considers how the consensus mechanism supports transaction volumes reflective of the SCM's size.

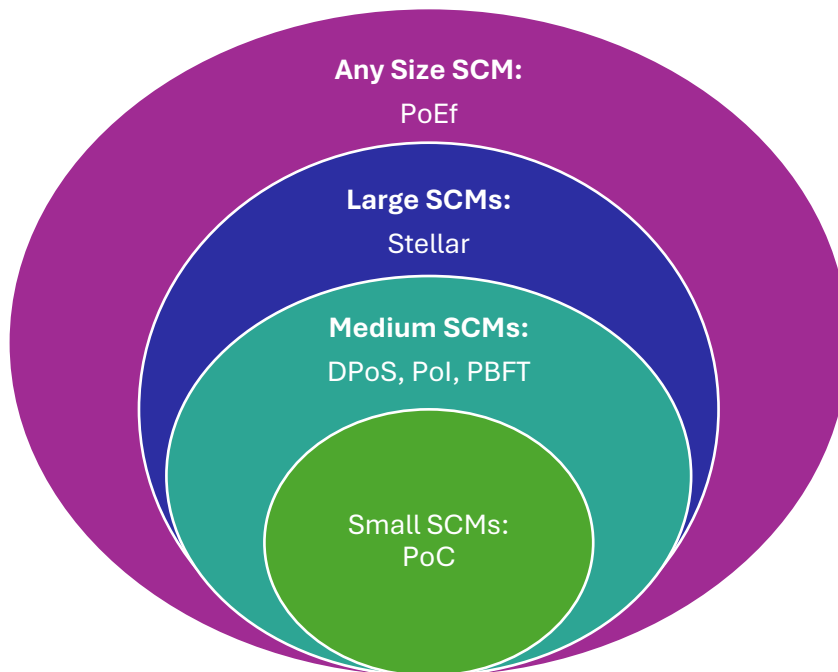


FIGURE 7.6: illustrating the consensus selection matrix for Blockchain-based SCM.

7.9.1 Recommendations for Consensus Mechanisms in SCM:

Based on table 7.2 and the results of the efficiency metrics, each mechanism is categorised to fit a particular blockchain-based supply chain size below:

1. Any Size SCM: PoEf

PoEf is the most efficient consensus mechanism for SCMs of **any size**. Its combination of high throughput and low latency allows for scalability across small, medium, and large supply chains. Whether the supply chain handles a few nodes or manages thousands, PoEf can consistently maintain high performance, making it appropriate for dynamic and distributed operations. It is particularly suited for real-time, high-transaction environments common in global SCMs. Offering **high throughput** (3497 TPS) and **low latency** (620ms), making it highly scalable for global supply chains with complex logistics and high transaction volumes. Its efficiency in processing large numbers of transactions while maintaining real-time performance makes it the most robust option for any size network.

2. Medium-Large SCMs: Stellar

Stellar is best suited for **medium-large** scale SCMs because it handles **high throughput** with **medium latency**. Stellar offers efficiency in processing large transaction volumes across multiple stakeholders, ensuring that performance remains efficient even in complex, distributed supply chains. However, Stellar's latency is slightly higher than PoE, which means as the network scale transaction speed degrades faster than that of PoE, assigning it to the medium-large scale SCM. Nonetheless Stellar would perform well in SCM scenarios where transaction speed is important, but some delay is acceptable, making it optimal for global operations and large supply networks.

3. Medium SCMs: DPoS, PoI, PBFT

- **DPoS Medium-sized supply chains** can benefit from DPoS due to its **medium throughput** and **medium latency**. It works well for supply chains with regional operations requiring moderate transaction speeds but not the extreme real-time processing that larger or global supply chains require. (DPoS) offers **moderate throughput** (1617 TPS) and manageable **latency** (1290ms), making it a good fit for **small supply chains** where transaction volumes are low and real-time speed is less important to the SCM system being built. Its simplicity and efficiency in smaller networks allow it to perform well without significant delays. DPoS especially shines here because of its delegate-based consensus approach, which reduces the need for full communication across all nodes.
- **PoI** offers an alternative for medium SCMs that also deliver **medium throughput** and **moderate latency**, but it also incorporates a reputation model, making it ideal for medium-sized supply chains where importance or reputation-based validation is crucial.
- **PBFT** is a suitable option for **medium SCMs** where **fault tolerance** is prioritised, given PBFT's technical underpinnings. It provides **low throughput** but ensures consensus even in networks with malicious actors, making it a good choice for **medium-sized SCMs** where security and stability are more important than speed. PBFT performs poorly in large-scale SCMs, with **low throughput** (446 TPS) and **very high latency** (45,265ms), making it inefficient for handling the demands of large, distributed SCM networks. Its inability to scale effectively makes it one of the least suitable options for global SCM systems.

4. Small SCMs: PoC

PoC is ideal for **small SCMs** due to its **low throughput** and **high latency**, which are manageable in supply chains with fewer nodes and transactions. PoC can be implemented in small, localised

supply chains where high transaction volumes or speed are not critical requirements. Its simplicity and resource efficiency make it a practical choice for smaller networks. PoC delivers **very low throughput** (370 TPS) and **high latency** (5902ms), which significantly limits its ability to handle moderate transaction volumes in medium-sized networks. These performance limitations make PoC unsuitable for supply chains that require efficient and timely operations.

5. Least Recommended for SCM: PoW

PoW is the least efficient option for any size SCM. With extremely low throughput and very high latency, PoW is not designed for the high-speed, high-volume demands of modern supply chains. Its resource-intensive nature also makes it unsuitable for supply chain networks where energy efficiency and cost are major considerations. PoW cannot meet the demands of real-time decision-making, transaction validation, or the dynamic requirements of SCM operations, making it the least recommended option overall. PoW is highly inefficient for any SCM, with very low throughput (24 TPS) and extremely high latency (up to 3,500,000ms), making it unsuitable for even small supply chains. Its resource-intensive nature and slow transaction speeds make it impractical for modern SCM systems

Fig. 7.6 illustrates the implementation guidance in selecting of the right consensus mechanism for varying SCM deployments. It provides guidelines for choosing a mechanism that aligns with the SCM's operational goals and security requirements. The diagrams help manufacturers select a blockchain consensus mechanism that aligns with the SCM size, demand, and operational priorities. Considering the nuanced requirements of SCM systems, solutions like PoEf, promise to enhance the adaptability and use of blockchains of supply chains in the digital era.

7.10 Chapter Summary

This chapter presented a comparative analysis of various consensus mechanisms, including PoW, DPoS, Stellar, PBFT, Pol, and PoEf, based on experimental simulations evaluating throughput, latency, and scalability. A total of 896 individual simulation runs were conducted to assess the performance of these consensus mechanisms. The findings highlight PoEf's superiority in critical performance metrics, particularly for supply chain management (SCM) systems, where throughput, latency, and scalability are essential for smooth and efficient operations. PoEf represents a noteworthy evolution in consensus mechanisms, particularly for Supply Chain applications that require high throughput, low latency, and enhanced security. By incorporating a multi-layer node structure, reputation-based validation, and shard-like communication, PoEf addresses the key

limitations of its predecessor, PBFT. It ensures scalability without sacrificing security, making it a robust solution for current and future blockchain applications. As demonstrated through theoretical analysis and practical simulations, PoEf is well-suited for industries that demand real-time transaction processing and secure, scalable networks. Its ability to mitigate common blockchain vulnerabilities while maintaining operational efficiency positions it as a leading consensus mechanism for large-scale, distributed systems like SCM.

Key Takeaways:

- **PoEf's Performance:** PoEf consistently demonstrated the highest throughput and lowest latency across different network sizes and transaction volumes, making it a highly efficient and scalable option for SCM applications. Its unique reputation-based, multi-layer structure enables it to process high transaction volumes in real-time, essential for modern SCM networks.
- **Stellar's Scalability:** Stellar also exhibited strong scalability, with relatively high throughput and moderate latency, positioning it as a viable option for large-scale SCM systems. However, its performance slightly lags behind PoEf in larger networks, especially as the number of transactions grows.
- **PBFT and Smaller Networks:** PBFT performs well in small and medium-sized networks, with decent throughput and latency. However, as the network size and transaction volumes increase, PBFT's scalability challenges become apparent, making it less suitable for large-scale SCM systems.
- **Consensus Mechanisms for Medium-Sized SCMs:** Consensus mechanisms like DPoS, PoI, and PBFT can handle medium-sized SCMs effectively. They offer balanced throughput and latency but cannot match the high efficiency of PoEf and Stellar in larger systems.
- **PoW's Inefficiency for SCM:** PoW was found to be the least efficient consensus mechanism for any SCM size, with extremely low throughput and prohibitively high latency. It is unsuitable for modern SCM systems that require high-speed and high-volume transaction processing.

This chapter concludes with an overall evaluation, confirming PoEf as a superior choice for blockchain-based SCM applications thanks to its enhanced efficiency, scalability, and security when compared to the traditional consensus methods. Stellar for large systems, PBFT, DPoS, and PoI may be suitable for medium-sized SCMs, PoC is only viable for small networks and PoW is the least recommended consensus mechanism due to its inefficiency in handling SCM demands. The findings emphasise that PoEf is the most scalable and efficient consensus mechanism for any size SCM.

8 Conclusion and Future Directions

8.1 Introduction

Blockchain technology has transformed supply chain management (SCM), enabling more open, efficient, and safe global supply networks. This thesis examined blockchain-integrated SCM systems in Industry 4.0, focussing on efficiency and security improvements through the blockchain's consensus layer. The topic is highly relevant due to the increasing adoption of blockchain in industries like SCM, where transparency, speed, and security are vital. As global supply chains become more complex, the need for scalable and efficient blockchain solutions becomes more important. PoEf's ability to improve consensus efficiency directly addresses industry needs, ensuring blockchain can meet the demands of modern supply chains.

Over the years, various consensus mechanisms (Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Stellar PoC and PoI) have been developed to address specific issues like decentralisation, scalability, and security. Each consensus mechanism was designed with unique challenges in mind. For example, PoW focuses on security but suffers from scalability issues and high energy consumption, while PBFT offers fault tolerance but struggles with communication overhead in large-scale networks. As research pointed to investigating inefficiencies in blockchain consensus mechanisms, particularly in SCM, the thesis then focused on exploring, designing, and implementing a novel consensus mechanism, Proof of Efficiency (PoEf), tailored to blockchain-based SCM systems. By developing the PoEf consensus mechanism, the goal was to enhance scalability, improve throughput, reduce latency, and strengthen security in blockchain-based SCM systems. The research aimed to fill gaps in the existing blockchain mechanisms, offering a more effective way to handle increasing transaction volumes and network size without compromising performance.

The research presented in the thesis has taken noteworthy strides toward addressing the efficiency, scalability, and security challenges blockchain-based SCM systems face. The development and validation of the PoEf consensus mechanism represents a notable advancement in the intersecting fields (SCM, Cybersecurity and Blockchain), offering a practical solution to the pressing needs of modern supply chains. By leveraging PoEf's novel architecture, SCM systems can achieve real-time

transaction processing, enhanced security, and overall better scalability, ensuring they can meet the demands of an increasingly interconnected and fast-paced global marketplace. While there is some suggested work (see *Section 8.5*) that can be done to refine and expand PoEf's capabilities, the findings of this thesis provide a solid foundation for future research and development in blockchain technology in SCM. The proposed future directions will serve as a roadmap for continued innovation, ensuring that blockchain remains at the forefront of supply chain transformation in the years to come.

8.2 Resolution of the Aim and Objectives

8.2.1 Aim

The aim of this research was to investigate the efficiency and security capabilities of blockchain-based SCM systems. Through extensive simulations and a rigorous review of existing literature, the thesis proposed the PoEf consensus mechanism as an optimised solution to the challenges inherent in current consensus protocols PoW, DPoS, Stellar, PBFT and Pol.

8.2.2 Objectives

Objective (i): Appraisal of Literature in Blockchain, SCM, and Cybersecurity

- The research began with a Systematic Literature Review (SLR) in Chapter 4, where 108 peer-reviewed articles were analysed to uncover vulnerabilities in blockchain that affect its performance from an efficiency standpoint. The SLR identified gaps in current research, particularly the need for more secure and efficient consensus mechanisms that can scale with increasing network demands. This exploration highlighted inefficiencies linked to four layers within the blockchain (the consensus mechanisms, network-level attacks, smart contract vulnerabilities and cryptographic challenges).

Objective (ii): Identifying Key Architectural Factors Affecting Efficiency

- In the same Chapter 4, having looked at the triumvirate, *Blockchain + SCM + Cybersecurity* and identified the four key areas for further exploration (layers within the blockchain susceptible to cyber-risks that compromise efficiency), the consensus layer (through the consensus mechanism) was prioritised as the area for further investigation, as it is the area in the blockchain which predominantly manages how efficient the blockchain is. As

cyberattacks on blockchain systems continue to rise, enhancing the consensus mechanisms is crucial to maintaining security and operational efficiency within SCM networks.

Objective (iii): Evaluation of Consensus Mechanisms in SCM

- Chapter 5 explored various blockchain consensus mechanisms used in SCM, including PoW, DPoS, PBFT, Pol, and Stellar. It identified that while these mechanisms offer various benefits, each has significant trade-offs between throughput, latency, and security. For example, PoW suffers from low throughput and high energy consumption, making it unsuitable for SCM. PBFT, while offering strong security, struggles to scale in large networks due to communication overhead.
- To evaluate the efficiency parameters of the consensus mechanisms, simulations were conducted using the BlockSim tool. These simulations modelled a range of network configurations and transaction volumes to assess throughput, latency, and scalability across PoW, DPoS, PBFT, and Stellar, Pol and PoC mechanisms. The BlockSim simulations confirmed that these limitations are major architectural bottlenecks that affect the overall performance of blockchain systems in SCM and opened the gap for the exploration of a more efficient mechanism.

Objective (iv): Design and Testing of the Novel PoEf Consensus Mechanism

- The key contribution of this thesis is the design of the PoEf consensus mechanism, discussed in Chapter 6. PoEf is a novel approach that integrates sharding and a reputation-based scoring system to optimise the efficiency of blockchain-based SCM. By dynamically adjusting the reputation of nodes and distributing workloads across multiple shards, PoEf reduces communication overhead and latency. Its multi-layered architecture ensures that only the most trusted and efficient nodes are selected to participate in consensus, enhancing security and efficiency. This is an enhancement over existing systems, where the consensus process often becomes a bottleneck, impeding the blockchain's overall performance. The simulation results validated PoEf's ability to surpass traditional consensus mechanisms like PBFT and Stellar in performance, especially in high-demand environments like global supply chains.

Objective (v): Proposing a Decision Matrix for Consensus Mechanism Selection

- In Chapter 7, a decision matrix was introduced to guide practitioners and researchers in selecting the most suitable consensus mechanism for the SCM needs. The matrix compared

the performance of various mechanisms based on throughput, latency, scalability, and security, with PoEf emerging as the most efficient solution for both medium and large-scale SCM systems. The matrix is a practical tool for industry stakeholders looking to implement blockchain technology in the supply chains. It gives key insights into existing consensus mechanisms and offers a route to identifying the best consensus approach based on specific operational requirements.

8.3 Key Contributions

The thesis made several significant contributions to the field of blockchain, cybersecurity and SCM:

- **SLR on Blockchain Vulnerabilities:** The literature review identified and categorised key vulnerabilities in blockchain consensus mechanisms that affect SCM efficiency and security.
- **Simulation Evaluation:** The BlockSim-based simulations provided a robust evaluation of existing consensus mechanisms, offering new insights into the scalability and performance under different network conditions.
- **Development of PoEf:** The Proof of Efficiency (PoEf) consensus mechanism represents a novel approach to optimising SCM systems. It integrates sharding and reputation-based scoring to enhance both scalability and security.
- **Decision Matrix:** The decision matrix offers a valuable tool for selecting appropriate consensus mechanisms based on network size, transaction volume, and security needs.

8.4 Challenges and Ethical Considerations

8.4.1 Challenges

- **Limited Test Conditions:** Controlled simulation environment, BlockSim, was used to evaluate consensus mechanisms like PoEf. While the simulation tool effectively tested performance indicators throughput, latency, and scalability. However, these controlled environments may not accurately reflect real-world scenarios. These include factors like network disruptions, malicious attacks, and resource constraints, which are hard to replicate fully in a simulation. These external conditions, prevalent in real-world supply chain systems, pose a challenge to the robustness and security of consensus mechanisms. To mitigate this, real-world testing on blockchain networks across different industry case studies could further validate the findings.

- **Simulating Large-Scale Networks:** Simulating large-scale blockchain networks is usually resource-intensive and a challenge. It was time-consuming and computationally demanding to run 896 simulations spanning 10 to 200 nodes and 1 to 50,000 transactions. BlockSim allowed for extended testing, but scaling the nodes and transactions required high computing power which would lead to several crashes. The simulations revealed PoEf's performance, but applying these findings to real-world situations would require further validation, especially considering hardware limits, network capacity, and attack paths that were not studied.

8.4.2 Ethical Considerations

- Data quality and transparency are important to research validity and reliability. Efforts were taken to ensure that all data collected from simulations and the literature review were managed accurately and consistently. To eliminate inaccuracies and distortion of the findings a thorough cross-checking was done. For example, PoEf consensus mechanism simulation results were carefully logged and tested against predicted parameters to avoid data loss or corruption.
- The simulation process was detailed for transparency. This included explaining how BlockSim processed network settings, node sizes, and transaction volumes during simulations. The collated results when compared with PoEf can be considered objective and in essence valid and reliable also. The systematic literature review used PRISMA principles to choose unbiased and complete research.

8.5 Future Work

- Despite the noteworthy advancements made through the development of PoEf, there remain several areas for future exploration:

8.5.1 Additional Layers within the blockchain

The work presented in this thesis explored the consensus layer of the blockchain. As highlighted in Chapter 4, there are three other areas of exploration (network layer, smart contracts, and data layer's cryptographic challenges). As indicated in Table 8.1, future research could focus on further developing this mechanism into a complete blockchain system exploring the other layers and the application in SCM scenarios; this is important to get to an all-round "close to real-world" adoption and aligns with the research objectives of comprehensively analysing the integration of blockchain

into SCM as well as contributing to the evolving discourse on blockchain technology's role in enhancing SCM security and efficiency.

TABLE 8.1: illustrating recommended areas for future research

| Priority Area 1 - Completed | Priority Area 2 | Priority Area 3 | Priority Area 4 |
|---|---|---|---|
| Investigation, evaluation, and testing of different types of Consensus Mechanisms in SCM systems. | Investigation, evaluation, and testing of Smart Contract deployments in SCM | Investigation, evaluation, and testing of different Network-Level attacks of Blockchain-based in SCMs | Investigation, evaluation, and testing of different Cryptographic Techniques used Blockchain-based SCMs |

8.5.2 Expanding PoEf’s Security Features

PoEf’s reputation-based node selection already provides enhanced security, but future work could explore integrating additional security layers, such as quantum-resistant cryptographic techniques (*mentioned in Chapter 4*), to safeguard against emerging cyber threats. Performing rigorous stress testing under various circumstances and possible attack scenarios might also yield insightful findings regarding PoEf's resistance to sophisticated new and emerging cybersecurity attacks.

8.5.3 Applying PoEf Beyond SCM

While this thesis focused on SCM applications, PoEf’s efficiency and scalability makes it suitable for other industries that require high transaction throughput and low latency, such as finance, healthcare, and IoT networks. Future research could explore adapting PoEf to these domains, conducting sector-specific simulations to validate its applicability. To fully explore and comprehend the adaptability of PoEf, it could be tested in a real-world use case to include a wide range of industries and operational scales. Future researchers have the potential to expand the utilisation of the PoEf mechanism in different scenarios within SCM.

8.5.4 Real-World Deployment of PoEf

PoEf was implemented and simulated in a simulator. Future work could focus on implementing PoEf in a real-world SCM environment. Conducting pilot studies within actual supply chains would provide invaluable insights into the practical challenges of deploying the mechanism at scale. Such studies could also identify potential refinements to the PoEf mechanism, ensuring that it meets the demands of diverse, dynamic supply chain ecosystems and reveals concrete effects in genuine business scenarios.

9 References

- [1] Y. Sun, S. Jiang, W. Jia, and Y. Wang, 'Blockchain as a cutting-edge technology impacting business: A systematic literature review perspective', *Telecomm Policy*, vol. 46, no. 10, p. 102443, Nov. 2022, doi: 10.1016/j.telpol.2022.102443.
- [2] A. K. Jain, N. Gupta, and B. B. Gupta, 'A survey on scalable consensus algorithms for blockchain technology', *Cyber Security and Applications*, vol. 3, p. 100065, Dec. 2025, doi: 10.1016/j.csa.2024.100065.
- [3] M. Kopyto, S. Lechler, H. A. von der Gracht, and E. Hartmann, 'Potentials of blockchain technology in supply chain management: Long-term judgments of an international expert panel', *Technol Forecast Soc Change*, vol. 161, p. 120330, Dec. 2020, doi: 10.1016/j.techfore.2020.120330.
- [4] S. Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System', *SSRN Electronic Journal*, 2008, doi: 10.2139/ssrn.3440802.
- [5] M. Swan, *BLOCKCHAIN: Blueprint for a new economy*, 1st ed. Sebastopol: O'Reilly Media, Inc., 2015.
- [6] C. Devecchi *et al.*, 'Blockchain Educational Passport: Decentralised Learning Ledger (DLL)', CCEG Blockchain UN Lab, Apr. 2017. doi: oai:nectar.northampton.ac.uk:12582.
- [7] G. Hofbauer and A. Sangl, 'Blockchain Technology and Application Possibilities in the Digital Transformation of Transaction Processes', *Forum Scientiae Oeconomia*, vol. 7, no. 4, pp. 25–40, Dec. 2019, doi: https://doi.org/10.23762/FSO_VOL7_NO4_2.
- [8] N. Upadhyay, 'Demystifying blockchain: A critical analysis of challenges, applications and opportunities', *Int J Inf Manage*, vol. 54, p. 102120, Oct. 2020, doi: 10.1016/j.ijinfomgt.2020.102120.
- [9] F. Casino, T. K. Dasaklis, and C. Patsakis, 'A systematic literature review of blockchain-based applications: Current status, classification and open issues', *Telematics and Informatics*, vol. 36, pp. 55–81, 2019, doi: <https://doi.org/10.1016/j.tele.2018.11.006>.
- [10] O. Ali, M. Ally, P. Clutterbuck, and Y. Dwivedi, 'The state of play of blockchain technology in the financial services sector: A systematic literature review', *Int J Inf Manage*, vol. 54, p. 102199, Oct. 2020, doi: 10.1016/j.ijinfomgt.2020.102199.
- [11] T. A. Almeshal and A. A. Alhogail, 'Blockchain for Businesses: A Scoping Review of Suitability Evaluations Frameworks', *IEEE Access*, vol. 9, pp. 155425–155442, Nov. 2021, doi: 10.1109/ACCESS.2021.3128608.
- [12] J. S. Arlbjørn, H. de Haas, and K. B. Munksgaard, 'Exploring supply chain innovation', *Logistics Research*, vol. 3, no. 1, pp. 3–18, Apr. 2011, doi: 10.1007/s12159-010-0044-3.
- [13] H. Kagermann, 'Change Through Digitization - Value Creation in the Age of Industry 4.0', in *Management of Permanent Change*, Wiesbaden: Springer Fachmedien Wiesbaden, 2015, pp. 23–45. doi: 10.1007/978-3-658-05014-6_2.
- [14] J. Heppelmann, 'How the Internet of Things Could Transform the Value Chain', *McKinsey & Company*, vol. 92, no. 11, Nov. 2014. Accessed: Oct. 02, 2023. Available: <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/how-the-internet-of-things-could-transform-the-value-chain>
- [15] M. Attaran and A. Gunasekaran, 'Blockchain-enabled technology: The emerging technology set to reshape and decentralise many industries', *International Journal of Applied Decision Sciences*, vol. 12, no. 4, pp. 424–444, 2019, doi: 10.1504/IJADS.2019.102642.
- [16] Y. Chang, E. Iakovou, and W. Shi, 'Blockchain in global supply chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities', *Int J Prod Res*, vol. 58, no. 7, pp. 2082–2099, Apr. 2020, doi: 10.1080/00207543.2019.1651946.
- [17] G. Tripathi, M. A. Ahad, and G. Casalino, 'A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges', *Decision Analytics Journal*, vol. 9, p. 100344, Dec. 2023, doi: 10.1016/J.DAJOUR.2023.100344.

- [18] I. Abu-elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-alrazaq, 'The benefits and threats of blockchain technology in healthcare: A scoping review', Oct. 01, 2020, *Elsevier Ireland Ltd.* doi: 10.1016/j.ijmedinf.2020.104246.
- [19] A. J. D. P. Isravel, K. M. Sagayam, B. Bhushan, Y. Sei, and J. Eunice, 'Blockchain for healthcare systems: Architecture, security challenges, trends and future directions', *Journal of Network and Computer Applications*, vol. 215, p. 103633, Jun. 2023, doi: 10.1016/J.JNCA.2023.103633.
- [20] F. M. Abdelsalam, 'Blockchain Revolutionizing Healthcare Industry: A Systematic Review of Blockchain Technology Benefits and Threats', *Perspectives Health Information Management*, vol. 20, no. 3, Sep. 2023.
- [21] N. Kshetri, '1 Blockchain's roles in meeting key supply chain management objectives', *Int J Inf Manage*, vol. 39, pp. 80–89, Apr. 2018, doi: 10.1016/j.ijinfomgt.2017.12.005.
- [22] P. Jahanbin, S. C. Wingreen, R. Sharma, B. Ijadi, and M. M. Reis, 'Enabling affordances of blockchain in agri-food supply chains: A value-driver framework using Q-methodology', *International Journal of Innovation Studies*, vol. 7, no. 4, pp. 307–325, Dec. 2023, doi: 10.1016/J.IJIS.2023.08.001.
- [23] C. Ganeshkumar, M. Rajalaksmi, and A. David, 'Exploring the challenges and adoption hurdles of blockchain technology in agri-food supply chain', *Handbook of Research on AI-Equipped IoT Applications in High-Tech Agriculture*, pp. 257–270, Aug. 2023, doi: 10.4018/978-1-6684-9231-4.CH014.
- [24] D. Mechkaroska, V. Dimitrova, and A. Popovska-Mitrovikj, 'Analysis of the Possibilities for Improvement of Blockchain Technology', in *2018 26th Telecommunications Forum (TELFOR)*, 2018, pp. 1–4. doi: 10.1109/TELFOR.2018.8612034.
- [25] M. Torky and A. E. Hassanein, 'Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges', Nov. 01, 2020, *Elsevier B.V.* doi: 10.1016/j.compag.2020.105476.
- [26] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, 'Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges', 2020, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2020.2973178.
- [27] C. Giménez and H. R. Lourenço, 'e-SCM: Internet's impact on supply chain processes', Nov. 07, 2008. doi: 10.1108/09574090810919189.
- [28] M. Tajima, 'Strategic value of RFID in supply chain management', *Journal of Purchasing and Supply Management*, vol. 13, no. 4, pp. 261–273, 2007, doi: <https://doi.org/10.1016/j.pursup.2007.11.001>.
- [29] İ. Z. Akyurt, Y. Kuvvetli, and M. Deveci, 'Enterprise resource planning in the age of industry 4.0', in *Logistics 4.0. Digital Transformation of Supply Chain Management*, 1st ed., vol. 1, T. Paksoy, C. Gonul Kochan, and S. Samar Ali, Eds., Boca Raton: CRC Press, 2020, pp. 1–8. doi: <https://doi.org/10.1201/9780429327636>.
- [30] E. W. T. Ngai, L. Xiu, and D. C. K. Chau, 'Application of data mining techniques in customer relationship management: A literature review and classification', *Expert Syst Appl*, vol. 36, no. 2, Part 2, pp. 2592–2602, 2009, doi: <https://doi.org/10.1016/j.eswa.2008.02.021>.
- [31] C. A. Hill, G. P. Zhang, and K. E. Miller, 'Collaborative planning, forecasting, and replenishment & firm performance: An empirical evaluation', *Int J Prod Econ*, vol. 196, pp. 12–23, 2018, doi: <https://doi.org/10.1016/j.ijpe.2017.11.012>.
- [32] W.-H. Hung, C.-P. Lin, Y.-M. Tai, C.-F. Ho, and J.-J. Jou, 'Exploring the impact of Web-based e-procurement on performance: organisational, interorganisational, and systems perspectives', *International Journal of Logistics Research and Applications*, vol. 17, no. 3, pp. 200–215, May 2014, doi: 10.1080/13675567.2013.837431.
- [33] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, 'Blockchain technology and its relationships to sustainable supply chain management', *Int J Prod Res*, vol. 57, no. 7, pp. 2117–2135, Apr. 2019, doi: 10.1080/00207543.2018.1533261.
- [34] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, 'When Intrusion Detection Meets Blockchain Technology: A Review', *IEEE Access*, vol. 6, pp. 10179–10188, 2018, doi: 10.1109/ACCESS.2018.2799854.

