

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:
enhancing efficiency and cybersecurity in Blockchain-based
Supply Chain Management Systems.

by

Odayne R. Haughton

Director of Studies: Professor (Associate) Carlene Campbell

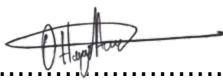
Co-Supervisors: Dr Irina Neaga & Dr Terry Walcott

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

January 2024

Declaration

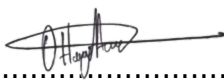
This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed  (candidate)

Date 10/01/2024

STATEMENT 1

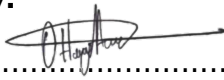
This thesis is the result of my own investigations, except where otherwise stated. Where correction services have been used the extent and nature of the correction is clearly marked in a footnote(s). Other sources are acknowledged by footnotes giving explicit references. A bibliography is appended.

Signed  (candidate)

Date 10/01/2024

STATEMENT 2

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

Signed  (candidate)

Date 10/01/2024

Abstract

With its revolutionary implications for Supply Chain Management (SCM), the rapidly emerging topic of blockchain technology has attracted a lot of attention from academics and practitioners. This thesis delves deeply into the complex cybersecurity issues and technological shortcomings that prevent blockchain from being fully utilised in supply chain management. The creation of a strategic framework to avoid these security threats and create a more efficient blockchain models suited for SCM applications is essential to this project. The main objective of the research is to carefully find, evaluate, and address the technological flaws and security vulnerabilities that are common in SCM systems that rely on blockchain technology. In order to achieve this goal, a thorough examination of relevant case studies and the application of innovative modelling approaches are required.

Adopting a triangulated multifaceted mixed-methods methodology, this research integrates an extensive literature review, relevant case studies, and experimental simulations to obtain a holistic understanding of the security challenges and opportunities to improve the inherent efficiency in blockchain-based SCM systems.

The main findings of the thesis are as follows:

- **Technological Security Gaps Analysis:** The present study conducts an examination of the available literature to analyse the many technological security gaps that exist within the SCM system based on blockchain technology. These gaps span a range of concerns including scalability inefficiencies, security around consensus methods, and other related issues.
- **Case Studies:** Examining real-world blockchain applications in supply chain management, the thesis clarifies the security flaws and practical difficulties associated with various consensus methods. These case studies provide vital insights into real-world situations by acting as a bridge between theoretical concepts and their practical applications.
- **Experimental Simulations:** the BlockSim platform is utilised to conduct experimental simulations that is used to assess and analyse security vulnerabilities and inform more secure and efficient deployment of blockchain on SCM. The highlighted consensus mechanisms are all built differently and are each characterised by their innovative underlining architecture. The simulations employ advanced techniques to enhance real-world scenarios and evaluate the effectiveness of existing and proposed consensus strategies. The simulations conducted offer empirical evidence pertaining to the efficiency of these tactics in augmenting the security of supply chain management systems based on blockchain technology.

Blockchain technology, heralded for revolutionizing SCM through enhanced transparency, traceability, and efficiency, also brings forth unique cybersecurity concerns that need comprehensive understanding and effective mitigation. This thesis presents an in-depth exploration of the cybersecurity challenges inherent in blockchain-based SCM systems, with a specific focus on the inefficiencies and vulnerabilities associated with various consensus mechanisms. The implications of this research are significant as they provide

insights into the efficiency and security strains that are encountered by deploying “unfit” blockchains in supply chain management systems. Additionally, the study offers practical solutions that can be implemented by businesses and regulators to address these inefficiency challenges. Key contributions proposed from the development of this research include the emergence of novel cryptographic algorithms, advancements in smart contract security methodologies, and the proposition of a specialised cybersecurity framework designed exclusively for SCM systems.

Blockchain technology will shape SCM's future, thus solving its efficiency and security issues is crucial. This thesis contributes to the academic conversation and advances existing knowledge by providing a framework for mitigating inefficient deployments and technological security issues. This framework can improve blockchain-based supply chain management security and efficiency. The academic work synthesises literature and case studies to show how specific consensus methods can influence supply chain management transactions. BlockSim is used to model the consensus networks, providing a full view of SCM consensus systems' efficiency and security, essentially proposing a more efficient and secure supply chain management consensus approach.

Conclusively, this research provides a framework for addressing inefficiencies and cybersecurity issues in blockchain-based SCM systems, marking a step forward towards more secure and efficient supply chain operations in the digital era. It underscores the ongoing imperative for researchers and practitioners to develop robust, adaptive, and scalable solutions to counter the evolving challenges of scalability and cybersecurity threats in blockchain technology.

Keywords: Blockchain Technology, Supply Chain Management (SCM), Consensus Mechanisms, Security Vulnerabilities, Technological Inefficiencies, Efficiency Evaluation, Scalability 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 realizing this project. Their 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 for my research, leading to 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 express my gratitude to Professor Stephen Hole, my examination chair, for his constructive feedback, support, and consistent encouragement.

I wish to extend my appreciation to the staff in the School of Applied Computing and WISA at UWTSD for creating an enriching and motivational study environment. Their support has been effective.

I am also thankful to the team at Blockchain Connected for their initial grant, which laid the groundwork for the development of the blockchain facility that was crucial in the early stages of my research.

My heartfelt appreciation goes to my family for their 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 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 that is a source of light in my life. Both your presence and support have been my constant source of motivation, and for this, I am eternally grateful.

Finally, my warmest regards to my friends Camir, 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.

Table of Contents

1	INTRODUCTION	1
1.1	BACKGROUND & CONTEXT: BLOCKCHAIN-BASED SUPPLY CHAIN MANAGEMENT SYSTEMS AND THEIR SIGNIFICANCE IN INDUSTRY 4.0	1
1.2	PROBLEM STATEMENT: OVERVIEW OF CYBERSECURITY CHALLENGES AND THE NEED FOR IMPROVED SOLUTIONS	3
1.3	RESEARCH AIM AND OBJECTIVES	5
1.3.1	AIM	5
1.3.2	OBJECTIVES	5
1.4	MOTIVATIONS FOR THE STUDY	6
1.4.1	CYBERSECURITY AND EFFICIENCY: PREDOMINANT CONCERNS IN DIGITAL SCM	7
1.4.2	PRACTICAL, ECONOMIC AND SOCIAL SIGNIFICANCE	7
1.4.3	INNOVATION AND PROGRESS	7
1.5	SCOPE AND LIMITATIONS	8
1.5.1	SCOPE OF THE RESEARCH	8
1.5.2	LIMITATIONS.....	8
1.6	RESEARCH APPROACH	9
1.7	KEY CONTRIBUTIONS TO KNOWLEDGE.....	11
1.7.1	TECHNOLOGICAL SECURITY GAPS ANALYSIS	11
1.7.2	CASE STUDY INSIGHTS	11
1.7.3	SIMULATION TECHNIQUES.....	11
1.7.4	PROPOSITION OF A NOVEL CONSENSUS MECHANISM	12
1.7.5	DEVELOPMENT OF A BLOCKCHAIN SELECTION METHODOLOGY FOR EFFICIENT SCM SYSTEMS	12
1.7.6	DEVELOPMENT OF A BLOCKCHAIN FRAMEWORK METHODOLOGY FOR EFFICIENT SCM SYSTEMS.....	12
1.8	STRUCTURE OF THE THESIS	13
1.9	LIST OF PUBLICATIONS	15
2	SYSTEMATIC LITERATURE REVIEW: BLOCKCHAIN-BASED SCM SYSTEMS	16
2.1	INTRODUCTION	16
2.1.1	JUSTIFICATION FOR THE SLR	17
2.2	PRIOR RESEARCH	18
2.3	SLR METHODOLOGY	19
2.3.1	SYSTEMATIC LITERATURE REVIEW RESEARCH QUESTIONS.....	20
2.3.2	DATABASE SEARCHES.....	20
2.3.3	PAPER SCREENING PROCESS: INCLUSION AND EXCLUSION CRITERIA.....	21
2.3.4	PAPER CLASSIFICATION	22
2.3.5	DATA EXTRACTION AND MAPPING PROCESS	22
2.4	SEARCH RESULTS	22
2.4.1	QUALITY ASSESSMENT	24
2.4.2	DATA EXTRACTION	25
2.4.3	DATA ANALYSIS	25
2.4.4	FINDINGS	26
2.4.5	TAXONOMY OF CYBERSECURITY ISSUES IN BLOCKCHAIN-BASED SUPPLY CHAIN MANAGEMENT	27
2.5	DISCUSSION	28
2.5.1	CONSENSUS MECHANISM FAILURES (PRIORITY LEVEL: HIGH).....	29
2.5.2	SMART CONTRACT VULNERABILITIES (PRIORITY LEVEL: MEDIUM-HIGH)	29
2.5.3	NETWORK-LEVEL ATTACKS (PRIORITY LEVEL: MEDIUM).....	30
2.5.4	CRYPTOGRAPHIC CHALLENGES (PRIORITY LEVEL: MEDIUM-LOW)	30
2.5.5	SEQUENTIAL ORDER OF INVESTIGATION	31

2.6	CHAPTER SUMMARY	31
3	RESEARCH DESIGN & METHODOLOGY.....	33
3.1	OVERVIEW OF THE RESEARCH DESIGN AND METHODOLOGY EMPLOYED IN THIS STUDY.....	34
3.1.1	RESEARCH STRUCTURE	34
3.1.2	RESEARCH METHODOLOGY	34
3.2	DATA COLLECTION METHODS	36
3.2.1	SYSTEMATIC LITERATURE REVIEW	36
3.2.2	CASE STUDY ANALYSIS	36
3.2.3	EXPERIMENTAL COMPUTER SCIENCE	36
3.3	SELECTION CRITERIA FOR REVIEWED LITERATURE AND CASE STUDIES.....	38
3.3.1	SYSTEMATIC LITERATURE REVIEW	38
3.3.2	CASE STUDIES SELECTION.....	39
3.4	THESIS FRAMEWORK STRUCTURE.....	39
3.5	TOOLS AND RESOURCES	41
3.5.1	BLOCKSIM AS A SIMULATION TOOL FOR TESTING THE PROPOSED METHOD.	41
4	UNDERSTANDING BLOCKCHAIN AND ITS USE CASES IN SUPPLY CHAIN MANAGEMENT.....	42
4.1	FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY	42
4.1.1	BLOCKCHAIN ARCHITECTURE	43
4.1.2	BLOCKCHAIN LAYERS	45
4.2	HOW DO BLOCKCHAINS WORK?	48
4.3	TYPES OF CONSENSUS MECHANISMS IN SCM	51
4.3.1	PROOF-BASED CONSENSUS:	52
4.3.2	CAPABILITY-BASED CONSENSUS ALGORITHMS:	53
4.3.3	VOTING-BASED CONSENSUS ALGORITHMS:	54
4.4	THE INFLUENCE OF CONSENSUS MECHANISMS ON THE SECURITY AND PERFORMANCE OF BLOCKCHAIN-BASED SUPPLY CHAINS	55
4.5	A DEEPER LOOK INTO EACH CONSENSUS MECHANISM	57
4.5.1	PROOF OF WORK (PoW).....	57
4.5.2	DELEGATED PROOF OF STAKE (DPoS)	58
4.5.3	PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT).....	59
4.5.4	PROOF OF CAPACITY (PoC)	59
4.5.5	PROOF OF IMPORTANCE (PoI)	60
4.5.6	STELLAR CONSENSUS PROTOCOL (SCP)	61
4.5.7	RIPPLE CONSENSUS PROTOCOL ALGORITHM (RCPA)	61
4.5.8	WRAP-UP.....	62
4.6	USE CASES OF BLOCKCHAIN IN SCM	63
4.6.1	PROVENANCE TRACKING AND TRACEABILITY	63
4.6.2	SMART CONTRACTS FOR AUTOMATED PROCESSES	63
4.6.3	CIRCULAR ECONOMY AND SUSTAINABILITY	64
4.6.4	SUPPLY CHAIN FINANCE AND RISK MANAGEMENT	65
5	SIMULATION MODELLING TOOL, BLOCKSIM.....	66
5.1	BACKGROUND	66
5.2	MODELLING AND SIMULATION	67
5.2.1	THEORETICAL FOUNDATIONS OF MODELLING	67
5.2.2	CLASSIFICATION OF SYSTEM MODELS	67
5.3	STEPS OF A SIMULATION STUDY.....	69
5.4	BLOCKSIM: AN EXTENSIBLE SIMULATION TOOL FOR BLOCKCHAIN SYSTEMS	71

5.4.1	BLOCKSIM BASE MODEL.....	72
5.4.2	BLOCKSIM'S NETWORK LAYER	73
5.4.3	BLOCKSIM'S CONSENSUS LAYER	75
5.4.4	BLOCKSIM'S APPLICATION LAYER.....	77
5.5	BLOCKSIM IMPLEMENTATION	78
5.5.1	BLOCKSIM SIMULATION LAYERS	79
6	<u>CONSENSUS MECHANISM, DATA COLLECTION</u>	<u>82</u>
6.1	BACKGROUND AND CONTEXT.....	82
6.2	DATA COLLECTION.....	83
6.2.1	THROUGHPUT EFFICIENCY	84
6.2.2	CONSENSUS LATENCY.....	86
6.2.3	SCALABILITY THROUGHPUT.....	87
6.2.4	SCALABILITY LATENCY.....	89
7	<u>POEF, AN ENHANCED BLOCKCHAIN-COORDINATED SCM ARCHITECTURE</u>	<u>91</u>
7.1	AUTHORIZATION NETWORK.....	92
7.1.1	STAGES OF THE SCM AUTHORIZATION NETWORK.....	92
7.2	STAKEHOLDER NETWORK	94
7.2.1	STAGES OF THE SCM STAKEHOLDER NETWORK.....	95
7.3	DESIGN OF THE PROPOSED POEF ALGORITHM	96
7.3.1	CONSENSUS NODE SELECTION	97
7.3.2	TRANSACTIONS BROADCASTING.....	100
7.3.3	CONSENSUS BLOCK CONFIRMATION	103
7.4	THE ARCHITECTURE OF THE POEF CONSENSUS MECHANISM.....	105
7.4.1	NETWORK MODEL.....	105
7.4.2	SECURITY AND AUTHENTICITY MODEL	106
7.4.3	PROPOSED ENCRYPTION MODEL	109
7.4.4	THREAT MODEL.....	110
7.5	POEF, EXPERIMENTATION RESULTS	112
8	<u>EVALUATION AND DISCUSSION.....</u>	<u>117</u>
8.1	AN EVALUATION OF THROUGHPUT EFFICIENCY	117
8.2	AN EVALUATION OF LATENCY.....	120
8.3	AN EVALUATION OF SCALABILITY.	121
8.4	AN EVALUATION OF SCALABILITY DYNAMICS	123
8.5	ADDITIONAL VALIDATION OF THE POEF MODEL WITH SIMILAR MODELS.....	125
8.6	SECURITY VULNERABILITY ANALYSIS.....	126
8.6.1	SAFETY AND AUTHENTICITY	126
8.6.2	DOUBLE SPENDING ATTACK	127
8.6.3	RESILIENCE AGAINST CONSENSUS GROUP ATTACKS.....	127
8.6.4	SYBIL ATTACK.....	127
8.6.5	DENIAL-OF-SERVICE ATTACKS.....	128
8.6.6	UNDER 51% ATTACK.....	128
8.6.7	FAULT TOLERANCE IN POEF.....	128
8.7	SO... WHICH CONSENSUS THEN?	129
8.7.1	PROOF OF WORK (PoW).....	129
8.7.2	DELEGATED PROOF OF STAKE (DPoS).....	129
8.7.3	PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT).....	130
8.7.4	STELLAR AND RIPPLE	130

8.7.5	PROOF OF IMPORTANCE (POI) AND PROOF OF CAPACITY (POC)	131
8.7.6	PROOF OF EFFICIENCY (POEf).....	131
8.8	DEVELOPING A METHODOLOGY FRAMEWORK FOR CONSENSUS MECHANISM SELECTION IN SCM	132
8.8.1	FOUNDATION FOR CONSENSUS MECHANISM SELECTION.....	133
8.8.2	METHODOLOGY RECOMMENDATIONS BASED ON SCM CHARACTERISTICS.....	134
8.9	CHAPTER SUMMARY	135
9	<u>CONCLUSION, RECOMMENDATION AND FUTURE DIRECTIONS.....</u>	<u>136</u>
9.1	INTRODUCTION	136
9.2	CONCLUSIONS: THE TRIPARTITE REVIEW.....	137
9.2.1	LITERATURE REVIEW	137
9.2.2	THE BLOCKCHAIN AND ITS USE-CASES	138
9.2.3	SIMULATION MODELLING TOOL, BLOCKSIM	139
9.2.4	THE DATA COLLECTED	140
9.2.5	EXPERIMENTATION: THE NOVEL POEf CONSENSUS ALGORITHM.....	140
9.2.6	KEY CONTRIBUTIONS OF THESIS	142
9.3	CHALLENGES	143
9.4	FUTURE DIRECTIONS	144
9.4.1	STAGE 2: ASSESSMENT, EVALUATION, AND TESTING OF DIFFERENT TYPES OF SMART CONTRACT DEPLOYMENTS IN SCM	145
9.4.2	STAGE 3: ASSESSMENT, EVALUATION, AND TESTING OF DIFFERENT NETWORK-LEVEL ATTACKS OF BLOCKCHAIN-BASED SCMS. 146	
9.4.3	STAGE 4: ASSESSMENT, EVALUATION, AND TESTING OF DIFFERENT CRYPTOGRAPHIC TECHNIQUES USED BLOCKCHAIN-BASED IN SCMS. 147	
9.4.4	STAGE 5: DEVELOPMENT OF A COMPUTATIONAL FRAMEWORK FOR DESIGNING SECURE BLOCKCHAIN-BASED SCMS	148
10	<u>REFERENCES.....</u>	<u>150</u>