- [35] Q. Lu and X. Xu, 'Adaptable Blockchain-Based Systems: A Case Study for Product Traceability', *IEEE Softw*, vol. 34, no. 6, pp. 21–27, Nov. 2017, doi: 10.1109/MS.2017.4121227.
- [36] T. Aste, P. Tasca, and T. Di Matteo, 'Blockchain Technologies: The Foreseeable Impact on Society and Industry', *Computer (Long Beach Calif)*, vol. 50, no. 9, pp. 18–28, 2017, doi: 10.1109/MC.2017.3571064.
- [37] W. Li *et al.*, 'Designing supply chain models with blockchain technology in the fishing industry in Indonesia', *IOP Conf Ser Mater Sci Eng*, vol. 1072, no. 1, p. 012020, Feb. 2021, doi: 10.1088/1757-899X/1072/1/012020.
- [38] E. Hofmann and M. Rüsçh, 'Industry 4.0 and the current status as well as future prospects on logistics', *Comput Ind*, vol. 89, pp. 23–34, Aug. 2017, doi: 10.1016/J.COMPIND.2017.04.002.
- [39] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, 'Blockchain technology and its relationships to sustainable supply chain management', *Int J Prod Res*, vol. 57, no. 7, pp. 2117–2135, Apr. 2019, doi: 10.1080/00207543.2018.1533261.
- [40] Y. Wang, M. Singgih, J. Wang, and M. Rit, 'Making sense of blockchain technology: How will it transform supply chains?', *Int J Prod Econ*, vol. 211, pp. 221–236, May 2019, doi: 10.1016/J.IJPE.2019.02.002.
- [41] S. Al-Farsi, M. M. Rathore, and S. Bakiras, 'Security of Blockchain-Based Supply Chain Management Systems: Challenges and Opportunities', *Applied Sciences 2021, Vol. 11, Page 5585*, vol. 11, no. 12, p. 5585, Jun. 2021, doi: 10.3390/APP11125585.
- [42] A. Kiayias and G. Panagiotakos, 'Speed-security tradeoffs in blockchain protocols', *Cryptology ePrint Archive*, vol. 2015, p. 1019, 2015, Accessed: Feb. 28, 2024. Available: <https://eprint.iacr.org/2015/1019>
- [43] U. Agarwal *et al.*, 'Blockchain Technology for Secure Supply Chain Management: A Comprehensive Review', *IEEE Access*, 2022, doi: 10.1109/ACCESS.2022.3194319.
- [44] A. Kumar *et al.*, 'Securing logistics system and supply chain using Blockchain', *Appl Stoch Models Bus Ind*, vol. 37, no. 3, pp. 413–428, May 2021, doi: 10.1002/ASMB.2592.
- [45] L. K. Fachhochschule *et al.*, 'The Risks of the Blockchain A Review on Current Vulnerabilities and Attacks', *Journal of Internet Services and Information Security (JISIS)*, vol. 10, no. 3, pp. 110–127, Aug. 2020, doi: 10.22667/JISIS.2020.08.31.110.
- [46] H. Hasanova, U. jun Baek, M. gon Shin, K. Cho, and M. S. Kim, 'A survey on blockchain cybersecurity vulnerabilities and possible countermeasures', *International Journal of Network Management*, vol. 29, no. 2, p. e2060, Mar. 2019, doi: 10.1002/NEM.2060.
- [47] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W. C. Hong, 'A survey on decentralized consensus mechanisms for cyber physical systems', *IEEE Access*, vol. 8, pp. 54371–54401, 2020, doi: 10.1109/ACCESS.2020.2981415.
- [48] A. Kumar, R. Liu, and Z. Shan, 'Is Blockchain a Silver Bullet for Supply Chain Management? Technical Challenges and Research Opportunities', *Decision Sciences*, vol. 51, no. 1, pp. 8–37, Feb. 2020, doi: 10.1111/DECI.12396.
- [49] A. Yadlapalli, S. Rahman, and P. Gopal, 'Blockchain technology implementation challenges in supply chains – evidence from the case studies of multi-stakeholders', *The International Journal of Logistics Management*, vol. 33, no. 5, pp. 278–305, Jan. 2022, doi: 10.1108/IJLM-02-2021-0086.
- [50] U. Jüttner and S. Maklan, 'Supply chain resilience in the global financial crisis: an empirical study', *Supply Chain Management: An International Journal*, vol. 16, no. 4, pp. 246–259, Jan. 2011, doi: 10.1108/13598541111139062.
- [51] M. Kouhizadeh, Q. Zhu, and J. Sarkis, 'Blockchain and the circular economy: potential tensions and critical reflections from practice', *Production Planning & Control*, vol. 31, no. 11–12, pp. 950–966, Sep. 2020, doi: 10.1080/09537287.2019.1695925.
- [52] M. M. Queiroz, S. C. F. Pereira, R. Telles, and M. C. Machado, 'Industry 4.0 and digital supply chain capabilities', *Benchmarking: An International Journal*, vol. 28, no. 5, pp. 1761–1782, May 2021, doi: 10.1108/BIJ-12-2018-0435.
- [53] Institute of Supply Chain Management, 'Rising Threat of Cyber Fraud in Supply Chain Management', Institute of Supply Chain Management. Accessed: Aug. 12, 2024. Available: <https://www.ioscm.com/blog/the-rising-threat-of-cyber-fraud-in-supply-chain-management/>

- [54] G. Kovács and B. Illés, ‘Development of an Optimization Method and Software for Optimizing Global Supply Chains for Increased Efficiency, Competitiveness, and Sustainability’, Mar. 2019, doi: 10.3390/su11061610.
- [55] dena German Energy Agency, ‘Rethinking Blockchain’s Electricity Consumption A Guide to Electricity-Efficient Design of Decentralized Data Infrastructure’, Oct. 2023. Available: www.dena.de
- [56] M. A. Awwad *et al.*, ‘Blockchain Technology for Efficient Management of Supply Chain’, Jan. 2018. Available: <https://www.researchgate.net/publication/325065808>
- [57] M. W. Akram, N. Akram, F. Shahzad, K. U. Rehman, and S. Andleeb, ‘Blockchain technology in a crisis: Advantages, challenges, and lessons learned for enhancing food supply chains during the COVID-19 pandemic’, *J Clean Prod*, vol. 434, Jan. 2024, doi: 10.1016/j.jclepro.2023.140034.
- [58] M. S. Rahman, I. Khalil, and A. Bouras, ‘Designing an efficient consensus protocol for supply chain’, *Blockchain Driven Supply Chains and Enterprise Information Systems*, pp. 173–185, Sep. 2022, doi: 10.1007/978-3-030-96154-1_9.
- [59] L. Cai, A. Liu, and Y. Yan, ‘Blockchain Consensus Algorithm for Supply Chain Information Security Sharing Based on Convolutional Neural Networks’, Aug. 2024. doi: 10.21203/rs.3.rs-4627597/v1.
- [60] M. Kouhizadeh, S. Saberi, and J. Sarkis, ‘Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers’, *Int J Prod Econ*, vol. 231, p. 107831, Jan. 2021, doi: 10.1016/J.IJPE.2020.107831.
- [61] H. Min, ‘Blockchain technology for enhancing supply chain resilience’, *Bus Horiz*, vol. 62, no. 1, pp. 35–45, Jan. 2019, doi: 10.1016/j.bushor.2018.08.012.
- [62] S. S. Kamble, A. Gunasekaran, and R. Sharma, ‘Modeling the blockchain enabled traceability in agriculture supply chain’, *Int J Inf Manage*, vol. 52, p. 101967, Jun. 2020, doi: 10.1016/J.IJINFOMGT.2019.05.023.
- [63] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, ‘Blockchain challenges and opportunities: A survey’, *International Journal of Web and Grid Services*, vol. 14, p. 352, Oct. 2018, doi: 10.1504/IJWGS.2018.095647.
- [64] A. G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, ‘Emerging Trends in Blockchain Technology and Applications: A Review and Outlook’, *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 9, pp. 6719–6742, 2022, doi: <https://doi.org/10.1016/j.jksuci.2022.03.007>.
- [65] O. Ali, A. Jaradat, A. Kulakli, and A. Abuhalmeh, ‘A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities’, *IEEE Access*, vol. 9, pp. 12730–12749, 2021, doi: 10.1109/ACCESS.2021.3050241.
- [66] K. E. Wegrzyn and E. Wang, ‘Types of Blockchain: Public, Private, or Something in Between’, Foley & Lardner LLP. Accessed: Dec. 11, 2022. Available: <https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between>
- [67] ImmuneBytes, ‘Comparison of Various Blockchain Protocols’. Accessed: Aug. 12, 2024. Available: <https://www.immunebytes.com/blog/comparison-of-various-blockchain-protocols/>
- [68] S. Pahlajani, A. Kshirsagar, and V. Pachghare, ‘Survey on Private Blockchain Consensus Algorithms’, *Proceedings of 1st International Conference on Innovations in Information and Communication Technology, ICICT 2019*, Apr. 2019, doi: 10.1109/ICICT1.2019.8741353.
- [69] W. Yao, J. Ye, R. Murimi, and G. Wang, ‘A Survey on Consortium Blockchain Consensus Mechanisms’, *Int. J. Adv. Telecommun*, vol. 11, no. 1, pp. 51–64, 2018.
- [70] E. Androulaki *et al.*, ‘Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains’, *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, vol. 2018-January, Apr. 2018, doi: 10.1145/3190508.3190538.
- [71] O. Haughton, C. Campbell, G. Howe, and T. H. Walcott, ‘Evaluating the integration of Blockchain Technologies in Supply Chain Management: A case study of sustainable fishing’, in *Proceedings - 2022 International Conference on Computing, Networking, Telecommunications and Engineering Sciences Applications, CoNTESA 2022*, 2022. doi: 10.1109/CoNTESA57046.2022.10011252.

- [72] Y. Xu *et al.*, ‘Suitability analysis of consensus protocols for blockchain-based applications in the construction industry’, *Autom Constr*, vol. 145, p. 104638, Jan. 2023, doi: 10.1016/J.AUTCON.2022.104638.
- [73] M. Du, X. Ma, Z. Zhang, X. Wang, and Q. Chen, ‘A review on consensus algorithm of blockchain’, *2017 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2017*, vol. 2017-January, pp. 2567–2572, Nov. 2017, doi: 10.1109/SMC.2017.8123011.
- [74] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Portfolio, 2016.
- [75] K. Christidis and M. Devetsikiotis, ‘Blockchains and Smart Contracts for the Internet of Things’, *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
- [76] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, ‘BlockChain Technology: Beyond Bitcoin’, *Applied Innovation Review*, no. 2, Jun. 2016.
- [77] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, ‘The Blockchain as a Decentralized Security Framework’, *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, Mar. 2018, doi: 10.1109/MCE.2017.2776459.
- [78] Arvind. Narayanan, E. W. Felten, Joseph. Bonneau, Andrew. Miller, Steven. Goldfeder, and Jeremy. Clark, *Bitcoin and cryptocurrency technologies : a comprehensive introduction*. New Jersey: Princeton University Press, 2016.
- [79] S. Bano, M. Al-Bassam, and George. Danezis, ‘The Road to Scalable Blockchain Designs Functional Components of a Blockchain’, *Login USENIX; magazine*, 2017. Accessed: Jan. 28, 2024. Available: https://www.usenix.org/system/files/login/articles/login_winter17_06_bano.pdf
- [80] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, ‘Where Is Current Research on Blockchain Technology?- A Systematic Review’, *PLoS One*, vol. 11, no. 10, p. e0163477, Oct. 2016, doi: 10.1371/journal.pone.0163477.
- [81] I. Eyal and E. G. Sirer, ‘Majority is not enough’, *Commun ACM*, vol. 61, no. 7, pp. 95–102, Jun. 2018, doi: 10.1145/3212998.
- [82] F. Saleh, ‘Blockchain without Waste: Proof-of-Stake’, *Rev Financ Stud*, vol. 34, no. 3, pp. 1156–1190, Feb. 2021, doi: 10.1093/rfs/hhaa075.
- [83] N. El Ioimi and C. Pahl, ‘A Review of Distributed Ledger Technologies’, in *Panetto, H., Debruyne, C., Proper, H., Ardagna, C., Roman, D., Meersman, R. (eds) On the Move to Meaningful Internet Systems*, Springer Verlag, 2018, pp. 277–288. doi: 10.1007/978-3-030-02671-4_16.
- [84] A. Wright and P. De Filippi, ‘Decentralized Blockchain Technology and the Rise of Lex Cryptographia’, *SSRN Electronic Journal*, Mar. 2015, doi: 10.2139/SSRN.2580664.
- [85] Y.-C. Chen, Y.-P. Chou, and Y.-C. Chou, ‘An Image Authentication Scheme Using Merkle Tree Mechanisms’, *Future Internet*, vol. 11, no. 7, p. 149, Jul. 2019, doi: 10.3390/fi11070149.
- [86] M. Singh and S. Kim, ‘Blockchain Based Intelligent Vehicle Data sharing Framework’, Jul. 2017. Accessed: Dec. 19, 2023. Available: <http://arxiv.org/abs/1708.09721>
- [87] J. A. Kroll, I. C. Davey, and E. W. Felten, ‘The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries’, in *The Twelfth Workshop on the Economics of Information Security (WEIS 2013)*, Washington: Pennsylvania State University, Jun. 2013.
- [88] M. Vasek and T. Moore, ‘There’s No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams’, in *In: Böhme, R., Okamoto, T. (eds) Financial Cryptography and Data Security. FC 2015*, Berlin, Heidelberg: Springer Verlag, Jul. 2015, pp. 44–61. doi: 10.1007/978-3-662-47854-7_4.
- [89] A. Sapirshstein, Y. Sompolinsky, and A. Zohar, ‘Optimal Selfish Mining Strategies in Bitcoin’, in *In: Grossklags, J., Preneel, B. (eds) Financial Cryptography and Data Security*, Berlin, Heidelberg: Springer Verlag, Jul. 2015, pp. 515–532. doi: 10.1007/978-3-662-54970-4_30.
- [90] C. Cachin and M. Vukolić, ‘Blockchain Consensus Protocols in the Wild’, *Leibniz International Proceedings in Informatics, LIPIcs*, vol. 91, Jul. 2017, doi: 10.4230/LIPIcs.DISC.2017.1.
- [91] V. Buterin and V. Griffith, ‘Casper the Friendly Finality Gadget’, Oct. 2017, Accessed: Dec. 20, 2023. Available: <https://arxiv.org/abs/1710.09437v4>
- [92] Y. Sompolinsky and A. Zohar, ‘Accelerating Bitcoin’s Transaction Processing. Fast Money Grows on Trees, Not Chains’, *Cryptology ePrint Archive*, 2013.

- [93] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, ‘On blockchain and its integration with IoT. Challenges and opportunities’, *Future Generation Computer Systems*, vol. 88, pp. 173–190, Nov. 2018, doi: 10.1016/J.FUTURE.2018.05.046.
- [94] A. Nember, ‘NEM Technical Reference’, Feb. 2018.
- [95] A. Kiayias, A. Russell, B. David, and R. Oliynykov, ‘Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol’, in *In: Katz, J., Shacham, H. (eds) Advances in Cryptology – CRYPTO 2017. CRYPTO 2017*, Springer Verlag, 2017, pp. 357–388. doi: 10.1007/978-3-319-63688-7_12.
- [96] D. Ongaro and J. Ousterhout, ‘In Search of an Understandable Consensus Algorithm (Extended Version)’, in *Proceedings of the 2014 USENIX annual technical conference (USENIX ATC 14)*, Philadelphia, PA: USENIX Association, 2014, pp. 305–320.
- [97] K. Venkatesan and S. B. Rahayu, ‘Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques’, *Sci Rep*, vol. 14, no. 1, p. 1149, Dec. 2024, doi: 10.1038/S41598-024-51578-7.
- [98] C. Lepore, M. Ceria, A. Visconti, U. P. Rao, K. A. Shah, and L. Zanolini, ‘A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS’, *Mathematics MDPI*, vol. 8, no. 10, p. 1782, Oct. 2020, doi: 10.3390/math8101782.
- [99] G. Zhang, S. Ji, H. Dong, and P. Zhang, ‘An Improved PBFT Consensus Algorithm for Supply Chain Finance’, *Communications in Computer and Information Science*, vol. 1897 CCIS, pp. 339–352, 2024, doi: 10.1007/978-981-99-8104-5_25.
- [100] S. Liu, R. Zhang, C. Liu, and D. Shi, ‘P-PBFT: An improved blockchain algorithm to support large-scale pharmaceutical traceability’, *Comput Biol Med*, vol. 154, Mar. 2023, doi: 10.1016/J.COMPBIOMED.2023.106590.
- [101] W. Liu, Y. Li, X. Wang, Y. Peng, W. She, and Z. Tian, ‘A donation tracing blockchain model using improved DPoS consensus algorithm’, *Peer Peer Netw Appl*, vol. 14, no. 5, pp. 2789–2800, Sep. 2021, doi: 10.1007/S12083-021-01102-9/FIGURES/7.
- [102] S. Hattab, I. Fakhri, and T. Alyaseen, ‘Consensus Algorithms Blockchain: A comparative study’, *International Journal on Perceptive and Cognitive Computing*, vol. 5, no. 2, pp. 66–71, Dec. 2019, doi: 10.31436/IJPCC.V5I2.103.
- [103] A. Sarfaraz, R. K. Chakraborty, and D. L. Essam, ‘Reputation based proof of cooperation: an efficient and scalable consensus algorithm for supply chain applications’, *J Ambient Intell Humaniz Comput*, vol. 14, no. 6, pp. 7795–7811, Jun. 2023, doi: 10.1007/S12652-023-04592-Y.
- [104] S. Zhang and J. H. Lee, ‘Analysis of the main consensus protocols of blockchain’, *ICT Express*, vol. 6, no. 2, pp. 93–97, Jun. 2020, doi: 10.1016/J.ICTE.2019.08.001.
- [105] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, ‘A Survey of Distributed Consensus Protocols for Blockchain Networks’, *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2, pp. 1432–1465, Apr. 2020, doi: 10.1109/COMST.2020.2969706.
- [106] F. Tschorsch and B. Scheuermann, ‘Bitcoin and beyond: A technical survey on decentralized digital currencies’, *IEEE Communications Surveys and Tutorials*, vol. 18, no. 3, pp. 2084–2123, Jul. 2016, doi: 10.1109/COMST.2016.2535718.
- [107] C. Decker and R. Wattenhofer, ‘Information propagation in the Bitcoin network’, *13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P 2013 - Proceedings*, 2013, doi: 10.1109/P2P.2013.6688704.
- [108] Council of Supply Chain Management Professionals (CSCMP), ‘SCM Definitions and Glossary of Terms’. Accessed: Oct. 09, 2024. Available: https://cscmp.org/CSCMP/CSCMP/Educate/SCM_Definitions_and_Glossary_of_Terms.aspx
- [109] J. R. Stock and S. L. Boyer, ‘Developing a consensus definition of supply chain management: A qualitative study’, *International Journal of Physical Distribution and Logistics Management*, vol. 39, no. 8, pp. 690–711, Aug. 2009, doi: 10.1108/09600030910996323.
- [110] J. T. Mentzer *et al.*, ‘Defining Supply Chain Management’, *Journal of Business Logistics*, vol. 22, no. 2, pp. 1–25, Sep. 2001, doi: 10.1002/j.2158-1592.2001.tb00001.x.
- [111] D. M. Lambert and M. G. Enz, ‘Issues in Supply Chain Management: Progress and potential’, *Industrial Marketing Management*, vol. 62, pp. 1–16, Apr. 2017, doi: 10.1016/j.indmarman.2016.12.002.

- [112] K. Jeong and J.-D. Hong, 'The impact of information sharing on bullwhip effect reduction in a supply chain', *J Intell Manuf*, vol. 30, no. 4, pp. 1739–1751, Apr. 2019, doi: 10.1007/s10845-017-1354-y.
- [113] T. M. Fernandez-Carames and P. Fraga-Lamas, 'A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories', *IEEE Access*, vol. 7, pp. 45201–45218, 2019, doi: 10.1109/ACCESS.2019.2908780.
- [114] P. Dutta, T. M. Choi, S. Somani, and R. Butala, 'Blockchain technology in supply chain operations: Applications, challenges and research opportunities', *Transp Res E Logist Transp Rev*, vol. 142, Oct. 2020, doi: 10.1016/J.TRE.2020.102067.
- [115] A. Gurtu and J. Johny, 'Potential of blockchain technology in supply chain management: a literature review', *International Journal of Physical Distribution & Logistics Management*, vol. 49, no. 9, pp. 881–900, Nov. 2019, doi: 10.1108/IJPDLM-11-2018-0371.
- [116] R. Philipp, G. Prause, and L. Gerlitz, 'Blockchain and Smart Contracts for Entrepreneurial Collaboration in Maritime Supply Chains', *Transport and Telecommunication Journal*, vol. 20, no. 4, pp. 365–378, Dec. 2019, doi: 10.2478/ttj-2019-0030.
- [117] M. M. Queiroz, R. Telles, and S. H. Bonilla, 'Blockchain and supply chain management integration: a systematic review of the literature', *Supply Chain Management*, vol. 25, no. 2, pp. 241–254, Feb. 2020, doi: 10.1108/SCM-03-2018-0143.
- [118] S. R. Yerram, 'Smart Contracts for Efficient Supplier Relationship Management in the Blockchain', *American Journal of Trade and Policy*, vol. 9, no. 3, pp. 119–130, 2022.
- [119] D. Ivanov and A. Dolgui, 'New disruption risk management perspectives in supply chains: digital twins, the ripple effect, and resilience', *IFAC-PapersOnLine*, vol. 52, no. 13, pp. 337–342, Jan. 2019, doi: 10.1016/J.IFACOL.2019.11.138.
- [120] S. Kummer, D. M. Herold, M. Dobrovnik, J. Mikl, and N. Schäfer, 'A Systematic Review of Blockchain Literature in Logistics and Supply Chain Management: Identifying Research Questions and Future Directions', *Future Internet 2020, Vol. 12, Page 60*, vol. 12, no. 3, p. 60, Mar. 2020, doi: 10.3390/FI12030060.
- [121] R. Kumar Singh, R. Mishra, S. Gupta, and A. A. Mukherjee, 'Blockchain applications for secured and resilient supply chains: A systematic literature review and future research agenda', *Comput Ind Eng*, vol. 175, p. 108854, Jan. 2023, doi: 10.1016/J.CIE.2022.108854.
- [122] A. Jackson, V. L. M. Spiegler, and K. Kotiadis, 'Exploring the potential of blockchain-enabled lean automation in supply chain management: a systematic literature review, classification taxonomy, and future research agenda', *Production Planning & Control*, vol. 35, no. 9, pp. 866–885, Jul. 2024, doi: 10.1080/09537287.2022.2157746.
- [123] Y. Cui, V. Gaur, and J. Liu, 'Supply Chain Transparency and Blockchain Design', *Manage Sci*, vol. 70, no. 5, pp. 3245–3263, May 2024, doi: 10.1287/mnsc.2023.4851.
- [124] P. Helo and A. H. M. Shamsuzzoha, 'Real-time supply chain—A blockchain architecture for project deliveries', *Robot Comput Integr Manuf*, vol. 63, p. 101909, Jun. 2020, doi: 10.1016/J.RCIM.2019.101909.
- [125] J. Mendling *et al.*, 'Blockchains for Business Process Management - Challenges and Opportunities', *ACM Trans Manag Inf Syst*, vol. 9, no. 1, pp. 1–16, Mar. 2018, doi: 10.1145/3183367.
- [126] Feng Tian, 'A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things', in *2017 International Conference on Service Systems and Service Management*, IEEE, Jun. 2017, pp. 1–6. doi: 10.1109/ICSSSM.2017.7996119.
- [127] F. Tian, 'An agri-food supply chain traceability system for China based on RFID & blockchain technology', in *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, 2016, pp. 1–6. doi: 10.1109/ICSSSM.2016.7538424.
- [128] J. F. Galvez, J. C. Mejuto, and J. Simal-Gandara, 'Future challenges on the use of blockchain for food traceability analysis', *TrAC Trends in Analytical Chemistry*, vol. 107, pp. 222–232, 2018, doi: <https://doi.org/10.1016/j.trac.2018.08.011>.

- [129] M. Uddin, K. Salah, R. Jayaraman, S. Pesic, and S. Ellahham, 'Blockchain for drug traceability: Architectures and open challenges', *Health Informatics J*, vol. 27, no. 2, Apr. 2021, doi: 10.1177/14604582211011228.
- [130] G. M. Hastig and M. S. Sodhi, 'Blockchain for Supply Chain Traceability: Business Requirements and Critical Success Factors', *Prod Oper Manag*, vol. 29, no. 4, pp. 935–954, Apr. 2020, doi: 10.1111/poms.13147.
- [131] 'IBM Supply Chain Intelligence Suite - Food Trust'. Accessed: Oct. 09, 2024. Available: <https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust>
- [132] V. Sathiya, K. Nagalakshmi, K. Raju, and R. Lavanya, 'Tracking perishable foods in the supply chain using chain of things technology', *Sci Rep*, vol. 14, no. 1, p. 21621, Sep. 2024, doi: 10.1038/s41598-024-72617-3.
- [133] M. Kouhizadeh, Q. Zhu, L. Alkhuzaim, and J. Sarkis, 'Blockchain Technology and the Circular Economy: An Exploration', in *Circular Economy Supply Chains: From Chains to Systems*, L. Bals, W. L. Tate, and L. M. Ellram, Eds., Emerald Publishing Limited, 2022, pp. 189–213. doi: 10.1108/978-1-83982-544-620221010.
- [134] A. Di Vaio, S. Hasan, R. Palladino, and R. Hassan, 'The transition towards circular economy and waste within accounting and accountability models: a systematic literature review and conceptual framework', *Environ Dev Sustain*, vol. 25, no. 1, pp. 734–810, 2023, doi: 10.1007/s10668-021-02078-5.
- [135] H. Yusuf, I. Surjandari, and A. M. M. Rus, 'Multiple channel with crash fault tolerant consensus blockchain network: A case study of vegetables supplier supply chain', *2019 16th International Conference on Service Systems and Service Management, ICSSSM 2019*, Jul. 2019, doi: 10.1109/ICSSSM.2019.8887678.
- [136] R. Kamath, *Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM*, vol. 1, no. 1. 2018, pp. 1–12. doi: 10.31585/jbba-1-1-(10)2018.
- [137] Z. Liu, 'Literature Review of Supply Chain Finance Based on Blockchain Perspective', *Open Journal of Business and Management*, vol. 09, no. 01, pp. 419–429, 2021, doi: 10.4236/ojbm.2021.91022.
- [138] J. Parra Moyano and O. Ross, 'KYC Optimization Using Distributed Ledger Technology', *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 411–423, Dec. 2017, doi: 10.1007/s12599-017-0504-2.
- [139] G. Zhao *et al.*, 'Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions', *Comput Ind*, vol. 109, pp. 83–99, Aug. 2019, doi: 10.1016/j.compind.2019.04.002.
- [140] T. K. Mackey and G. Nayyar, 'A review of existing and emerging digital technologies to combat the global trade in fake medicines', *Expert Opin Drug Saf*, vol. 16, no. 5, pp. 587–602, May 2017, doi: 10.1080/14740338.2017.1313227.
- [141] M. H. Meng and Y. Qian, 'A Blockchain Aided Metric for Predictive Delivery Performance in Supply Chain Management', in *2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, IEEE, Jul. 2018, pp. 285–290. doi: 10.1109/SOLI.2018.8476723.
- [142] S. F. Turner, L. B. Cardinal, and R. M. Burton, 'Research Design for Mixed Methods: A Triangulation-based Framework and Roadmap', *Organ Res Methods*, vol. 20, no. 2, pp. 243–267, Nov. 2015, doi: 10.1177/1094428115610808.
- [143] P. S. Myers, *Knowledge Management and Organisational Design*, vol. 1. Routledge, 2009. doi: 10.4324/9780080509839.
- [144] P. Yetton, A. Martin, R. Sharma, and K. Johnston, 'A model of information systems development project performance', *Information Systems Journal*, vol. 10, no. 4, pp. 263–289, Oct. 2000, doi: 10.1046/j.1365-2575.2000.00088.x.
- [145] J. Leukel and S. Kirn, 'A supply chain management approach to logistics ontologies in information systems', in *Business Information Systems: 11th International Conference, BIS 2008, Innsbruck, Austria, May 5-7, 2008. Proceedings 11*, Springer, 2008, pp. 95–105.
- [146] T. Edgar and D. Manz, *Research Methods for Cyber Security*. Cambridge, Ma: Syngress, 2017.