List of Figures

FIGURE	TITLE	PAGE NO.
FIGURE 2.1	Illustrating steps of the Systematic Review.	19
FIGURE 2.2	PRISMA flow diagram illustrating the SLR paper gathering process	23
FIGURE 2.3	Graph illustrating the primary studies extracted to resolve the research questions.	25
FIGURE 2.4	Figure illustrating the main thematic areas in the primary studies.	26
FIGURE 3.1	Figure illustrating the structure of this thesis.	34
FIGURE 4.1	Figure illustrating the blockchain architecture categories.	44
FIGURE 4.2	Figure illustrating the various layers of the blockchain.	46
FIGURE 4.3	Figure illustrating how a transaction is initiated on the blockchain.	50
FIGURE 4.4	Figure illustrating Blockchain Consensus Mechanisms in SCM.	53
FIGURE 5.1	Figure illustrating system model taxonomy	70
FIGURE 5.2	Figure illustrating the procedure for a Simulated Study.	71
FIGURE 5.3	Figure illustrating the layers in the BlockSim Model.	76
FIGURE 5.4	Figure illustrating the process flow for the consensus activities in BlockSim's Base Model.	78
FIGURE 5.5	Figure illustrating BlockSim's Implementation Modules by layers.	81
FIGURE 6.1a	Illustrating Blockchain Mechanisms throughput efficiency collected from the simulator.	86
FIGURE 6.1b	Figure illustrating Blockchain Mechanisms throughput efficiency collected from the simulator.	87
FIGURE 6.2a	Figure illustrating Blockchain Mechanisms consensus latency collected from the simulator.	88
FIGURE 6.2b	Figure illustrating the PoW Mechanisms consensus latency collected from the simulator.	89
FIGURE 6.3a	Illustrating Scalability (from throughput) for various consensus mechanisms collected from the simulator.	90
FIGURE .6.3b	Illustrating Scalability (from throughput) for various consensus mechanisms collected from the simulator.	90
FIGURE 6.4a	Illustrating Consensus scalability (from latency) for various consensus mechanisms collected from the simulator.	91
FIGURE 6.4b	Illustrating Consensus scalability (from latency) for various consensus mechanisms collected from the simulator.	91
FIGURE 7.1	Figure illustrating the flow diagram proposed Authorization Network for this research.	94
FIGURE 7.2	Figure illustrating the proposed Registration Contract that is the Authorization Network algorithm for this research.	96
FIGURE 7.3	Figure illustrating the flow diagram of the proposed Stakeholder Network for this research.	97
FIGURE 7.4	Figure illustrating the Authentication Contract as a part of the Stakeholder's Network algorithm.	97
FIGURE 7.5	Figure illustrating the proposed Consensus Mechanism, PoEf.	101

FIGURE 7.6	Figure illustrating the Transaction Contract that happens inside of the Stakeholder's Network algorithm.	102
FIGURE 7.7	Figure illustrating the proposed Consensus Mechanism Algorithm 1 in plaintext.	103
FIGURE 7.8	Figure illustrating the proposed Consensus Mechanism Algorithm 1 in Python.	104
FIGURE 7.9	Figure illustrating the proposed Consensus Mechanism Algorithm 2 in plaintext.	106
FIGURE 7.10	Figure illustrating the proposed Consensus Mechanism Algorithm 2 in Python.	107
FIGURE 7.11	Figure illustrating PoEf's consensus throughput results from simulation.	115
FIGURE 7.12	Figure illustrating PoEf's consensus latency results from simulation.	116
FIGURE 7.13	Figure illustrating PoEf's Scalability throughput results from simulation.	117
FIGURE 7.14	Figure illustrating PoEf's Scalability latency results from simulation.	118
FIGURE 8.1	Figure illustrating Blockchain Mechanisms consensus throughput comparison including PoEF algorithm.	121
FIGURE 8.2	Figure illustrating Blockchain Mechanisms consensus latency comparison including PoEF algorithm.	123
FIGURE 8.3	Figure illustrating Blockchain Mechanisms Scalability (throughput) comparison including PoEF algorithm.	126
FIGURE 8.4	Figure illustrating Blockchain Mechanisms Scalability (latency) comparison including PoEF algorithm.	127
FIGURE 8.5	Figure illustrating the consensus selection methodology for Blockchain-based SCM.	137

List of Tables

TABLE	TITLE	PAGE NO.
TABLE 1.1	Table illustrating research stages.	10
TABLE 8.1	Table illustrating the properties of each Consensus Algorithm assessed.	135
TABLE 9.1	Table illustrating research stages.	148

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
DAG	Directed Acyclic Graph
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
PoI	Proof of Importance
PoPT	Proof of Previous Transaction
PoR	Proof of Reputation
PoS	Proof of Stake
PoSCS	Proof-of-supply-chain-share
PoW	Proof of Work
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
PoXR	Proof-of-X-Repute
RCPA	Ripple Consensus Protocol Algorithm
RFID	Radiofrequency identification
RPoC	Reputation Proof of Cooperation
RQ	Research Question
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
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	The Bullwhip Effect in supply chain management describes how changes in consumer demand become more pronounced as they proceed 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	describes a collection of procedures used by 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 in blockchain technology refers to a critical component that plays a fundamental role in ensuring the integrity, security, and agreement within a blockchain network.
Consensus mechanism	Refers to the entire stack of protocols, incentives and concepts 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.
Directed Acyclic Graph	A Directed Acyclic Graph (DAG) is a data structure and modelling tool used in cryptocurrencies and distributed ledger technology. Unlike traditional blockchains, which use a linear chain of blocks to record transactions, DAGs employ a more flexible structure.
Distributed Denial of Service	DDoS attack is a cybercrime 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 their transactions without using an intermediary.
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 organizations to manage and streamline their 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, etc.
Estimated delivery performance	A commonly used KPI in SCM. In measuring, the equation determines an organization's capacity to provide goods and services in accordance with the criteria set by its clients, while considering the organization'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 primarily used in blockchain and distributed network systems to achieve Byzantine Fault Tolerance (BFT) in a decentralized 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.
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.
Practical Byzantine Fault Tolerance	This is a system that has primary and secondary nodes that collaborate to obtain a consensus. 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.
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.
Smart contract	Automated agreements are carried out by use of blockchain-stored programmes that execute when predefined conditions are satisfied. Transactions are irreversible after they are completed, although they can still be tracked. Without the need for intermediaries, all parties involved can be informed of the outcome.
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 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 given amount of time. This is a crucial efficiency metric.
Metadata	Data that offers details about other data is known as metadata, and it helps with information management, organisation, and comprehension.
Double-spending attacks	Spending the same cryptocurrency or digital currency more than once, essentially duplicating money.
Network partitioning attacks	Malicious actions intended to break up or split a computer network into disparate, frequently isolated sections.
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.

1 Introduction

1.1 Background & Context: Blockchain-based Supply Chain Management systems and their significance in Industry 4.0

In recent times, there has been a growing fascination among the business community and Information Technology (IT) professionals towards blockchain technology. Blockchain technology has attracted significant attention as a viable technique for improving company operations. A blockchain can be described as a distributed and decentralised database. It operates by storing all confirmed transactions in a sequential chain of blocks, which is then copied across multiple nodes within a network [1]. The technology was initially introduced in 2008 and subsequently adopted in 2009. In recent times, technology has primarily been associated with cryptocurrency; nonetheless, it is now progressively highlighting its potential in transforming business models that underpin the operations and communication of industrial enterprises. Since its beginnings, the development of blockchain technology has undergone three distinct phases: Firstly, there is Blockchain 1.0, which is mostly centred around cryptocurrencies. Secondly, Blockchain 2.0 emerged with an emphasis on smart contracts. Smart contracts are programmable scripts capable of initiating transactions. Lastly, Blockchain 3.0 encompasses a wide range of applications spanning multiple industries such as government, health, insurance, education, the arts, and manufacturing [2], [3].

Blockchain technology has received widespread commendation for its ability to drive the electronic information era. It has been recognised as a catalyst that can enhance the performance of business processes in various industries and organisations that face challenges related to governance, transparency, infrastructure, and coordination inefficiencies [4]. Scholars propose that additional investigation is necessary to more precisely describe, evaluate, and acknowledge the suitability of blockchain technology in various industries [5], [6], [7], [8], [9]. The technology is perceived as a stimulus for innovation and economic expansion, although it remains in its early stages and encounters various challenges such as scalability, security, privacy breaches, energy consumption, legal and regulatory frameworks, and cybercrime [10].

Blockchain technologies are increasingly being adopted in the manufacturing industry, namely in the domain of Supply Chain Management (SCM). In the healthcare sector, through healthcare supply chains,

the use of blockchain technology faces various challenges, including but not limited to the sharing of extensive data among institutions, ensuring data security, managing data handling processes, and addressing the complexities associated with socio-economic data [11]. In agriculture supply chains, the utilisation of blockchain technology effectively addresses several challenges related to the integration of Internet of Things (IoT)-based precision agriculture equipment. However, it is important to acknowledge that this technology is not without its own set of security concerns [12], [13]. The adoption of blockchain is primarily driven by the desire to achieve decentralisation, facilitate information interchange and end-to-end integration, enhance transparency, and enable traceability. The technology in this industry encounters comparable challenges pertaining to security and efficiency.

As per the Council of Supply Chain Management Professionals, SCM encompasses two primary areas. Firstly, it involves the strategic planning, efficient execution, and effective management of operations involved in the creation and delivery of value to end consumers. This includes activities such as procurement, manufacturing, and logistics. Secondly, SCM involves the integration and coordination of pertinent business operations both within and across organisations. The Supply Chain encompasses both physical and informational flows, as well as internal and external distribution networks. The advancement of technology has a significant role in driving and depending on innovation within the supply chain [14]. The Fourth Industrial Revolution, sometimes referred to as 'Industry 4.0', has witnessed significant progress in various sectors such as manufacturing and logistics [15]. The concept of Industry 4.0 involves the presence of intelligent and interconnected physical assets, which refer to smart goods and equipment capable of autonomous operation. These assets have the potential to form self-coordinating systems, such as smart factories or smart supply chains [16].

Blockchain technology is widely regarded as a viable remedy for addressing traceability challenges in SCM [17]. Additionally, it is recognised for its potential to foster stronger and more reliable connections [18], [19], not only between firms and their suppliers but across the entire SCM ecosystem. The utilisation of blockchain-based infrastructures has the capacity to provide SCM with significant degrees of efficiency through a decentralised operational framework. Within the realm of supply chain management, this system and operational framework have the potential to provide a more robust basis of confidence, while also yielding benefits stemming from the absence of a centralised authority and middleman [20]. As a result, blockchain technology has the potential to be utilised to preserve asset ownership [21], permissions, and activity logs. This facilitates the ability to track information and process flows, hence enabling efficient tracking of products and services.

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 [22] and invest in these technologies to facilitate more efficient operations as compared to their traditional states. Radiofrequency identification (RFID), enterprise resource planning (ERP), customer relationship management (CRM), electronic data interchange, collaborative planning forecasting and restocking (CPFR), and e-procurement systems represent a few instances of electronic supply chain management (eSCM) that have been used to enhance the efficiency of traditional supply chains. The usage of technologies like RFID has been thoroughly examined in the academic literature on SCM because of its similarity to blockchain in providing a comprehensive solution for supply chain operations, including the ability to track and trace products [23], [24], [25]. Nevertheless, the impact of several of these technologies like the RFID technology has been underwhelming in many situations, and the implementation of such systems has encountered significant strains and inefficiencies in supply chains. Although ERP systems offer functionalities such as data integration, automation, reporting, analytics and enable organizations to streamline operations, ERP systems are restricted to one organization, as their installation is typically confined to the organisational boundaries of the company. Within the realm of eSCM solutions, blockchain technology has notable resemblances to both RFID and ERP systems.

Therefore, this thesis holds significance as it is imperative to examine how blockchain implementations might leverage the prior experiences of organisations with alternative eSCM technologies. Blockchain technology is a notable addition to the array of technologies available for supporting eSCM. It is important to ascertain whether blockchain can fulfil the anticipated outcomes and surpass the efficacy of its preceding technologies. In their 2018 study, Büyüközkan [26] conducted an examination of digital supply chain technologies, wherein they failed to consider the inclusion of blockchain. This omission highlights the limited attention given to this important topic within academic research, especially in more recent studies.

1.2 Problem Statement: Overview of cybersecurity challenges and the need for improved solutions

The current utilisation of blockchain technology in supply chains is primarily limited to specific applications, indicating an early phase of acceptance with limited opportunities for empirical investigation. Although it may be deemed early to conduct a comprehensive assessment of the effects of blockchain on supply chains, a proactive investigation using techniques such as action research can yield significant insights on

the adoption and integration of blockchain within supply chain management procedures [27]. The potential of blockchain technology in transforming SCM systems is accompanied by a range of complex blockchain adoptions and deployment obstacles [28], [29]. While blockchain offers inherent security measures to prevent tampering and fraudulent activities [30], [31] there are still vulnerabilities that may be exploited by malicious actors [32], [33], [34]. The vulnerabilities discussed in the statement pose substantial risks to SCM systems that depend on the operational integrity provided by blockchain's distributed ledger technology [35]. There is a lack of scholarly investigation into the convergence of blockchain, cybersecurity, and SCM. This is evident from an initial examination of the existing literature, which revealed a limited number of academic studies that specifically address the impact of cybersecurity on operations and blockchain-based supply chain management (BBSCM) systems. This highlights the scarcity of research in this field [36].

From a SCM standpoint, there exists a significant potential to enhance comprehension of cybersecurity concerns associated with blockchain technology and develop more efficient and resilient systems. Scholars in the field of SCM possess the capacity to make substantial contributions by investigating the security implications that arise during the initial stages of blockchain adoption. In doing so, they may play a pivotal role in influencing the actual implementation of this technology [37]. There are several knowledge gaps and deficiencies in the current body of literature and research that require attention. The inherent potential of blockchain technology in strengthening supply chain management comes in its ability to enhance transparency, traceability, and trustworthiness. Nevertheless, the literature on the optimal blockchain architecture for a robust and efficient integration of the technology necessitates tackling substantial efficiency and cybersecurity challenges. An in-depth investigation is required to address the security risks in supply chain management systems that rely on blockchain technology, given the confluence of these opportunities and problems. [38].

Notwithstanding, there is an apparent lack of comprehension of the influence of different consensus algorithms on the security and efficiency of supply chain management (SCM) systems that rely on blockchain technology, despite the significant potential advantages it provides. The complex and dynamic nature of SCM networks necessitates a blockchain system that ensures data accuracy, mitigates cybersecurity risks, and maintains a high transaction processing rate [39]. The choice of a consensus mechanism, such as Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT) or Proof of Importance (PoI), has a substantial impact on the characteristics of a system. [40]. Presently, there is a dearth of empirical investigation centred on assessing and contrasting the efficacy of these solutions within the realm of supply chain management [41].

1.3 Research Aim and Objectives

1.3.1 Aim

The main objective of this research is to analyse and evaluate the efficiency factors and cybersecurity obstacles in blockchain applications that are present in supply chain management (SCM) systems. The objective of this research is to assess the impact of different blockchain implementations on the security strength and operational efficiency of supply chain management frameworks that incorporate blockchain technology. Moreover, it aims to create and propose a framework for the careful selection and implementation of the most appropriate blockchain consensus mechanism for supply chain management. The purpose of this framework is to simplify the implementation of secure and efficient blockchain settings in SCM systems. The thesis will examine if enhancing the latency, blockchain throughput, and capacity to handle bigger workloads of blockchain implementations may improve efficiency and security in supply chain management procedures.

1.3.2 Objectives

Despite not being fully appreciated, manufacturers are progressively developing a more wide-ranging comprehension of the benefits associated with the utilisation of blockchain technology within their operational processes. The implementation and integration of blockchain technology have yielded significant advantages for numerous businesses. However, it remains crucial to develop a wide-ranging understanding of how this technology aligns with diverse business processes in different sectors. Considering this, the thesis will focus on the SCM domain within the manufacturing sector and investigate some cybersecurity measures employed in blockchain-based SCM systems. The objective is to enhance the implementation of blockchain technology, addressing the limitations that have hindered the success of existing technologies. This research aims to thoroughly investigate the complex connection between blockchain consensus mechanisms and SCM cybersecurity. The findings will help improve the efficiency and reduce the risks associated with SCM processes. This research intends to achieve the following objectives in order to improve understanding of the challenges and potential advantages associated with cyber security in the context of blockchain-based SCMs:

- (i) To undertake a comprehensive literature review that investigates the existing studies on blockchain in SCM, with a focus on the integration of cybersecurity protocols.
- (ii) To identify and critically analyse the cybersecurity challenges inherent in blockchain-based SCMs through case studies and assess the Efficiency of Blockchain Deployments in SCM

- (iii) To evaluate the Impact of Consensus Mechanisms on SCM Security and Efficiency
- (iv) Evaluate the Impact of Consensus Mechanisms (namely PoW, DPoS, PoC, PoI, PBFT, Stellar and Ripple) on SCM Security and Efficiency
- (v) To develop a theoretical and empirical framework for selecting the 'best' consensus mechanisms to meet varying SCM cybersecurity and performance criteria.
- (vi) To propose a decision-making model for practitioners and scholars for the selection of consensus mechanisms that align with the specific cybersecurity needs of SCM systems.
- (vii) To design and execute a series of simulation experiments to test the effectiveness of recommended consensus mechanisms in enhancing SCM security and operational performance.
- (viii) To critically assess the results from the experimental findings, integrating them with the theoretical framework to provide guidance for SCM efficiency and cybersecurity enhancement.
- (ix) To synthesize the findings to offer actionable insights for industry practitioners and formulate recommendations for future research directions in the domain of blockchain SCM security.