- [147] G. M. Nyabuto and F. Wabwoba, 'Philosophical paradigms in information technology research', *World Journal of Advanced Engineering Technology and Sciences*, vol. 11, no. 2, pp. 567–577, Apr. 2024, doi: 10.30574/wjaets.2024.11.2.0141.
- [148] V. L. Plano Clark, 'Mixed methods research', *J Posit Psychol*, vol. 12, no. 3, pp. 305–306, May 2017, doi: 10.1080/17439760.2016.1262619.
- [149] N. R. Haddaway, M. J. Page, C. C. Pritchard, and L. A. McGuinness, 'PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis', *Campbell Systematic Reviews*, vol. 18, no. 2, p. e1230, Jun. 2022, doi: 10.1002/CL2.1230.
- [150] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, 'Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement', *PLoS Med*, vol. 6, no. 7, p. e1000097, Jul. 2009, doi: 10.1371/journal.pmed.1000097.
- [151] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, 'Systematic Mapping Studies in Software Engineering', in *12th International Conference on Evaluation and Assessment in Software Engineering, EASE 2008*, BCS Learning & Development, Jun. 2008. doi: 10.14236/ewic/EASE2008.8.
- [152] B. A. Kitchenham, 'Systematic review in software engineering', in *Proceedings of the 2nd international workshop on Evidential assessment of software technologies*, New York, NY, USA: ACM, Sep. 2012, pp. 1–2. doi: 10.1145/2372233.2372235.
- [153] C. Wohlin, 'Guidelines for snowballing in systematic literature studies and a replication in software engineering', *ACM International Conference Proceeding Series*, 2014, doi: 10.1145/2601248.2601268.
- [154] M. Amir-Behghadami and A. Janati, 'Population, Intervention, Comparison, Outcomes and Study (PICOS) design as a framework to formulate eligibility criteria in systematic reviews', *Emergency Medicine Journal*, vol. 37, no. 6, pp. 387–387, Jun. 2020, doi: 10.1136/emered-2020-209567.
- [155] G. Dodig-Crnkovic, 'Scientific Methods in Computer Science', in *Proceedings of the Conference for the Promotion of Research in IT at New Universities and at University Colleges in Sweden*, Skövde, Suecia, Apr. 2002, pp. 126–130.
- [156] A. Hevner and S. Chatterjee, 'Design Science Research in Information Systems', in *MIS Quarterly*, vol. 22, no. 1, Boston, MA.: Springer, 2010, pp. 9–22. doi: 10.1007/978-1-4419-5653-8_2.
- [157] X. Ma, H. Wu, D. Xu, and K. Wolter, 'CBlockSim: A Modular High-Performance Blockchain Simulator', in *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, IEEE, May 2022, pp. 1–5. doi: 10.1109/ICBC54727.2022.9805504.
- [158] M. J. Ramezankhani, S. A. Torabi, and F. Vahidi, 'Supply chain performance measurement and evaluation: A mixed sustainability and resilience approach', *Comput Ind Eng*, vol. 126, pp. 531–548, Dec. 2018, doi: 10.1016/j.cie.2018.09.054.
- [159] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, 'Blockchain in healthcare applications: Research challenges and opportunities', *Journal of Network and Computer Applications*, vol. 135, pp. 62–75, Jun. 2019, doi: 10.1016/j.jnca.2019.02.027.
- [160] M. Attaran, 'RFID: an enabler of supply chain operations', *Supply Chain Management: An International Journal*, vol. 12, no. 4, pp. 249–257, Jun. 2007, doi: 10.1108/13598540710759763.
- [161] D. Tranfield, D. Denyer, and P. Smart, 'Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review', *British Journal of Management*, vol. 14, no. 3, pp. 207–222, Sep. 2003, doi: 10.1111/1467-8551.00375.
- [162] J. Webster and R. T. Watson, 'Analyzing the Past to Prepare for the Future: Writing a Literature Review', *MIS Quarterly*, vol. 26, no. 2, pp. xiii–xxiii, 2002, doi: 10.2307/4132319.
- [163] C. Okoli and K. Schabram, 'A Guide to Conducting a Systematic Literature Review of Information Systems Research', *SSRN Electronic Journal*, 2010, doi: 10.2139/ssrn.1954824.
- [164] M. Conoscenti, A. Vetro, and J. C. De Martin, 'Blockchain for the Internet of Things: A systematic literature review', *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, vol. 0, Jul. 2016, doi: 10.1109/AICCSA.2016.7945805.

- [165] S. Seebacher and R. Schüritz, 'Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review', in *Lecture Notes in Business Information Processing*, vol. 279, Springer Verlag, 2017, pp. 12–23. doi: 10.1007/978-3-319-56925-3_2.
- [166] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, 'Security Services Using Blockchains: A State of the Art Survey', *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 858–880, Jan. 2019, doi: 10.1109/COMST.2018.2863956.
- [167] Q. Song, Y. Chen, Y. Zhong, K. Lan, S. Fong, and R. Tang, 'A Supply-chain System Framework Based on Internet of Things Using Blockchain Technology', *ACM Trans. Internet Technol.*, vol. 21, no. 1, Jan. 2021, doi: 10.1145/3409798.
- [168] B. Liu, X. Si, and H. Kang, 'A Literature Review of Blockchain-Based Applications in Supply Chain', *Sustainability*, vol. 14, no. 22, 2022, doi: 10.3390/su142215210.
- [169] R. Kumar Singh, R. Mishra, S. Gupta, and A. A. Mukherjee, 'Blockchain applications for secured and resilient supply chains: A systematic literature review and future research agenda', *Comput Ind Eng*, vol. 175, Jan. 2023, doi: 10.1016/J.CIE.2022.108854.
- [170] Blockchain Development Services, 'Decoding the Cost of Implementing Blockchain Supply Chain Software', Medium Website. Accessed: Apr. 28, 2023. Available: <https://medium.com/@pamelawatsona3/decoding-the-cost-of-implementing-blockchain-supply-chain-software-75deabb8ab42>
- [171] S. Mollajafari and K. Bechkoum, 'Blockchain Technology and Related Security Risks: Towards a Seven-Layer Perspective and Taxonomy', *Sustainability*, vol. 15, no. 18, 2023, doi: 10.3390/su151813401.
- [172] A. Abhishta, R. Joosten, S. Dragomiretskiy, and L. J. M. Nieuwenhuis, 'Impact of Successful DDoS Attacks on a Major Crypto-Currency Exchange', in *2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*, IEEE, Feb. 2019, pp. 379–384. doi: 10.1109/EMPDP.2019.8671642.
- [173] S. De Angelis, F. Lombardi, G. Zanfino, L. Aniello, and V. Sassone, 'Security and dependability analysis of blockchain systems in partially synchronous networks with Byzantine faults', *International Journal of Parallel, Emergent and Distributed Systems*, pp. 1–21, Oct. 2023, doi: 10.1080/17445760.2023.2272777.
- [174] K. Dwivedi, A. Agrawal, A. Bhatia, and K. Tiwari, 'A Novel Classification of Attacks on Blockchain Layers: Vulnerabilities, Attacks, Mitigations, and Research Directions', Apr. 2024. Available: <http://arxiv.org/abs/2404.18090>
- [175] Y. Chen, H. Chen, Y. Zhang, M. Han, M. Siddula, and Z. Cai, 'A survey on blockchain systems: Attacks, defenses, and privacy preservation', *High-Confidence Computing*, vol. 2, no. 2, p. 100048, 2022, doi: <https://doi.org/10.1016/j.hcc.2021.100048>.
- [176] A. Alkhalifah *et al.*, 'A Taxonomy of Blockchain Threats and Vulnerabilities', 2019, doi: 10.20944/preprints201909.0117.v1.
- [177] L. Er-Rajy, M. A. El Kiram, El Ghazouani Mohamed, and O. Achbarou, 'Blockchain: Bitcoin Wallet Cryptography Security, Challenges and Countermeasures', *Journal of Internet Banking and Commerce*, vol. 22, no. 3, 2017, Accessed: Dec. 19, 2023. Available: <https://www.icommercecentral.com/open-access/blockchain-bitcoin-wallet-cryptography-security-challenges-and-countermeasures.php?aid=86561>
- [178] L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, 'Making smart contracts smarter', *Proceedings of the ACM Conference on Computer and Communications Security*, vol. 24-28-October-2016, pp. 254–269, Oct. 2016, doi: 10.1145/2976749.2978309.
- [179] N. Atzei, M. Bartoletti, and T. Cimoli, 'A Survey of Attacks on Ethereum Smart Contracts (SoK)', in *Proceedings of the 6th International Conference on Principles of Security and Trust*, M. Matteo and R. Mark, Eds., Berlin: Springer Verlag, Apr. 2017, pp. 164–186. doi: 10.1007/978-3-662-54455-6_8.
- [180] M. Apostolaki, A. Zohar, and L. Vanbever, 'Hijacking Bitcoin: Routing Attacks on Cryptocurrencies', *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 375–392, May 2017, doi: 10.1109/SP.2017.29.

- [181] M. Saad *et al.*, ‘Exploring the Attack Surface of Blockchain: A Systematic Overview’, Apr. 2019, Accessed: Dec. 19, 2023. Available: <https://arxiv.org/abs/1904.03487v1>
- [182] P. Zheng, Z. Zheng, X. Luo, X. Chen, and X. Liu, ‘A detailed and real-time performance monitoring framework for blockchain systems’, in *Proceedings of the 40th International Conference on Software Engineering: Software Engineering in Practice*, New York, NY, USA: ACM, May 2018, pp. 134–143. doi: 10.1145/3183519.3183546.
- [183] R. Paulavičius, S. Grigaitis, A. Igumenov, and E. Filatovas, ‘A Decade of Blockchain: Review of the Current Status, Challenges, and Future Directions’, *Informatica*, vol. 30, no. 4, pp. 729–748, Jan. 2019.
- [184] J. Yang, Z. Jia, R. Su, X. Wu, and J. Qin, ‘Improved Fault-Tolerant Consensus Based on the PBFT Algorithm’, *IEEE Access*, vol. 10, pp. 30274–30283, 2022, doi: 10.1109/ACCESS.2022.3153701.
- [185] R. Beck, C. Müller-Bloch, and J. L. King, ‘Governance in the Blockchain Economy: A Framework and Research Agenda’, *J Assoc Inf Syst*, vol. 19, no. 10, pp. 1020–1034, Oct. 2018, doi: 10.17705/1jais.00518.
- [186] C. Faria and M. Correia, ‘BlockSim: Blockchain Simulator’, GitHub. Accessed: Sep. 18, 2023. Available: <https://github.com/BlockbirdLabs/blocksim>
- [187] M. Alharby and A. van Moorsel, ‘BlockSim: An Extensible Simulation Tool for Blockchain Systems’, *Frontiers in Blockchain*, vol. 3, p. 459097, Apr. 2020, doi: 10.3389/fbloc.2020.00028.
- [188] M. Basile, G. Nardini, P. Perazzo, and G. Dini, ‘SegWit Extension and Improvement of the BlockSim Bitcoin Simulator’, in *2022 IEEE International Conference on Blockchain (Blockchain)*, IEEE, Aug. 2022, pp. 115–123. doi: 10.1109/Blockchain55522.2022.00025.
- [189] S. M. S. Saad, R. Z. R. M. Radzi, and S. H. Othman, ‘Comparative Analysis of the Blockchain Consensus Algorithm Between Proof of Stake and Delegated Proof of Stake’, in *2021 International Conference on Data Science and Its Applications (ICoDSA)*, IEEE, Oct. 2021, pp. 175–180. doi: 10.1109/ICoDSA53588.2021.9617549.
- [190] S. Tanwar, ‘Distributed Consensus for Permissioned Blockchain’, Springer, Singapore, 2022, pp. 211–249. doi: 10.1007/978-981-19-1488-1_8.
- [191] Q. Xiong, N. Sohrabi, H. Dong, C. Xu, and Z. Tari, ‘AICons: An AI-Enabled Consensus Algorithm Driven by Energy Preservation and Fairness’, *Distributed, Parallel, and Cluster Computing*, Apr. 2023, doi: 10.48550.
- [192] K. Prasanna, K. Ramana, G. Dhiman, S. Kautish, and V. D. Chakravarthy, ‘PoC Design: A Methodology for Proof-of-Concept (PoC) Development on Internet of Things Connected Dynamic Environments’, *Security and Communication Networks*, vol. 2021, no. 1, pp. 1–12, Oct. 2021, doi: 10.1155/2021/7185827.
- [193] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, ‘A Secure Sharding Protocol For Open Blockchains’, in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, Oct. 2016, pp. 17–30. doi: 10.1145/2976749.2978389.
- [194] B. Xiao, C. Jin, Z. Li, B. Zhu, X. Li, and D. Wang, ‘Proof of Importance: A Consensus Algorithm for Importance Based on Dynamic Authorization’, in *IEEE/WIC/ACM International Conference on Web Intelligence*, New York, NY, USA: ACM, Dec. 2021, pp. 510–513. doi: 10.1145/3498851.3499007.
- [195] M. U. Hassan, M. H. Rehmani, and J. Chen, ‘Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions’, *Future Generation Computer Systems*, vol. 97, pp. 512–529, Aug. 2019, doi: 10.1016/j.future.2019.02.060.
- [196] O. Aluko and A. Kolonin, ‘Proof-of-Reputation: An Alternative Consensus Mechanism for Blockchain Systems’, *International Journal of Network Security & Its Applications*, vol. 13, no. 04, pp. 23–40, Jul. 2021, doi: 10.5121/ijnsa.2021.13403.
- [197] D. Mazières, ‘The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus’, Jul. 2015.

- [198] E. K. Wang, R. Sun, C.-M. Chen, Z. Liang, S. Kumari, and M. Khurram Khan, ‘Proof of X-repute blockchain consensus protocol for IoT systems’, *Comput Secur*, vol. 95, p. 101871, Aug. 2020, doi: 10.1016/j.cose.2020.101871.
- [199] G. Xu, Y. Liu, and P. W. Khan, ‘Improvement of the DPoS Consensus Mechanism in Blockchain Based on Vague Sets’, *IEEE Trans Industr Inform*, vol. 16, no. 6, pp. 4252–4259, Jun. 2020, doi: 10.1109/TII.2019.2955719.
- [200] R. H. Pereira, M. J. Gonçalves, and M. A. G. Magalhães, ‘Reputation Systems: A framework for attacks and frauds classification’, *Journal of Information Systems Engineering and Management*, vol. 8, no. 1, p. 19218, Jan. 2023, doi: 10.55267/iadt.07.12830.
- [201] I. Malakhov, A. Marin, S. Rossi, and D. S. Menasché, ‘Confirmed or Dropped? Reliability Analysis of Transactions in PoW Blockchains’, *IEEE Trans Netw Sci Eng*, vol. 11, no. 4, pp. 3276–3288, Jul. 2024, doi: 10.1109/TNSE.2024.3360080.

10 Appendices

Appendix 1

Full List of Systematic Literature Review

The systematic literature review provides an analysis of 108 existing research and key literature findings relevant to the topics (Blockchain + Supply Chain Management + Cybersecurity) being assess. By synthesising data from multiple sources, the review establishes a foundation for further research and highlights areas for potential exploration.

| Refere | Authors | Title | Year | Abstract | Document Ty | Findings | Category |
|--------|---|--|------|--|---------------|--|--|
| D1 | Tan J.; Goyal S.B.; Singh Rajawat A.; Jan T.; Azizi N.; Prasad M. | Anti-Counterfeiting and Traceability Consensus Algorithm Based on Weightage to Contributors in a Food Supply Chain of Industry 4.0 | 2023 | Supply chain management can significan | Article | Enhances supply chain transparency and trust through a weight | Consensus Mechanism Failures/Enhancements |
| D2 | Dhyanesh B.; Shakkeera L.; Sharmasth V.Y.; Azath H.; Viswanathan S.K.; Poonuramu V | Improved privacy of data transaction in iot-enabled blockchain technology using privacy-based machine learning algorithms | 2023 | Conventional models rely on a trusted thir | Book chapter | Discusses the enhancement of data privacy in IoT systems usin | Consensus Mechanism Failures/Enhancements |
| D3 | Li Y.; Wang J.; Zhang H. | A survey of state-of-the-art sharding blockchains: Models, components, and attack surfaces | 2023 | Blockchain has been widely used in vario | Review | Reviews blockchain sharding to improve performance and secu | Consensus Mechanism Failures/Enhancements |
| D4 | Clohesy T. | Blockchain in Supply Chain Digital Transformation | 2023 | Blockchain and distributed ledger technol | Book | Explores the role of blockchain in enhancing global supply cha | Consensus Mechanism Failures/Enhancements |
| D5 | Viswanadham Y.V.R.S.; Jayavel K. | A Framework for Data Privacy Preserving in Supply Chain Management Using Hybrid Meta-Heuristic Algorithm with Ethereum Blockchain Technology | 2023 | Blockchain is a recently developed advan | Article | Describes a framework that integrates blockchain with a hybrid | Consensus Mechanism Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D6 | Pereira B.M.B.; Torres J.M.; Sobral P.M.; Moreira R.S.; Soares C.P.D.A.; Pereira I. | Blockchain-Based Electronic Voting: A Secure and Transparent Solution | 2023 | Since its appearance in 2008, blockchain | Article | Discusses the use of blockchain in voting systems to enhance s | Consensus Mechanism Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D7 | Zhang B.; Xu J.; Wang X.; Zhao Z.; Chen S.; Zhang X. | Research on the Construction of Grain Food Multi-Chain Blockchain Based on Zero-Knowledge Proof | 2023 | As the main food source of the world, AOs | Article | Focuses on improving grain food supply chain safety using bloc | Consensus Mechanism Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D8 | Verma R.; Dhanda N. | Blockchain types: A characteristic view | 2023 | Blockchain became the buzzword when it | Book chapter | Reviews different blockchain types and their evolution since Bri | Consensus Mechanism Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D9 | Kumar Singh R.; Mishra R.; Gupta S.; Mukherjee A.A. | Blockchain applications for secured and resilient supply chains: A systematic literature review and future research agenda | 2023 | Firms are using blockchain technology to | Article | Reviews blockchain's role in securing supply chains against fra | Consensus Mechanism Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D10 | Goyal A.; Kanyal H.S.; Sharma B. | Analysis of IoT and Blockchain Technology for Agricultural Food Supply Chain Transactions | 2023 | The Block chain is a peer to peer, distribu | Article | Analyses the integration of IoT and blockchain to secure agricul | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements |
| D11 | Dodmane R.; K. R.; R.; N. S.; K.R.; Kallapu, B.; Shetty, S.; Aslam, M.; Jilani, S.F. | Blockchain-Based Automated Market Makers for a Decentralized Stock Exchange | 2023 | The advancements in communication spe | Article | The findings highlight that the proposed framework for decentra | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements |
| D12 | Li D.; Han D.; Crespi N.; Minerva R.; Li K.-C. | A blockchain-based secure storage and access control scheme for supply chain finance | 2023 | Supply chain finance (SCF) provides cred | Article | Discusses a blockchain solution for secure storage and access | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements |
| D13 | Nanda S.K.; Panda S.K.; Dash M. | Medical supply chain integrated with blockchain and IoT to track the logistics of medical products | 2023 | Nowadays blockchain technology plays a | Article | Describes an integrated approach using blockchain and IoT to | Cryptographic Challenges/Enhancements |
| D14 | Aljabhan B.; Obaidat M.A. | Privacy-Preserving Blockchain Framework for Supply Chain Management: Perceptive Craving Game Search Optimization (PCGSO) | 2023 | The fierce competition in international ma | Article | Proposes a blockchain framework that enhances privacy and se | Cryptographic Challenges/Enhancements |
| D15 | Karumanchi M.D.; Sheeba J.I.; Devaneyan S.P. | An efficient integrity based multi-user blockchain framework for heterogeneous supply chain management applications | 2023 | Most of the traditional cloud-based applic | Article | Focuses on improving data integrity in cloud-based supply cha | Cryptographic Challenges/Enhancements |
| D16 | Patel H.; Shrimati B. | AgriOnBlock: Secured data harvesting for agriculture sector using blockchain technology | 2023 | The existing agriculture system is having | Article | Discusses blockchain in agriculture for secure data harvesting, | Smart Contract Vulnerabilities/Failures/Enhancements |
| D17 | Zhang G.; Yang Z.; Liu W. | Blockchain-based decentralized supply chain system with secure information sharing | 2023 | Supply chain management (SCM) has bee | Article | Highlights the implementation of a decentralised SCM system u | Smart Contract Vulnerabilities/Failures/Enhancements |
| D18 | Ghaleb, A.; Rubin, J.; Pattabiraman, K. | AChecker: Statically Detecting Smart Contract Access Control Vulnerabilities | 2023 | As most smart contracts have a financi | Article | The study introduces AChecker, a tool that statically detects ac | Smart Contract Vulnerabilities/Failures/Enhancements |
| D19 | W. -B. Hsieh, J. -S. Leu and J. -I. Takada, | Use chains to block DNS attacks: A trusty blockchain-based domain name system | 2022 | The internet has become one of the most | Article | The mechanism proposed uses blockchain to secure DNS and | Consensus Mechanism Failures/Enhancements, Network-Level Attacks Failures/Enhancements |
| D20 | N J.; Rampur V.; Gangodkar D.; M. A.; C. B.; N. A.K. | Improved block chain system for high secured IoT integrated supply chain | 2023 | The incredibly complex supply chains in | Article | Discusses advancements in blockchain technology to secure lo | Smart Contract Vulnerabilities/Failures/Enhancements |
| D21 | Zkik K.; Sebbar A.; Nejari N.; Lahlou S.; Fadi O.; Oudani M. | Secure Model for Records Traceability in Airline Supply Chain Based on Blockchain and Machine Learning | 2023 | With the enormous amount of sensitive d | Book chapter | Proposes a blockchain model to improve traceability and securi | Smart Contract Vulnerabilities/Failures/Enhancements |
| D22 | Wang D.; Yu A. | Supply Chain resources and economic Security Based on Artificial Intelligence and Blockchain Multi-Channel Technology | 2023 | With the rapid growth of social economy | Article | Analyses the impact of AI and blockchain on improving securi | Smart Contract Vulnerabilities/Failures/Enhancements |
| D23 | Magar S.; Doshi M.; Talib S.; Dalvi H. | Blockchain-based reliable supply chain management (SCM) for vaccine distribution and traceability using identity management approach | 2023 | The advent of the COVID-19 pandemic ha | Book chapter | Explores blockchain's role in enhancing traceability and securi | Smart Contract Vulnerabilities/Failures/Enhancements |
| D24 | Chen S.; Yang L.; Shi Y.; Wang Q. | Blockchain-Enabled Secure and Privacy-Preserving Data Aggregation for Fog-Based ITS | 2023 | As an essential component of intelligent t | Article | Discusses blockchain's application in intelligent transportation | Network-Level Attacks Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D25 | Li J.; Han D.; Wu Z.; Wang J.; Li K.-C.; Castiglione A. | A novel system for medical equipment supply chain traceability based on alliance chain and attribute and role access control | 2023 | With the increasing sales of the medical | Article | Focuses on blockchain for medical equipment traceability, addr | Smart Contract Vulnerabilities/Failures/Enhancements |
| D26 | Shittu H.; Nabil M. | Smart Supply Chain Management with Attribute-Based Encryption Access Control | 2023 | The traditional supply chain management | Conference pa | Examines the integration of attribute-based encryption access | Smart Contract Vulnerabilities/Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D27 | Ashraf M.; Ali I. | Evaluation of project completion time prediction accuracy in a disrupted blockchain-enabled project-based supply chain | 2023 | Disruption risks may arise in a project-bas | Article | Evaluates the accuracy of project completion predictions in bloc | Smart Contract Vulnerabilities/Failures/Enhancements |
| D28 | T. M.; Makkithaya K.; V.G. N. | A trusted IoT data sharing and secure oracle based access for agricultural production risk management | 2023 | Agricultural risks associated with weathe | Article | Discusses using blockchain for secure data sharing in agricultu | Smart Contract Vulnerabilities/Failures/Enhancements |
| D29 | Shinkar S.V.; Thankachan D. | SCMBOA: Design of a Customised SCM-Aware Sidechaining Model for QoS Enhancement under Attack Scenarios | 2022 | Storing & processing data for supply cha | Article | Designs a sidechaining model to enhance QoS in SCM, addres | Consensus Mechanism Failures/Enhancements |
| D30 | Huang X.; Zhang Y.; Li D.; Han L. | A Solution for Bilayer Energy-Trading Management in Microgrids Using MultiBlockchain | 2022 | In recent years, microgrids have attracte | Article | Focuses on using multiple blockchains to manage energy tradin | Consensus Mechanism Failures/Enhancements |
| D31 | Andrew J.; Deva Priya Isravel b. K. Martin Sagayam c. Bharat Bhushan d. Yuichi Sei e. | Blockchain for healthcare systems: Architecture, security challenges, trends and future directions | 2023 | Blockchain has become popular in recent | Article | The study finds that blockchain presents substantial opportuniti | Consensus Mechanism Failures/Enhancements |
| D32 | Saad, M.; Anwar, A.; Ahmad, A.; Alasmay, H.; Yuksel, M.; Mohaisen, D. | RouteChain: Towards Blockchain-Based Secure and Efficient BGP Routing. | 2022 | Routing on the Internet is defined among | Article | Findings suggest that the RouteChain mechanism enhances BGP | Network-Level Attacks Failures/Enhancements |
| D33 | Ravali B.R. | Introduction to blockchain in supply chain management | 2022 | In a volatile, uncertain, complex, and amb | Editorial | Discusses blockchain's role looking at the different applicatio | Consensus Mechanism Failures/Enhancements |
| D34 | Li X.; Lu W.; Xue F.; Wu L.; Zhao R.; Lou J.; Xu J. | Blockchain-Enabled IoT-BIM Platform for Supply Chain Management in Modular Construction | 2022 | Configuring a trustworthy Internet of Thin | Article | Implements a blockchain-enabled IoT-BIM platform to secure m | Consensus Mechanism Failures/Enhancements |
| D35 | Ali J.; Sofi S.A. | Blockchain-enabled architecture with selective consensus mechanisms for IoT-based saffron-Agri value chain | 2022 | The Internet of Things (IoT) is the backbo | Article | Explores how blockchain can optimize IoT networks for the saff | Consensus Mechanism Failures/Enhancements |
| D36 | Mubashar Iqbal; Raimundas Matulevicius | Exploring Sybil and Double-Spending Risks in Blockchain Systems | 2021 | The first step to realise the true potentia | Article | The framework developed by the authors successfully explores | Consensus Mechanism Failures/Enhancements |
| D37 | Platt, M.; McBurney, P.; | Sybil in the Haystack: A Comprehensive Review of Blockchain Consensus Mechanisms in Search of Strong Sybil Attack Resistance | 2023 | Consensus algorithms are applied in the | Article | Through a comprehensive review, the study identifies mechan | Consensus Mechanism Failures/Enhancements, Network-Level Attacks Failures/Enhancements |
| D38 | Burra M.S.; Maitly S. | Characteristics, advances, and challenges in blockchain-enabled cyber-physical systems | 2022 | A cyber-physical system (CPS) is a compl | Book chapter | Investigate blockchain integration in cyber-physical systems, en | Consensus Mechanism Failures/Enhancements |
| D39 | Rahman M.S.; Khalili I.; Bouras A. | Designing an efficient consensus protocol for supply chain | 2022 | Blockchain is being a game-changer for | Book chapter | Develops an efficient blockchain consensus protocol for supply | Consensus Mechanism Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D40 | Zheng K.; Zheng L.J.; Gauthier J.; Zhou L.; Xu Y.; Behl A.; Zhang J.Z. | Blockchain technology for enterprise credit information sharing in supply chain finance | 2022 | Credit data barriers, such as incomplete | Article | Tackles the challenge of unreliable credit data in supply chain | Consensus Mechanism Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D41 | Obero O.; Raj S. | Advanced Cryptographic Technologies in Blockchain | 2022 | Blockchain technology is a kind of distribu | Book chapter | Investigates advanced cryptography solutions in blockchain to | Consensus Mechanism Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D42 | Al-Shareeda, M.A.; Manickam, S.; Laghari, S.A.; Jaisan, A. | Replay-Attack Detection and Prevention Mechanism in Industry 4.0 Landscape for Secure SECS/GEM Communications. | 2022 | Starting from the First Industrial Revolutio | Article | This paper demonstrates that SECS/GEM systems are vulnerab | Network-Level Attacks Failures/Enhancements |
| D43 | Venkat Narayana Rao T.; Likhari P.P.; Kurni M.; Saritha K. | Blockchain: A new perspective in cyber technology | 2022 | The early days of cyberspace expansion | Book chapter | Addresses blockchain's role in cybersecurity by enhancing digit | Consensus Mechanism Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D44 | Ruan N.; Sun H.; Lou Z.; Li J.; | A General Quantitative Analysis Framework for Attacks in Blockchain | 2022 | Decentralized cryptocurrency systems ha | Article | The paper proposes a quantitative analysis framework for attac | Consensus Mechanism Failures/Enhancements, Network-Level Attacks Failures/Enhancements |
| D45 | Gao N.; Han D.; Weng T.-H.; Xia B.; Li D.; Castiglione A.; Li K.-C. | Modeling and analysis of port supply chain system based on Fabric blockchain | 2022 | With the development of international tra | Article | Examines the port supply chain system by employing blockchai | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements |
| D46 | Peng X.; Zhang X.; Wang X.; Li H.; Xu J.; Zhao Z.; Wang Y. | Research on the Cross-Chain Model of Rice Supply Chain Supervision Based on Parallel Blockchain and Smart Contracts | 2022 | Rice is one of the three major staple food | Article | Researches rice supply chain supervision using a cross-chain b | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements |
| D47 | Rasolroveicy M.; Fokaefs M.; | Impact of DDoS Attacks on the Performance of Blockchain Consensus as an IoT Data Registry: An Empirical Study | 2022 | The current proliferation of blockchain tec | Article | This study highlights the impact of DDoS attacks on the | Consensus Mechanism Failures/Enhancements, Network-Level Attacks Failures/Enhancements |
| D48 | Bhat S.A.; Huang N.-F.; Sofi I.B.; Sultan M. | Agriculture-Food Supply Chain Management Based on Blockchain and IoT: A Narrative on Enterprise Blockchain Interoperability | 2022 | Modern-day agriculture supply chains hav | Review | Reviews blockchain applications in agriculture-food supply cha | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements |
| D49 | Liu B.; Si X.; Kang H. | A Literature Review of Blockchain-Based Applications in Supply Chain | 2022 | Blockchain technology is an emerging tec | Review | Provides a review of blockchain applications in supply chain m | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D50 | Bhushan B.; Kadam K.; Parashar R.; Kumar S.; Shakur A.K. | Leveraging Blockchain Technology in Sustainable Supply Chain Management and Logistics | 2022 | Traditional supply chain management (SC | Book chapter | Utilises blockchain technology to augment the sustainability of | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D51 | Poquiz W.A. | Blockchain Technology in Healthcare: An Analysis of Strengths, Weaknesses, Opportunities, and Threats | 2022 | SUMMARYThe dawn of the crypto age ha | Article | Assesses the various uses of blockchain technology in the heal | Cryptographic Challenges/Enhancements |
| D52 | Aranda R.S.; Silva R.F.; Cugnasca C.E. | Requirements Identification for a Blockchain-Based Traceability Model for Animal-Based Medicines ,A | 2021 | In this paper, the traceability of heparin m | Article | Focuses on developing a blockchain-based traceability model fo | Consensus Mechanism Failures/Enhancements |
| D53 | Wen, Y.; Lu, F.; Liu, Y.; Huang, X. | Attacks and countermeasures on blockchains: A survey from layering perspective | 2021 | Blockchain is an emerging technology wit | Article | A survey of attacks and countermeasures on blockchain networ | Consensus Mechanism Failures/Enhancements, Network-Level Attacks Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D54 | Qun Song A.; Chen Y.; Zhong Y.; Lan K.; Fong S.; Rui Tang B. | A Supply-chain System Framework Based on Internet of Things Using Blockchain Technology | 2021 | Numerous supply-chain combines with in | Article | Proposes a supply chain system framework integrating IoT with | Consensus Mechanism Failures/Enhancements |
| D55 | Tang G.; Zeng H. | Collaborative management and control of blockchain in cloud computing environment | 2021 | Cloud computing, as a product of the fusi | Article | Discusses the integration of blockchain in cloud computing env | Consensus Mechanism Failures/Enhancements |
| D56 | Al-Rakhami M.S.; Al-Mashari M. | A blockchain-based trust model for the internet of things supply chain management | 2021 | Accurate data and strategic business pro | Article | Develops a blockchain-based trust model for IoT supply chain | Consensus Mechanism Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D57 | Li, Z.; Gao, S.; Peng, Z.; Guo, S.; Yang, Y.; Xiao, B. | B-DNS: A Secure and Efficient DNS Based on the Blockchain Technology | 2021 | The Domain Name System (DNS) plays a | Article | The findings show that the proposed blockchain-based DNS sy | Network-Level Attacks Failures/Enhancements |
| D58 | Yiu N.C.K. | Decentralizing supply chain anti-counterfeiting and traceability systems using blockchain technology | 2021 | An interesting research problem in the su | Article | Investigates the decentralisation of supply chain-systems for an | Consensus Mechanism Failures/Enhancements, Cryptographic Challenges/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements |
| D59 | Abidi M.H.; Alkhalafah H.; Umer U.; Mohammed M.K. | Blockchain-based secure information sharing for supply chain management: Optimization assisted data sanitization process | 2021 | Currently, the furious competitiveness in | Article | Explores the utilisation of blockchain technology to provide sec | Cryptographic Challenges/Enhancements |
| D60 | Al-Farsi S.; Rathore M.M.; Bakiras S. | Security of blockchain-based supply chain management systems: Challenges and opportunities | 2021 | Blockchain is a revolutionary technology t | Article | Explores the security aspects of blockchain-based supply chain | Smart Contract Vulnerabilities/Failures/Enhancements |
| D61 | Kearney, J.J.; Perez-Delgado, C.A. | Vulnerability of Blockchain Technologies to Quantum Attacks | 2021 | Blockchain has revolutionized numerous | Article | The study explores the vulnerability of blockchain technologies | Cryptographic Challenges/Enhancements |
| D62 | Bayramova A.; Edwards D.J.; Roberts C. | The role of blockchain technology in augmenting supply chain resilience to cybercrime | 2021 | Using a systematic review of literature, th | Review | Reviews the role of blockchain in augmenting the resilience of | Smart Contract Vulnerabilities/Failures/Enhancements |
| D63 | Cheung K.-F.; Bell M.G.H.; Bhattacharjya J. | Cybersecurity in logistics and supply chain management: An overview and future research directions | 2021 | Technological applications have increas | Article | Discusses the topic of cybersecurity in logistics and supply cha | Cryptographic Challenges/Enhancements |
| D64 | Sai, A.R.; Buckley, J.; Fitzgerald, B.; Le Gear, A. | Taxonomy of Centralization in Public Blockchain Systems: A Systematic Literature Review | 2021 | Bitcoin introduced delegation of control | Article | public blockchain systems, developing a taxonomy to measure | Smart Contract Vulnerabilities/Failures/Enhancements, Network-Level Attacks Failures/Enhancements |
| D65 | Chen, H.; Pendleton, M.; Njilla, L.; Xu, S. | A Survey on Ethereum Systems Security | 2021 | Blockchain technology is believed by mar | Article | A comprehensive survey of Ethereum's security vulnerabilities | Smart Contract Vulnerabilities/Failures/Enhancements |