This thesis produces a cohesive and in-depth analysis of the cybersecurity dimensions of blockchain technology within SCM, offering valuable insights for academic researchers, industry practitioners, and policymakers.

1.4 Motivations for the study

While blockchain has emerged as a disruptive force within traditional business paradigms, offering decentralized, immutable ledger systems, its application in SCM remains a labyrinthine challenge. Supply chains are the backbone of the global economy, and their efficiency and security are paramount. The integration of blockchain technology within SCM has the potential to revolutionize this domain. However, this potential cannot be realized without a clear understanding of the underlying consensus mechanisms that govern blockchain operations. [36] assert the necessity for a holistic exploration of blockchain in SCM, a call this thesis heeds by scrutinizing consensus mechanisms to bolster SCM security and operational effectiveness. The motivation behind conducting this extensive investigation stems from the dynamic convergence of blockchain technology, cybersecurity, and SCM. The research presented in this thesis holds immense importance in the context of the fast-changing digital environment of the present period. This significance is underscored by three (3) compelling factors highlighted below.

1.4.1 Cybersecurity and Efficiency: Predominant Concerns in Digital SCM

The digital landscape of SCM is fraught with sophisticated cyber threats [38]. As SCM systems are laden with critical data, including transactional and proprietary information, the protection of this data is paramount. Blockchain offers a compelling solution with its secure ledger, yet understanding the cybersecurity ramifications of various consensus mechanisms remains a pressing research imperative. As SCM infrastructures increasingly become targets for cyber adversaries, safeguarding the integrity and confidentiality of supply chain data has become a critical concern [42]. The intrinsic value of SCM data, spanning from transactional details to sensitive logistics information, underscores the imperative for robust cybersecurity measures. This thesis seeks to fortify the foundations of secure blockchain SCM practices in an era where cybersecurity is inseparable from supply chain integrity, i.e., the adoption and efficacy of blockchain's consensus mechanisms in enhancing cybersecurity warrant rigorous academic investigation.

1.4.2 Practical, Economic and Social Significance

The thesis's rationale encompasses its practical ramifications. This project aims to improve the security and efficiency of blockchain deployments in SCM by identifying security concerns and evaluating mitigation measures through experimental simulations. By dissecting and addressing security vulnerabilities within blockchain-enabled SCM systems, this thesis aspires to develop concrete mitigation strategies. These strategies are poised to offer tangible benefits to a range of beneficiaries, from industries to end consumers, with the potential to revolutionise SCM security practices [43]. These solutions have the potential to provide substantial advantages to several stakeholders, including industries, businesses, and consumers. The economic and social importance of protecting SCM systems is of great significance due to their significant role in global economies. The protection of SCM systems carries immense socioeconomic weight, given their centrality to global commerce [44]. The findings of the research propose significant potential for risk mitigation, vulnerability reduction, and better assurance of continuous supply chain flows, which are critical in maintaining societal and economic stability.

1.4.3 Innovation and Progress

Innovation stands at the forefront of the evolving triad of blockchain, cybersecurity, and SCM. This thesis ventures beyond contemporary challenges, exploring emergent trends and their potential harmonization within SCM processes. It aims to broaden the horizons of knowledge and contribute to pioneering safer,

more innovative blockchain applications in SCM. Supply chain ecosystems are inherently scalable. [45] emphasize the necessity for consensus mechanisms that can scale without compromising security or efficiency of which the critical aspects this thesis will investigate in-depth.

The motivation for doing this thesis arises from the recognition of the substantial influence that blockchain technology might exert on SCM, together with the pressing necessity to address the cybersecurity concerns related with it. Considering the importance of the situation, it is crucial to thoroughly assess the consensus processes in order to provide guidance for the use of blockchain in supply chain management. The motivation for this research is based on the acknowledgment of blockchain's revolutionary influence on SCM and the necessity to tackle the related cybersecurity challenges. An assessment of consensus mechanisms is crucial for well-informed blockchain adoption in SCM situations. This thesis aims to provide practitioners and scholars with evidence-based recommendations to promote progress in secure, efficient, and resilient supply chain systems in a globally interconnected society.

1.5 Scope and Limitations

1.5.1 Scope of the Research

This research endeavours to provide a comprehensive examination of the intersection of blockchain technology, cybersecurity, and SCM. The scope of this thesis encompasses the following areas:

- **Blockchain in SCM:** This research focuses on the application of blockchain technology in supply chain management, with particular emphasis on its potential to enhance transparency, traceability, and security.
- **Cybersecurity Challenges:** The thesis delves into the cybersecurity challenges that emerge in the context of blockchain-based SCM systems, including data privacy, network security, and access control.
- **Mitigation Strategies:** The research aims to develop and test mitigation strategies to address the identified cybersecurity challenges in blockchain-based SCM.
- **Emerging Trends:** It explores emerging trends in blockchain and cybersecurity and evaluates their relevance and integration prospects within SCM.

1.5.2 Limitations

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

- **Generalizability:** The findings of this thesis are based on a specific set of case studies and simulations, which may not represent the entire spectrum of blockchain-based SCM scenarios. Consequently, the generalizability of the results to all contexts may be limited.
- **Data Availability:** The research relies on available data from case studies and simulations, which might have inherent constraints and biases. The accuracy and completeness of the data could affect the research outcomes.
- **Dynamic Nature:** The fields of blockchain and cybersecurity are highly dynamic, with continuous technological advancements and evolving threats. This research captures a snapshot of the state of these fields as of mid 2023, and developments after this period may not be covered.
- **Resource Constraints:** The extent of the research, including the number of case studies and simulations, may be constrained by available resources, such as time and funding.
- **Legal and Ethical Considerations:** Ethical and legal considerations can affect the extent to which certain data can be accessed and used in research. Adherence to ethical and legal standards is paramount.
- **Human Factor:** The effectiveness of cybersecurity measures can be influenced by human behaviour and decision-making. While this thesis considers technical aspects, it may not comprehensively address human factors.

The research scope encompasses critical aspects of blockchain, cybersecurity, and SCM, with a focus on practical applications. However, it is vital to recognize these limitations to interpret the findings accurately and consider potential constraints in the research process. Despite these limitations, this thesis aims to make meaningful contributions to the fields under investigation.

1.6 Research Approach

The goal of this thesis is to examine and navigate the interplay between cybersecurity and efficiency in blockchain-enabled supply chain management systems. It aims to dissect the impact of various consensus mechanisms on the security and functional performance of these systems and to devise a strategic framework that guides the selection of the most fitting consensus mechanism to bolster security in SCM. The overarching aim is to determine if and how bolstering security within blockchain frameworks can concurrently elevate the efficiency throughout the entire lifecycle of SCM. This research will unfold in a methodically segmented approach, ensuring a thorough and systematic exploration of the subject.

To achieve this overall aim, a structured approach is established, and the project has been divided into six stages, as shown in Table 1.1.

Stage 1	Stage 2	Stage 3	Stage 4	Stage 5
Assessment, evaluation, and testing of different types of Consensus Mechanisms in SCM systems	Assessment, evaluation, and testing of different types of Smart Contract deployments in SCM	Assessment, evaluation, and testing of different Network-Level attacks of Blockchain-based in SCMs	Assessment, evaluation, and testing of different Cryptographic Techniques used Blockchain-based in SCMs	Development of a computational framework for designing blockchain-based SCMs

TABLE 1.1: Table illustrating research stages.

To maintain a concentrated and structured approach in this thesis, the decision was made to primarily focus on Stage 1, encompassing an initial simulation employing the proposed consensus method. This foundational stage paves the way for the subsequent phases of the research project. The progression beyond this stage is anticipated to require the involvement of at least two additional PhD candidates. As outlined in Section 1.3, the ultimate objective of this research is indeed an extensive endeavour, and we are currently at the initial stages of this journey. Nonetheless, the work completed in this thesis represents a significant stride towards achieving the overarching goals of this research, bringing the realization of these objectives perceptibly closer.

The initial stages of this research focused on a review of relevant literature, including books, research papers in the form of conference proceedings and peer-reviewed journals, standards, and white papers, in order to critically review, (i), the existing body of literature about the use of blockchain technology in SCM predominantly focuses on theoretical implications and prospective benefits, sometimes neglecting an in-depth technical examination of the actual technology. The objective of this thesis is to address the existing gap in knowledge by examining the ways in which different consensus methods might meet the unique requirements of SCM systems, while also considering the crucial aspects of security and operational performance. Secondly, (ii) the dynamic and ever-changing landscape of technology developments necessitates a constant state of attention and flexibility to successfully harness their advantages while mitigating any threats. Therefore, the focal point of this research pertains to the necessity of doing a thorough examination that encompasses an extensive assessment of existing literature, the examination of illustrative case studies, and the implementation of empirical simulations to address these problems and opportunities.

1.7 Key Contributions to Knowledge

This thesis contributes significantly to the burgeoning field of blockchain in SCM through several key areas:

1.7.1 Technological Security Gaps Analysis

- **Comprehensive Literature Synthesis:** This research systematically analyses the available literature to identify a range of technological vulnerabilities and inefficiencies in supply chain management systems based on blockchain technology. It rigorously analyses issues related to security and efficiency.
- **Identification and Classification of Gaps:** The research identifies and classifies gaps to categorise them into specific topics. This approach offers a systematic understanding of the various obstacles that blockchain faces in supply chain management.
- **Guidance for Future Research:** By emphasising these specific areas, the thesis steers future research towards tackling these crucial gaps, enabling progress in the utilisation of blockchain technology in supply chain management.

1.7.2 Case Study Insights

- **Real-World Application Analysis:** The thesis provides a review of practical implementations of blockchain technology in SCM, presenting empirical evidence of both successful implementations and encountered difficulties.
- **Bridging Theory and Practice:** These case studies serve as a crucial connection between theoretical frameworks and practical applications, providing significant insights for both academics and professionals in the field.
- **Lessons Learned and Best Practices:** Through the analysis of these practical instances, the thesis highlights optimal strategies and typical mistakes, enhancing our comprehension of blockchain integration in supply chain management with greater subtlety.

1.7.3 Simulation Techniques

- **Innovative Methodology Application:** The thesis employs state-of-the-art simulation tools to apply advanced approaches for modelling and evaluating the security and efficiency of blockchain systems.

- Replication of Real-World Scenarios: These simulations provide the reproduction of intricate supply chain management scenarios, enabling the evaluation of blockchain applications under diverse circumstances.
- Empirical Data Generation: The utilisation of simulations in blockchain implementations generates empirical data, which adds to evidence-based decision-making.

1.7.4 Proposition of a Novel Consensus Mechanism

- Innovative Consensus Mechanism Design: The thesis presents a unique consensus process that is supposed to be more efficient and safer, specifically tailored to meet the requirements of SCM applications.
- Addressing Efficiency and Security: The primary objective of this new technique is to address common problems seen in current consensus models, including sluggish transaction rates and susceptibilities to security breaches.
- Potential for Industry Impact: The suggested technique has the capacity to significantly transform consensus methods in blockchain for supply chain management, establishing a fresh benchmark for both efficiency and safety.

1.7.5 Development of a Blockchain Selection Methodology for efficient SCM systems

- Custom Methodology for SCM: A bespoke methodology for selecting SCM is developed, focusing on efficiency measures that are customised to meet the unique demands of SCM systems.
- Enhanced Efficiency Proprieties: The Methodology introduces rules to guarantee the efficiency and security of SCM systems. It sets a standard for future blockchain advancements.

1.7.6 Development of a Blockchain Framework Methodology for efficient SCM systems

- Cybersecurity Advancements: This research introduces the creation of a ground-breaking framework, facilitating the construction of a thoroughly secure blockchain tailored for SCM. This framework integrates advanced elements such as consensus algorithms, smart contract security techniques, network security protocols, and cryptographic functionalities, thereby significantly enhancing the cybersecurity landscape within blockchain technology.

Overall, these contributions represent a significant advancement in the understanding and application of blockchain technology in SCM. They offer a foundation for future research and development, aiming to

enhance both the security and efficiency of blockchain systems in the complex and dynamic environment of supply chain management.

1.8 Structure of the Thesis

Chapter 1: Introduction

The Chapter begins laying the foundation of the thesis, detailing the significance of blockchain in Supply Chain Management (SCM) within Industry 4.0. It outlines the cybersecurity challenges and the need for improved solutions in blockchain-based SCM systems. The research aims, objectives, and motivations are clearly defined, emphasizing the focus on cybersecurity and efficiency in digital SCM. The chapter also discusses the scope, limitations, and approach of the research, highlighting key contributions like technological security gaps analysis, case study insights, advanced simulation techniques, and the development of a novel consensus mechanism and an efficient SCM system framework.

The remainder of the thesis is organized as follows:

- **Chapter 2: Blockchain-Based SCM Systems: A Systematic Mapping Study of Academic Research**

The second chapter presents a thorough systematic literature review (SLR), justifying its necessity and detailing the research methodology. It covers prior research, paper screening processes, classification, data extraction, and mapping. The findings include a taxonomy of cybersecurity issues in blockchain-based SCM and a discussion on consensus mechanism failures, smart contract vulnerabilities, network-level attacks, and cryptographic challenges.

- **Chapter 3: Research Design & Methodology**

The third chapter explains the research approach. The chapter elaborates on the research design and methodology employed in the thesis, including the structure, data collection methods, and the criteria for literature and case study selection. This chapter also defines the criteria for selecting relevant literature and case studies and presents a nuanced conceptual framework to address cybersecurity issues and identify technological security holes in blockchain-based SCM systems. For credibility, the chapter discusses tools and resources, emphasising BlockSim as a major simulation tool and laying the framework for future chapters.

- **Chapter 4: Understanding Blockchain and its Use Cases in SCM**

Chapter four This chapter delves into the fundamentals of blockchain technology, exploring its architecture, layers, and working mechanism. It examines various types of consensus mechanism in SCM and their impact on security and performance. The goal is to critically test and evaluate SCM deployment options that improve efficiency and security. Additionally, it provides a deeper analysis of each consensus mechanism and discusses blockchain use cases in SCM, including provenance tracking, smart contracts, circular economy, and supply chain finance. Blockchain-based SCM deficiencies enable fresh knowledge contributions and help to determine what areas are left to be explored more.

- **Chapter 5: Simulation Modelling Tool, BlockSim**

The chapter focuses on BlockSim, the simulation modelling tool used in the research. It provides background information, discusses the theoretical foundations of modelling, classifies system models, and outlines the steps of a simulation study. The chapter gives a detailed overview of BlockSim's base model, network layer, consensus layer, application layer, and overall implementation.

- **Chapter 6: Consensus Mechanism, Data Collection**

Having explored the simulation tool, the sixth chapter simulates consensus processes to illuminate their practical applications and ramifications. This chapter evaluates various consensus mechanisms, highlighting their throughput efficiency, latency, and scalability. It provides context for the need for efficient consensus mechanisms in SCM and presents data collected from simulations to assess the performance of these mechanisms. The experimental simulation phase will employ BlockSim to test these methods.

- **Chapter 7: PoEf: An Enhanced Blockchain-Coordinated SCM Architecture**

The chapter introduces the Proof of Efficiency (PoEf) consensus mechanism, designed to enhance throughput efficiency, reduce latency, and improve scalability in SCM systems. This is the main contribution chapter, and it is devoted to interpreting the research findings and reflecting on their technical and practical implications into a novel mechanism. It thoroughly discusses the architecture, design, and experimentation results of PoEf, demonstrating its effectiveness compared to traditional consensus mechanisms.

- **Chapter 8: Discussion and Analysis of Findings**

This chapter engages in a detailed discussion of the findings. It dissects the insights gleaned from the simulations, weaving them into a coherent narrative that aligns with the research objectives. It also involves a synthesized presentation of the gathered data, drawing from the literature review, case studies, and experimental simulations through the comparison the PoEf mechanism with traditional ones like PoW, DPoS, PBFT, Stellar, Ripple, PoI, and PoC across criteria such as efficiency, latency, scalability, and security. The chapter culminates in developing a framework for selecting the most appropriate consensus mechanism for SCM, based on various operational characteristics.

- The **concluding chapter 9** synthesizes the research findings and contributions. It reflects on the systematic literature review, blockchain understanding, simulation modelling, and data collection. The novel PoEf consensus algorithm is highlighted, and the key contributions of the thesis are summarized. Challenges encountered during the research are discussed, and future directions are suggested, including further stages of assessment, evaluation, and development for secure blockchain-based SCM systems.

1.9 List of publications

- 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. (PENDING)
- 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.

2 Systematic Literature Review: Blockchain-based SCM systems

2.1 Introduction

Blockchain's unique attributes have catalysed its exploration across diverse corporate sectors, including but not limited to banking [17], governmental systems [18], healthcare provisions [9], and, most importantly in the context of this research, SCM [22], [23]. SCM is the comprehensive coordination of the flow of commodities from their creation to their consumption, including a complex network of interconnected organisations involved in the manufacturing and distribution of items. The progression from early trade systems to advanced, technology-driven SCM has provided organisations with the ability to proactively detect and address errors, meet consumer requests, and attain economic goals concurrently. In this customer-centric era, that prioritises customer needs, the flexibility in acquiring products amplifies the strategic focus inside supply chain management and how they are deployed. Blockchain technology's promise of creating secure and efficient digital systems is rooted in its infrastructure, which is typically stratified into the incentive layer, consensus layer, and network layer. Each layer plays a pivotal role in defining the blockchain's overall performance and security profile. The emerging scholarly discourse surrounding the incorporation of blockchain technology into SCM, as introduced by [46] and further elaborated upon by Saberi et al., [43] and Casino et al., [7] highlights the inherent capabilities and complexities associated with this innovation.

It is therefore crucial to thoroughly examine the body of research about the cybersecurity challenges of blockchain in supply chain management to effectively address the dangers associated with the emerging technology for SCM. An examination of both foundational and current research works is necessary to evaluate the state of cybersecurity and efficiency in blockchain applications within the context of supply chain management.

Even though there have been some positive steps forward, there is still a big gap in the research that investigates how blockchain is used in real-life SCM ecosystems and the security issues that come up as a result. This shortfall occurs amidst a backdrop of expeditious technological evolution and the critical role of SCM in the modern commercial environment. This research endeavours to focus on existing studies addressing the cybersecurity concerns engendered by blockchain infrastructural choices within SCM, such

as susceptibility to 51% attacks, the prevalence of Sybil attacks, and vulnerability to Denial-of-Service (DoS) incursions. The primary aim is to forge a community-driven blueprint for secure and efficient blockchain implementations in SCM, dissecting the interplay between infrastructural choices and sectoral requirements. To do this, we need to take a close look at the research that has already been done on cybersecurity strategies for blockchain-based supply chain management systems and figure out how to use what we learn to plan and leverage these insights to navigate future trajectories.

2.1.1 Justification for the SLR

A systematic approach to the literature review is crucial in integrating the gains achieved thus far and giving a full overview of the current knowledge, methods employed, and trajectory of the continuing academic discourse. Utilizing a SLR in this research on blockchain in SCM is essential for several key reasons. Firstly, an SLR offers a detailed and structured assessment of existing knowledge, crucial for establishing a robust theoretical and conceptual framework for the thesis [47]. This approach ensures a thorough understanding of the current state of blockchain applications in SCM, identifying both the advancements and shortcomings in the field. Additionally, SLRs are instrumental in uncovering gaps in the existing literature, which is vital for directing the research towards areas that can contribute novel insights and avoid redundancy [48]. By methodically analysing previous studies, the SLR in this research will lay a solid foundation, ensuring that the investigation is grounded in a substantial body of existing knowledge and theories relevant to blockchain and SCM.

The application of the SLR in this thesis will guide the research methodology and inform the development of simulation models and theoretical frameworks moving forward. Insights derived from the SLR will directly influence the design and implementation of experimental simulations and case studies, ensuring that these components of the research are both relevant and effective [49]. For instance, understanding the technological limitations and cybersecurity challenges highlighted in the SLR will allow for the tailoring of simulation scenarios that specifically address these issues. Moreover, the SLR will play a crucial role in the development of a specialized cybersecurity framework and a novel consensus mechanism for SCM systems. It will provide a comprehensive background on current challenges and inefficiencies, thereby informing the design of these innovative solutions [50].

Finally, the SLR will serve as a benchmark for evaluating the effectiveness and advancement of the proposed solutions in this research. By comparing the research findings with existing literature, the thesis will demonstrate its contribution to the field of blockchain in SCM [51]. Additionally, the SLR will inform

policy recommendations and best practices, ensuring that they are based on a thorough and up-to-date understanding of the field. Furthermore, it will suggest future research directions, ensuring the continual advancement of blockchain technology in SCM. In essence, the SLR is a fundamental component of this research, providing the necessary background, guidance, and validation for the thesis's objectives and outcomes. The SLR lays the way for empirical investigations defined by innovative cryptographic algorithms, resilient consensus mechanisms, and network protocols designed for SCM systems, pointing the way towards more secure and efficient blockchain-based SCM systems.

2.2 Prior research

In the domain of SCM systems, there is a shortage of thorough SLRs relevant to the cybersecurity problems connected with blockchains in Supply Chain. Salman et al., [52] produced a new survey paper on the topic of blockchain and cyber security. This thesis aims to elucidate the challenges and concerns related to the implementation of security and efficiency within a centralised architecture spanning numerous application domains. In addition, the thesis provides an assessment of contemporary blockchain-based approaches for delivering efficiency and security in several domains, including authentication, access control, data and resource provenance, and integrity assurance inside distributed networks. Although the thesis did not focus on specific supply chain applications, it still serves as a crucial foundation for scholars interested in studying the efficiency and security issues of supply networks using blockchain technology. Furthermore, a restricted quantity of scholarly studies pertaining to blockchain technology, as well as its broader implications, have also been documented. In the following analysis, these papers were assessed to identify the disparities in the subject areas selected for this thesis.

Yli-Huumo and colleagues conducted a systematic literature review (SLR) in 2016 to gather and analyze published research findings on blockchain technology [53]. Their review specifically excluded legal, economic, and regulatory studies, focusing instead on technical aspects of blockchain technology, with an 80% emphasis on Bitcoin and related security and privacy concerns. However, their review did not address blockchain applications in SCM. Since then, blockchain technology has seen wider application diversification, prompting this research to delve into cybersecurity challenges and blockchain applications in SCM.

Later in 2016, Conoscenti et al. [54] carried out an SLR examining blockchain's adaptability and usage, particularly in relation to the Internet of Things (IoT) and peer-to-peer devices. In 2017, Seebacher et al.,

[55] conducted another SLR, highlighting blockchain's growing influence on service systems. Despite these studies, there remained a gap in research specifically focused on tailoring and integrating blockchain technology optimally for diverse supply chain scenarios.

Most previous studies have explored broader aspects of blockchain technology, yet still lacked a detailed focus on its specific applications for enhancing security or efficiency in SCM. Given the rapid evolution and expansion of blockchain research, there's a scholarly need to consolidate and analyze recent studies that intersect blockchain technology, SCM, and cybersecurity. This necessitates a fresh review of more current research in the domain of blockchain and cybersecurity, to guide and inform future research endeavours. Such a review is critical to understanding how specific blockchain deployments can impact the security and efficiency of SCM solutions and to identify potential areas for improvement and innovation in this burgeoning field.

2.3 SLR Methodology

The research methodology chosen for this study is the systematic mapping approach as proposed by Patersen et al., specifically tailored to investigate the current landscape of blockchain technology efficiency and security research. This approach facilitates the identification and categorization of pertinent research themes related to smart contracts, while simultaneously highlighting gaps for potential future research [56]. As illustrated in Figure 2.1, this systematic mapping study 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. The execution of the SLR adheres to the guidelines set forth by Kitchenham, ensuring a structured and comprehensive approach to address the research questions [57]. Choosing an iterative approach throughout the planning, conducting, and reporting phases of the study enables a thorough and rigorous assessment of the findings from the systematic literature review.

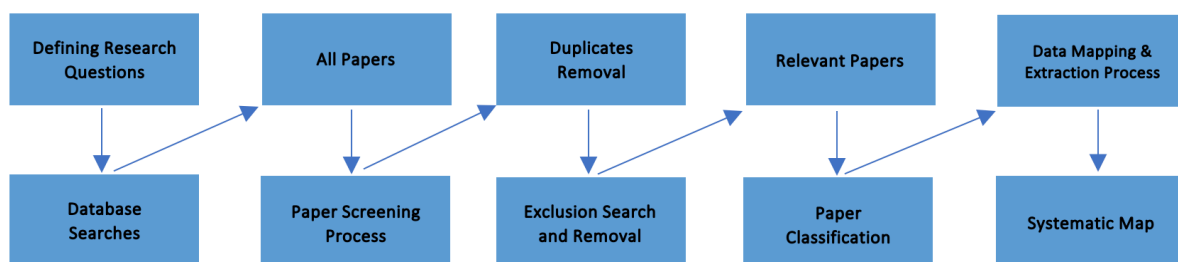


FIGURE 2.1: Illustrating steps of the Systematic Review, adopted from [56].

2.3.1 Systematic Literature Review Research Questions

To initiate a systematic mapping project, the initial phase involves establishing the research inquiries that will be addressed by the thesis. Thus, this thesis poses the following three questions:

- **RQ1:** What are the key theoretical foundations and empirical contributions identified in the existing literature that link blockchain technology, cybersecurity, and SCM, and how have these shaped current methodological approaches in the field?
- **RQ2:** How do current methodological advances in blockchain technology address cybersecurity challenges in SCM, and what gaps or opportunities exist for further research and development?
- **RQ3:** What are the emerging trends in blockchain integration within SCM, and how do these trends potentially impact the security and efficiency of SCM processes, considering the specific needs and expectations of the SCM sector.

2.3.2 Database searches

The second step is to search and gather all research papers related to security in blockchain-based supply chains. Passing keywords to a particular publication's or search engine's search facility highlighted primary studies. The keywords were selected to promote the emergence of research results that would assist in answering the research questions. The boolean operators were restricted to AND and OR. The search strings were:

- ("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 carry out the 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, symposiums, workshops, 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 searches were carried out between May and October 2023, and all studies that had been published until this date were analysed. The outcomes of these searches underwent filtration based on the inclusion/exclusion criteria, which will be outlined below. The utilisation of certain criteria facilitated the generation of a collection of outcomes that could then be subjected to the snowballing process, as

described by Wohlin [58]. Successive cycles of forward and backward snowballing were performed until no additional publications that met the inclusion criteria were identified.

2.3.3 Paper Screening process: Inclusion and exclusion criteria

The third step is to exclude all research papers that are 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 [59]. 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 types of blockchain deployments. The "Outcome" relates to the potential efficiency and cybersecurity concerns that may arise from 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:

- Mentioned Blockchain: Explored the implications of blockchain technology in the context of supply chain management.
- Security Context: The paper examines the cybersecurity concerns that arise from the adoption and utilisation of blockchain technology.
- Blockchain performance: The paper assessed the performance of blockchain in the environment in which it is applied, which will allow for comparisons of different blockchain applications. The publication in question has undergone a rigorous peer-review process 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 the present.

Irrelevant research publications were eliminated by assessing their titles in this method. If the pertinence of a paper could not be ascertained only from its title, an additional subsequent measure was employed to assess the abstract of the study. Aside from excluding articles based on their title and abstract, additional exclusion criteria were employed 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 that were not based on technology were disqualified.

2.3.4 Paper Classification

In the fourth stage of the systematic mapping procedure, the identified research papers were categorised. The classification was conducted using the keyword strategy described in Yli-Huomo et al. [53]. A comprehensive 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 did not contain enough information for accurate classification, a brief examination of the document was conducted to determine the most suitable category for it. The systematic technique employed guaranteed the precise categorization of each paper, so enabling a better organised and cohesive study of the research environment.

2.3.5 Data Extraction and Mapping Process

The final phase of the systematic review process involved gathering all pertinent data to address the research questions of this study comprehensively. This step entailed meticulously collecting a range of data elements from each research paper, focusing on capturing the core objectives and key contributions of the studies. This comprehensive data collection was instrumental in ensuring a thorough and insightful analysis, directly aligned with the overarching research aims of this review.

2.4 Search results

Considering the keywords, the following results have been obtained, divided by platform, a comprehensive search on the selected platforms yielded a total of 10,894 studies. The total number of studies was decreased to 6,465 following the elimination of duplicate entries. Upon conducting a thorough examination of the research based on the predetermined inclusion and exclusion criteria, it was determined that a total of 703 papers met the requirements and were deemed suitable for further review. After a thorough examination of the 703 papers, adhering to the inclusion/exclusion criteria, a total of 72 papers were found to meet the specified requirements. Employing both forward and backward snowballing methodologies led to the discovery of an extra 20 and 16 publications, respectively. As a result, the cumulative count of

research papers included in this Systematic Literature Review (SLR) reached 108. The process and progression of paper selection, including the attrition rate from initial keyword searches to the final inclusion of primary studies, are illustrated in Figure 2.2. This figure utilizes the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) Flow Diagram by Haddaway et.al as a reference model to depict the stages of paper selection and filtration throughout the review process [60].

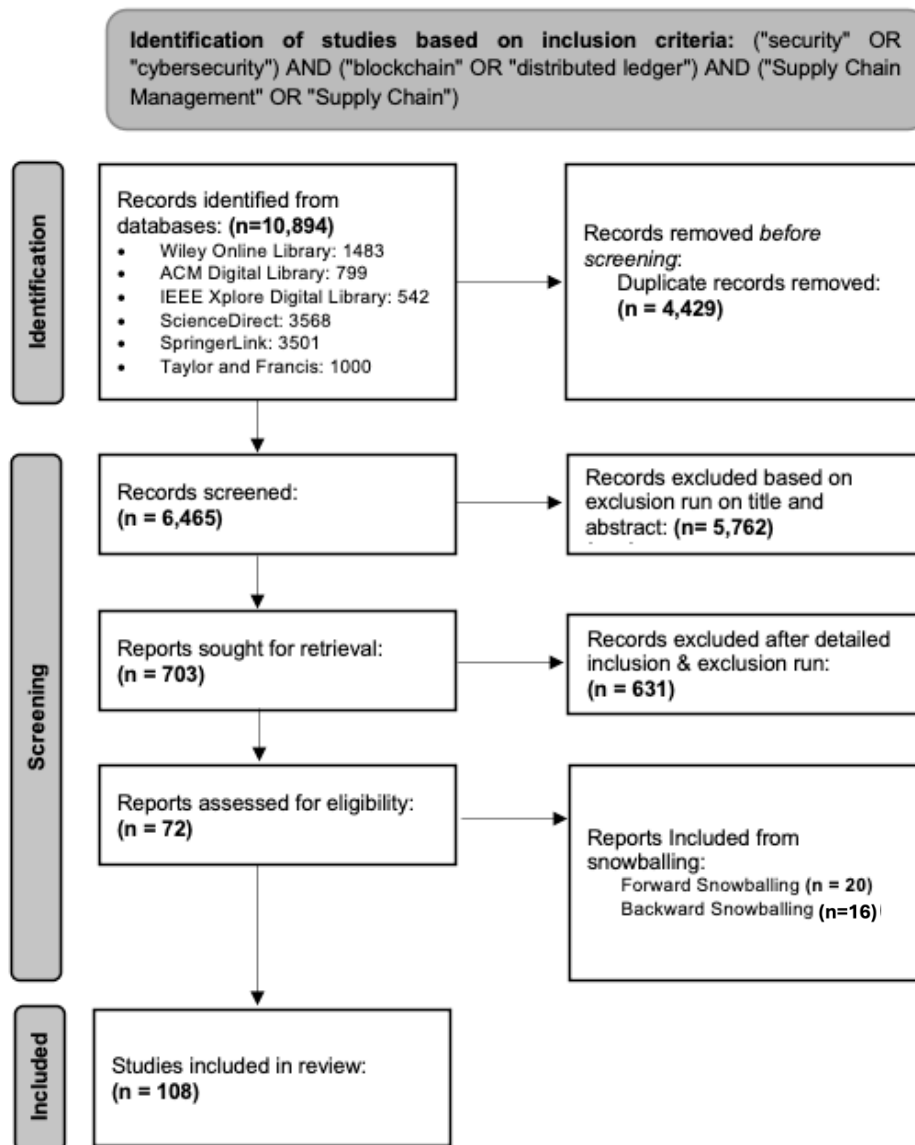


FIGURE 2.2: PRISMA flow diagram illustrating the SLR paper gathering process.

The omission of many papers from the systematic review can be ascribed to three main issues. Firstly, a substantial proportion of these articles did not correspond to the specific technical emphasis of this thesis on blockchain-based SCM systems. A significant number of individuals approached the subject matter from economic or legal standpoints, deviating from the intended technical investigation in this research. Furthermore, other papers focused on cryptocurrencies or the broader concept of blockchain technology, rather than its specific use in supply chain management. As a result, these papers were not pertinent to

the study topics of the thesis. Finally, a number of publications were dismissed because they mostly focused on grey literature concerning cryptocurrencies, and blockchain's usefulness in enhancing transparency, or made speculative claims about the technology's possible uses in different areas such as finance, without providing significant technical advancements that focused on the technology to the field. As a result, these considerations resulted in the inclusion of 188 papers in the systematic mapping study.