| | | | | | | | |
|------|---|---|------|---|------------------|--|---|
| D66 | Khanfar A.A.A.; Iranmanesh M.; Ghobakhloo M.; Senali M.G.; Fathi M. | Applications of blockchain technology in sustainable manufacturing and supply chain management: A systematic review | 2021 | Developing sustainable products and processes | Review | Examines the use of blockchain technology in sustainable manufacturing | Smart Contract Vulnerabilities/Failures/Enhancements |
| D67 | Nanayakkara S.; Perera S.; Senaratne S.; Weerasuriya G.T.; Bandara H.M.N.D. | Blockchain and smart contracts: A solution for payment issues in construction supply chains | 2021 | The construction industry has dynamic supply chains | Article | Discusses blockchain and smart contracts as solutions for addressing payment issues | Smart Contract Vulnerabilities/Failures/Enhancements |
| D68 | Pathak S. | Blockchain-Enabled Supply Chain Management System | 2021 | In the value of Organizational assets - Blockchain | Book chapter | Aims to improve supply chain management systems by utilising blockchain | Smart Contract Vulnerabilities/Failures/Enhancements |
| D69 | Sadawi A.A.; Hassan M.S.; Ndiaye M. | A Survey on the Integration of Blockchain with IoT to Enhance Performance and Eliminate Challenges | 2021 | Internet of things IoT is playing a remarkable role in various industries | Article | Investigates the integration of blockchain with IoT to boost performance | Smart Contract Vulnerabilities/Failures/Enhancements |
| D70 | Turjo M.D.; Khan M.M.; Kaur M.; Zaquia A. | Smart Supply Chain Management Using the Blockchain and Smart Contract | 2021 | The manufacture of raw materials to deliver products to the end user | Article | Examines a sophisticated supply chain management system by using blockchain and smart contracts | Smart Contract Vulnerabilities/Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D71 | Yang X.; Li M.; Yu H.; Wang M.; Xu D.; Sun C. | A Trusted Blockchain-Based Traceability System for Fruit and Vegetable Agricultural Products | 2021 | Traditional traceability system has problem of information asymmetry | Article | Creates a reliable blockchain-powered system to track agricultural products | Smart Contract Vulnerabilities/Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D72 | Bodkhe U.; Tanwar S.; Parekh K.; Khanpara P.; Tyagi S.; Kumar N.; Alazab M. | Blockchain for Industry 4.0: A comprehensive review | 2020 | Due to the proliferation of ICT during the last decade, the industry has been transformed | Article | Offers a thorough analysis of how blockchain technology influences industry 4.0 | Consensus Mechanism Failures/Enhancements |
| D73 | Lao L.; Li Z.; Hou S.; Xiao B.; Guo S.; Yang Y. | A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling | 2020 | Blockchain technology can be extensively used in various industries | Review | Surveys IoT applications in blockchain systems, focusing on architecture, consensus, and traffic modeling | Consensus Mechanism Failures/Enhancements |
| D74 | Dwivedi S.K.; Amin R.; Vollala S. | Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism | 2020 | The concept of Supply Chain Management (SCM) is changing rapidly | Article | Discusses secured information sharing in supply chain management system | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D75 | Dutta P.; Choi T.-M.; Somani S.; Butala R. | Blockchain technology in supply chain operations: Applications, challenges and research opportunities | 2020 | Blockchain is a technology with unique characteristics | Article | Explores blockchain applications in supply chain operations, addressing challenges and opportunities | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements, Network-Level Attacks Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D76 | Khan.K.M.; Arshad, J.; Khan, M.M. | Simulation of Transaction Malleability Attack for Blockchain-Based e-Voting | 2020 | Blockchain has been adopted to address various issues in various industries | Article | The paper simulates transaction malleability attacks in blockchain-based e-voting | Cryptographic Challenges/Enhancements |
| D77 | NicolasK.; Wang Y.; Giakos G.; Wei B.; Shen H. | Blockchain System Defensive Overview for Double-Spend and Selfish Mining Attacks: A Systematic Approach | 2020 | Blockchain is a technology that ensures data integrity and security | Article | The systematic review focuses on defensive strategies for double-spend and selfish mining attacks | Consensus Mechanism Failures/Enhancements |
| D78 | Mirkin M.; Ji Y.; Pang J.; Klages-Mundt A.; Eyal I.; Juels A. | BDoS: Blockchain Denial-of-Service | 2020 | Proof-of-work (PoW) cryptocurrency blockchain is vulnerable to denial-of-service attacks | Conference paper | The BDoS study reveals the vulnerability of Proof-of-Work blockchain to denial-of-service attacks | Consensus Mechanism Failures/Enhancements |
| D79 | Ali M.A.; Bhaya W.S. | Blockchain technology's applications and challenges: An overview | 2020 | Blockchain emerges as a novel distributed ledger technology | Conference paper | Offers an in-depth review of the obstacles and prospects of blockchain technology | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements |
| D80 | Sangeetha A.S.; Shunmugan S.; Murugan G. | Blockchain for IoT enabled supply chain management - A systematic review | 2020 | Blockchain will increase supply chains' productivity and efficiency | Conference paper | Examines the potential of blockchain technology to improve supply chain management | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements |
| D81 | Wang Z.; Guo L.; Xu W.; Kang T. | A Secure and Credible Supply Chain System Based on Blockchain | 2020 | In traditional supply chain systems, a central authority is required to manage the supply chain | Conference paper | Explores the development of a robust and trustworthy supply chain system based on blockchain | Consensus Mechanism Failures/Enhancements |
| D82 | Supreet Y.; Vasudev P.; Pavitra H.; Naravani M.; Narayan D.G. | Performance Evaluation of Consensus Algorithms in Private Blockchain Networks | 2020 | Blockchain, one of the modern technologies, has gained significant attention | Conference paper | Focuses on evaluating the performance of consensus algorithms in private blockchain networks | Consensus Mechanism Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D83 | Dwivedi S.K.; Amin R.; Vollala S. | Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism | 2020 | The concept of Supply Chain Management (SCM) is changing rapidly | Article | Examines secure information sharing protocols based on blockchain technology | Cryptographic Challenges/Enhancements |
| D84 | Choo K.-K.R.; Ozcan S.; Dehghantanha A.; Parizi R.M. | Editorial: Blockchain Ecosystem - Technological and Management Opportunities and Challenges | 2020 | Blockchain is increasingly deployed in a variety of industries | Review | Examines the technological and managerial obstacles and possibilities of blockchain ecosystem | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements |
| D85 | Luca Serena; Gabriele D'Angelo; Stefano Ferretti | Security Analysis of Distributed Ledgers and Blockchains through Agent-based Simulation | 2021 | In this paper, we describe LUNES-BlockChain, a novel blockchain simulation framework | Article | The study on agent-based simulation of blockchains identifies its strengths and weaknesses | Consensus Mechanism Failures/Enhancements |
| D86 | Lao L.; Li Z.; Hou S.; Xiao B.; Guo S.; Yang Y. | A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling | 2020 | Blockchain technology can be extensively used in various industries | Review | This study examines the use of Internet of Things (IoT) applications in blockchain systems | Consensus Mechanism Failures/Enhancements |
| D87 | Abinaya G.; Benigna S.M.S.; Devi H.; Balaji V.; Ashwin Chakravarthy K. | Analysis of on-chain and off-chain scalability solutions in blockchain technology | 2019 | Blockchain Technology is becoming extremely popular in various industries | Article | Examines scaling solutions in blockchain technology, with a special focus on on-chain and off-chain solutions | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements |
| D88 | Huang Y.; Bian Y.; Li R.; Zhao J.L.; Shi, P. | Smart Contract Security: A Software Lifecycle Perspective | 2019 | Smart contract security is an emerging research area | Article | This paper focuses on smart contract security throughout the software lifecycle | Smart Contract Vulnerabilities/Failures/Enhancements |
| D89 | Saberi S.; Kouhizadeh M.; Sarkis J.; Shen L. | Blockchain technology and its relationships to sustainable supply chain management | 2019 | Globalisation of supply chains makes the need for blockchain technology more urgent | Article | Discusses blockchain technology's role in sustainable supply chain management | Smart Contract Vulnerabilities/Failures/Enhancements |
| D90 | Khalifa, A.M.; Bahaa-Eldin, A.M.; Sobh, M.A. | Quantum Attacks and Defenses for Proof-of-Stake | 2019 | Advances in both quantum computation and cryptography have led to the development of quantum attacks on Proof-of-Stake | Article | The study explores the impact of quantum computing on Proof-of-Stake consensus mechanism | Cryptographic Challenges/Enhancements |
| D91 | Wang Y.; Han J.H.; Beynon-Davies P. | Understanding blockchain technology for future supply chains: a systematic literature review and research agenda | 2019 | Purpose: This paper aims to investigate the current state of blockchain technology and its potential for future supply chains | Review | Offers an analysis of how blockchain technology can potentially transform supply chains | Smart Contract Vulnerabilities/Failures/Enhancements |
| D92 | Sai K.; Tipper D. | Disincentivizing Double Spend Attacks Across Interoperable Blockchains | 2019 | Blockchain was originally developed to solve the double-spend problem | Article | The authors present a protocol to prevent double-spend attacks across interoperable blockchains | Consensus Mechanism Failures/Enhancements |
| D93 | Khosla D.; Sharma M.; Sharma A.; Budhiraja A.; Singh S. | Blockchain based supply chain management: An overview | 2019 | Blockchain is recently a much talked about technology | Article | Offers an overview of blockchain's application in supply chain management | Cryptographic Challenges/Enhancements |
| D94 | Rouhani S.; Deters R. | Security, performance, and applications of smart contracts: A systematic survey | 2019 | Blockchain is the promising technology of the future | Review | Surveys security, performance, and applications of smart contracts | Smart Contract Vulnerabilities/Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D95 | Pratheeshan, P.; Pan, L.; Yu, J.; Liu, J.; Doss, R. | Security Analysis Methods on Ethereum Smart Contract Vulnerabilities: A Survey | 2019 | Smart contracts are software programs that execute automatically | Article | A survey on Ethereum smart contract vulnerabilities reveals 16 common attack vectors | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements |
| D96 | Khatoun A.; Verma P.; Southernwood J.; Massey B.; Corcoran P. | Blockchain in energy efficiency: Potential applications and benefits | 2019 | Blockchain technology is ready to disrupt various industries | Article | Explores blockchain's potential applications in the energy sector | Smart Contract Vulnerabilities/Failures/Enhancements |
| D97 | Damliare Peter Oyinloye; Je Sen The; Norziana Jamil; Moatsum Alawida | Blockchain Consensus: An Overview of Alternative Protocols | 2021 | Blockchain networks are based on consensus protocols | Article | This paper reviews lesser-known blockchain consensus protocols | Consensus Mechanism Failures/Enhancements |
| D98 | Liao D.-Y.; Wang X. | Applications of blockchain technology to logistics management in integrated casinos and entertainment | 2018 | The gaming industry has evolved into a multi-billion dollar industry | Article | Discusses blockchain applications in logistics for integrated casinos and entertainment | Smart Contract Vulnerabilities/Failures/Enhancements, Cryptographic Challenges/Enhancements |
| D99 | Kitakami M.; Matsuo K. | An Attack-Tolerant Agreement Algorithm for Blockchain | 2018 | This paper proposes a method to protect blockchain from Sybil attacks | Article | The authors propose an attack-tolerant agreement algorithm for blockchain | Consensus Mechanism Failures/Enhancements |
| D100 | Antonopoulos, A.; Wood, G. | Mastering Ethereum: Building Smart Contracts and Dapps | 2018 | Ethereum represents the gateway to a world of decentralized applications | Book chapter | The book Mastering Ethereum outlines best practices for building smart contracts and dapps | Smart Contract Vulnerabilities/Failures/Enhancements |
| D101 | Xu, Y. | Section-Blockchain: A Storage Reduced Blockchain Protocol, the Foundation of an Autotrophic Decentralized Storage-Architecture. | 2018 | Bitcoin-derived blockchain has shown promise in various industries | Conference paper | This paper proposes a storage-reduced blockchain protocol aimed at reducing storage requirements | Network-Level Attacks Failures/Enhancements |
| D102 | Kuhi K.; Kaare K.; Koppel O. | Ensuring performance measurement integrity in logistics using blockchain | 2018 | Information and communication technology (ICT) is transforming the logistics industry | Conference paper | Focuses on ensuring performance measurement integrity in logistics using blockchain | Smart Contract Vulnerabilities/Failures/Enhancements |
| D103 | Sward, A.; Vecna, I.; Stonedahl, F. | Data Insertion in Bitcoin's Blockchain. | 2018 | comprehensive survey of methods for data insertion in Bitcoin's blockchain | Conference paper | blockchain. The findings reveal how data can be inserted in a secure and efficient manner | Cryptographic Challenges/Enhancements |
| D104 | Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. | Blockchain technology innovations | 2017 | The digital supply chain has produced efficiencies in various industries | Conference paper | Examines the advancements in blockchain technology, specifically in supply chain management | Cryptographic Challenges/Enhancements |
| D105 | Kshetri N. | Blockchain's roles in strengthening cybersecurity and protecting privacy | 2017 | This paper evaluates blockchain's roles in enhancing cybersecurity and protecting privacy | Article | Evaluates the roles of blockchain in enhancing cybersecurity and protecting privacy | Smart Contract Vulnerabilities/Failures/Enhancements |
| D106 | Zibin Zheng; Shaoran Xie; Hongning Dai; Xiangping Chen; Huaimin Wang | An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends | 2017 | Blockchain, the foundation of Bitcoin, has gained significant attention | Conference paper | Offers a thorough examination of blockchain technology, including its architecture, consensus, and future trends | Consensus Mechanism Failures/Enhancements |
| D107 | Yli-Huumo J.; Ko D.; Choi S.; Park S.; Smolander K. | Where is Current Research on Blockchain Technology?—A Systematic Review | 2016 | Blockchain is a decentralized transaction system | Article | Performs a systematic review of existing studies on blockchain technology | Consensus Mechanism Failures/Enhancements, Smart Contract Vulnerabilities/Failures/Enhancements |
| D108 | Joseph Bonneau | Why buy when you can rent? Bribery attacks on bitcoin-style consensus | 2016 | The Bitcoin cryptocurrency introduced a new paradigm in digital currency | Article | This study investigates bribery attacks in Bitcoin-style consensus | Consensus Mechanism Failures/Enhancements |

Appendix 2

Simulation Data Summary Table

Table 10.1: Illustrating the complete set of simulated throughput and latency for different consensus

| Throughput @ 10 Nodes | | | | | | | |
|------------------------|---------------|--------------|------------------|--------------|--------------|---------------|---------------|
| Number of Transactions | DPoS (Tx/sec) | Pol (Tx/sec) | Stellar (Tx/sec) | PoW (Tx/sec) | PoC (Tx/sec) | PBFT (Tx/sec) | PoEF (Tx/sec) |
| 1 | 3598 | 1493 | 5476 | 268 | 665 | 2479 | 5927 |
| 50 | 3343 | 1485 | 5253 | 268 | 623 | 2474 | 5780 |
| 100 | 3088 | 1451 | 5172 | 260 | 596 | 2109 | 5686 |
| 500 | 2833 | 1380 | 5001 | 260 | 502 | 1809 | 4984 |
| 1000 | 2583 | 1312 | 4562 | 260 | 487 | 1552 | 4664 |
| 5000 | 2300 | 1286 | 4250 | 232 | 481 | 981 | 4331 |
| 10000 | 2100 | 1193 | 4076 | 192 | 462 | 762 | 4248 |
| 50000 | 1800 | 1060 | 3970 | 122 | 460 | 600 | 4100 |
| Throughput @ 15 Nodes | | | | | | | |
| Number of Transactions | DPoS (Tx/sec) | Pol (Tx/sec) | Stellar (Tx/sec) | PoW (Tx/sec) | PoC (Tx/sec) | PBFT (Tx/sec) | PoEF (Tx/sec) |
| 1 | 3459 | 1480 | 5375 | 267 | 645 | 2476 | 5900 |
| 50 | 3210 | 1470 | 5150 | 264 | 610 | 2470 | 5750 |
| 100 | 2961 | 1430 | 5070 | 260 | 580 | 2090 | 5650 |
| 500 | 2713 | 1360 | 4900 | 260 | 490 | 1785 | 4950 |
| 1000 | 2463 | 1290 | 4470 | 251 | 475 | 1530 | 4630 |
| 5000 | 2200 | 1260 | 4150 | 227 | 470 | 960 | 4300 |
| 10000 | 2000 | 1141 | 3923 | 196 | 458 | 789 | 4192 |
| 50000 | 1700 | 1040 | 3875 | 118 | 440 | 575 | 4075 |
| Throughput @ 30 Nodes | | | | | | | |
| Number of Transactions | DPoS (Tx/sec) | Pol (Tx/sec) | Stellar (Tx/sec) | PoW (Tx/sec) | PoC (Tx/sec) | PBFT (Tx/sec) | PoEF (Tx/sec) |
| 1 | 3320 | 1450 | 5275 | 266 | 625 | 2469 | 5850 |
| 50 | 3077 | 1440 | 5050 | 264 | 590 | 2460 | 5700 |
| 100 | 2835 | 1400 | 4970 | 260 | 560 | 2070 | 5600 |
| 500 | 2592 | 1330 | 4800 | 253 | 470 | 1750 | 4900 |
| 1000 | 2342 | 1260 | 4370 | 246 | 455 | 1500 | 4580 |
| 5000 | 2100 | 1230 | 4050 | 218 | 450 | 930 | 4250 |
| 10000 | 1900 | 1180 | 3901 | 182 | 433 | 716 | 4136 |
| 50000 | 1600 | 1000 | 3775 | 108 | 420 | 550 | 3950 |
| Throughput @ 45 Nodes | | | | | | | |
| Number of Transactions | DPoS (Tx/sec) | Pol (Tx/sec) | Stellar (Tx/sec) | PoW (Tx/sec) | PoC (Tx/sec) | PBFT (Tx/sec) | PoEF (Tx/sec) |
| 1 | 3181 | 1400 | 5175 | 236 | 605 | 2440 | 5800 |
| 50 | 2945 | 1395 | 4950 | 220 | 570 | 2435 | 5650 |
| 100 | 2708 | 1360 | 4870 | 218 | 540 | 2030 | 5550 |
| 500 | 2472 | 1300 | 4700 | 212 | 455 | 1700 | 4850 |
| 1000 | 2222 | 1230 | 4270 | 210 | 440 | 1450 | 4530 |
| 5000 | 2000 | 1200 | 3950 | 195 | 430 | 900 | 4200 |
| 10000 | 1800 | 1112 | 3867 | 165 | 421 | 743 | 4078 |
| 50000 | 1500 | 1075 | 3675 | 95 | 400 | 520 | 3853 |
| Throughput @ 60 Nodes | | | | | | | |
| Number of Transactions | DPoS (Tx/sec) | Pol (Tx/sec) | Stellar (Tx/sec) | PoW (Tx/sec) | PoC (Tx/sec) | PBFT (Tx/sec) | PoEF (Tx/sec) |
| 1 | 3042 | 1375 | 5075 | 198 | 585 | 2400 | 5750 |
| 50 | 2812 | 1360 | 4850 | 185 | 550 | 2395 | 5600 |
| 100 | 2582 | 1330 | 4770 | 180 | 520 | 2000 | 5500 |
| 500 | 2351 | 1275 | 4600 | 178 | 440 | 1650 | 4800 |
| 1000 | 2101 | 1205 | 4170 | 175 | 420 | 1400 | 4480 |
| 5000 | 1900 | 1175 | 3850 | 163 | 410 | 870 | 4150 |
| 10000 | 1700 | 1080 | 3798 | 140 | 396 | 670 | 4006 |
| 50000 | 1400 | 950 | 3575 | 82 | 380 | 500 | 3791 |
| Throughput @ 75 Nodes | | | | | | | |
| Number of Transactions | DPoS (Tx/sec) | Pol (Tx/sec) | Stellar (Tx/sec) | PoW (Tx/sec) | PoC (Tx/sec) | PBFT (Tx/sec) | PoEF (Tx/sec) |
| 1 | 2793 | 1340 | 4975 | 163 | 565 | 2375 | 5700 |
| 50 | 2589 | 1325 | 4750 | 145 | 530 | 2350 | 5550 |
| 100 | 2385 | 1300 | 4670 | 142 | 500 | 1950 | 5450 |
| 500 | 2181 | 1250 | 4500 | 140 | 425 | 1600 | 4750 |
| 1000 | 1981 | 1180 | 4070 | 138 | 400 | 1350 | 4430 |
| 5000 | 1750 | 1150 | 3750 | 128 | 390 | 850 | 4100 |
| 10000 | 1600 | 1030 | 3729 | 115 | 344 | 524 | 3962 |
| 50000 | 1350 | 920 | 3475 | 75 | 360 | 480 | 3644 |
| Throughput @ 100 Nodes | | | | | | | |
| Number of Transactions | DPoS (Tx/sec) | Pol (Tx/sec) | Stellar (Tx/sec) | PoW (Tx/sec) | PoC (Tx/sec) | PBFT (Tx/sec) | PoEF (Tx/sec) |
| 1 | 1998 | 1300 | 4875 | 90 | 550 | 2306 | 5656 |
| 50 | 1912 | 1290 | 4650 | 86 | 515 | 2291 | 5503 |
| 100 | 1826 | 1260 | 4570 | 83 | 485 | 1920 | 5407 |
| 500 | 1741 | 1215 | 4400 | 80 | 410 | 1552 | 4713 |
| 1000 | 1617 | 1150 | 3970 | 78 | 385 | 1328 | 4382 |
| 5000 | 1601 | 1125 | 3650 | 72 | 370 | 821 | 4053 |
| 10000 | 1532 | 967 | 3607 | 66 | 305 | 627 | 3901 |
| 50000 | 1354 | 869 | 3546 | 50 | 340 | 461 | 3593 |
| Throughput @ 200 Nodes | | | | | | | |
| Number of Transactions | DPoS (Tx/sec) | Pol (Tx/sec) | Stellar (Tx/sec) | PoW (Tx/sec) | PoC (Tx/sec) | PBFT (Tx/sec) | PoEF (Tx/sec) |
| 1 | 1889 | 1250 | 4775 | 32 | 530 | 2211 | 5606 |
| 50 | 1844 | 1240 | 4550 | 33 | 500 | 2172 | 5453 |
| 100 | 1800 | 1220 | 4470 | 31 | 470 | 1856 | 5353 |
| 500 | 1789 | 1175 | 4300 | 29 | 390 | 1502 | 4656 |
| 1000 | 1673 | 1110 | 3870 | 28 | 370 | 1214 | 4337 |
| 5000 | 1654 | 1100 | 3550 | 27 | 350 | 807 | 4021 |
| 10000 | 1623 | 922 | 3682 | 25 | 265 | 772 | 3872 |
| 50000 | 1592 | 726 | 3450 | 24 | 225 | 446 | 3497 |
| Latency @ 10 Nodes | | | | | | | |
| Number of Transactions | DPoS (ms) | Pol (ms) | Stellar (ms) | PoW (ms) | PoC (ms) | PBFT (ms) | PoEF (ms) |
| 1 | 506 | 803 | 202 | 9800 | 1901 | 264 | 87 |
| 50 | 515 | 961 | 221 | 10400 | 2205 | 288 | 142 |
| 100 | 578 | 1084 | 256 | 12700 | 2503 | 362 | 197 |
| 500 | 814 | 1285 | 306 | 15300 | 3411 | 481 | 242 |
| 1000 | 1262 | 1491 | 484 | 30400 | 5300 | 1294 | 286 |
| 5000 | 2306 | 2635 | 662 | 198600 | 8521 | 5385 | 350 |
| 10000 | 5053 | 3803 | 689 | 298900 | 10728 | 8435 | 397 |
| 50000 | 16190 | 4900 | 730 | 1267400 | 14034 | 14704 | 472 |
| Latency @ 15 Nodes | | | | | | | |
| Number of Transactions | DPoS (ms) | Pol (ms) | Stellar (ms) | PoW (ms) | PoC (ms) | PBFT (ms) | PoEF (ms) |
| 1 | 505 | 840 | 210 | 10200 | 1952 | 312 | 90 |
| 50 | 512 | 990 | 230 | 11600 | 2256 | 339 | 145 |
| 100 | 575 | 1115 | 265 | 12700 | 2555 | 417 | 200 |
| 500 | 805 | 1320 | 320 | 16500 | 3509 | 532 | 245 |
| 1000 | 1250 | 1525 | 500 | 32100 | 5401 | 1504 | 290 |
| 5000 | 2250 | 2700 | 680 | 202500 | 8606 | 6124 | 355 |
| 10000 | 5703 | 3961 | 701 | 305000 | 10937 | 10562 | 401 |
| 50000 | 16000 | 5100 | 750 | 1300000 | 14507 | 20403 | 480 |
| Latency @ 30 Nodes | | | | | | | |
| Number of Transactions | DPoS (ms) | Pol (ms) | Stellar (ms) | PoW (ms) | PoC (ms) | PBFT (ms) | PoEF (ms) |
| 1 | 502 | 870 | 220 | 11000 | 2003 | 340 | 95 |
| 50 | 510 | 1030 | 240 | 12500 | 2305 | 348 | 150 |
| 100 | 570 | 1155 | 280 | 13800 | 2606 | 420 | 205 |
| 500 | 800 | 1365 | 340 | 18400 | 3603 | 550 | 250 |
| 1000 | 1235 | 1575 | 525 | 34500 | 5608 | 1480 | 295 |
| 5000 | 2220 | 2780 | 710 | 210000 | 8701 | 6081 | 360 |
| 10000 | 6403 | 3254 | 726 | 320000 | 12256 | 10903 | 406 |
| 50000 | 15850 | 5300 | 780 | 1350000 | 15160 | 23071 | 490 |
| Latency @ 45 Nodes | | | | | | | |
| Number of Transactions | DPoS (ms) | Pol (ms) | Stellar (ms) | PoW (ms) | PoC (ms) | PBFT (ms) | PoEF (ms) |
| 1 | 510 | 910 | 230 | 13400 | 2051 | 386 | 100 |
| 50 | 518 | 1075 | 255 | 14900 | 2354 | 375 | 160 |
| 100 | 580 | 1200 | 300 | 16300 | 2653 | 450 | 210 |
| 500 | 812 | 1410 | 360 | 21500 | 3702 | 582 | 260 |
| 1000 | 1260 | 1630 | 550 | 39000 | 5607 | 1450 | 305 |
| 5000 | 2280 | 2860 | 740 | 230000 | 8804 | 5906 | 370 |
| 10000 | 7209 | 3582 | 799 | 350000 | 13431 | 11462 | 418 |
| 50000 | 16100 | 5500 | 810 | 1500000 | 15503 | 26310 | 500 |
| Latency @ 60 Nodes | | | | | | | |
| Number of Transactions | DPoS (ms) | Pol (ms) | Stellar (ms) | PoW (ms) | PoC (ms) | PBFT (ms) | PoEF (ms) |
| 1 | 513 | 950 | 240 | 16700 | 2107 | 420 | 120 |
| 50 | 520 | 1120 | 270 | 18100 | 2404 | 415 | 180 |
| 100 | 585 | 1245 | 320 | 19800 | 2703 | 495 | 230 |
| 500 | 820 | 1460 | 385 | 25700 | 3800 | 610 | 280 |
| 1000 | 1270 | 1690 | 580 | 46000 | 5703 | 1600 | 320 |
| 5000 | 2290 | 2945 | 770 | 260000 | 8902 | 6304 | 390 |
| 10000 | 8109 | 3808 | 843 | 400000 | 13695 | 12051 | 435 |
| 50000 | 16200 | 5700 | 850 | 1700000 | 16014 | 32107 | 520 |
| Latency @ 75 Nodes | | | | | | | |
| Number of Transactions | DPoS (ms) | Pol (ms) | Stellar (ms) | PoW (ms) | PoC (ms) | PBFT (ms) | PoEF (ms) |
| 1 | 515 | 990 | 250 | 20500 | 2152 | 460 | 135 |
| 50 | 522 | 1165 | 285 | 22000 | 2452 | 462 | 200 |
| 100 | 590 | 1290 | 335 | 24000 | 2754 | 531 | 250 |
| 500 | 825 | 1505 | 405 | 31200 | 3903 | 650 | 300 |
| 1000 | 1280 | 1745 | 600 | 52500 | 5801 | 1750 | 340 |
| 5000 | 2300 | 3030 | 800 | 300000 | 9004 | 6808 | 420 |
| 10000 | 8895 | 4071 | 857 | 460000 | 13972 | 14520 | 464 |
| 50000 | 16300 | 5867 | 870 | 2000000 | 16503 | 38069 | 550 |
| Latency @ 100 Nodes | | | | | | | |
| Number of Transactions | DPoS (ms) | Pol (ms) | Stellar (ms) | PoW (ms) | PoC (ms) | PBFT (ms) | PoEF (ms) |
| 1 | 520 | 1030 | 260 | 25400 | 2204 | 508 | 150 |
| 50 | 528 | 1210 | 300 | 26700 | 2511 | 490 | 225 |
| 100 | 595 | 1340 | 350 | 29000 | 2806 | 572 | 275 |
| 500 | 835 | 1560 | 430 | 37000 | 4181 | 704 | 325 |
| 1000 | 1290 | 1805 | 630 | 62000 | 5902 | 1906 | 365 |
| 5000 | 2350 | 3120 | 830 | 350000 | 9109 | 7301 | 450 |
| 10000 | 10520 | 4805 | 990 | 530000 | 14621 | 15241 | 495 |
| 50000 | 16500 | 6100 | 900 | 2300000 | 18910 | 42092 | 590 |
| Latency @ 200 Nodes | | | | | | | |
| Number of Transactions | DPoS (ms) | Pol (ms) | Stellar (ms) | PoW (ms) | PoC (ms) | PBFT (ms) | PoEF (ms) |
| 1 | 500 | 1100 | 275 | 45000 | 2321 | 536 | 170 |
| 50 | 506 | 1300 | 315 | 46500 | 2606 | 551 | 250 |
| 100 | 520 | 1450 | 370 | 49800 | 2904 | 610 | 300 |
| 500 | 717 | 1680 | 450 | 60000 | 4218 | 743 | 350 |
| 1000 | 1200 | 1950 | 650 | 90000 | 6204 | 2062 | 400 |
| 5000 | 1902 | 3300 | 870 | 500000 | 9427 | 7806 | 480 |
| 10000 | 11300 | 4687 | 1028 | 800000 | 14699 | 17824 | 530 |
| 50000 | 18900 | 6600 | 1028 | 3500000 | 20615 | 45265 | 620 |

Publications



The Chartered
Institute of Logistics
and Transport


Aston University
BIRMINGHAM UK



LOGISTICS
RESEARCH
NETWORK

Full Papers

Logistics Research Network Conference 2022

Supply Chain Innovation: People, Process, Technology

Date: 7 – 9 September 2022 | **Location:** Aston University



ciltuk.org.uk/lrn2022 | [#LRNConf22](https://twitter.com/LRNConf22)

THE ROLE OF INFORMATION SHARING AND ANALYTICS



EVALUATING THE INTEGRATION OF BLOCKCHAIN TECHNOLOGIES IN SUPPLY CHAIN MANAGEMENT: A CASE STUDY ON SUSTAINABLE FISHING

Odayne Haughton

University of Wales Trinity St. David, United Kingdom, o.haughton@uwtsd.ac.uk

Introduction

It was 2009, more than a decade ago, that Satoshi Nakamoto, the anonymous creator of Bitcoin, revealed how blockchain technology, a decentralized, distributed peer-to-peer, immutable linked-ledger, could be used to address the financial challenges of maintaining transaction orders and double-spending (Nakamoto, 2008). Bitcoin arranges transactions into a “chain of blocks” all having the same timestamp. A blockchain can be explained as a distributed database organized as a list of ordered blocks with immutable committed blocks. Each block is linked to the one before it and a block can be considered as a data packet that comprises all of the preliminary data as well as some fresh data. The whole chain is a database that is shared among numerous people who all share control of the blocks (i.e. it is not controlled centrally).

The information in the data that makes up the chain of blocks can be any kind of data such as personally identifiable information (PII), transactions details (such as payments), operations in a supply chain management (SCM), bar codes, etc. As a result, the scope and potential of blockchain varies depending on the use case. In developing a blockchain, the ledger’s nodes (i.e. blockchain miners) are in charge of chronologically connecting the block, ensuring each block comprises of the hash of the preceding block (Crosby et. al, 2016). As a result, the blockchain system keeps a reliable and auditable record of all transactions.

One of the practical uses of blockchain is supply-chain management, and the recent Coronavirus (COVID-19) pandemic emphasized the significance of how developing technologies can provide genuine and reliable commercial advantages. Growing customer expectations, diverse marketing channels, international obstacles, and a number of other issues have all made supply chains increasingly difficult to manage. A supply chain might involve several partners, span a large number of phases, operate different countries, entail hundreds of invoices and payments, and last for a considerable amount of time due to shipping challenges (PWC, 2020).

Within the supply chain sector, adoption of blockchain technology is still in its infancy. Two of the key elements influencing their acceptance inside SCM systems are traceability and trust. Breaking down these two essential elements into three additional sub-factors; increased supply chain visibility, digital supply chain transformation, and improved supply chain security and transparency will help to better understand how blockchain technology can progress the supply chain management industry (PWC, 2020).

Literature Review

Since its inception, the landscape of blockchain have been rapidly evolving as blockchain is used for other use cases beyond Bitcoin and other similar cryptocurrencies, with Smart Contracts (SC) playing a significant role (Casino, Dasaklis & Patsakis, 2019). Blockchain started out with its first iteration, Blockchain 1.0, which included applications that enabled digital cryptocurrency transactions. Over time, the technology further developed into Blockchain 2.0, which includes SCs and a set of applications going beyond cryptocurrency transactions. Blockchain 3.0 includes applications in fields beyond the first two iterations, such as Industry 4.0 and SCM, government digitization, healthcare, science, and IoT (Zhao et al., 2016).

In 1994, Szabo described SCs as “a computerized transaction protocol that implements the provisions of a contract” (Szabo, 1994). Szaboo explored converting contractual clauses into embeddable code using SCs (Szabo, 1997), which reduces the need for external involvement and risks. Specifically, a SC is an agreement between parties whose terms are automatically enforced even while they do not trust one another. In the context of blockchain, SCs are scripts that execute in a decentralized fashion and are kept in the blockchain without relying on a trusted authority (Christidis and Devetsikiotis, 2016). Therefore, blockchain-based systems that allow SCs enable more complicated processes and interactions, hence establishing a new paradigm with virtually endless applications.



In recent years, blockchains have significantly disrupted traditional business processes since activities and transactions that once required centralized systems or reliable third parties to authenticate, may now function in a decentralized fashion with the same (or even higher) level of certainty. Fundamental characteristics that blockchain offers include immutability, traceability, transparency, resilience, and security (Greenspan, 2015a; Christidis and Devetsikiotis, 2016).

Consequently, Blockchain technology is growing in importance (Zhao et al., 2016). According to a 2017 report by IBM, almost a thousand (33%) of C-suite executives said they were exploring blockchains or were currently actively utilizing them (IBM, 2017). Researchers and developers are already familiar with the potential of the new technology and are investigating its many uses across a broad range of industries (Christidis and Devetsikiotis, 2016).

Application areas of blockchain in supply chain management

There is a wide spectrum of possible use-cases for blockchain technologies in SCM. Helo and Hao, 2019 summarized these use cases in three categories namely: (i) assets, (ii) identity and (iii) transactions (Fig. 1).

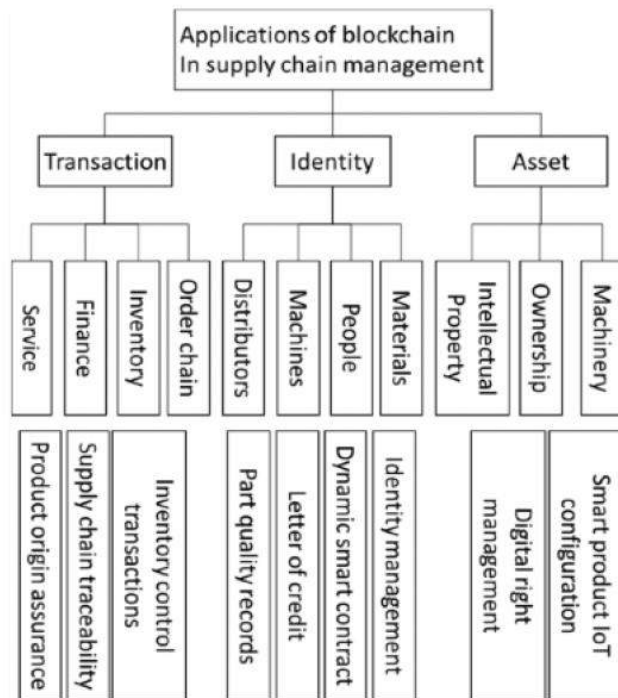


Fig. 1: Examples of applications of blockchain in supply chain management, adopted from (Helo and Hao, 2019).

Assets: It is essential to maintain accurate and trustworthy records to identify ownership and assure the accuracy and completeness of property-related important information for both tangible assets (i.e., physical property) and intangible assets (i.e., files) (Abeyratne & Monfared, 2016; Mizrahi, 2016). By registering and trading the properties via blockchains as smart property or digital property management, further management over the physical assets may be accomplished. It is feasible to establish traceability via IoTs, which is a mix of blockchain and digital twins (Francisco & Swanson, 2018). The cryptographic management of keys and signatures to identify who can trade inside the shared ledger ensures the security and veracity of the ledger’s stored assets (Yeoh, 2017).

Identity: Digital identity and private records can be stored and confirmed with blockchains through securely encoded legal documents. These non-financial applications include health records, licenses, ID cards, contracts, signatures, etc. (Crosby et al., 2016; Swan, 2015). In future, code-based smart contracts are computer programs that can execute most of the agreements, contractual relationships and governance (Yeoh, 2017). When a pre-configured condition in a smart contract among participating entities is met, the parties involved in a contractual agreement can automatically make payments based on the contract in a transparent manner (Crosby et al., 2016).



Transaction: The decentralized and distributed transaction ledger is one of the defining features of blockchain. This creates a permanent and verifiable record of transactions between parties (Swan, 2015p.10). All supply chain-related transactions, including orders, inventories, and goods, may be recorded and validated on the blockchain.

Supply chains are complicated because they consist of dispersed operations upstream, which involve people, physical resources, and industrial processes, to downstream, which encompasses the entire selling process, including contracts, client sales, distribution, and disposal (Tian, 2016). The objective of the supply chain is to develop a multi-stakeholder collaborative environment based on mutual trust, eliminate communication obstacles, and ensure that diverse businesses are interconnected to seek regular integration of the complete supply network (Korpela, Hallikas, & Dahlberg, 2017; Tuominen, Kitaygorodskaya, & Helo, 2009). In the end, supply chain stakeholders may increase overall efficiency and provide higher value and advantages to their businesses. Helo and Hao, 2019, further simplified these objectives into five (5) key indicators as seen in Table 1.

| Supply chain indicators | Blockchain key concepts | | |
|-------------------------|----------------------------------|---------------------------------------|--------------------------|
| | Tamper-proof transaction records | Information sharing & synchronization | Smart contract execution |
| Improve overall quality | X | X | X |
| Reduce cost | X | X | X |
| Shorten delivery time | | X | |
| Reduce risk | X | | X |
| Increase trust | X | | X |

Table 1: Benefits of applying blockchain in supply chain management, adopted from (Helo and Hao, 2019).

Problem Statement

The purpose of SCM systems is often to boost sales, lower manufacturing costs and complexity, eliminate fraud, and speed up production and delivery. Many businesses lack an integrated picture of the complete supply chain as supply networks are growing increasingly complicated in structure, challenging in terms of tasks, and diverse in terms of stakeholders. While big corporations have created their own identities and systems to sustain worldwide oversight of their operations and have the authority to engage and instruct their suppliers (Chen et al., 2018), many are struggling due to the pandemic. The situation is even worse for medium-size and smaller corporations (Lee and Klassen, 2008). Many of them must rely on centralized regulatory authorities or middlemen. Which has recently led to several internal and external constraints, including greater complexity, demand volatility, and a shifting retail environment, are posing increasingly difficult problems for present SCM networks (PWC, 2020).

In terms of security, traceability, authentication, and the verification system, this lack of transparency creates a few concerns and challenges for the supply chain mechanism. In severe circumstances like COVID-19, this is more significant. As a result, certain chain suppliers temporarily stopped producing, and logistics companies were unable to move vital items like masks and ventilators as smoothly, especially across borders. It is noteworthy, that blockchain is well-suited to handle the difficulties of supply chains. Consequently, it is imperative to implement blockchain technology, with its immutability, transparency, and trustworthiness (Chen et al., 2018), to increase supply chain visibility and security.

Consumers are also requesting greater information about the origins of the products they purchase. Because of this, customers are prepared to pay more to businesses that have more transparent supply chains, which boosts not only sales but also customer happiness and confidence networks (PWC, 2020). In today’s globalized corporate environment, success is driven by speed and agility. Clients now demand more from their purchasing experiences, and businesses in a variety of sectors must now be prepared to offer new customers through new channels. Only a supply chain that is flexible enough to accommodate shifting market trends will be able to do this. Effectively utilizing blockchain technology is a key enabler in addressing these SCM difficulties.



Research Work

Sustainable supply chains

Sustainable supply chains have been explored by Hutchins and Sutherland (2008). For the purpose of this research, sustainability measures for the seafood sector were analyzed, enhanced through blockchain technology and recommended for future supply chain-related decisions. In general, sustainable supply chains require the known origin of raw materials and procedures which are in accordance with generally accepted practices.

As described in the preceding section, blockchain is believed to provide enormous promise for strengthening supply chain management procedures and business models. The characteristics of blockchain enable a variety of operational and supply chain management applications. To demonstrate the technical architecture of a blockchain-based supply chain management system (BSCMS), a reference implementation was designed and implemented in the form of a proof of concept (POC). The purpose of the implementation was to provide a solution to trace the complete seafood lifecycle by capturing, recording and tracking all relevant activities and data (e.g. video, photo, documents) from “bait to plate” and to provide an open and immutable history record for each transaction in the supply chain. The seafood industry is one of the world’s largest and oldest market sectors. It is also the longest logistic network for food. The industry is made up of complex global supply chains which creates numerous social and environmental challenges. Both illegal fishing and unreported fishing are malpractices destroying and depleting marine habitats threatening sustainability. Enhancing provenance certainty, traceability and transparency along these supply chains could be a way to resolve these problems. Blockchain technology is well positioned to achieve these goals.

Depending on the underlining technologies, blockchain systems can be accessed in different ways and are categorized based on how they are accessed. According to Yeoh (2017) and Wu et al. (2017), there are three types of blockchain systems:

1. Permissioned-based (private), in which verification nodes are recognized and identified by a central authority or database.
2. Permissionless-based (public), in which anybody can participate in the verification process without permission.
3. Hybrid, in which both permissioned and permissionless ledgers are utilized.

In this research, a **hybrid blockchain** was selected to handle the process. Using either a fully public or entirely private ledger architecture for the flow of information makes it challenging to meet the practical needs of blockchain applications. For a solution, it is vital to synchronize the two types of ledgers. For example, a private ledger is utilized for sensitive data, whereas a public ledger is utilized for material that requires a high level of confidence. Without relying on a centralized governing body, each participant can control information access via the two forms of ledgers (Wu et al., 2017).

The framework and the corresponding system architecture are composed of four layers, as seen in Fig. 2. This platform consists of several fundamental technologies and provides technical modules. This architecture is flexible and can be adapted based on realistic requirements for a varying SCM sectors.



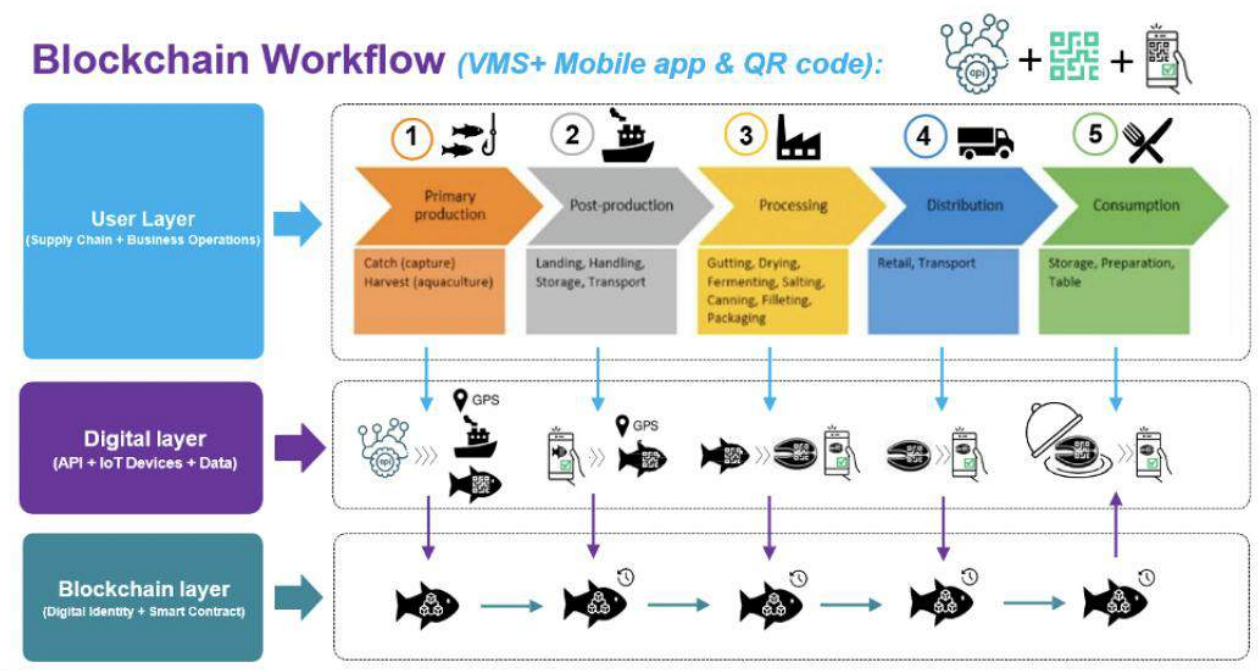


Fig. 2: Blockchain-based supply chain management system architecture

- **User Layer:** This layer comprises of the supply chain and business operations. This layer includes various users. Each partner can monitor the quality of the supply chain and perform various business activities with the support of blockchain.
- **The Digital Layer:** This comprises of data collection and amalgamation to feed to the blockchain. Along the supply chain different types of data (geo-location, weight, species, transactions, etc.) are either captured by IoT devices in real-time or imputed by users. All users, including logistics operators and consumers, keep a copy of different aspects of the data supply chain operations.
- **The Blockchain Layer:** This layer offers a secure data sharing infrastructure in a distributed network, and it can cope with the data trust challenges. When the data is gathered and shared in a digital layer, the data will be digitally signed and added to the blockchain in order to execute supply chain monitoring and traceability to improve the efficiency of the supply chain process. Digital identity is used to secure authenticity of the data while the Smart contracts perform real time quality monitoring by using real time data.