2.4.1 Quality assessment

The primary studies included in this research were meticulously assessed for quality according to the parameters given by Kitchenham [57]. The quality assessment played a crucial role in determining the relevance of the studies to the research objectives, as well as in evaluating for possible study bias and the legitimacy of experimental data. The evaluation approach was derived from the work of Hosseini et al. [61]. Ten papers were randomly chosen and then evaluated to assess their effectiveness. The procedure consisted of six discrete stages:

- Stage 1: 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.
- Stage 2: Context. The research must furnish sufficient context regarding its objectives and findings, facilitating accurate interpretation and relevance to the research questions.
- Stage 3: Blockchain application. Papers needed to offer comprehensive details on the implementation of blockchain technology in SCM systems, aiding in the resolution of research queries.
- Stage 4: Security context. The studies were expected to elucidate the security challenges they addressed, aligning with the research questions of this thesis.
- Stage 5: Blockchain performance. The papers should evaluate the performance of blockchain technology in their respective application environments, allowing for comparative analysis across different blockchain deployments.
- Stage 6: Data acquisition. The studies were assessed for their methodology in data collection, measurement, and reporting to gauge the accuracy and reliability of the data presented.

The checklist served as the foundation for evaluating the quality of the SLR and its relevance. It was then used to examine the primary studies that were discovered, ensuring a high standard of research quality.

2.4.2 Data extraction

The data extraction process was a crucial stage in this research, guaranteeing that every study that passed the quality review supplied relevant and detailed information for this research. At first, this procedure was implemented on a specific set of ten research to improve and authenticate the methods for extracting data. Later on, it was broadened to include other research that matched the criteria for assessing quality. Throughout this stage, pertinent data from each document were carefully collected, methodically classified, and securely stored in a spreadsheet format. The data were categorised systematically, facilitating a methodical and thorough investigation of the material. The systematic technique below guarantees the reliability and usefulness of the data for future analysis and debate:

- 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.

2.4.3 Data analysis

In order to address the research questions, we combined the qualitative and quantitative data and then conducted a meta-analysis on the studies that underwent the final data extraction process.

2.4.3.1 Publications over time

The blockchain technology, which was first linked to Bitcoin in 2008, only started to witness significant primary research papers around 2016. The existence of this gap highlights the developing status of blockchain technology in relation to cybersecurity and its potential to improve efficiency in supply chain management. Figure 2.3 illustrates a noticeable and consistent rise in yearly research publications that centre on SCMs based on blockchain technology. These publications specifically highlight the importance of cybersecurity and operational efficiency. This trend indicates a growing interest and investment in the exploration and improvement of blockchain applications in SCM. In the future, it is anticipated that this field will keep growing, resulting in a vast and valuable collection of studies focused on improving and optimising the real-world implementation of blockchain technology in supply chains.

Each paper's focus was further grouped into broader categories to allow for a simplified classification of the themes of the primary studies. The main technology areas identified are classified into 4 main thematic areas namely (i) Consensus Mechanism Failures, (ii) Smart Contract Vulnerabilities, (iii) Network-Level Attacks and (iv) Cryptographic Challenges.

2.4.5 Taxonomy of Cybersecurity Issues in Blockchain-Based Supply Chain Management

By applying the Keywording technique, papers were classified into four categories, namely, (i) Consensus Mechanism Failures, (ii) Smart Contract Vulnerabilities, (iii) Network-Level Attacks and (iv) Cryptographic Challenges. The advent of blockchain technology in SCM has been pivotal in revolutionizing traceability, transparency, and security within the domain. However, despite its robust security features, blockchain technology is susceptible to a range of cybersecurity threats. Understanding these challenges is critical for maintaining secure and efficient blockchain-based SCM systems.

2.4.5.1 Consensus Mechanism Failures

Consensus mechanisms, such as PoW and PoS, are the bedrock of blockchain technology, ensuring that all participants in the network agree on a single version of the truth, i.e. they are the backbone of transaction validation on blockchain networks. However, they are not immune to failures, which can have dire consequences for SCM systems relying on blockchain. Failures or attacks within these mechanisms can severely compromise the integrity of the entire SCM system. Authors like Eyal and Sirer [62] and Saleh [63] have explored vulnerabilities in these mechanisms, including 51% attacks in PoW systems and the 'Nothing at Stake' problem in PoS systems. These failures can lead to fraudulent transactions or double spending, posing significant risks to SCM integrity and reliability. Understanding the vulnerabilities in consensus mechanisms and their implications for SCM is crucial in ensuring the reliability and security of blockchain-based SCM systems. As this research progresses, it aims to not only highlight these issues but also to contribute to the development of more resilient consensus mechanisms that are specifically tailored to meet the unique demands of SCM systems. The goal is to foster a blockchain environment in SCM that is both secure and efficient, overcoming the limitations posed by current consensus mechanisms.

2.4.5.2 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 their code can be exploited, leading to substantial losses or disruptions in SCM operations. Authors like Luu et al., [64] and Atzei et. al., [65] have documented various types of vulnerabilities in smart contracts, ranging from re-entrancy attacks to issues with contract dependencies. These vulnerabilities necessitate rigorous security protocols in the design and testing phases of smart contract development to mitigate potential risks in SCM systems.

2.4.5.3 Network-Level Attacks

Blockchain networks, despite their decentralized nature, are vulnerable to various network-level attacks that can impede their availability and integrity. Apostolaki et. al., [66], along with Saad, Spaulding et al. [67], have highlighted the susceptibility of blockchain networks to attacks such as routing attacks, Sybil attacks, and DDoS (Distributed Denial of Service) attacks. These can disrupt SCM operations by delaying or blocking transaction confirmations and thus require robust network security measures to prevent and mitigate such attacks.

2.4.5.4 Cryptographic Challenges

The security and integrity of blockchain heavily rely on cryptographic algorithms. Li et al., [68] along with several other authors like Yu et al., [69] and Latifa et al., [70], emphasize that flaws in cryptographic algorithms or their implementations can lead to systemic failures in blockchain networks. This is especially critical in SCM systems where data integrity is of utmost importance. Ensuring the use of strong, well-tested cryptographic algorithms and keeping them updated to counter emerging threats is essential for maintaining the security of blockchain-based SCM systems.

2.5 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 a wide range of experimental concepts and conceptual solutions that tackle current difficulties. Nevertheless, a significant number of these research suffer from a dearth of sufficient quantitative data and practical application proof. Within the realm of practical technical solutions, a wide range of novel methodologies arise in various research studies. These solutions tackle crucial concerns including as consensus procedures, data security, weaknesses in smart contracts, cryptographic hurdles, and network-level attacks. The combination of theoretical and practical study

highlights the dynamic character of blockchain technology and its increasing significance in addressing intricate technological challenges.

As blockchain technology increasingly permeates SCM, understanding its cybersecurity landscape is paramount. The identified taxonomy of cybersecurity issues: consensus mechanism failures, smart contract vulnerabilities, network-level attacks, and cryptographic challenges, highlights critical areas requiring attention to fortify blockchain SCM systems. This chapter sets the scene to discuss the importance of scrutinizing these areas to enhance both security and efficiency in SCM's entire lifecycle. To achieve the goal of enhancing both the security and efficiency of blockchain-based SCM systems, it is crucial to sequentially prioritize the investigation of the identified cybersecurity areas. Each area will be explored and compared, leading to a recommended order of investigation based on their impact and interdependencies.

2.5.1 Consensus Mechanism Failures (Priority Level: High)

The role of consensus mechanisms in maintaining the integrity and trustworthiness of blockchain transactions is crucial. Failures or attacks, such as those outlined by authors like Eyal and Sirer [62], can undermine the entire SCM system. The transition to more energy-efficient and secure mechanisms like PoS [63] not only enhances security but also improves the efficiency of transaction processing, which is vital for SCM operations that require speed and reliability. A secure and efficient consensus mechanism ensures that SCM processes remain uninterrupted and trustworthy, which is essential for real-time decision-making and maintaining operational continuity.

The consensus mechanism is the backbone of blockchain functionality, directly impacting both security and efficiency. It is the first line of defence against various attacks and is critical in transaction validation and network integrity. As such, securing the consensus layer can have a cascading effect on the overall robustness of the SCM system. This area should be addressed first because it lays the foundation for the blockchain's operational integrity. Unlike smart contracts or cryptographic methods, which are more about safeguarding specific transactions or data, the consensus mechanism affects the entire network's operation. Its efficiency and security directly impact network-level security and the effectiveness of cryptographic measures.

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

Smart contracts, as Luu et al., [64] and Atzei et al., [65] have noted, are pivotal for automating SCM processes. However, their vulnerabilities pose significant security risks. Addressing these concerns is not

just about preventing data breaches or financial losses; it's about ensuring that the automated processes upon which modern SCM relies are reliable and trustworthy. Enhancing smart contract security directly translates to more robust and efficient SCM operations, as it ensures that automated processes are executed as intended, reducing errors and delays.

Once the consensus layer is secured, focusing on smart contract vulnerabilities is crucial. Smart contracts automate key SCM processes; thus, their security is paramount. Vulnerabilities here can lead to significant disruptions in SCM operations. While consensus mechanisms ensure the validity of the entire blockchain, smart contracts are about the correctness and security of individual operations. Their vulnerabilities can have direct financial and operational impacts, making this area a high priority, though secondary to the consensus layer.

2.5.3 Network-Level Attacks (Priority Level: Medium)

The susceptibility of blockchain networks to various attacks, as discussed by Apostolaki et al., [66] and Saad et al. [67], impacts their availability and integrity. In SCM, where the timely and accurate transmission of data is crucial, such attacks can cause significant disruptions. Strengthening network security protocols and adopting advanced measures like decentralized node distribution can mitigate these risks, thereby ensuring that SCM systems are both secure and efficient, with minimal downtime and reduced risk of data tampering.

Securing the network layer is crucial for ensuring the availability and integrity of the blockchain network. This becomes more critical after ensuring the security of the consensus mechanisms and smart contracts, as attackers may turn to network vulnerabilities once other security measures are in place. Network security supports the robust operation of consensus mechanisms and smart contracts. Although not the first line of defence, it provides a necessary shield against external threats, making it a crucial area to address sequentially after the above two.

2.5.4 Cryptographic Challenges (Priority Level: Medium-Low)

The integrity of a blockchain is heavily reliant on its cryptographic underpinnings. Flaws in cryptographic algorithms or their implementations, as explored by Li et al., [68], Yu et al., [69] and Latifa et al., [70], can lead to systemic failures. The evolution of cryptographic techniques is, therefore, integral to the advancement of blockchain SCM. Enhancing cryptographic security directly correlates with the ability to protect sensitive SCM data, ensuring both the confidentiality and integrity of supply chain transactions.

Cryptography is inherent in every blockchain operation. However, cryptographic challenges typically involve more advanced and evolving threats, such as quantum computing. Addressing cryptographic challenges is essential for long-term sustainability but can be prioritized after more immediate and directly impactful areas are secured. While critical for data integrity and security, cryptographic challenges often require a long-term strategic approach. Their impact, while potentially severe, often manifests differently than direct attacks on consensus mechanisms or smart contracts.

2.5.5 Sequential Order of Investigation

- 1st: Consensus Mechanism Failures: Establish a secure and efficient foundation for the blockchain.
- 2nd: Smart Contract Vulnerabilities: Ensure the automation crucial 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 not just about fortifying the blockchain against attacks; it is about integrating security measures in a manner that also enhances operational efficiency. Efficient consensus mechanisms, secure and reliable smart contracts, robust network defences, and advanced cryptographic techniques can reduce transaction times, minimize errors, and streamline SCM processes. This integration of security and efficiency is vital for SCM systems that must operate at scale and handle complex, multi-faceted operations.

2.6 Chapter Summary

This chapter carried out a longitudinal systematic mapping of peer-reviewed, technology-oriented research to identify and analyse the current state of knowledge regarding blockchain technology and its cybersecurity challenges in supply chain management. In the evolving landscape of supply chain technology, blockchain's integration into mainstream applications presents a complex interplay of technical foundations and practical implications. Key concepts underpinning blockchain technology, such as

consensus algorithms, smart contracts, the network architecture and hashing techniques transcend mere technological jargon. These concepts are fundamental in determining blockchain's suitability, optimal application areas, and strategies for efficient and cost-effective implementation and adoption. Despite inherent security mechanisms within blockchain architectures, such as built-in encryption and decentralized control, these systems are not entirely impervious to cybersecurity threats as there is a growing number of successful attacks on blockchain networks and applications such as DDoS attacks, smart contract vulnerabilities, malicious nodes, risks associated with private key protection, and the potential for 51% attacks are becoming quite common [71]. This review focused on analysing peer-reviewed scientific publications to gain insights into the scholarly investigation and proven discoveries of blockchain technologies in supply chain management. A systematic mapping methodology was utilised to collect research papers from prominent scientific databases. This approach enabled the categorization of these documents into four clearly defined groups: Consensus Mechanism Failures, Smart Contract Vulnerabilities, Network-Level Attacks, and Cryptographic Challenges. This concentrated approach guaranteed a comprehensive comprehension of the extent to which academic research has contributed to the domain of blockchain-based supply chain innovations.

Examining peer-reviewed articles, highlighted the main cybersecurity problems in applying blockchain technology to SCM. Blockchain in SCM and related businesses has several challenges, issues, and vulnerabilities. Blockchain has created a paradigm change in SCM, improving security and operational efficiency, but it has also created four cybersecurity issues that must be addressed. Researchers and practitioners must constantly improve their understanding and methods to protect against these emerging vulnerabilities. This thesis investigates consensus mechanism failures and proposes ways to make blockchain-based SCMs more secure and efficient. The complex relationship between security and efficiency in blockchain-based SCM systems is crucial. Future research can improve SCM system security, efficiency, dependability, and effectiveness by addressing cybersecurity issues. This integrated approach to understanding and resolving blockchain SCM cybersecurity is essential for its sustained acceptance and supply chain transformation.

3 Research Design & Methodology

The construct of the research methodology within this thesis is inherently informed by the empirical insights gleaned from the preceding literature review. This synthesis of knowledge provides a foundational basis for shaping the research design in profound and multifaceted ways. For the Research Structure (Section 3.1.1), a rigorous comprehension of the technical constructs governing blockchain technology, and its application within the domain of SCM, alongside the pertinent cybersecurity challenges associated with different blockchain deployments delineated in Section 2.5, is paramount for setting the type of analysis that will be conducted. The complexity inherent in the technological subject matter necessitates a research design of commensurate robustness to adeptly navigate and address the articulated research issues. Subsequently, the Research Methodology (Section 3.1.2) is crafted with a keen awareness of the prevailing cybersecurity limitations inherent within extant blockchain-based SCM systems, as reviewed in Section 4.5. The research will zone into one of these vulnerability areas (Section 2.5) to formulate a methodology that will address the cybersecurity limitations to recommend the deployment of a more secure and efficient blockchain, alongside an assiduous investigation of nascent trends and advancements within the cybersecurity and efficiency spheres relevant to blockchain infrastructures.

Insights derived from the literature review, pertaining to the deployment confines of blockchain applications in SCM and their cybersecurity implications, strategically inform the methodology for Data Collection (Section 3.2). The thematic paradigms and issues extrapolated from the literature review will steer the Selection of Relevant Literature and Case Studies (Section 3.3), privileging discourses that elucidate the intersection of (i) blockchains deployed within SCM systems, (ii) the cybersecurity challenges therein, and strategies for more secure and efficient deployments of blockchain-based SCMs. Further, an overview of the extant cybersecurity challenges and the limitations of current redressive deployment methods (Sections 2.2) underpin the genesis of the Framework for addressing cybersecurity challenges and efficiency Gaps that exist with different deployments (Section 4.5). The schematic of the framework (Subsection 9.4.4) is intentionally architected to be responsive to the fluid dynamics of blockchain technologies and cybersecurity threats, whereas the selection of tools and resources (Chapter 5) is predicated on their demonstrated efficacy in simulating and testing various blockchain deployments.

In summation, the research methodology is meticulously aligned with the predominant themes emergent in the literature review, functioning as a navigational beacon to ensure the research is strategically positioned to delve into the challenges with granularity and yield substantive contributions to the body of knowledge.

This dissertation proceeds to delineate the research design and methodology with meticulous and scholarly rigour, standing on the shoulders of established methodological precedents within the disciplines of information systems, blockchain technologies, and cybersecurity [72].

3.1 Overview of the research design and methodology employed in this study.

3.1.1 Research Structure

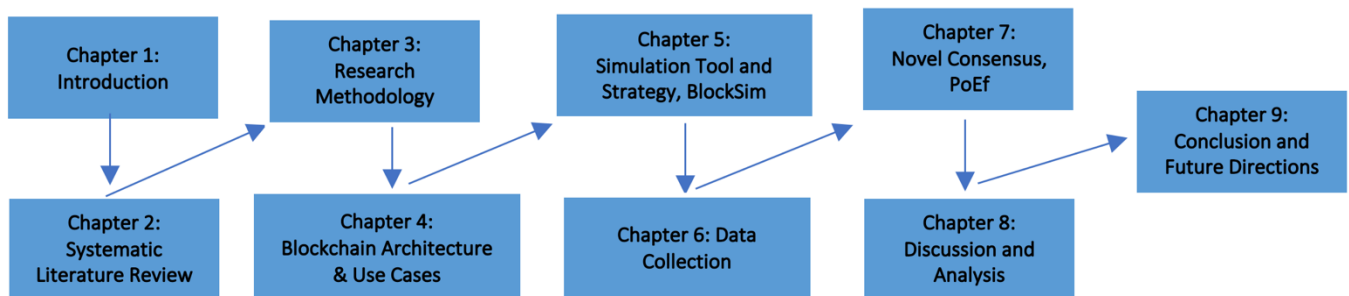


FIGURE 3.1: Figure illustrating the structure of this thesis.