Conceptually, a blockchain is governed by decentralized consensus and coherence. The logistical history data are reliable, precise and consistent. They can be preserved without the participation of a reliable mediator. Customers and logistics providers have complete access to their respective data (Esposito et al., 2018). The conceptual environment of the BSCMS established for this study is depicted in Figure 2. This system focuses mostly on the fishing industry in the United Kingdom.

Software implementation

The functionalities of the system consist of transaction entry for supply chain operators which includes five (5) main stages:

1. Operators are authorized users. The user logs a transaction containing information on supply chain operations, seafood types, geolocation, timestamps, and health certificates. In addition, the transaction comprises the package's state, such as pickup, receipt, quality check, or final delivery.
2. A new block is offered and distributed to all peers in the supply chain network whenever a new logistical transaction is created.



3. Participants in the network get the block for validation. The system will place the new block into the chain after all participants have authorized it. This enables both clients and operators to have an efficient, verifiable, and permanent global perspective of the transaction history.
4. Once a block has been included in the chain, its data cannot be altered. Because the block is connected to a preceding block, it is simple to notice any mutation. As block material is open to the public, logistical data must be safeguarded prior to their inclusion in the block (e.g. encrypted).
5. The transaction is complete after the authorized block has been added to the chain.

The architecture of BMLS is structured into two parts: (1) back-end: which comprises of the digital layer and the blockchain network working together to issue and verify digital certificates, and (2) the front-end: where users interface and interact with transactions.

The blockchain’s backend design facilitates distributed transaction operations. Each block in the blockchain includes transaction information and a link to the preceding block. Multiple server computers performed the verification procedure, which ensures the data’s immutability. Data can also be saved on distributed servers, although for the sake of this proof-of-concept, local storage was employed for speedy package number searches.

Results/ Analysis

Using blockchain technology, the POC for this project is to improve supply chain management and fishing sustainability. The implementation accounted for the entirety of the supply chain, from ‘bait to plate’ (Catching the seafood straight through to consumption). The developers created a uniform API that uses blockchain technology to record verified transactions. The API employs several data types, data sources, and data formats to generate and issue digital passports. Figure 3 depicts how data supplied via the API is added to a blockchain to issue.

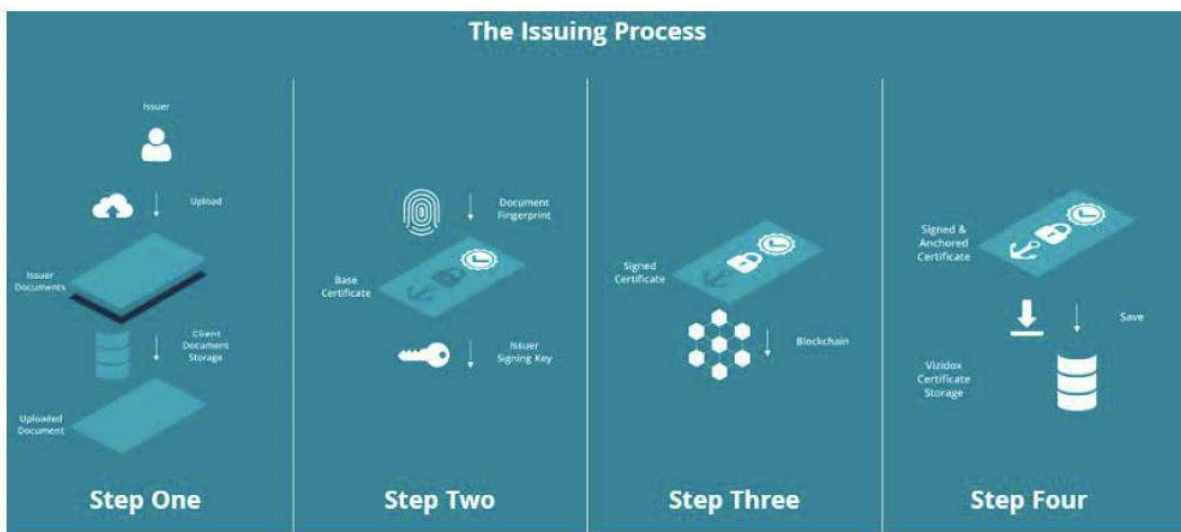


Fig. 3: Highlight the digital certificate issuing process

This certificate is an immutable record that will encompass all pertinent information, documents, data, and assets as a sequence of unalterable occurrences.

As seen in Figure 4, any user or third party will be able to check the validity and file integrity of digital passports using the application. Users may also download the digital passport, submit it to a protected portal, and verify its validity by comparing it to the original digital passport that is stored on the blockchain.



The Verification Process

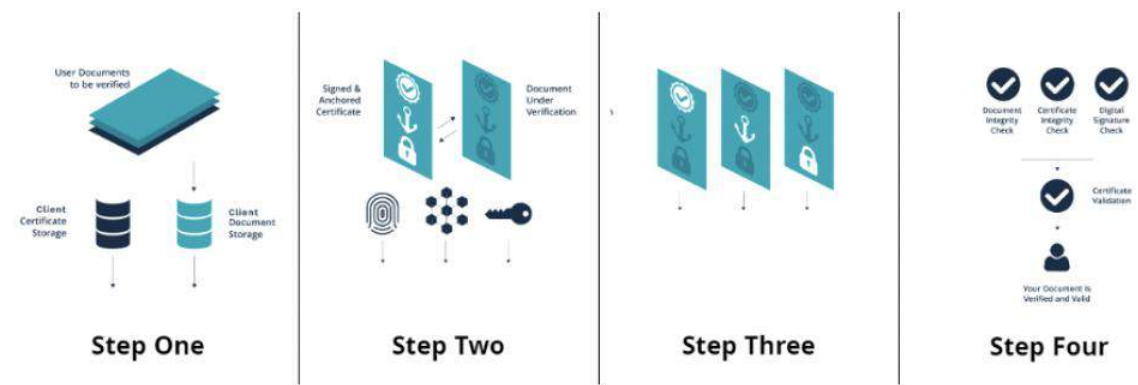


Fig. 4: Highlight the digital certificate verification process

As a result of the complete procedure, a digital passport is produced containing all pertinent information, data, or assets to be anchored to the blockchain. The digital passport becomes an immutable record that serves as the record’s gold standard. The digital passport will have a unique, clickable and scannable QR code that redirects and validates against the original file stored on the blockchain. Every stage of the seafood’s journey is made accessible to customers, therefore increasing their understanding and transparency.

Digital passport for fish

1) Certificate issued on the blockchain

Haddock Passport #342B

| Origin | Trajectory | Fish | Certificates |
|--------|------------|------|--------------|
| | | | |

Digital passport:

- Accessible
- Secure
- Immutable
- Transparent
- Traceable
- Transferable
- Enforceable
- Revocable
- Compliant

2) Easy verification. Undisputable truth. Fraud eliminated.

CERTIFICATE VERIFICATION

| VERIFICATION STEP | STATUS |
|---|--------|
| 1. Checking certificate integrity | PASS |
| 2. Checking certificate is anchored to the blockchain | PASS |
| 3. Checking issuer authenticity | PASS |
| 4. Checking the origin | PASS |
| 5. Checking expiry date | PASS |
| 6. Checking document date | PASS |

Fig. 5

Discussion

In this study, the BSCMS is an exploratory reference implementation. We chose this method because blockchain is still considered to be in its infancy. Our objective was to provide a platform to increase the sustainability of supply chain-related operations while ensuring the confidentiality and transparency of all activity records. Numerous real-world business applications are adopting other use cases for transparency and security throughout a dispersed chain of activities, namely:

- The supply chain for diamonds and other rare earth elements is an excellent example of this difficulty. Occasionally, diamonds are mined by parties sponsoring war-zone operations and then sold to obscure the provenance of the raw materials. These “blood diamonds” and the exploitation of child labor in mining are well-known sustainable supply chain issues (Epstein & Yuthas, 2011). Everledger established a permanent log of diamond certification and



transaction history by establishing a digital identity for each diamond within a blockchain network (Crosby et al., 2016). This facilitates the authenticity of the transaction, for instance by preventing the entry of “blood diamonds” into the jewelry market. It is possible for insurance companies, law enforcement agencies, owners, and claims to verify gems. Everledger provides an easy-to-use web service API (application programming interface) for examining a diamond and filing, reviewing, or amending insurance claims, as well as diamond police reports.

- Additionally, safety plays a crucial part in several businesses. Authentic food, for example, is a vital aspect of sustainability. Tracking and tracing are common supply chain operations for achieving informational transparency. Transactions, users, locations, and containers necessitate a centralized and immutable database. The food sector is a classic use of traceability in supply networks. Generally, counterfeit food poses a concern to public health. To resolve food safety challenges, good food supply chain management is essential. In the case of a foodborne illness epidemic, for instance, merchants must identify the source of contamination and additional impacted items. In 2016, Walmart teamed with IBM to build a blockchain-based system to allow food item origin and movement monitoring. In conventional IT systems, internal control of central databases and participant confidence were necessary. Walmart has significantly improved the transparency of both local and international supply chains by merging the new blockchain-based system with barcodes or auto-ID technology. On the blockchain, information such as farm origin, batch numbers, factory and processing data, expiration dates, and shipment details were recorded and instantly made available to all network participants. These data allow Walmart to immediately trace the origin of food in the event of a foodborne illness epidemic (Shaffer, 2017).
- In addition, counterfeit pharmaceuticals pose a concern. Digital technology and serialization techniques in general have been offered for the development of medication identification systems (Mackey & Nayyar, 2017). Bocek et al. (2017) have tried blockchain technology in the pharmaceutical supply chain as a remedy for this problem. In the medical industry, it is well-known that counterfeit pharmaceuticals, such as anti-cancer treatments, can have fatal repercussions if patients do not receive therapy as recommended (Mackey & Nayyar, 2017). By enabling supply chain transparency from manufacturers to wholesalers and pharmacies to individual patients, blockchain can improve patient safety. Through barcodes or auto ID technology, patients may verify that they have got the correct medication (DeCovny, 2017; Mackey & Nayyar, 2017).

As more parties in the supply chain use blockchain technology, it becomes more legitimate and valuable, eventually becoming an industry standard. However, early stakeholder buy-in will be challenging due to varying levels of digital preparedness and the first need to grasp the mutual benefits of blockchain-based cooperation. This will be especially challenging when legacy procedures, rules, and laws regulate diverse business elements, since stakeholders will suffer expenses while migrating from legacy systems and integrating new systems and practices.

Due to the competitive nature of business, many businesses, both in the private and governmental sectors, will invest in a blockchain-based logistics system in the future. To ensure interoperability across various blockchain-based systems, it is crucial to establish standards and agreements (Kückelhaus & Chung, 2018, p.7). Blockchain Connected is an organization that facilitates blockchain use and develops standards for the Welsh manufacturing sector. Its primary objective is to address industrial difficulties via blockchain-enabled applications.

Conclusion

Blockchain technology adoptions are still considered to be in the early stages within the supply chain industry. Traceability and trust are two of the major factors driving their adoption within SCM systems. Understanding how blockchain technologies advance the supply chain management sector, lies in breaking down these two key factors into a further three sub-factors (i) increased visibility along the supply chain, (ii) digital transformation of supply chains, and (iii) enhanced security and transparency within the supply chain.

There are several challenging aspects of the supply chain that make it extremely complex to manage. For example, numerous parties are engaged in the supply chain, a shared common database is required, and once recorded, transactions are seldom altered. Therefore, the supply chain may be progressively optimized utilizing a digital infrastructure environment such as blockchain, in which all involved parties can exchange and access product-related information in real-time, such as invoices, the current status, and payments. Participants may digitally monitor items and transactions in real-time and in great detail. Such an inclusive infrastructure relies on a shared ledger that offers all supply chain-related data and simultaneously secures global data and information authenticity and security. This considerably decreases the current systems' complexity (Orman, 2016).



However, logistics and supply chain management blockchain research is still in its infancy, and potential applications should be considered. Numerous logistics operators, particularly small and medium-sized businesses, claim to have limited awareness of blockchain and to view its influence as a danger (Hackius & Petersen, 2017). Small-scale experiments such as the one done in this research should be conducted by businesses to get first-hand knowledge.

Over the next decade, blockchain technology has the potential to increase the world gross domestic product (GDP) by \$1.76 trillion. As organizations cope with the effects of COVID-19 and the way the pandemic has expedited other disruptive trends – such as the push toward more digital modes of working, interacting, and transacting with consumers – they are reconsidering how they conduct business. In a digital age, trust is tenuous. Investing in digitalization to build trust and openness is a focus that has gained momentum during COVID-19. PwC study indicates that 61 percent of CEOs worldwide rank the digital transformation of fundamental business operations and procedures among their top three objectives as they seek to reconfigure their operations. (PWC, 2020)

To increase the understanding of blockchain technologies, this project has constructed a prototype of a blockchain-based supply chain management system (BSCMS). This BSCMS acquired and communicated logistical data utilizing a blockchain approach. The capability of the system enables clients, logistic operators, and any other partners to follow the complete lifecycle of seafood, from capture to consumption. The proposed reference architecture illustrates how blockchain may be implemented utilizing software components in operational and supply chain contexts. Our findings indicate that, in contrast to traditional IT designs, blockchain technology is a potential platform to improve supply chain management operations by introducing transparency, automation, and trust.

References

- Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*, 5(09), 1–10.
- Badzar, A. (2016). Blockchain
- Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017). Blockchains everywhere – a use-case of blockchains in the pharma supply-chain. 2017 IFIP/IEEE symposium on integrated network and service management (IM) (pp. 772–777). IEEE.
- Casino, F., Dasaklis, T.K. and Patsakis, C. (2019) “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” *Telematics and Informatics*. Elsevier Ltd, pp. 55–81. <https://doi.org/10.1016/j.tele.2018.11.006>.
- Chen, G., Xu, B., Lu, M., & Chen, N. S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, 5(1), 1.
- Christidis, K., Devetsikiotis, M., (2016). Blockchains and smart contracts for the internet of things. *IEEE Access* 4, 2292–2303.
- Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: beyond bitcoin. *Applied Innovation Review*, 2.
- DeCovny, S. (2017). Experts discuss tackling pharma supply chain
- Epstein, M. J., & Yuthas, K. (2011). Conflict minerals: Managing an emerging supply chain problem. *Environmental Quality Management*, 21(2), 13–25.
- Esposito, C., Santis, A. D., Tortora, G., Chang, H., & Choo, K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Computing*, 31–37.
- Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. *Logistics*, 2(1), 2.
- Greenspan, G., 2015a. Ending the bitcoin vs blockchain debate, <http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate>.



- Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: Trick or treat? Proceedings of the hamburg international conference of logistics (HICL) (pp. 3–18).epubli.
- IBM, 2017. Three ways blockchain Explorers chart a new direction, <https://www-935.ibm.com/services/studies/csuite/pdf/GBE03835USEN-00.pdf>.
- IBM, 2017. 10 Key Marketing Trends for 2017, <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN>.
- IBM Corporation, 2016. Making Blockchain Real for Business. Explained with HighSecurity Business Network Service. <https://www.ibm.com/systems/data/flash/it/technicalday/pdf/Making%20blockchain%20real%20for%20business.pdf>.
- Hutchins, M. J., & Sutherland, J. W. (2008). An exploration of measures of social sustainability and their application to supply chain decisions. *Journal of Cleaner Production*, 16(15), 1688–1698.
- Korpela, K., Hallikas, J., & Dahlberg, T. (2017). Digital supply chain transformation toward blockchain integration. Proceedings of the 50th hawaii international conference on system sciences (pp. 4182–4191).
- Kückelhaus, M., & Chung, G. (2018). Blockchain in logistics. DHL Customer Solutions & Innovation.
- Lee, S.Y. and Klassen, R.D. (2008) “Drivers and enablers that foster environmental management capabilities in small- and medium-sized suppliers in supply chains,” *Production and Operations Management*, 17(6), pp. 573–586. <https://doi.org/10.3401/poms.1080.0063>.
- Mackey, T. K., & Nayyar, G. (2017). A review of existing and emerging digital technologies to combat the global trade in fake medicines. *Expert Opinion on Drug Safety*, 16(5), 587–602.
- Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system
- Omran, Y. (2016). Inclusive supply chain finance approach: Integrated supply chain finance solution with digitalization. White paper. Fraunhofer IML.
- PWC (2020) Time for trust The trillion-dollar reasons to rethink blockchain. Available at: <https://www.pwc.com/gx/en/industries/technology/publications/blockchain-report-transform-business-economy.html#:~:text=Trust%2C%20transparency%2C%20efficiency%3A%20The,%2C%20cut%20costs%20and...> (Accessed: June 22, 2022).
- Shaffer, E. (2017). Walmart, IBM provide blockchain update. Accessed at:<https://www.meatpoultry.com/articles/16484-walmart-ibm-provide-blockchain-update>.
- Swan, M. (2015). *Blockchain: Blueprint for a new economy*. Sebastopol, CA: O'Reilly Media, Inc.
- Szabo, N., 1994. Smart contracts.
- Szabo, N., 1997. The idea of smart contracts.
- Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID and blockchain technology. 13th international conference on service systems and service management (ICSSSM) (pp. 1–6).
- Tuominen, T., Kitaygorodskaya, N., & Helo, P. (2009). Benchmarking Russian and Finnish food industry supply chains. *Benchmarking: An International Journal*, 16(3), 415–431.
- Yeoh, Peter (2017). Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance*, 25(2), 196–208. <https://doi.org/10.1108/JFRC-08-2016-0068>.
- Wu, H., Li, Z., King, B., Ben Miled, Z., Wassick, J., & Tazelaar, J. (2017). A distributed ledger for supply chain physical distribution visibility. *Information*, 8(4), 137.
- Zhao, J.L., Fan, S., Yan, J., 2016. Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation* 2 (1), 28.



Evaluating the integration of Blockchain Technologies in Supply Chain Management: a case study of sustainable fishing

Odayne Haughton

Manufacture Advance Design
Engineering (MADE) Cymru
University of Wales Trinity Saint David
Swansea, Wales, United Kingdom
o.haughton@uwtsd.ac.uk

Carlene Campbell

Wales Institute of Science and Art
University of Wales Trinity Saint David
Swansea, Wales, United Kingdom
carlene.campbell@uwtsd.ac.uk

Graham Howe

Manufacture Advance Design
Engineering (MADE) Cymru
University of Wales Trinity Saint David
Swansea, Wales, United Kingdom
graham.howe@uwtsd.ac.uk

Terry H. Walcott

Wales Institute of Science and Art
University of Wales Trinity Saint David
Swansea, Wales, United Kingdom
t.walcott@uwtsd.ac.uk

Abstract—As a consequence of the Global pandemic, Supply Chain Management (SCM) is becoming more complex due to market uncertainty across value chains; from sourcing materials to logistics and production. With the development of contemporary technology, blockchain may allay this worry by providing the SCM industry with automated software solutions. Blockchain is an emerging technology that supports a distributed and transparent approach to transactions between various entities. Due to increased digital usage across many sectors, the technology is being adopted more commonly in real-world business applications that aim to achieve transparency and security along a distributed chain of processes. Examining how these applications are deployed, based on the respective domain creates opportunities for future research and in advancing current thought processes of supply chain practitioners. This research aims to assess the fishing industry and provide a solution to trace the complete seafood lifecycle by capturing, recording, and tracking all relevant activities and data (e.g., video, photo, documents) from “bait to plate” and provide an open and immutable history record for each transaction in the supply chain of this lifecycle. The research offers valuable insight for supply chain practitioners into how blockchain technology has the potential to disrupt existing supply chain deployments and highlights some challenges of its successful adoption. Emerging blockchain applications aim to help businesses, including supply-chain transparency for a wide range of products

Keywords— *Blockchain Technology, Seafood Industry, Sustainability, Supply Chain Management*

I. INTRODUCTION

In 2008, more than a decade ago, Satoshi Nakamoto, the anonymous creator of Bitcoin, revealed how blockchain technology, a decentralized, distributed peer-to-peer, immutable linked ledger, could be used to address the financial challenges of maintaining transaction orders and double-spending [1], [2]. ‘Blockchain’ can be explained as a distributed database, organized as a list of ordered blocks with immutable committed blocks. Each block can be considered as a data packet that is linked to the one before it and comprises all previous data as well as new data. The whole chain is a database that is shared among numerous people who share control of the blocks (i.e. it is not controlled centrally) [3].

The blocks in the blockchain can be made up of any kind of data such as personally identifiable information (PII), transaction details (such as payments), operations in a supply chain management (SCM), barcodes, etc. This means that the scope and potential of blockchain are vast and vary depending on the use case. In developing a blockchain, the ledger’s nodes (i.e. blockchain miners) are in charge of chronologically connecting the blocks, ensuring each block includes the hash of the preceding block [3] allowing the system to keep reliable and auditable records for all transactions.

One of the practical uses of blockchain is supply-chain management, and the recent Coronavirus (COVID-19) pandemic emphasized the significance of how developing technologies can provide genuine and reliable commercial advantages. Growing customer expectations, diverse marketing channels, international obstacles, and a number of other issues have all made supply chains increasingly difficult to manage. A supply chain might involve several partners, spanning a large number of phases, operate in different countries, entail hundreds of invoices and payments, and last for a considerable amount of time due to shipping challenges [4].

Within the supply chain sector, the adoption of blockchain technology is still in its infancy. Two of the key elements influencing their acceptance inside SCM systems are traceability and trust. Breaking down these two essential elements into three additional sub-factors; increased supply chain visibility, digital supply chain transformation, and improved supply chain security and transparency will help to better understand how blockchain technology can progress the supply chain management industry [4]

II. LITERATURE REVIEW

Since its inception, the landscape of blockchain has rapidly evolved as technology expands beyond Bitcoin and other similar cryptocurrencies to other use cases, where Smart Contracts (SC) play a significant role [5]. Blockchain started out with its first iteration, Blockchain 1.0, which included applications that enabled digital cryptocurrency transactions. Over time, the technology further developed into Blockchain 2.0, which includes SCs and applications going beyond cryptocurrency transactions. The technology, now its third iteration, Blockchain 3.0 includes applications in fields

beyond the first two iterations, such as Industry 4.0 and SCM, government digitization, healthcare, science, and IoT [6].

In 1994, Szabo described SCs as “a computerized transaction protocol that implements the provisions of a contract” [7]. Szabo explored converting contractual clauses into embeddable code using SCs [8], which reduces the need for external involvement and risks. Specifically, an SC is an agreement between parties whose terms are automatically enforced even if they do not trust one another [9]. In a blockchain, SCs are scripts that execute in a decentralized fashion, based on set terms and are kept in the blockchain without relying on a trusted authority [9], [10]. Therefore, blockchains designed with SCs enable complicated processes and interactions, establishing new paradigms and the potential for virtually endless blockchain use cases.

In recent years, blockchains have significantly disrupted traditional business processes since activities and transactions that once required centralized systems or reliable third parties to authenticate, may now function in a decentralized fashion with the same (or even higher) level of certainty. Fundamental characteristics that blockchain offers include immutability, traceability, transparency, resilience, and security [9], [11].

Consequently, Blockchain technology is growing in importance [6]. According to a 2017 report by IBM, almost a thousand (33%) of C-suite executives said they were exploring blockchains or were currently actively utilizing them [12]. Researchers and developers are already familiar with the potential of the new technology and are investigating its many uses across a broad range of industries [9].

III. APPLICATION AREAS OF BLOCKCHAIN IN SUPPLY CHAIN MANAGEMENT

There is a wide spectrum of possible use cases for blockchain technologies in SCM. As illustrated in Fig. 1, in 2019, Helo and Hao [13] summarized these use cases in three categories namely: (i) assets, (ii) identity and (iii) transactions.

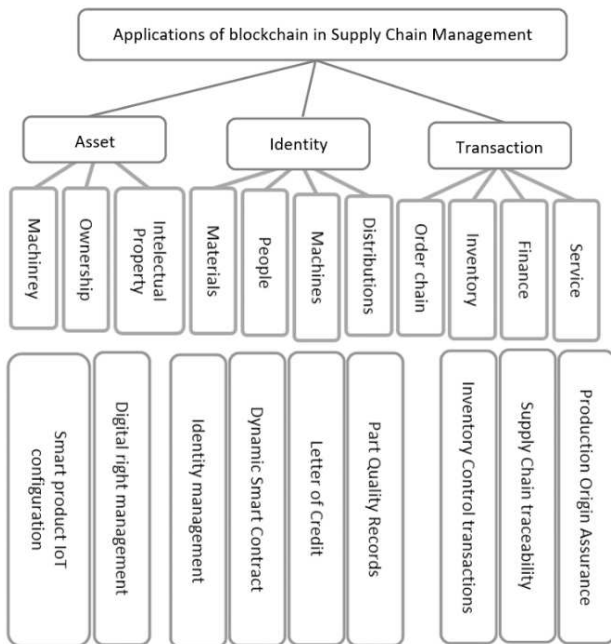


Fig. 1. Examples of applications of blockchain in supply chain management, adopted from Helo and Hao. [13]

A. Assets

It is essential to maintain accurate and trustworthy records to identify ownership and assure the accuracy and completeness of property-related important information for both tangible assets (i.e., physical property) and intangible assets (i.e., files) [14], [15]. By registering and trading the properties via blockchains through digital property management, it is feasible to establish the transfer of ownership and traceability of assets and their lifecycle via IoTs, [16]. Blockchain’s cryptographic management of keys and signatures identifies who owns and can trade inside the shared ledger, ensuring the provenance, security and veracity of the ledger’s stored assets [17].

B. Identity

Digital identity and private records, such as health records, licenses, ID cards, contracts, signatures, etc can be stored and authenticated with blockchain through securely encoded legal smart contracts. [3], [18]. Ultimately, code-based smart contracts are computer programs that can execute most of the agreements, contractual relationships, and governance [10], [17]. When a pre-configured condition in a smart contract among participating entities is met, the parties involved in the contractual agreement can automatically make transfers based on the contract in a transparent manner [3], [10].

C. Transactions

As relationships and interactions increasingly move online and are handled by automated processes rather than intermediary people, the traditional trust and confidence that most customers have relied on, are now either absent or can be forged through these online transactions [14]. The decentralized, immutable and distributed transaction ledger is one of the defining features of blockchain. This creates a permanent and verifiable record of transactions between parties [15]. All supply chain-related transactions, including orders, inventories, and goods, may be recorded and validated on the blockchain.

Supply chains are complicated because they consist of dispersed operations upstream, involving people, physical resources, and industrial processes, to downstream operations involving the entire selling process, including contracts, client sales, distribution, and disposal [16]. The objective of the supply chain is to develop a multi-stakeholder collaborative environment based on mutual trust, eliminate communication obstacles, and ensure that diverse businesses are interconnected to seek regular integration of the complete supply network [17], [18]. In the end, supply chain stakeholders may increase overall efficiency and provide higher value and advantages to their businesses through blockchain. Helo and Hao [13], simplified these advantages into five (5) key indicators as seen in Table 1.

TABLE I: TABLE ILLUSTRATING THE BENEFITS OF APPLYING BLOCKCHAIN IN SUPPLY CHAIN MANAGEMENT, ADOPTED FROM HELO AND HAO [13]

| Supply chain indicators | Blockchain key concepts | | |
|-------------------------|----------------------------------|---------------------------------------|--------------------------|
| | Tamper-proof transaction records | Information sharing & synchronization | Smart contract execution |
| Improve overall quality | X | X | X |
| Reduce cost | X | X | X |
| Shorten delivery time | | X | |
| Reduce risk | X | | X |

| | | | |
|----------------|---|--|---|
| Increase trust | X | | X |
|----------------|---|--|---|

IV. PROBLEM STATEMENT

The purpose of SCM systems is often to boost sales, lower manufacturing costs and complexity, eliminate fraud, and speed up production and delivery. Many businesses lack an integrated picture of the complete supply chain as supply networks are growing increasingly complicated in structure, challenging in terms of tasks, and diverse in terms of stakeholders. While big corporations have created their own identities and systems to sustain worldwide oversight of their operations and have the authority to engage and instruct their suppliers, many are struggling due to the pandemic. The situation is even worse for medium-sized and smaller corporations [19]. Many of them must rely on centralized regulatory authorities or middlemen. This has recently led to several internal and external constraints, including greater complexity, demand volatility, and a shifting retail environment, which are posing increasingly difficult problems for present SCM networks [4].

In terms of security, traceability, authentication, and the verification system, this lack of transparency creates a few concerns and challenges for the supply chain mechanism. In severe circumstances like COVID-19, this is more significant. As a result, certain chain suppliers temporarily stopped producing, and logistics companies were unable to move vital items like masks and ventilators as smoothly, especially across borders. It is noteworthy, that blockchain is well-suited to handle the difficulties of supply chains. Consequently, it is imperative to implement blockchain technology, with its immutability, transparency, and trustworthiness [20], to increase supply chain visibility and security.

Consumers are also requesting greater information about the origins of the products they purchase. Because of this, customers are prepared to pay more to businesses that have more transparent supply chains, which boosts not only sales but also customer happiness and confidence networks [4].

V. RESEARCH WORK

For the purpose of this research, sustainable supply chains, as explored by Hutchins and Sutherland [21], were assessed in an effort to design ‘sustainability measures’ for the seafood sector as well as guide similar future supply chain-related decisions. As described in the preceding section, blockchain is believed to provide enormous promise for strengthening supply chain management procedures and business models. A reference blockchain-based supply chain management system (BSCMS) was designed and implemented in the form of a proof of concept (POC) to provide a solution to trace the complete seafood lifecycle. The solution captures, cryptographically records and tracks all relevant activities and data (e.g. video, photo, documents) from “bait to plate” and provides an open and immutable history record for each transaction in the supply chain. The seafood industry is one of the world’s largest and oldest market sectors. It is also the longest logistic network for food and is made up of complex global supply chains which creates numerous social and environmental challenges. Both illegal fishing and unreported fishing are malpractices destroying and deplete marine habitats, threatening sustainability. Enhancing provenance certainty, traceability, and transparency along these supply chains could be a way to resolve these problems. Blockchain technology is well-positioned to achieve these goals.

As illustrated in Fig. 2 below, depending on the underlying technologies, blockchain systems can be accessed in different ways and are categorized based on how they are accessed [22]. According to Yeoh [23] and Wu et. all [24], as illustrated in figure 2 below [22], there are three categories of blockchain systems:

- Permissioned based (private), in which verification nodes are recognized and identified by a central authority or database.
- Permissionless-based (public), in which anybody can participate in the verification process without permission.
- Hybrid, in which both permissioned and permissionless ledgers are utilized.

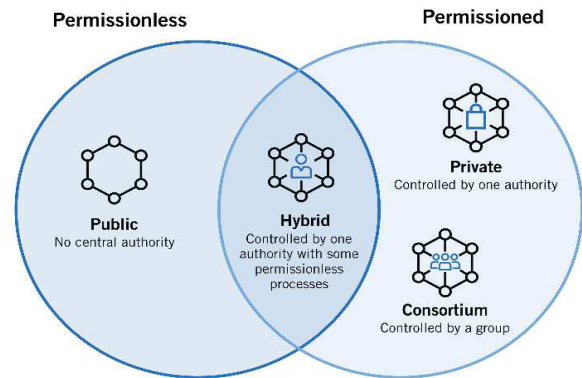


Fig. 2. Illustrating the blockchain architecture categories, adopted from Wegrzyn and Wang. [25]

In this research, a hybrid blockchain was selected to handle the process. Using either a fully public or entirely private ledger architecture for the flow of information makes it challenging to meet the practical needs of blockchain applications. For the proposed solution, it is vital to synchronize the two types of ledgers, a private ledger is utilized for sensitive data, whereas a public ledger is utilized for material that requires a high level of confidence. Without relying on a centralized governing body, each participant can control information access via the two forms of ledgers [24].

VI. DESIGNING THE BLOCKCHAIN WORKFLOW

The framework and the corresponding system architecture are composed of three layers, as seen in Fig. 3. This platform consists of several fundamental technologies and provides technical modules. This architecture is flexible and can be adapted based on realistic requirements for varying SCM sectors.

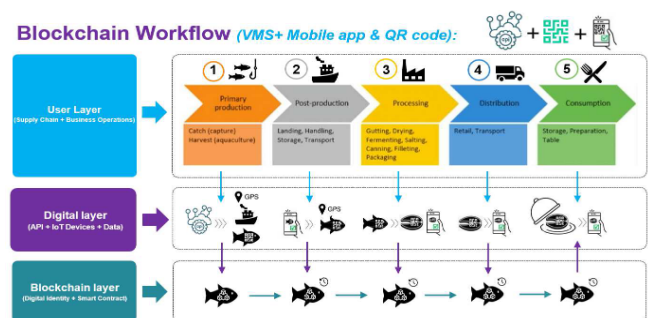


Fig. 3. Blockchain-based supply chain management system architecture.

User Layer: This layer comprises the supply chain and business operations. This layer includes various users.

Each partner can monitor the quality of the supply chain and perform various business activities with the support of blockchain.

The Digital Layer: This layer comprises both data collection and amalgamation to feed into the blockchain. Along the supply chain, different types of data (geo-location, weight, species, transactions, etc.) are either captured by IoT devices in real-time or imputed by users. All users, including logistics operators and consumers, keep a copy of different aspects of the data supply chain operations.

The Blockchain Layer: This layer offers a secure data-sharing infrastructure in a distributed network. When the data is gathered and shared in the digital layer, it will be digitally signed and added to the blockchain, facilitating supply chain monitoring and traceability. Digital identity is used to secure the authenticity of the data while the Smart contracts perform real-time quality monitoring by using real-time data.

Conceptually, a blockchain is governed by decentralized consensus and coherence. The logistical history data are reliable, precise and consistent. They can be preserved without the participation of a reliable mediator. Customers and logistics providers have complete access to their respective data [25]. The conceptual environment of the BSCMS established for this study is depicted in Fig. 3. The system focuses on the fishing industry in the United Kingdom.

VII. SOFTWARE IMPLEMENTATION

The functionalities of the system consist of transaction entry for supply chain operators which includes five (5) main stages:

1. Operators are authorized users. The user logs a transaction containing information on supply chain operations, seafood types, geolocation, timestamps, and health certificates. In addition, the transaction comprises the package's state, such as pickup, receipt, quality check, or final delivery.
2. A new block is offered and distributed to all peers in the supply chain network whenever a new logistical transaction is created.
3. Participants in the network get the block for validation. The system will place the new block into the chain after all participants have authorized it. This enables both clients and operators to have an efficient, verifiable, and permanent global perspective of the transaction history.
4. Once a block has been included in the chain, its data cannot be altered because the block is signed to the preceding block's cryptographic hash.
5. The transaction is complete after the authorized block has been added to the chain.

The architecture of BMLS is structured into two parts: (1) the back-end: which comprises the digital layer and the blockchain network working together to issue and verify digital certificates, and (2) the front-end: where users interface and interact with transactions.

The blockchain's backend design facilitates distributed transaction operations through codes SCs. Each block in the blockchain includes transaction information that links to the

preceding block. In the verification process, multiple server computers perform the verification procedure, flag anomalies and ensure the data's immutability. Data can also be saved on distributed servers, although for the sake of this proof-of-concept, local storage was employed for speedy package number searches.

VIII. RESULTS/ANALYSIS

A. The Issuing Process

Using blockchain technology, the POC designed for this research aimed to improve sustainability for supply chain management in the fishing sector. The implementation accounted for the entirety of the supply chain, from 'bait to plate' (Catching the seafood straight through to consumption). The developers created a uniform API that uses blockchain technology to record verified transactions. The API employs several data types, data sources, and data formats to generate and issue digital passports. Fig. 4 depicts how data supplied via the API is added to a blockchain to issue.

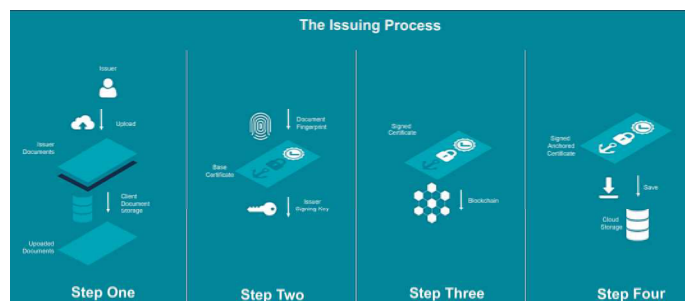


Fig. 4. The digital certificate issuing process.

Users have the opportunity to upload documents, which would automatically be digitally encoded and added to the blockchain. The final generated certificate is an immutable record that will encompass all pertinent information, documents, data, and assets as a sequence of unalterable occurrences in the seafood life cycle.

B. The Verification Process

Fig. 5 illustrates the verification process, where users or third parties are able to check the validity and file integrity of the generated certificated (digital passports) using the application. Users may also download the digital passport, submit it to an external protected portal, and verify its validity by comparing it to the original digital passport that is stored on the blockchain.

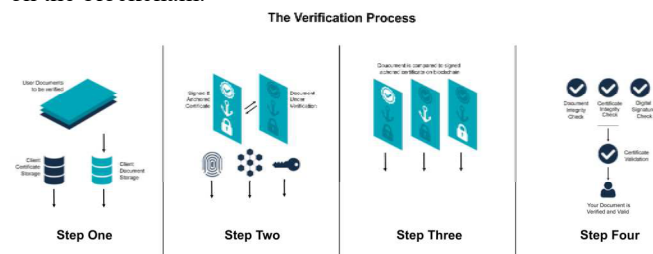


Fig. 5. The digital certificate verification process.

The result is a digital passport containing all pertinent information or assets to be anchored to the blockchain. The digital passport becomes an immutable record that serves as the record's gold standard. The digital passport has a unique, clickable and scannable QR code that redirects and validates against the original file stored on the blockchain. Every stage of the seafood's journey is made accessible to customers, through a digital passport (as seen in Fig. 6), therefore increasing their understanding and transparency.

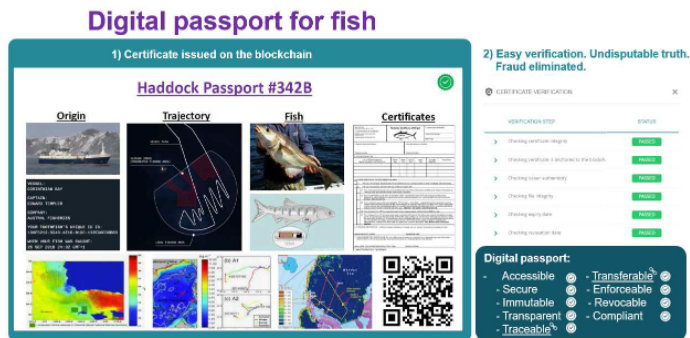


Fig. 6. The digital passport segments.

IX. DISCUSSION

In this study, the BSCMS is an exploratory reference implementation. We chose this method because blockchain is still considered to be in its infancy. Our objective was to provide a platform to increase the sustainability of supply chain-related operations while ensuring the confidentiality and transparency of all activity records. Numerous real-world business applications are adopting other use cases for transparency and security throughout a dispersed chain of activities. Two examples are mentioned below:

A. Safety and Tracking

Safety plays a crucial part in several businesses. Authentic food, for example, is a vital aspect of sustainability. Generally, counterfeit food poses a concern to public health. To resolve food safety challenges, transparency in food supply chain management is essential. Tracking and tracing are common supply chain operations for achieving informational transparency. Blockchain facilitates this transparency through an immutable database for transactions, users, locations, containers, etc. within the food sector. [26]. In 2016, Walmart teamed with IBM to build a blockchain-based system which significantly improved the transparency of both local and international supply chains. The use case merged blockchain with auto-ID technology to immediately trace the provenance of food in the event of a foodborne illness epidemic [26].

B. Identification Systems

Counterfeit pharmaceuticals pose a concern that blockchain technology can help to remediate [27], [28]. In the medical industry, it is well-known that counterfeit pharmaceuticals, such as anti-cancer treatments, can have fatal repercussions if patients do not receive therapy as recommended [27]. By enabling supply chain transparency from manufacturers to wholesalers to pharmacies to consumers, blockchain can improve patient safety. Through auto-ID technology, patients may verify that they have got the correct medication [27], [29] and trace it back to the point of origin.

As more parties in the supply chain use blockchain technology, it becomes more legitimate and valuable, eventually becoming an industry standard. However, early stakeholder buy-in will be challenging due to varying levels of digital preparedness [29], high implementation costs and a lack of supportive regulatory mechanisms around the technology [2]. It is crucial to establish standards and agreements around the technology to ensure interoperability across various blockchain-based systems [30]

X. CONCLUSION

Blockchain technology adoptions are still considered to be in the early stages within the supply chain industry. Traceability and trust are two of the major factors driving their adoption within SCM systems. Understanding how blockchain technologies advance the supply chain management sector lies in breaking down these two key factors into further three sub-factors (i) increased visibility along the supply chain, (ii) digital transformation of supply chains, and (iii) enhanced security and transparency within the supply chain.

There are several challenging aspects of the supply chain that make it extremely complex to manage. For example, numerous parties are engaged in the supply chain, a shared common database is required, and once recorded, transactions are rarely altered. Therefore, supply chains may be progressively optimized by utilizing a digital infrastructure environment such as blockchain, in which all involved parties can exchange, access and meticulously monitor product-related information in real time. Ultimately, the technology considerably decreases SCM's complexity [31] and increases sustainability.

Numerous logistics operators, particularly small and medium-sized businesses, claim to have limited awareness of blockchain and view its influence as a danger [32]. Although logistics and supply chain management blockchain research is still in its infancy, small-scale experiments such as the one in this research should be conducted by businesses to gain first-hand knowledge [4].

To increase the understanding of blockchain technologies, this project designed a prototype of a blockchain-based supply chain management system (BSCMS). This BSCMS acquired and communicated logistical data utilizing a blockchain approach. The capability of the system enables clients, logistic operators, and any other partners to follow the complete lifecycle of seafood, from capture to consumption. The proposed reference architecture illustrates how blockchain may be implemented utilizing components in operational and supply chain contexts. Our findings indicate that, in contrast to traditional IT designs, blockchain technology is a potential platform to improve supply chain management sustainability by introducing transparency, automation, and trust.

XI. REFERENCES

- [1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: www.bitcoin.org
- [2] A. al Hussain, M. A. Emon, T. A. Tanna, R. I. Emon, and M. M. H. Onik, "A Systematic Literature Review of Blockchain Technology Adoption in Bangladesh," *Annals of Emerging Technologies in Computing*, vol. 6, no. 1.

- International Association for Educators and Researchers (IAER), pp. 1–30, 2022. doi: 10.33166/AETiC.2022.01.001.
- [3] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, “BlockChain Technology: Beyond Bitcoin,” *Applied Innovation Review*, no. 2, Jun. 2016.
- [4] PWC, “Time for trust The trillion-dollar reasons to rethink blockchain,” 2020. Accessed: Jun. 22, 2022. [Online]. Available: <https://www.pwc.com/gx/en/industries/technology/publications/blockchain-report-transform-business-economy.html#:~:text=Trust%2C%20transparency%2C%20efficiency%3A%20The,%2C%20cut%20costs%20and>
- [5] F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” *Telematics and Informatics*, vol. 36. Elsevier Ltd, pp. 55–81, Mar. 01, 2019. doi: 10.1016/j.tele.2018.11.006.
- [6] J. L. Zhao, S. Fan, and J. Yan, “Overview of business innovations and research opportunities in blockchain and introduction to the special issue,” *Financial Innovation*, vol. 2, no. 1. SpringerOpen, Dec. 01, 2016. doi: 10.1186/s40854-016-0049-2.
- [7] N. Szabo, “Smart contracts.” 1994.
- [8] N. Szabo, “The idea of smart contracts.” 1997.
- [9] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” *Ieee Access*, vol. 4, pp. 2292–2303, 2016.
- [10] E. Leka and B. Selimi, “Development and evaluation of blockchain based secure application for verification and validation of academic certificates,” *Annals of Emerging Technologies in Computing*, vol. 5, no. 2, pp. 22–36, 2021, doi: 10.33166/AETiC.2021.02.003.
- [11] G. Greenspan, “Ending the bitcoin vs blockchain debate,” *MultiChain*. Available online: [http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/\(accessed on 15 January 2020\)](http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/(accessed on 15 January 2020)), 2015.
- [12] IBM, “Key Marketing Trends for 2017,” *IBM Website*, 2017. <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN> (accessed Nov. 12, 2022).
- [13] P. Helo and Y. Hao, “Blockchains in operations and supply chains: A model and reference implementation,” *Comput Ind Eng*, vol. 136, pp. 242–251, Oct. 2019, doi: 10.1016/j.cie.2019.07.023.
- [14] O. Dib and K. Toumi, “Decentralized identity systems: Architecture, challenges, solutions and future directions,” *Annals of Emerging Technologies in Computing*, vol. 4, no. 5. International Association for Educators and Researchers (IAER), pp. 19–40, 2020. doi: 10.33166/AETiC.2020.05.002.
- [15] M. Swan, *Blockchain: Blueprint for a new economy*. “O’Reilly Media, Inc.,” 2015.
- [16] F. Tian, “An agri-food supply chain traceability system for China based on RFID & blockchain technology,” in *2016 13th International Conference on Service Systems and Service Management, ICSSSM 2016*, Aug. 2016. doi: 10.1109/ICSSSM.2016.7538424.
- [17] K. Korpela, J. Hallikas, and T. Dahlberg, “Digital Supply Chain Transformation toward Blockchain Integration,” in *In proceedings of the 50th Hawaii international conference on system sciences*, 2017. [Online]. Available: <http://hdl.handle.net/10125/41666>
- [18] T. Tuominen, N. Kitaygorodskaya, and P. Helo, “Benchmarking Russian and Finnish food industry supply chains,” *Benchmarking*, vol. 16, no. 3, pp. 415–431, May 2009, doi: 10.1108/14635770910961416.
- [19] S. Y. Lee and R. D. Klassen, “Drivers and enablers that foster environmental management capabilities in small- and medium-sized suppliers in supply chains,” *Prod Oper Manag*, vol. 17, no. 6, pp. 573–586, Nov. 2008, doi: 10.3401/poms.1080.0063.
- [20] G. Chen, B. Xu, M. Lu, and N.-S. Chen, “Exploring blockchain technology and its potential applications for education,” *Smart Learning Environments*, vol. 5, no. 1, Dec. 2018, doi: 10.1186/s40561-017-0050-x.
- [21] M. J. Hutchins and J. W. Sutherland, “An exploration of measures of social sustainability and their application to supply chain decisions,” *J Clean Prod*, vol. 16, no. 15, pp. 1688–1698, Oct. 2008, doi: 10.1016/j.jclepro.2008.06.001.
- [22] K. E. Wegrzyn and E. Wang, “Types of Blockchain: Public, Private, or Something in Between.” Aug. 19, 2021. <https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between> (accessed Dec. 11, 2022).
- [23] P. Yeoh, “Regulatory issues in blockchain technology,” *Journal of Financial Regulation and Compliance*, vol. 25, no. 2, pp. 196–208, May 2017, doi: 10.1108/JFRC-08-2016-0068.
- [24] H. Wu, Z. Li, B. King, Z. ben Miled, J. Wassick, and J. Tazelaar, “A distributed ledger for supply chain physical distribution visibility,” *Information (Switzerland)*, vol. 8, no. 4, Nov. 2017, doi: 10.3390/info8040137.
- [25] C. Esposito, A. de Santis, G. Tortora, H. Chang, and K. K. R. Choo, “Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?,” *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, Jan. 2018, doi: 10.1109/MCC.2018.011791712.
- [26] E. Shaffer, “Walmart, IBM provide blockchain update,” *Meat & Poultry (June 2, 2017)*. Retrieved June, vol. 22, p. 2018, 2017.
- [27] T. K. Mackey and G. Nayyar, “A review of existing and emerging digital technologies to combat the global trade in fake medicines,” *Expert Opin Drug Saf*, vol. 16, no. 5, pp. 587–602, May 2017, doi: 10.1080/14740338.2017.1313227.
- [28] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, “Blockchains everywhere - A use-case of blockchains in the pharma supply-chain,” in *Proceedings of the IM 2017 - 2017 IFIP/IEEE International Symposium on Integrated Network and Service Management*, Jul. 2017, pp. 772–777. doi: 10.23919/INM.2017.7987376.
- [29] S. DeCovny, “Experts discuss tackling pharma supply chain issues with blockchain,” URL: <http://www.nasdaq.com/article/experts-discuss-tackling-pharma-supply-chain-issues-with-blockchain-cm808938>, 2017.
- [30] M. Kückelhaus, G. Chung, J. González-Peralta, K. Turner, B. Gockel, and T. Acar, “Blockchain in logistics,” *DHL Customer Solutions and Innovation*, 2018.
- [31] Y. Omran, “Inclusive supply chain finance approach: Integrated supply chain finance solution with digitalization,” *White paper, Fraunhofer IML*, 2016.
- [32] N. Hackius and M. Petersen, “Blockchain in logistics and supplychain: Trick or treat?,” in *Proceedings of the Hamburg International Conference of Logistics (HICL)*, 2017, vol. 23, pp. 3–18. doi: <https://doi.org/10.15480/882.1444>.

Blockchain-based Supply Chain Management Systems: A Systematic Mapping Study of Academic Research

Odayne Haughton
Manufacture Advance Design
Engineering (MADE) Cymru
University of Wales Trinity Saint
David
Wales, United Kingdom
o.haughton@uwtsd.ac.uk

Carlene Campbell
Wales Institute of Science and Art
University of Wales Trinity Saint
David
Wales, United Kingdom
carlene.campbell@uwtsd.ac.uk

Terry H. Walcott
Wales Institute of Science and Art
University of Wales Trinity Saint
David
Wales, United Kingdom
t.walcott@uwtsd.ac.uk

Irina Neaga
Wales Institute of Science and Art
University of Wales Trinity Saint
David
Wales, United Kingdom
irina.neaga@uwtsd.ac.uk

Abstract— This research provides an in-depth exploration of the cybersecurity challenges in blockchain technology within the context of Supply Chain Management (SCM). By conducting a systematic literature review (SLR), the study identifies and classifies key cybersecurity issues, revealing the intricate balance between security and operational efficiency in blockchain-integrated SCM systems. The primary focus areas include consensus mechanism failures, smart contract vulnerabilities, network-level attacks, and cryptographic challenges. The study prioritizes these cybersecurity concerns, proposing a sequential approach to address them effectively. It emphasizes the need for continuous refinement in understanding and methodologies to enhance the security and efficiency of blockchain-based SCM systems. The research culminates in the proposition of strategic directions for future research, aiming to fortify blockchain SCM against emerging threats while optimizing its operational efficacy. The findings offer valuable insights for both academia and industry, highlighting the critical role of cybersecurity in the successful integration and sustainability of blockchain technology in SCM.

Keywords— *Blockchain Technology, Cybersecurity, Supply Chain Management, Systematic Literature Review.*

I. INTRODUCTION

The exploration of blockchain technology, characterized by its distinctive attributes, has gained significant traction across various corporate sectors. This exploration is not limited to but prominently includes areas such as banking [1], governmental systems [2], healthcare [3], and notably, Supply Chain Management (SCM) [4], [5]. SCM, defined as the holistic coordination of commodity flow from inception to consumption, encompasses a complex network of interlinked organizations engaged in the production and distribution of goods. The evolution from nascent trade systems to sophisticated, technology imbued SCM paradigms has afforded organizations the capacity for proactive error detection, fulfilment of consumer demands, and simultaneous attainment of economic objectives. In an era increasingly centred around customer-centricity and the strategic

importance of flexible product acquisition within SCM, the role of technology, especially blockchain, becomes pivotal.

Blockchain technology, renowned for its potential to forge secure and efficient digital frameworks, is underpinned by a multi-layered infrastructure typically comprising the incentive, consensus, and network layers. Each layer is integral to shaping the blockchain's performance and security profile. The burgeoning academic discourse on blockchain integration within SCM which was initiated by Kamble, Gunasekaran, and Arha [6] and subsequently expanded by Saberi et al. [7] and Casino et al. [8] both underscore the capabilities and complexities inherent in this technological innovation.

In light of this, a meticulous examination of the cybersecurity challenges presented by blockchain in SCM is imperative. This involves a comprehensive review of both foundational and contemporary research to ascertain the current state of cybersecurity and operational efficiency in blockchain applications specifically within SCM contexts.

Despite significant advancements, there remains a pronounced gap in empirical research focused on the practical deployment of blockchain within SCM systems and the associated security challenges. This gap, evident against the backdrop of rapid technological evolution and SCM's crucial role in contemporary commerce, signifies a lacuna that extends from academic discourse to tangible industrial implications. This research aims to address this gap by concentrating on existing studies that explore the cybersecurity implications of blockchain infrastructure choices within SCM, including vulnerabilities to attacks such as 51% Attacks, Sybil Attacks, and Denial-of-Service (DoS) intrusions. The overarching goal is to develop a community-driven framework for secure and efficient blockchain implementation in SCM. This entails a nuanced analysis of the existing literature and empirical studies on cybersecurity strategies within blockchain-enabled SCM systems, leveraging these insights to inform and guide future developments in this field.

II. PRIOR RESEARCH

In the expansive realm of Supply Chain Management (SCM) systems, a conspicuous paucity of comprehensive Systematic Literature Reviews (SLRs) exists, particularly concerning the cybersecurity challenges associated with blockchain technology in SCM contexts. Notably, Salman et al. [9] contributed a seminal survey paper delving into the interplay between blockchain and cybersecurity. Their study pivots on elucidating the myriad issues and intricacies inherent in deploying security services within centralized architectures across diverse application domains. The authors proffer an exhaustive assessment of contemporary blockchain-centric methodologies, encompassing a spectrum of security services such as authentication, confidentiality, privacy, access control, data and resource provenance, and integrity assurance within distributed networks. Although their focus is not exclusively tethered to SCM, their research lays a foundational bedrock for scholars exploring the security dimensions of blockchain-based supply networks.

Furthermore, the academic landscape reveals a limited corpus of scholarly works addressing the broader implications of blockchain technology. In the ensuing discourse, these studies will be scrutinized to discern the thematic divergences between their focal points and the objectives of this present study. Yli-Huumo et al. embarked on an SLR in 2016, aiming to aggregate and analyze research findings about the overarching concept of blockchain technology [10]. Their review, intentionally eschewing legal, economic, and regulatory dimensions, centred on literature germane to blockchain technology. A key observation from their analysis was that a staggering 80% of the research publications concentrated on Bitcoin-related initiatives, predominantly tackling security and privacy concerns. Notably absent was a focus on blockchain applications in SCM. Since 2016, the application spectrum of blockchain has considerably diversified, prompting this research to probe into existing scholarly works that specifically address the intersection of cybersecurity and blockchain applications in SCM.