This thesis offers a comprehensive examination of blockchain technology in SCM, focusing on its application, challenges, and the development of an innovative consensus mechanism, PoEf. As illustrated in Fig. 3.1, the thesis is broken down into 9 Chapters, each summarized at the end of Chapter 1.

3.1.2 Research Methodology

This research is based on the philosophy of positivism as it shall utilize theories and applications of blockchain, Information and Communications Technology (ICT) devices and related data from available literature to generate, test and obtain noteworthy results from a hypothesis. The objectives and the specific research question aimed to be answered by this project shall be addressed through the adoption of the exploratory sequential mixed methods design, which is a methodology that combines both qualitative and quantitative approaches. This form of research design has been advocated by Creswell and Plano Clark [73] as a valuable approach when investigating complex phenomena, such as the implementation of blockchain technology in supply chain management and its cybersecurity implications. The process involves Blockchain prototypes being simulated, investigated, and evaluated to conduct experiments and action research to

gain an in-depth understanding of the cybersecurity challenges and technological security gaps in blockchain-based supply chain management systems. The research follows a methodological triangulation approach, combining systematic literature review and case study analysis as used by Denzin [74] and experimentation. This mixed-method approach allowed for a more comprehensive understanding of the subject matter and helped to cross-verify findings.

The methodology follows a three-phase process. Firstly, a systematic literature review was conducted to identify and analyse the current state of knowledge regarding blockchain technology and its cybersecurity challenges in supply chain management. The systematic review follows the PICOS framework guidelines [75], ensuring a rigorous, transparent, and replicable process. The review included a wide range of sources, including peer-reviewed journal articles, conference proceedings, and industry reports, to provide a comprehensive overview of the topic. The second phase of the research is a qualitative phase which looks at a few case studies to investigate the real-world application of blockchain in supply chain management and the associated cybersecurity issues. The case studies will take an interpretive approach. This will enable the researcher to develop a deep understanding of the subject being studied by getting insights into the intersubjective meanings that participants of the study associate with and attempt to portray a particular phenomenon through the interpretations that people assign to real-life situations [76]. The addition of the interpretive approach will therefore give the researcher insights into the challenges of developing and adopting blockchain in the SCM sector, as this paradigm depends on an individual's perceptions and assumes that people create and associate unique subjective meanings with the world, they live in [77] i.e., encapsulating people's perceptions of their own world. In the case where research findings from this approach cannot be generalized, interpretivism will allow the researcher to use qualitative data from similar perspectives [78]. These case studies followed the principles outlined by Yin [79], ensuring robust and reliable results. The third phase of the research is a more quantitative phase which will employ an experimental blockchain deployment, using BlockSim, to test proposed mitigation strategies for identified cybersecurity challenges. The performance of these strategies will be analysed using various statistical techniques.

This mixed-method design, combining systematic review, case study analysis, and experimental simulations, provides an effective way to explore the complex, multifaceted issue of blockchain technology in supply chain management. It allows for an in-depth understanding of the topic, combining breadth from the systematic review, depth from the case studies, and empirical testing from the simulations.

3.2 Data collection methods

3.2.1 Systematic Literature Review

The systematic literature review, a cornerstone of academic research, provides a rigorous framework for aggregating and synthesizing relevant studies pertinent to a defined research question [80]. This thesis employs this method to accurately map the scholarly landscape encompassing blockchain technology, cybersecurity, and SCM. The review adheres to the PICOS guidelines [75] ensuring a methodical, transparent, and reproducible process. Key stages include formulating research questions, developing a strategic search methodology, selecting pertinent studies, extracting, and analysing data, and synthesizing findings. This review forms the bedrock upon which the case study analysis and experimental simulations are constructed.

3.2.2 Case Study Analysis

Case study analysis, a qualitative research approach, delves into phenomena within their real-life contexts using multiple evidence sources [79]. In this investigation, case studies are utilized to probe the deployment of blockchain in SCM and the entwined cybersecurity challenges. Selection criteria for these case studies are based on relevance and the richness of available data. Data sources encompass company reports, industry publications, and interviews with key stakeholders, all analysed following Yin's established methodology [79]. This analysis provides granular insights into the practical deployment of blockchain in SCM, uncovering potential cybersecurity mitigation strategies.

3.2.3 Experimental Computer Science

This research embraces experimental computer science to probe the innovation at the heart of this thesis. The approach entails proposing and developing a solution to a real-world problem, followed by creating a proof-of-concept and assessing its security [81], [82]. To achieve the research objectives defined above in Chapter 1, preliminary steps include a thorough literature review focusing on theory application in blockchain, e-SCM systems, relevant cybersecurity literature and the supporting literature in the fields of Supply Chain Management ecosystems and cybersecurity risks and vulnerabilities in blockchain implementations. Further literature review will include articles, books, conference and journal papers, and IEEE and other relevant standards. This review prioritizes technical aspects, aligning with the researcher's expertise, but also encompasses theoretical and operational elements to ensure a complete understanding during the research's design and execution phases.

3.2.3.1 Experimental Validation and Performance Evaluation

The creation of novel methods for enhancing the security and efficiency of blockchain-based SCM systems necessitates stringent experimental validation and performance evaluation. This section details the steps and considerations for establishing an experimental setup using BlockSim, a blockchain simulation framework [83], to evaluate the performance of the newly proposed method.

3.2.3.2 BlockSim: A Simulation Framework for Blockchain Systems

BlockSim serves as a robust tool for modelling and evaluating blockchain system performance under varied conditions, including different network scenarios, consensus mechanisms, and workload cases. It allows for the simulation of a blockchain-based SCM system to implement and assess the proposed method's efficacy in addressing security challenges [83]. This versatile framework can be utilized to simulate a blockchain-based SCM system and implement the proposed new method, enabling researchers to assess its effectiveness in addressing the identified security challenges and limitations. BlockSim provides a flexible and customizable environment that can be tailored to replicate the specific characteristics and requirements of the target supply chain management system.

3.2.3.3 Experimental Setup and Simulation Parameters

To set up an experimental blockchain arrangement using BlockSim, researchers must define the simulation parameters, such as network topology, consensus mechanism, transaction rate, and block size. These parameters were selected to reflect the real-world conditions and constraints of the target SCM system, ensuring that the simulation results are applicable and relevant to the specific use case. Additionally, the proposed new method should be integrated into the simulation model, enabling its performance and security properties to be assessed in the context of the blockchain-based SCM system.

3.2.3.4 Performance Metrics and Evaluation Criteria

To evaluate the performance of the proposed new method, researchers must establish a set of performance metrics and evaluation criteria [84]. For this research, metrics included security-related measures, such as the number of successful attacks, as well as efficiency-related measures, such as transaction throughput, latency, and resource utilization. By comparing the performance of the proposed new method against these metrics, researchers can determine its effectiveness in addressing the identified security challenges and enhancing the overall performance of the blockchain-based SCM system.

3.2.3.5 Sample simulation test case

The experimental validation and performance evaluation of the proposed new method are essential steps in the research process, ensuring that the developed solution effectively addresses the security challenges and limitations of existing blockchain deployments in supply chain management systems. By leveraging the BlockSim simulation framework and conducting a performance analysis, researchers can contribute to the ongoing development of more secure and efficient blockchain-based SCM solutions.

3.2.3.6 Critical Analysis of Results and Suggestions for Future Work

Upon obtaining the simulation results, a critical analysis of the data will be conducted, examining the strengths and weaknesses of the proposed new method in the context of the target supply chain management system. This analysis should consider potential trade-offs between security and performance, as well as any limitations or assumptions associated with the simulation model. Based on this analysis, researchers can provide suggestions for future work, such as refining the proposed method, exploring alternative techniques, or conducting further experiments under different conditions or with different simulation parameters.

3.3 Selection criteria for reviewed literature and case studies

The criteria for the selection of literature and case studies were carefully defined to ensure a comprehensive, yet targeted, investigation of the research topic.

3.3.1 Systematic Literature Review

For the systematic literature review, the inclusion and exclusion criteria were defined according to the PICOS framework which is widely used in evidence-based research [75]. The 'Population' referred to supply chain management systems, 'Intervention' to the implementation of blockchain technology, 'Comparison' to traditional systems without blockchain, 'Outcome' to cybersecurity challenges, and 'Study design' to empirical studies providing evidence on the topic. Literature was included if it:

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

3.3.2 Case Studies Selection

For case study selection, the criteria were designed to ensure that selected cases were representative of the real-world implementation of blockchain technology in supply chain management. Cases were included if they:

- Involved in the deployment of blockchain technology in a supply chain management context.
- Provided detailed information on the implementation process and the associated cybersecurity challenges.
- Represented a variety of sectors and geographical locations to ensure a broad perspective.
- Could provide access to primary data sources, such as company reports, industry publications, and interviews with key personnel.
- These selection criteria ensured that the research was grounded in rigorous academic scholarship and reflected real-world practices. By adhering to these criteria, the study was able to provide a comprehensive, yet focused, investigation of the research topic.

3.4 Thesis Framework Structure

Identifying and addressing cybersecurity challenges and technological security gaps within blockchain deployment in SCM requires a methodical approach. For this thesis, a framework was developed based on existing models in information systems and cybersecurity literature, particularly drawing from the works of Yetton et al. [85], Leukel [86] and Edgar and Manz [87].

The proposed framework consists of six main steps:

- **Identification of Cybersecurity Challenges:** The first step involves a systematic literature review and case study analysis to identify the cybersecurity challenges that are commonly faced in the deployment of blockchain technology in SCM. These challenges are then classified according to their nature, such as technical challenges (e.g., scalability, interoperability), organizational challenges (e.g., lack of expertise, resistance to change), and regulatory challenges (e.g., data privacy laws, compliance requirements).
- **Exploration of the technical Security Gaps:** The second step focuses on identifying the technical security gaps in the current blockchain deployments in SCM. These gaps could be in the form of vulnerabilities in the blockchain architecture, weaknesses in the consensus mechanism, or flaws in

the cryptographic algorithms. The identification of these gaps is primarily based on case study analysis and the experimental simulation of blockchain deployment.

- **Comparative Analysis** **Comparative analysis of different consensus approaches and methodologies:** This third step involves systematically comparing various consensus deployments and methodologies used in blockchain-based SCM systems. The objective is to gain an understanding of each approach's strengths, weaknesses, and suitability in different contexts. Based on the literature, a framework will be developed to evaluate each approach based on several criteria such as level of security, efficiency throughput scalability, ease of implementation, and adaptability to changing cyber threats.
- **Exploration of emerging trends and opportunities for the enhancement of cybersecurity and efficiency in blockchain-based systems:** This step aims to identify emerging trends in cybersecurity and blockchain technology, assess their impact on the SCM sector, and explore opportunities for their integration in blockchain-based SCM systems.
 - **Trend Identification:** This will involve monitoring industry reports, tech news, and academic journals, and attending relevant conferences and seminars. The goal is to stay informed of the latest advancements in cybersecurity and blockchain technology.
 - **Impact Analysis and Opportunity Exploration:** Once the emerging trends have been identified, their potential impact on SCM will be analysed. This could involve predicting changes in security requirements, operational processes, and overall SCM efficiency. The focus will then shift to identifying how these trends could be used to improve cybersecurity in blockchain-based SCM systems. This could involve integrating new security protocols or using advanced cryptographic techniques.
- **Evaluation and Testing of Mitigation Strategies:** The fifth step in the framework is the evaluation and testing of the proposed mitigation strategies. This is done through a further experimental simulation of blockchain deployment, where the performance of the strategies is tested and analysed. The evaluation provides insights into the effectiveness of the strategies and guides the refinement and further development of these strategies.
- **Development of Secure and Efficient Strategy for Deployment:** The last step involves the development of security and efficient strategies tailored to address the identified cybersecurity challenges and technological security gaps in distinct types of blockchain-based SCM systems. These

strategies could include one of the identified issues, highlighted in the taxonomy in Section 2.4, but this research will only explore implementing more secure blockchains in SCMs.

- **Experimental Simulation:** Consensus approaches will be tested in a simulated SCM environment using tools like BlockSim. The results of these experiments will provide empirical evidence of the effectiveness of these approaches.

This six-step framework forms the backbone of the research methodology, aiming to build an understanding of the current landscape and future possibilities for cybersecurity in blockchain-based SCM systems. The framework also provides a systematic approach to identifying technical security gaps in various deployment strategies of blockchain technology in SCM. By following this framework, the study aims to contribute to the development of more secure and efficient blockchain deployments in SCM.

3.5 Tools and Resources

3.5.1 BlockSim as a simulation tool for testing the proposed method.

The research will take place in a simulated environment, using BlockSim, a well-known simulation tool, to create and imitate models of discrete-event dynamic systems that are relevant to blockchain systems. The inclusion of BlockSim in this research is crucial because of its Base Model feature, which encompasses essential model structures that are shared by many blockchain systems. The tool efficiently enables the setting of model constructs across the three main abstraction levels (network, consensus, and application) often seen in most blockchain installations. The versatility of BlockSim's Base Model in accommodating different blockchain systems is a vital feature, enabling effortless integration and customisation to incorporate specific system requirements or deployment specifications, with a special emphasis on cybersecurity architecture.

3.5.1.1 Other Tools and Resources employed.

Microsoft Word and Excel will also be used for more general functions, such as word processing and the visualisation of results. In addition, specialised software, such as LaTeX and Mendeley, will be used for the creation and modification of research documentation and research referencing, respectively. The project would involve a combination of simulations, field trials, questionnaires, and emulator-based tools (where feasible) for developing and testing the proposed blockchain prototypes and/or protocols in a SCM ecosystem.

4 Understanding Blockchain and its Use Cases in Supply Chain Management

The integration of blockchain technology into SCM represents a pivotal shift in how information is traced, transactions are recorded, and trust is established among stakeholders. The convergence of blockchain within the SCM domain has yielded an array of use cases, each highlighting the technology's capacity to enhance transparency, efficiency, and security. This Chapter first explores the fundamental architecture of Blockchains, then delves into use cases, drawing on academic literature to contextualize their impact and potential.

4.1 Fundamentals of Blockchain Technology

The field of supply chain management (SCM) has experienced a notable increase in interest in blockchain technology. This can largely be linked to the growing trend of digitization 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 greatly increased interest in the application of 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 4.1 below.

- Public blockchains are distinguished by their inclusive nature since they enable the involvement and membership of any individual in the blockchain network [88].
- Private blockchains are characterised by their restriction of transaction participation to authorised parties. In this type of blockchain, the administrator possesses the power to override, modify, or eliminate any recorded entries[88], [89].
- Consortium blockchains are characterised by their governance structure, which involves several organisations rather than a single entity [90]. One such instance is Hyperledger Fabric [91].

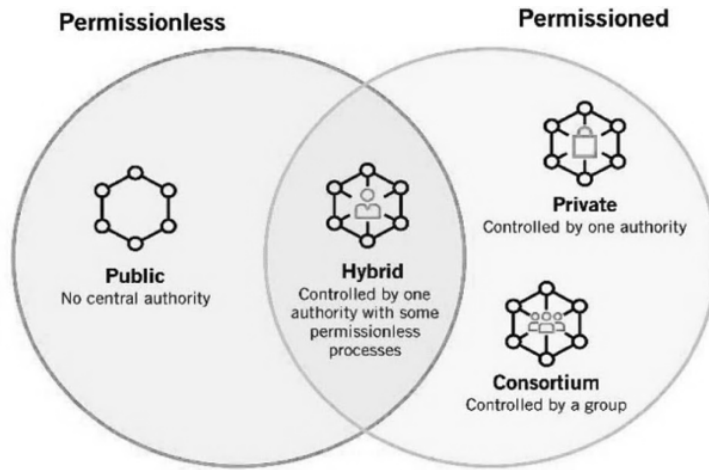


FIGURE 4.1: Figure illustrating the blockchain architecture categories [92].

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., [93], Sarfaraz et al., [94] and Saberi et al., [43]. Private blockchains are well-suited for implementation inside supply chain systems [95] because of the inherent characteristics of private blockchains. The incorporation of blockchain technology into conventional SCM poses a notable obstacle, namely due to the lack of customised consensus algorithms that can effectively integrate with and address supply chain issues [96]. Information validation in the blockchain architecture is achieved using a consensus method that involves network nodes, hence eliminating the requirement for intermediaries. According to Du et al. [97], the consensus mechanism serves the purpose of establishing a tamper-proof environment and ensuring the reliability and validity of stored information.

4.1.1 Blockchain Architecture

Blockchain is a form of Distributed Ledger Technology (DLT) that facilitates the safe, transparent, and immutable storing of data [98]. The system is comprised of a network of computers, referred to as nodes, which maintain a collective and synchronised ledger of transactions. The transactions are inserted into blocks, which are subsequently interconnected in a sequential chain. Each block within this chain has a date and a reference to the preceding block. This configuration facilitates the establishment of a robust, distributed database that exhibits resistance to unauthorised manipulation and alteration. The blockchain architecture is designed with the objective of decentralisation, meaning that it operates without the oversight or control of a singular central authority. In contrast, the preservation of the 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 [98], [99].