In late 2016, Conoscenti et al. conducted an SLR exploring the adaptability and application of blockchain, especially in relation to IoT and other peer-to-peer networks [11]. Concurrently, Seebacher et al. in 2017, presented an SLR underscoring the burgeoning impact of blockchain on service systems [12]. These studies, foreshadowing the trajectory of this research, emphasize the necessity of examining real-world blockchain applications, particularly in the context of their implications for security and efficiency in SCM solutions. The prior research, while addressing broad aspects of blockchain technology, falls short in specifically analyzing its role in enhancing the security and operational efficiency of SCM solutions. The field of blockchain, characterized by its relatively nascent stage and rapid evolution, imposes an academic imperative to synthesize and interpret recent research that converges blockchain technology, SCM, and cybersecurity. This synthesis is crucial in guiding future investigative endeavours in this rapidly developing domain. Thus, it becomes imperative to present an updated review of contemporary research in the realms of blockchain and cybersecurity, to chart a course for future research initiatives.

III. SYSTEMATIC LITERATURE REVIEW (SLR) METHODOLOGY

The research methodology adopted for this study is the systematic mapping study as proposed by Patersen et al. [13], with a specific focus on exploring the burgeoning realm of smart contracts technology within the context of Supply Chain Management (SCM) systems. This systematic mapping approach is instrumental in identifying, categorizing, and elucidating research themes pertinent to smart contracts, while concurrently pinpointing potential research gaps for future scholarly exploration. Figure 1 delineates this systematic mapping study, which is segmented into five distinct phases: defining research questions, initiating the search process, selection of relevant papers, keywording (using abstracts) along with data extraction, and finally, the mapping process. This SLR adheres stringently to the guidelines set forth by Kitchenham [14], ensuring a robust and comprehensive review encompassing planning, conducting, and reporting phases, each executed iteratively to guarantee an exhaustive evaluation.

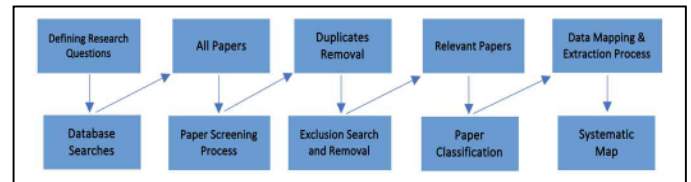


Fig. 1. Steps included in the Systematic Literature Review.

A. Research Questions for Systematic Literature Review

The initiation of a systematic mapping study necessitates the formulation of research questions that guide the investigative trajectory of the study. For this research, four pivotal questions are posited:

RQ1: What foundational theories and empirical evidence in existing literature interconnect blockchain technology, cybersecurity, and SCM, and how have these influenced methodological developments in this field?

RQ2: What are the latest methodological innovations in blockchain technology concerning cybersecurity challenges in SCM, and what are the identified research gaps and opportunities for advancement?

RQ3: What are the nascent trends in the integration of blockchain within SCM, and how might these trends influence the security and operational efficiency of SCM processes, especially considering the unique requirements of the SCM sector?

B. Database Search Strategy

The second phase involves an extensive search for research papers addressing security in blockchain-based supply chains. The selection of keywords, crafted to unearth relevant research findings, involved the use of Boolean operators "AND" and "OR". The search strings included combinations of terms such as "security", "cybersecurity", "blockchain", "distributed ledger", "Supply Chain Management", and "Supply Chain".

Six esteemed scientific databases were chosen for this search: Wiley Online Library, ACM Digital Library, IEEE Xplore Digital Library, ScienceDirect, SpringerLink, and Taylor & Francis. The inclusion criteria were restricted to peer-reviewed papers published in journals, conferences, symposia, workshops, and books.

Searches, executed between May and October 2023, were based on titles, keywords, and abstracts, as per each platform's specific search functionalities. All publications up to the search date were considered. The initial search results were then filtered based on inclusion/exclusion criteria, detailed subsequently, and subjected to a rigorous snowballing process as described by Wohlin [15], employing both forward and backward snowballing until no further relevant publications were identified.

C. Paper Screening Process: Inclusion and Exclusion Criteria

The third phase involves the systematic exclusion of papers irrelevant to the research questions, guided by the PICOS framework [16]. This framework delineates criteria based on Population (pertaining to SCM systems), Intervention (blockchain deployment and integration), Comparison (evaluation of various blockchain deployments), Outcome (efficiency and cybersecurity concerns in blockchain implementation in SCM), and Study design (empirical research offering evidence on the topic). Preference was given to the most recent publications from authors where multiple similar works existed.

The inclusion criteria are as follows:

Mentioned Blockchain: Papers exploring blockchain technology within the SCM context.

Security Context: Studies examining cybersecurity concerns arising from blockchain adoption and use.

Blockchain Performance: Assessments of blockchain's performance in its applied environment, including peer-reviewed publications in recognized academic journals or conference proceedings.

Language: Publications available in English.

Time: Publications from the inception of blockchain technology in 2008 to the present.

Exclusion criteria involved removing papers based on titles, and where necessary, abstracts. Papers in languages other than English, those lacking full text, or those contributing non-critical content such as popular articles or grey literature were excluded. Duplicates and non-technology-focused papers were also removed.

D. Paper Classification

In the fourth phase, papers were categorized based on the keyword approach proposed by Yli-Huumo J [10]. This involved analyzing abstracts to extract crucial keywords and key contributions, aiding in the classification of papers into relevant categories. Papers difficult to classify based solely on

abstracts were quickly skimmed to facilitate appropriate categorization.

E. Data Extraction and Mapping Process

The final phase encompassed collecting data necessary to address the research questions. This involved extracting key goals and contributions from each selected paper.

IV. SEARCH RESULTS AND ANALYSIS

The comprehensive search, structured around pre-defined keywords, yielded a substantial corpus of studies across the selected databases, totalling 10,894. Post-elimination of duplicates, this number was refined to 6,465. A meticulous evaluation against the predetermined inclusion and exclusion criteria further distilled the pool to 703 papers deemed relevant for an in-depth review. Subsequent rigorous assessment of these 703 papers, strictly adhering to the inclusion/exclusion criteria, identified 72 papers that fully met the specified requirements. The adoption of systematic snowballing techniques, both forward and backwards, further enriched this selection, adding 20 and 16 publications respectively. Ultimately, the total count of papers incorporated into this systematic literature review (SLR) stood at 108. Utilizing the PRIMA Flow Diagram [17], Figure 2 delineates the attrition rate and selection stages of papers from the initial keyword search to the final curation of primary studies.

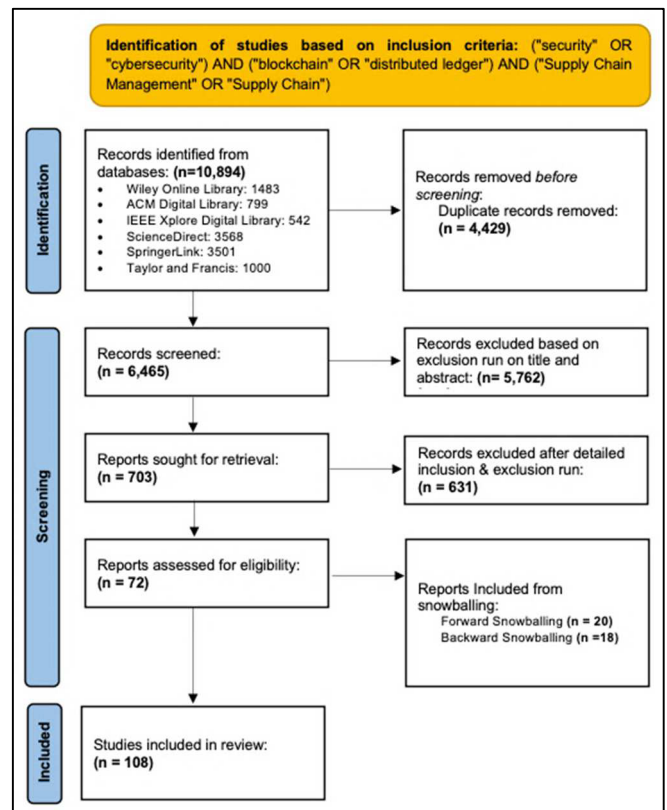


Fig. 2. Paper gathering flow diagram.

The exclusion of a significant number of papers primarily hinged on three factors. Firstly, many studies were tangential to the core focus of this research, exploring blockchain-based

SCMs from non-technical perspectives such as economic or legal viewpoints. Secondly, several papers were excluded as they predominantly discussed cryptocurrencies or blockchain in a broader context, not directly contributing to the research questions at hand. Lastly, papers focusing on grey literature about smart contracts or speculative applications in domains like the Internet of Things, without offering substantial technical insights, were also omitted. As a result, 188 papers were deemed pertinent and included in the systematic mapping study.

A. Quality assessment

The quality of primary studies was rigorously evaluated following the guidelines by Kitchenham and Charters [18], ensuring relevance to the research questions and scrutinizing for potential research bias and validity of experimental data. This process, inspired by Hosseini et al. [19], involved a multi-stage assessment:

Stage 1. Focus on Blockchain in SCM: Papers should specifically address blockchain usage in SCM or examine its technical aspects influencing supply chain security and efficiency.

Stage 2. Contextual Clarity: Papers must provide sufficient context for their research objectives and findings, enabling accurate interpretation.

Stage 3. Detailed Blockchain Application: Studies should detail the implementation of blockchain technology in SCM systems, aiding in addressing the research questions.

Stage 4. Security Contextualization: Papers need to clearly articulate the security challenges being addressed.

Stage 5. Performance Analysis: The papers should assess blockchain performance in their respective application environments, facilitating comparative analyses.

Stage 6. Data Acquisition Integrity: Information on how data was acquired, measured, and reported should be detailed to ascertain accuracy.

This checklist for quality assessment was then applied to all other primary studies identified.

B. Data extraction

The data extraction phase involved scrutinizing papers that passed the quality assessment, focusing on the completeness and accuracy of information. Initially tested on five studies, this process was then extended to all qualified papers. Extracted data were categorized and recorded in a spreadsheet under:

Context data: Pertinent to the SRL's purpose.

Qualitative data: Author-provided findings and conclusions.

Quantitative data: Data obtained through experimentation and research.

C. Data analysis

The data analysis aimed to synthesize insights from the qualitative and quantitative data to address the research questions. This involved aggregating data followed by a meta-analysis of studies that had undergone the final data extraction phase.

D. Publications over time

A notable observation is the absence of definitive primary research papers on blockchain until 2016, despite the concept's inception with Bitcoin in 2008. This delay underscores the emergent nature of blockchain research, particularly in the context of cybersecurity and SCM efficiency. Figure 3 graphically charts the annual publication trend, highlighting an increasing focus on blockchain in SCM systems, paralleled by growing research on cybersecurity and operational efficiency. This trend suggests an anticipated surge in future research aimed at optimizing blockchain integration in practical SCM applications.

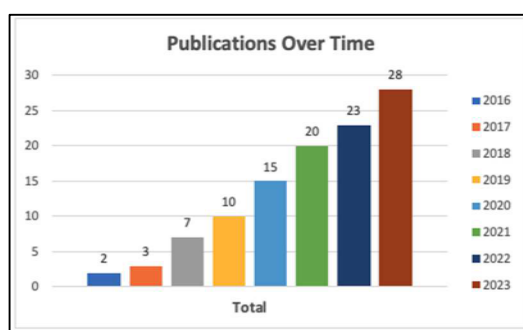


Fig. 3. Distribution of primary studies extracted

V. RESEARCH FINDINGS

A meticulous review process was undertaken for each primary research article, leading to the extraction and condensation of both qualitative and quantitative data. These data points were systematically summarized in Figure 4, illustrating the thematic convergence of the primary studies within the overarching realm of blockchain's application in addressing specific challenges. The 108 primary studies, each rigorously vetted through a quality assessment process, were then thematically categorized in Figure 4.

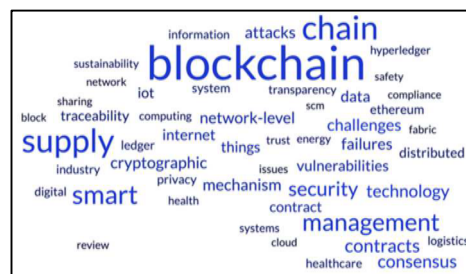


Fig. 4. Distribution of primary studies extracted

The thematic analysis led to the classification of each paper into broader categories, delineating the technological focal points within blockchain application. These categories, delineated into four primary thematic areas, include: (i) Consensus Mechanism Failures, (ii) Smart Contract Vulnerabilities, (iii) Network-Level Attacks, and (iv)

Cryptographic Challenges. This classification aids in understanding the diverse technological challenges and potential vulnerabilities within the domain of blockchain technology.

A. Taxonomy of Cybersecurity Challenges in Blockchain-Enhanced Supply Chain Management

Employing the Keywording technique, as illustrated in Figure 5., the research papers were categorized into four distinct yet interconnected categories: (i) Consensus Mechanism Failures, (ii) Smart Contract Vulnerabilities, (iii) Network-Level Attacks and (iv) Cryptographic Challenges. The integration of blockchain technology in SCM has been revolutionary, offering enhanced traceability, transparency, and security. Nonetheless, blockchain is not impervious to cybersecurity threats. A profound comprehension of these challenges is crucial for the development, deployment, and maintenance of robust blockchain-based SCM systems.

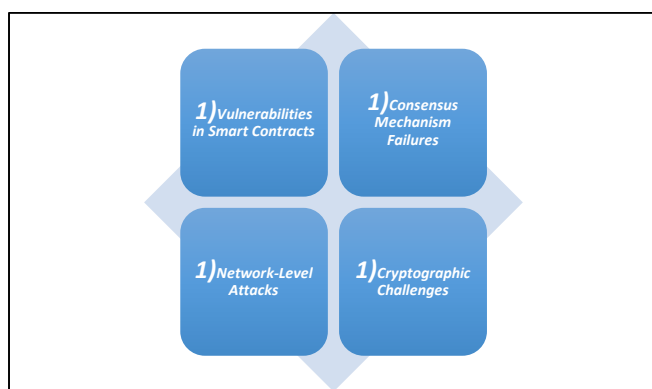


Fig. 5. Summarized Systematic Categories

1) Consensus Mechanism Failures

The consensus mechanisms, including Proof of Work (PoW) and Proof of Stake (PoS), are critical for transaction validation in blockchain networks. Failures or vulnerabilities within these mechanisms can severely undermine the reliability and integrity of the entire SCM system.

2) Vulnerabilities in Smart Contracts

Smart contracts, the self-executing contracts with terms embedded in code, are fundamental to the automation processes in blockchain SCM. Despite their efficiency, they introduce significant cybersecurity risks that must be addressed.

3) Network-Level Attacks

Blockchain networks are vulnerable to a variety of network-level attacks that can impact their availability, reliability, and integrity. Such attacks pose a significant threat to the stability and functionality of blockchain systems.

4) Cryptographic Challenges

The foundation of blockchain security lies in its cryptographic underpinnings. However, weaknesses in cryptographic algorithms or their implementations can precipitate systemic vulnerabilities, posing substantial risks to the integrity and security of blockchain frameworks.

In the realm of blockchain-based Supply Chain Management (SCM), four critical areas are pivotal for maintaining the system's integrity and operational efficiency. Firstly, consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS) are crucial for validating transactions and preserving ledger integrity. Failures in these mechanisms, such as the 51% attack, can lead to significant trust issues within the supply chain due to incorrect transaction confirmations. Secondly, smart contracts, vital for automating SCM processes like payments and tracking, can suffer from vulnerabilities leading to substantial disruptions and losses. Thirdly, blockchain networks face the risk of network-level attacks like DDoS, which can compromise data availability and integrity, crucial for SCM operations. Lastly, the security of blockchain heavily relies on cryptographic algorithms. Weaknesses in these algorithms pose risks of data breaches and tampering, especially problematic in SCM due to the sensitivity of the stored data. These vulnerabilities necessitate robust cryptographic practices to protect against evolving threats such as quantum computing, ensuring the long-term security and reliability of blockchain in SCM. This analysis underscores the multifaceted nature of cybersecurity challenges in blockchain-based SCM systems. It highlights the imperative for ongoing research and development efforts to fortify these systems against a spectrum of technological vulnerabilities.

VI. DISCUSSION

The preliminary keyword searches unveiled a substantial body of literature pertaining to blockchain technology, a relatively young topic that has shown swift advancement in the past decade. The majority of these studies consist of theoretical recommendations or conceptual solutions that tackle current difficulties. These studies are typified by a lack of quantitative data and limited actual implementations. Nevertheless, a portion of these initial investigations showcases pioneering technical remedies for a range of problems in blockchain technology, such as failures in consensus mechanisms, vulnerabilities in smart contracts, attacks at the network level, and cryptographic obstacles. To effectively utilise blockchain in Supply Chain Management (SCM), it is crucial to have a comprehensive grasp of its cybersecurity environment. The classification of cybersecurity concerns, namely consensus mechanism failures, smart contract vulnerabilities, network-level attacks, and cryptographic challenges, highlights the key areas that require attention to enhance the security and operational effectiveness of blockchain supply chain management (SCM) systems. This research seeks to emphasise the importance of analysing these factors, pushing for a systematic prioritisation based on their influence and interconnectedness in improving the security and efficiency of the full lifecycle of supply chain management (SCM).

A. Consensus Mechanism Failures

Consensus mechanisms, as elaborated by Eyal and Sirer [20], are fundamental in maintaining the integrity of blockchain transactions. Failures or vulnerabilities in these mechanisms can critically undermine the SCM system. Adopting more secure and energy-efficient consensus mechanisms, such as Proof of Stake (PoS), as discussed by

Saleh [21], not only bolsters security but also augments the efficiency of transaction processing. This is crucial for SCM operations that demand promptness and reliability. Prioritizing the security of the consensus mechanism is essential, as it underpins the operational integrity of the entire blockchain network, affecting every aspect of its functionality.

B. Smart Contract Vulnerabilities

Smart contracts, integral to automating SCM processes, harbour significant security risks as identified by Luu et al. [22] and Atzei et al. [23]. Securing smart contracts directly translates to more robust SCM operations, ensuring the reliability and accuracy of automated processes. Addressing smart contract vulnerabilities follows the fortification of the consensus layer, given its pivotal role in the execution of individual operations within the SCM framework.

C. Network-Level Attacks

Network-level vulnerabilities as highlighted by authors like Apostolaki et al. [23] and Saad et al. [24], can adversely affect the availability and integrity of blockchain networks. In SCM, where timely and precise data transmission is crucial, network-level attacks can cause significant disruptions. Therefore, securing the network layer, through advanced measures like decentralized node distribution, is critical once the consensus mechanisms and smart contracts are safeguarded.

D. Cryptographic Challenges

The cryptographic foundation of blockchain, as discussed by Li et al. [25], is vital for maintaining its integrity. Addressing cryptographic challenges, while crucial for long-term sustainability, can be prioritized subsequent to the immediate and more directly impactful areas. These challenges often require a strategic approach, considering advanced threats like quantum computing.

The proposed strategic areas are pivotal for an integrated enhancement of security and efficiency in blockchain-based SCM systems. It ensures that each security layer reinforces the subsequent one, culminating in a comprehensive and efficient SCM system. The integration of security measures not only fortifies the blockchain against potential threats but also optimizes operational efficiency, crucial for SCM systems handling complex operations at scale.

E. Critical Analysis and Reflection on Limitations of Existing Literature on Blockchain in SCM

Evolutionary Nature of Technology: Blockchain technology is rapidly evolving, and many studies may become outdated quickly. The dynamic nature of this technology poses a challenge for researchers to provide timely and relevant insights. Consequently, some literature may not reflect the latest technological advancements or emerging trends in the field. Future research should strive for a more comprehensive, empirically validated, and multi-disciplinary approach that considers the evolving nature of technology, diverse geographical contexts, and the balance between technological and business implications.

VII. CONCLUSION

In the rapidly evolving domain of industrial technology, the integration of blockchain into diverse applications delineates a complex nexus of technical foundations and practical ramifications. Core aspects of blockchain technology, such as consensus algorithms, hashing techniques, distributed ledger systems, and the nuances of Bitcoin mining, extend beyond the realm of mere technical terminology. These elements are critically integral in evaluating blockchain's applicability, identifying optimal areas for deployment, and formulating strategies for efficient and economically viable implementation. Despite blockchain's inherent security features, including robust encryption and decentralized governance, these systems are not entirely immune to cybersecurity vulnerabilities. Increasing incidents of successful breaches in blockchain networks and the prevalence of vulnerabilities like Distributed Denial of Service (DDoS) attacks, smart contract flaws, malicious nodes, private key security risks, and the potential for 51% attacks, as noted by Ravikumar et al. [26], underscore this reality.

This paper has meticulously examined peer-reviewed literature from esteemed journals to unearth the predominant cybersecurity challenges associated with blockchain technology in Supply Chain Management (SCM). The terrain of blockchain-empowered SCM is fraught with an array of challenges, issues, and vulnerabilities. It is evident that while blockchain technology has catalysed a revolutionary shift in SCM, enhancing security and operational efficiency, it concurrently introduces four distinct cybersecurity dilemmas that demand rigorous scrutiny and resolution. This necessitates a continuous refinement of understanding and methodologies by researchers and practitioners to effectively counter these emerging vulnerabilities. The focus of this thesis is to delve into the complexities surrounding failures in consensus mechanisms, to unravel and propose efficacious strategies for a more secure and efficient blockchain-based SCM.

The symbiosis between security and efficiency in blockchain-based SCM systems is intricate yet indispensable. Addressing the identified cybersecurity challenges not only promises to bolster the security of SCM systems but also to enhance their efficiency, reliability, and overall functionality. Adopting a holistic approach to understanding and addressing cybersecurity within blockchain-enabled SCM is imperative for the enduring success and transformative potential of this technology in reshaping the supply chain paradigm.

VIII. REFERENCES

- [1] Q. Lu and X. Xu, "Adaptable Blockchain-Based Systems: A Case Study for Product Traceability," *IEEE Softw*, vol. 34, no. 6, pp. 21–27, Nov. 2017, doi: 10.1109/MS.2017.4121227.
- [2] T. Aste, P. Tasca, and T. Di Matteo, "Blockchain Technologies: The Foreseeable Impact on Society and Industry," *Computer (Long Beach Calif)*, vol. 50, no. 9, pp. 18–28, 2017, doi: 10.1109/MC.2017.3571064.
- [3] T. McGhin, K. K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *Journal of Network and*

- Computer Applications*, vol. 135. Academic Press, pp. 62–75, Jun. 01, 2019. doi: 10.1016/j.jnca.2019.02.027.
- [4] M. Attaran, “RFID: An enabler of supply chain operations,” *Supply Chain Management*, vol. 12, no. 4, pp. 249–257, 2007, doi: 10.1108/13598540710759763.
- [5] C. Giménez and H. R. Lourenço, “e-SCM: Internet’s impact on supply chain processes,” *The International Journal of Logistics Management*, vol. 19, no. 3, pp. 309–343, Nov. 07, 2008. doi: 10.1108/09574090810919189.
- [6] S. Kamble, A. Gunasekaran, and H. Arha, “Understanding the Blockchain technology adoption in supply chains-Indian context,” *Int J Prod Res*, vol. 57, no. 7, pp. 2009–2033, Apr. 2019, doi: 10.1080/00207543.2018.1518610.
- [7] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, “Blockchain technology and its relationships to sustainable supply chain management,” *Int J Prod Res*, vol. 57, no. 7, pp. 2117–2135, Apr. 2019, doi: 10.1080/00207543.2018.1533261.
- [8] F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” *Telematics and Informatics*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/J.TELE.2018.11.006.
- [9] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, “Security services using blockchains: A state of the art survey,” *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 858–880, Jan. 2019, doi: 10.1109/COMST.2018.2863956.
- [10] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where Is Current Research on Blockchain Technology?—A Systematic Review,” *PLoS One*, vol. 11, no. 10, p. e0163477, Oct. 2016, doi: 10.1371/JOURNAL.PONE.0163477.
- [11] M. Conoscenti, A. Vetro, and J. C. De Martin, “Blockchain for the Internet of Things: A systematic literature review,” *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, vol. 0, Jul. 2016, doi: 10.1109/AICCSA.2016.7945805.
- [12] S. Seebacher and R. Schüritz, “Blockchain technology as an enabler of service systems: A structured literature review,” *Lecture Notes in Business Information Processing*, vol. 279, pp. 12–23, 2017, doi: 10.1007/978-3-319-56925-3_2/COVER.
- [13] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, “Systematic Mapping Studies in Software Engineering,” *12th International Conference on Evaluation and Assessment in Software Engineering, EASE 2008*, Jun. 2008, doi: 10.14236/EWIC/EASE2008.8.
- [14] B. A. Kitchenham, “Systematic review in software engineering,” pp. 1–2, Sep. 2012, doi: 10.1145/2372233.2372235.
- [15] C. Wohlin, “Guidelines for snowballing in systematic literature studies and a replication in software engineering,” *ACM International Conference Proceeding Series*, 2014, doi: 10.1145/2601248.2601268.
- [16] M. Amir-Behghadami and A. Janati, “Population, Intervention, Comparison, Outcomes and Study (PICOS) design as a framework to formulate eligibility criteria in systematic reviews,” *Emergency Medicine Journal*, vol. 37, no. 6, p. 387, Apr. 2020, doi: 10.1136/EMERMED-2020-209567.
- [17] N. R. Haddaway, M. J. Page, C. C. Pritchard, and L. A. McGuinness, “PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis,” *Campbell Systematic Reviews*, vol. 18, no. 2, p. e1230, Jun. 2022, doi: 10.1002/CL2.1230.
- [18] B. Kitchenham and S. Charters, “Guidelines for performing systematic literature reviews in software engineering.” UK, 2007.
- [19] S. J. Hosseini Dehshiri and M. Amiri, “Evaluation of blockchain implementation solutions in the sustainable supply chain: A novel hybrid decision approach based on Z-numbers,” *Expert Syst Appl*, vol. 235, Jan. 2023, doi: 10.1016/J.ESWA.2023.121123.
- [20] A. E. Gencer, S. Basu, I. Eyal, R. van Renesse, and E. G. Sirer, “Decentralization in Bitcoin and Ethereum Networks,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10957 LNCS, pp. 439–457, 2018, doi: 10.1007/978-3-662-58387-6_24/COVER.
- [21] F. Saleh, “Blockchain without Waste: Proof-of-Stake,” *Rev Financ Stud*, vol. 34, no. 3, pp. 1156–1190, Feb. 2021, doi: 10.1093/RFS/HHAA075.
- [22] L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making smart contracts smarter,” *Proceedings of the ACM Conference on Computer and Communications Security*, vol. 24–28–October–2016, pp. 254–269, Oct. 2016, doi: 10.1145/2976749.2978309.
- [23] M. and C. T. Atzei Nicola and Bartoletti, “A Survey of Attacks on Ethereum Smart Contracts (SoK),” in *Principles of Security and Trust*, M. Maffei Matteo and Ryan, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2017, pp. 164–186.
- [24] M. Saad, J. Choi, D. Nyang, J. Kim, and A. Mohaisen, “Toward characterizing blockchain-based cryptocurrencies for highly accurate predictions,” *IEEE Syst J*, vol. 14, no. 1, pp. 321–332, Mar. 2020, doi: 10.1109/JSYST.2019.2927707.
- [25] Q. L. Li, J. Y. Ma, Y. X. Chang, F. Q. Ma, and H. B. Yu, “Markov processes in blockchain systems,” *Comput Soc Netw*, vol. 6, no. 1, pp. 1–28, Dec. 2019, doi: 10.1186/S40649-019-0066-1/FIGURES/4.
- [26] C. Ravikumar, I. Batra, and A. Malik, “A Comparative Analysis on Blockchain Technology Considering Security Breaches,” *Lecture Notes in Networks and Systems*, vol. 376, pp. 555–565, 2022, doi: 10.1007/978-981-16-8826-3_48/COVER.