Blockchain technology frequently employs a sequential data structure, where distinct data blocks are interconnected in chronological order based on their respective creation times. The initial block in the blockchain is commonly referred to as the genesis block. The data structure within the blockchain that represents essential information pertaining to transactions is known as transaction information. This data structure facilitates the expression of value transfer through immutable digitally signed operations. The block refers to the compilation of transactional data and is comprised of two components: a block header and a block content. The block header typically consists of the following components:

- The version, which is commonly used to monitor and document the progress of software or protocol modifications.
- The preceding block hash is recorded in the current block. The hash algorithm generates a distinct hash value by irreversibly processing the block information. The hash value, which possesses a concise and unchanging length, serves the purpose of uniquely identifying the block. To establish a connection between the current block and its preceding block, the hash value of the prior block is saved within the current block.
- The Merkle Root is responsible for storing the hash value of the root node of the Merkle tree associated with the current block.
- The block creation timestamp. The inclusion of a timestamp in the blockchain 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 which 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 as well as 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*, which is a metric that quantifies the amount of storage space used by the *NumTransactions*.
- The *NumTransactions*, which is a metric is utilised to document the total count of transactions included within a given block.
- The *Transactions*, which is the recording of the amount of transaction data within a block.

4.1.2 Blockchain Layers

This section introduces three levels of blockchain systems: network, consensus, and application, as illustrated in Figure 4.2. The architecture of blockchain systems can be dissected into five principal layers, each with its 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 blockchain networks and will be pivotal in the construction of the simulator discussed in Chapter 5.

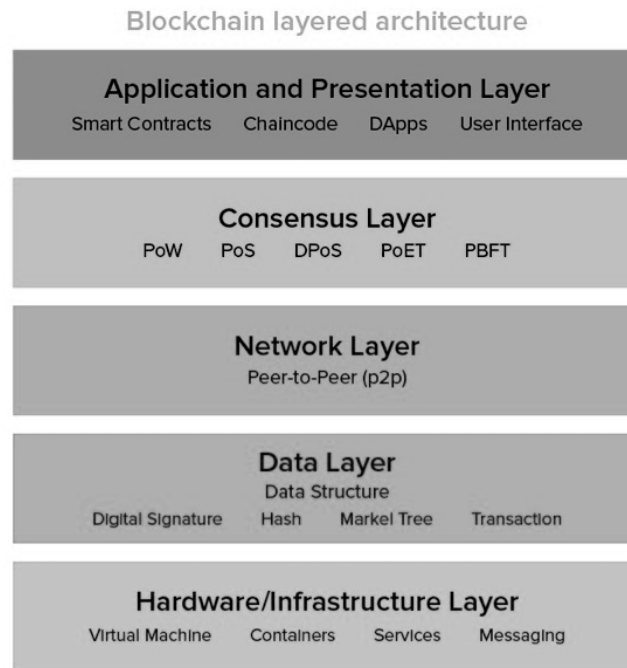


FIGURE 4.2: Figure illustrating the various layers of the blockchain.

4.1.2.1 The Application and Presentation Layer (Incentives Layer)

The uppermost layer in the blockchain architecture is referred to as 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 systems of rewards and the underlying rules that dictate their distribution [100]. 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 incentivizing miners to maintain the blockchain ledger. The incentive scheme plays a crucial role in ensuring the resilience and effectiveness of a permissionless

blockchain ecosystem [62], [101]. 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 [102], and detrimental behaviours exhibited by nodes, such as selfish mining strategies [103]. In non-cryptocurrency blockchain systems, it is common practice to associate rewards with the creation of blocks and the handling of transactions. The incentive mechanisms differ in intricacy across different blockchain networks.

4.1.2.2 The Consensus Layer

The Consensus Layer, which usually sits above the Network Layer plays a crucial role in blockchain design and how it operates. It contains fundamental protocols and ways to establish a collective agreement on the current status of the blockchain ledger. This layer serves to synchronise the whole network by enabling consensus and enforcing protocols that guarantee the accuracy and orderliness of the ledger. [104]. This means that the Consensus Layer in blockchain systems is largely responsible for the efficiency and security within a blockchain by devising and implementing a collection of algorithms and protocols that mandate nodes around the network to get a unanimous agreement on the state of the ledger within a certain timeframe. According to Nakamoto, the protocols define the criteria for selecting nodes that are allowed to add the next block, determine the schedule for block generation, and offer solutions for resolving conflicts in situations when different versions of the ledger exist among nodes [1].

On the efficiency side of things, the implementation of the Consensus Layer is especially vital in decentralised blockchains, such as Bitcoin, designed with the Proof-of-Work (PoW) algorithm and Ethereum, designed with the Proof-of-Stake (PoS) algorithm. Consensus algorithms like PoW and PoS were both specifically devised to oversee the consensus process in blockchain networks but they both operate differently. In the PoW architecture, nodes, commonly referred to as miners, allocate computational resources to expand the ledger by appending new blocks. In contrast, the PoS model necessitates that nodes possess financial stakes, so establishing a connection between ledger upkeep and financial investment. The fundamental concept behind these algorithms is to enforce a monetary expense on ledger upkeep, discouraging nodes from engaging in destructive actions, while also incentivizing adherence to specified regulations and the integrity of the ledger [105]. In the context of these blockchains, the rate at which a miner generates blocks is directly proportional to their processing power. This relationship guarantees the decentralised and safe character of the blockchain.

When it comes to security, the latency in propagating blocks among nodes can sometimes result in forks, which are malicious situations where multiple blocks are spread simultaneously, resulting in different representations of the ledger. The Consensus Layer is responsible for resolving conflicts and determining the official blockchain by applying particular criteria defined by the consensus algorithm. For example, the PoW protocol used in Bitcoin follows the longest chain rule. However, alternative approaches such as the GHOST (Greedy Heaviest Observed Subtree) proposed by Sompolinsky & Zohar, suggest accepting the chain with the highest workload as the genuine ledger [106]. Stale or orphan blocks, which are blocks omitted from the main chain, are discarded, and do not affect the ledger's state. Nodes play a crucial role in enhancing the transaction queue and updating the ledger with new transactions or blocks when they are added to the system and maintaining security.

Selecting the right consensus mechanism is therefore crucial in deciding the validation of transactions and achieving agreement among nodes regarding the state of the ledger (how efficient and secure) inside a blockchain system. The choice of a consensus protocol holds great significance in SCM, considering their 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 state of the ledger inside a blockchain system. The primary objective of this research is to compare several consensus protocols and determine which ones enhance efficiency and security in blockchain applications for SCM scenarios.

4.1.2.3 The Network Layer

The foundational element of blockchain architecture is the Network Layer. It encompasses an array of nodes and incorporates a broadcast protocol for inter-node communication. This layer is tasked with the critical function of cataloguing the diverse node entities within the network infrastructure and facilitating their data interchange through the implementation of an underlying broadcast protocol. Nodes are the essential agents within the blockchain environment, undertaking transaction generation, dissemination, and execution, as well as endorsing and annexing blocks to perpetuate the ledger's continuum [107]. Conversely, the broadcast protocol is instrumental in orchestrating the distribution of data constructs such as transactions and blocks throughout the network, as explicated by Eyal and Sirer [62]. The network layer portrays not only the nodal constituents and their respective locational attributes but also their interconnectedness, thus defining both the typology of information to be propagated and the methodologies employed therein. A 'node', the principal entity within the network layer, may represent either a standard stakeholder, whose aim is to engender and transmit transactions for execution and ledger inclusion, or a specialized variant, known as a 'miner',

charged with the ledger's augmentation via block appendages. Each node is characterized by a unique identifier, managing its own ledger balance, a localized version of the blockchain ledger, and, in the miner's case, an exclusive transaction pool that aggregates pending transactions from the network [108].

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. Miner nodes, upon the formulation of a new block, engage their network in a verification and acceptance process, to synchronize this new block with their ledger instances. The transmission of such information within blockchain networks is governed by a plethora of protocols, notably inclusive of relay networks and the prevalent advertisement-based protocols, as identified by Nakamoto [1] and further investigated by Decker and Wattenhofer [109]. 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, in the absence of a request, the data transfer is deemed redundant, presuming the peer's pre-existing data possession.

4.2 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 [110], [111], [112]. A blockchain is essentially a decentralised ledger system that connects blocks of data in chronological order, without any 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 [113].

As illustrated in Fig. 4.3, transactions within a blockchain commence with nodes, which could be individuals or entities, creating data packets known as transactions. 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 [45]. Miners oversee collating pending transactions from a pool of unconfirmed transactions and crafting them into a new block

by engaging in a consensus protocol, such as PoW or PoS, to compete for the right to append this block to the ledger [114].

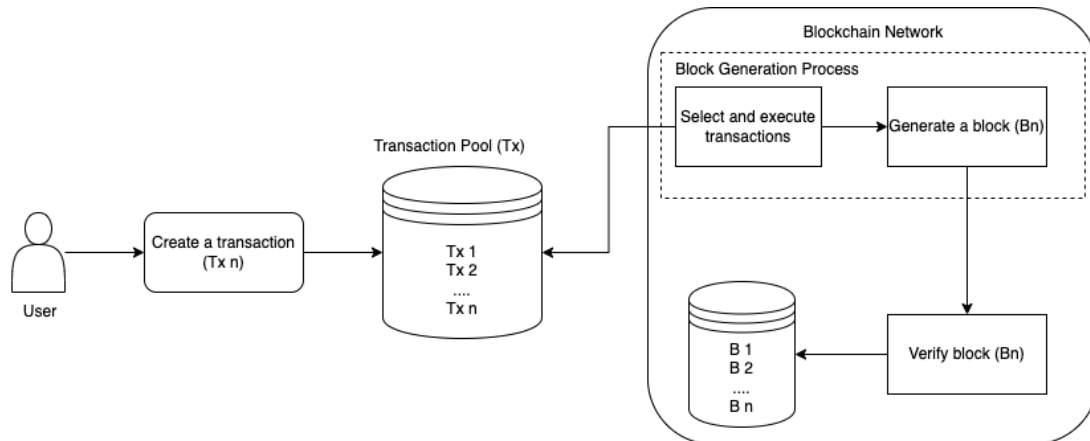


FIGURE 4.3: Figure illustrating how a transaction is initiated on the blockchain.

The freshly assembled block is then broadcasted to the network for validation, a critical process where other nodes verify the block's integrity and the validity of the transactions within the blockchain [115]. This verification step includes but is not limited to, ensuring the correct application of the consensus algorithm, confirming transaction signatures, and upholding the network's rules. Post-verification, the block is added to the blockchain, providing an unalterable and transparent record of all transactions [53].

The operational procedure 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 that has been disseminated and engage in a competitive process to choose the authority to account for the block, which is contingent upon their computational capabilities. Nodes that possess accounting privileges can compile transaction information into blocks and receive rewards that are predetermined by the reward mechanism inside the blockchain protocol. In applications like Bitcoin, the rewards frequently yield economic advantages and serve as incentives for nodes to consistently contribute computational power to the blockchain network.
- **The consensus verification stage:** the accounting node disseminates the packed block 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 have the capability to store the data that has been verified during the consensus verification phase for an extended duration. This allows for retrospective verification of the data based on the timestamp and hash value present in the block. Consequently, the node can offer an access interface to the upper-layer application, facilitating queries for ledger information. The computer power offered by the nodes within the blockchain network contributes to the decentralised, open, stable, honest, and credible nature of the blockchain system.

As highlighted in the previous section, central to blockchain's operational ethos, consensus mechanisms are pivotal in sustaining transactional integrity and fostering trust across networks. The repercussions of consensus vulnerabilities, as delineated by seminal researchers such as Eyal and Sirer [62], extend to the potential destabilization of entire SCM systems. This means that a shift towards mechanisms that synergize energy efficiency with fortified security, as explored by Saleh [63], is instrumental in optimizing transaction throughput, which is a quintessential element for SCM processes that demand efficiency and dependability. Having explored the fundamental workings of blockchain technology in Section 4.2, where the focus was on the transaction initiation, block creation, and the critical role of consensus in maintaining the blockchain's integrity, we now transition to a more specific aspect of this technology in Section 4.3. Here, the research delves into the several types of consensus mechanisms that underpin blockchain operations, particularly within the context of SCM. Section 4.3 will examine various categories of consensus mechanisms, including proof-based, capability-based, and voting-based algorithms. Each type plays a distinct role in validating transactions and ensuring the cohesiveness and security of the blockchain network. The consensus mechanism serves as a crucial component in the architecture of the blockchain, overseeing the confirmation of transactions and maintaining the integrity of the network. The fortification is essential, acting as the main defence against different threats and guaranteeing the continual dependability of the SCM. Giving priority to the consensus layer is not just a tactical decision, but a strategic requirement that supports the general stability of the blockchain. The overarching goal of this research is to advance the field of SCM by fostering a blockchain environment that is both secure and efficient. By addressing the limitations of current consensus mechanisms and introducing innovative solutions, this research enhances the resilience and effectiveness of blockchain-based SCM systems. Ultimately achieving the aim of creating a blockchain environment in SCM that not only meets the current operational needs but is also adaptable to future advancements and challenges in the SCM domain. Understanding these mechanisms is crucial for identifying the most suitable and efficient consensus protocol for SCM applications, ensuring both the reliability and scalability of blockchain-based SCM systems.

4.3 Types of Consensus Mechanisms in SCM

The ascendancy of blockchain technology within SCM has been precipitated by the digital revolution and the advent of Industry 4.0. The integrity and robustness of consensus mechanisms play a pivotal role in ensuring system reliability and security. Given the diverse and dynamic nature of SCM operations, it is essential to thoroughly understand and address the vulnerabilities inherent in various blockchain consensus mechanisms. These vulnerabilities, ranging from security loopholes to scalability issues, can significantly impact the efficiency and reliability of SCM systems. Initiated by the creation of Bitcoin by Nakamoto [1], blockchain's potential to engender decentralized, scalable, and efficient transactional ecosystems has been increasingly recognized in SCM discourse. Traditional blockchain frameworks, while pioneering, are marred by computational inefficiencies, characterized by limited throughput, and elongated transactional latency. Conventional blockchain systems depend on consensus techniques that require significant computational resources, resulting in limited transaction processing capacity and substantial time delays. The increasing fascination with blockchain technology has garnered significant interest within the field of SCM, leading to a pursuit of consensus solutions that are decentralised, scalable, efficient, and reliable.

Contemporary SCM applications are engineered to integrate industry best practices, optimizing the whole delivery procedures, commencing from order placement via the customer application to the final delivery at the customer's designated location. The nexus of blockchain within SCM lies in consensus algorithms that orchestrate and streamline interactions across the multifaceted supply chain network as the technology's tamper-proof chain transactions and business operations contribute to the whole delivery cycle [31]. Consensus algorithms are of paramount importance in SCM since they catalyse business processes, enhancing the dynamism and accuracy of logistics operations amongst many stakeholders, including vendors and customers. Over recent decades, the challenges with the expansion of organizational scale and the diversification of geographical operational scopes have underscored the need for adaptive and cohesive communication practices among SCM stakeholders. A 2017 report on "Supply Chain Trends Recap" by Eye for Transport indicates that over 60% of vendors in the SCM industry are considering the adoption of blockchain technology to ensure timely and validated processes [116]. This increased growth of SCM networks coupled with the rapid advancement of internet-based technologies, e-business, and commercial technologies have led to a growing demand for improving product efficiency and security inside supply chains. While blockchain's promise to elevate traceability, efficiency, and transparency has been lauded, the consensus models that underpin blockchain architectures still introduce distinct security challenges [43]. One such challenge is the integration of the "right fit" of blockchain into conventional SCM,

especially due to the lack of specialised consensus algorithms designed to address and include supply chain issues [117].

The development of consensus algorithms in blockchain has progressed with the expansion of SCM systems. These algorithms have undergone advancements with the aim of constructing intelligent, resilient, and secure SCM systems. Therefore, it is crucial to comprehend the fundamental elements, operational traits, and structure of various consensus algorithms that might be employed in supply chain management systems. Numerous consensus algorithms have been documented in the academic literature, each possessing its own set of functions, performance characteristics, and computing services. The strategic implementation of consensus mechanisms in blockchain networks is pivotal for the operational integrity and directional progression of SCM. In-depth research is crucial, particularly in addressing security challenges posed by tendencies towards centralization and the imperative for efficient solutions. The taxonomy as proposed by Bodkhe et al [34] in Fig. 4.4 categorizes these mechanisms into proof-based, capability-based, voting-based, compute-intensive, and miscellaneous algorithms, each bearing distinct operational implications.

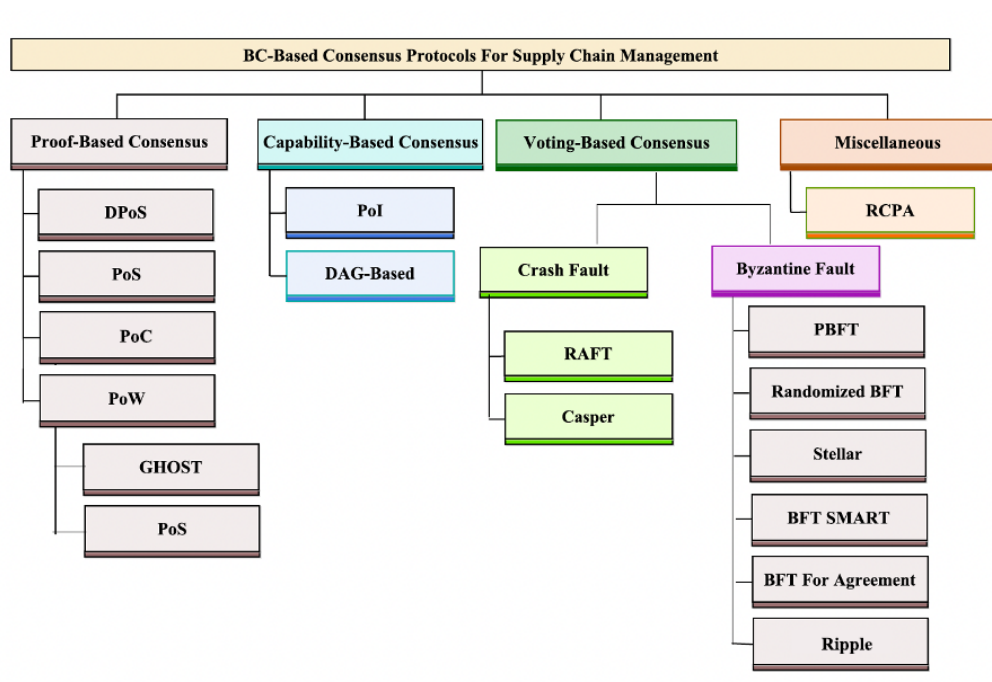


FIGURE 4.4: Figure illustrating Blockchain Consensus Mechanisms in SCM [34].

4.3.1 Proof-based consensus:

Proof-based consensus mechanisms constitute the bedrock upon which blockchain networks ascertain the veracity and commitment of participating nodes. Consensus mechanisms like PoW epitomize the original consensus mechanism, compelling nodes to undertake significant computational efforts to solve cryptographic challenges, thereby validating transactions and mining new blocks [1]. Conversely, PoS shifts the focus from

computational expenditure to the possession of the native cryptocurrency, positing that the probability of mining a block correlates with a node's stake in the network [118]. Delegated Proof of Stake (DPoS) refines the PoS concept by introducing a democratic election process, where stakeholders vote to elect block creators. This model not only conserves energy but also maintains operational integrity, even amid most node failures, due to its community-driven governance model that swiftly substitutes underperforming producers [119], [120] Litke et al. provided a comprehensive evaluation of these decentralized consensus protocols, advocating for their potential within SCM systems. Their comparative analysis underscores the necessity for SCM businesses to align their blockchain integration strategies with consensus mechanisms that optimize for reduced energy consumption and enhanced transactional throughput, especially in consensus like PoW that are computationally intensive. The integration of some proof-based consensus into SCM still encounters computational bottlenecks, predominantly due to their resource-intensive nature. The high trust associated with consensus like PoW comes at the cost of significant energy demands and the need for specialized hardware, tailored for high performance [114]. Such challenges necessitate a reevaluation of consensus protocols to identify mechanisms that align with the efficiency, scalability, and sustainability requirements of modern SCM systems.

4.3.2 Capability-based consensus algorithms:

Capability-based consensus algorithms have been developed to enhance the functionality and fairness of node participation in blockchain systems. Proof of Importance (PoI) and Directed Acyclic Graph (DAG)based consensus are two prominent examples that seek to address the limitations of traditional mechanisms like PoS. PoI distinguishes itself by evaluating the value of nodes through a multifaceted scoring system. Nodes are assigned an importance score based on various metrics, including net transfers, the quantity of vested currency, and the degree of involvement in activity clusters [121]. Unlike PoS, where the probability of creating a block may correlate directly with the stake, PoI incorporates additional factors such as transaction partners, frequency, and size, aiming to create a more detailed assessment of a node's contribution to the network's health and vitality [122]. The PoI model incentivizes active participation and transactional throughput, potentially leading to more vibrant and transaction-rich blockchain networks. For SCM systems, this could translate to enhanced transparency and velocity in the supply chain operations, ensuring that contributions to the network are recognized and rewarded, thus fostering a more engaged stakeholder community.

DAG-based consensus employs a graph structure that allows multiple chains of blocks to coexist and intertwine. This structure enables the parallel processing of transactions, which can lead to increased

scalability and reduced transaction confirmation times [123]. In DAG-based systems, a message carrying a transaction includes references to previous messages, thus creating a web of interconnected transactions that collectively contribute to the network's consensus. DAG-based consensus mechanisms have significant implications for SCM, as they can handle high volumes of transactions efficiently, a common requirement in large-scale supply chains. By potentially circumventing the scalability issues of traditional blockchains, DAG can facilitate faster transaction verifications, crucial for SCM operations where speed and efficiency are paramount [123]. The development of capability-based consensus algorithms like Pol and DAG-based consensus addresses certain inefficiencies and centralization concerns associated with earlier consensus models. In the context of SCM, these mechanisms may offer more equitable and performance-oriented alternatives that can align with the dynamic needs of modern supply chains. However, their effectiveness and security in various operational contexts require further empirical study to ensure that they can reliably support the nuanced demands of SCM systems.

4.3.3 Voting-based consensus algorithms:

Voting-based consensus algorithms, a paradigm shift from the traditional compute-intensive mechanisms, employ a democratic process to designate block producers. This approach significantly reduces energy requirements and mitigates wealth-centric miner selection, promoting a more equitable and sustainable blockchain environment. Such algorithms, exemplified by PBFT and the Stellar Consensus Protocol (SCP), have distinct implications for blockchain networks, especially within SCM. Voting-based consensus algorithms democratize the block production process by enabling network stakeholders to vote on miner selection. This election-based approach not only conserves energy but also avoids the competition-based miner selection that characterizes PoW systems, thereby reducing the associated computational and energy expenditures [124]. Capability-based consensus mechanisms, while more energy-efficient than Proof-Based, often skew miner selection toward wealthier nodes, potentially leading to centralization. Voting-based algorithms 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 [125].

Voting-based consensus mechanisms such as PBFT efficiently work on top of permissioned Hyperledger Fabric platforms on the principle, that the network can withstand up to i faulty nodes among a minimum of least $n = 3i + 1$ peers. This robustness makes PBFT an attractive consensus mechanism for SCM applications that require high levels of reliability and security in transaction processing [126]. Stellar Consensus Protocol (SCP), one of the first byzantine agreement protocols, pioneers a flexible approach to

consensus with its federated byzantine agreement system. It allows SCM stakeholders to nominate and choose participants, preserving trust even when some nodes become unreliable. This flexibility positions SCP as an optimal consensus protocol for diverse and dynamic SCM networks, where trust and security are paramount, and network failure must not impede operations [127]. Voting-based consensus algorithms represent a critical advancement for blockchain SCM systems, offering a sustainable and equitable alternative to traditional consensus mechanisms. Their potential to improve network security, trust, and fault tolerance holds considerable promise for SCM systems that are rapidly adapting to the challenges of globalization and digitalization. By reducing energy consumption, these algorithms also align with the sustainability goals increasingly demanded by consumers and regulators. The robustness of PBFT and the adaptability of SCP can significantly enhance the resilience and efficiency of SCM blockchain networks, ensuring uninterrupted and secure transaction flow across the supply chain. Continued research and development are needed to fully realize their potential and to integrate these mechanisms seamlessly into the next generation of SCM solutions.

4.4 The Influence of Consensus Mechanisms on the Security and Performance of Blockchain-Based Supply Chains

Within the domain of SCM, the utilisation of blockchain technology has emerged as a significant catalyst for transformation. Nevertheless, there is a noticeable gap in understanding the degree to which different prevalent consensus mechanisms, such as PoW, DPoS, Proof of Capacity (PoC), Pol, PBFT, SCP, and Ripple Consensus Protocol Algorithm (RCPA), affect the security and operational effectiveness of SCM systems based on blockchain technology. The importance of a blockchain system in SCM networks cannot be overstated, due to their complex and ever-changing nature. Such a system is crucial as it provides assurance of data integrity, mitigates cybersecurity risks, and enables efficient transaction processing [43]. The accepted significance of consensus methods in shaping these traits is still being shaped and documented [128] and concurrently there is a lack of empirical research that directly compares their performance in the context of supply chain management [41]. This section aims to clarify the consequences of various consensus techniques in the SCM context, with a particular focus on the relationship between cybersecurity requirements and operational efficiency. The utilisation of blockchain technology in the digitization of supply chains presents considerable prospects for large advancements in the realm of global commerce. To fully harness the potential of blockchain technology, it is crucial to have a thorough understanding of the consensus mechanisms that form the basis of its functioning [36]. Protecting supply chain data is essential due to the blockchain's tamper-proof ledger, which is a crucial element of its dedication to

security. To ensure the strength of supply chain operations, it is crucial to thoroughly analyse various consensus mechanisms and their impact on cybersecurity [38]. Furthermore, enhancing transaction efficiency is crucial for achieving a competitive advantage in SCM. Hence, it is crucial to ascertain the optimal consensus methodology for enhancing operational efficiency and fostering supply chain agility [129].

Given the intrinsically scalable characteristics of supply chain ecosystems, it is crucial for a selected consensus mechanism to be capable of accommodating growth while maintaining the integrity of security and efficiency. The topic at hand presents a promising opportunity for scholarly investigation [45]. Furthermore, the heterogeneous characteristics of supply chains need the implementation of blockchain solutions that are customised to meet their unique demands. The objective of this research is to connect different consensus methods with the specific requirements of diverse supply chains, to enhance their efficiency and applicability [130]. Given the paramount importance of these factors, it is imperative to conduct a comprehensive assessment of consensus mechanisms to effectively navigate the incorporation of blockchain technology into supply chain management. The primary objective of this inquiry is to offer empirically supported knowledge and recommendations that cater to the needs of both practitioners and academics [131].

To design and execute a series of simulation experiments to test the effectiveness of SCM-based consensus mechanisms, the thesis involved evaluating a spectrum of consensus algorithms, ranging from proofs-based consensus (PoW, DPoS, PoC), a capability-based consensus (PoI), and a few voting-based algorithms (PBFT, Stellar, Ripple), within the proposed blockchain-based SCM framework. This evaluation aims to discern their respective efficiencies and limitations to enhance SCM security and operational performance. The selection of an appropriate consensus mechanism is crucial for the optimal functioning of SCM systems. This research delves into the various types of consensus mechanisms currently in use or proposed for blockchain applications and their suitability for SCM. Factors such as transaction speed, system scalability, resistance to tampering, and energy efficiency are considered in evaluating each mechanism. The aim is to identify consensus mechanisms that not only ensure data integrity and security but also cater to the high-throughput and real-time processing needs of SCM systems.

4.5 A Deeper look into each Consensus Mechanism

Within the complex realm of supply chain management (SCM), the choice of a blockchain consensus mechanism is a crucial decision that has a substantial impact on the security and efficiency of the system. The following discussion offers a thorough analysis of various prominent consensus algorithms, such as the PoW, DPoS, PoC, PoI, PBFT, SCP, and RCPA. This analysis aims to assess the suitability of these mechanisms within the SCM paradigm, based on relevant scholarly literature. This will help to support informed decision-making. Consensus algorithms are fundamental protocols that enable synchronisation among nodes in a distributed ledger environment, as emphasised by Xiao et al. [107]. The nodes in a blockchain network are discrete computational units that synchronise to maintain a consistent and unchangeable ledger of transactions. This eliminates the need for a centralised authority. Attaining consensus is crucial to guarantee that all participants in the network maintain a uniform ledger state.

However, there are also obstacles that continue to exist in the development of blockchain technology, especially when it comes to supply chain management (SCM). Zheng et al. (P. Zheng et al., 2018) emphasise the limitations of throughput, transaction latency, and the inherent trade-offs associated with decentralisation initiatives. Significantly, the ability of traditional blockchains to handle transactions becomes insufficient as the complexity of supply chain management increases. For instance, the PoW consensus paradigm, which is commonly used in public blockchains, requires all nodes to perform extensive computational tasks, resulting in significant energy consumption, as described by Bach et al. [132]. Consequently, there is an increase in the time it takes to reach agreement and a decrease in the amount of work that can be done, making these models less than ideal for big or complex supply chain systems, where effectiveness and ability to handle growth are of utmost importance.

4.5.1 Proof of Work (PoW)

PoW, the foundational consensus mechanism used by Bitcoin involves solving complex computational problems to authenticate transactions and add new blocks. PoW is the oldest and most well-known consensus mechanism. It is used by Bitcoin and other early blockchains. The consensus involves solving a cryptographic puzzle, which effectively secures the network against fraudulent modifications by making such attempts computationally infeasible and economically non-viable [1]. The initial miner to successfully solve the problem is granted the privilege of appending the subsequent block to the blockchain. The procedure is characterised by high computing costs and substantial energy consumption, which, in turn, enhances the security of the blockchain. The security of PoW is renowned for its robustness, mostly

attributed to the substantial computing effort necessary to authenticate transactions and generate new blocks [114]. The cybersecurity features that stand out with the PoW mechanism include:

- **Robustness:** It is extremely secure against double-spending and 51% attacks unless an attacker controls most of the network's hashing power.
- **Immutability:** Transactions are immutable once enough blocks are added after them, ensuring a tamper-evident ledger [133].

Although it offers robust security, an attribute beneficial for SCM [134], its high energy consumption and slower processing rates [135] may hinder its application in fast-paced and eco-conscious SCM operations.

4.5.2 Delegated Proof of Stake (DPoS)

DPoS represents a significant advancement in blockchain consensus mechanisms, particularly in terms of energy efficiency and governance structure. Unlike PoW, which requires substantial computational effort and energy expenditure to mine blocks through solving complex mathematical problems, DPoS delegates the responsibility of transaction validation to a select cadre of representatives. DPoS is a more energy-efficient alternative to PoW. In DPoS, a select group of validators is elected to validate transactions. This makes the system more efficient, but it can also make it more vulnerable to centralization. This democratic approach to consensus can result in a more engaged and participatory network of stakeholders, fostering a community-driven governance model. As an evolution of PoS, DPoS enables stakeholders to elect delegates for transaction validation, enhancing transaction speed and energy efficiency [136]. The cybersecurity features that stand out with the DPoS mechanism include:

- **Elected Delegates:** In DPoS, stakeholders elect a limited number of delegates to validate transactions and produce blocks. This election process can enhance security because delegates have a vested interest in maintaining the integrity of the network to preserve their reputation and position.
- **Stake-Based Voting:** The ability to vote for delegates is often proportional to the number of tokens a stakeholder holds. This stake-based voting system incentivizes token holders to act in the best interest of the network's health, as any security breaches could devalue their holdings [118].

Nevertheless, the very characteristics that potentially augment the cybersecurity of Delegated Proof of Stake (DPoS) can also pose potential hazards. The centralization of authority within a limited number of representatives may result in collusion, wherein a select few could possibly manipulate the network, rendering it susceptible to corruption and security breaches. Furthermore, the preservation of the voting process's integrity is of utmost importance. Any compromise to this procedure could lead to the election

of malicious stakeholders, thereby threatening the entire network. DPoS expedites transaction validation by restricting the participation of nodes in the consensus process, hence improving the performance of SCM systems that demand high transaction throughput [136]. However, the risk of centralization in DPoS, where only a few delegates are responsible for the network's security, could be a concern.

4.5.3 Practical Byzantine Fault Tolerance (PBFT)

Tailored for distributed networks, PBFT ensures consensus amidst untrustworthy nodes [137] offering a high-security level suitable for SCM environments with moderate trust. PBFT is designed to withstand the Byzantine Generals Problem, ensuring that the system can continue to operate even if some nodes act maliciously or malfunction [90]. Noteworthy cybersecurity features are:

- **Fault tolerance:** Can tolerate up to $\frac{n-1}{3}$ malicious nodes in a network of n nodes.
- **Finality:** Transactions are considered final as soon as consensus is reached, which is essential for the integrity of SCM.

PBFT's limitation arises from its non-trivial communication overhead, which can hinder scalability. A hindrance in scalability is an important consideration for global supply chains. Its efficient transaction processing is advantageous, but scalability issues may limit its applicability in larger SCM systems.

4.5.4 Proof of Capacity (PoC)

PoC consensus mechanism stands as a salient exemplar of innovation in distributed ledger technologies, presenting a noteworthy departure from the energy-intensive computational paradigm of PoW. As elucidated by Dziembowski et al. [138], PoC leverages the unused storage capacity of nodes within the blockchain network to engage in the mining process. This approach not only demonstrates a commitment to energy efficiency but also embodies a more sustainable utilization of computational resources. In the PoC model, participants, or stakeholders, employ available disk space to store a large set of potential solutions to cryptographic puzzles, commonly referred to as plots. When a new block is to be forged, the network determines which miner's stored plot has the closest solution to the challenge, thereby granting them the right to forge the block. This precomputation of solutions markedly reduces the energy required for mining operations when juxtaposed with the continuous, intensive hashing required in PoW.

From a cybersecurity perspective, PoC is distinguished by several features that merit attention. The utilization of storage space as a cornerstone of the mining process inherently discourages wasteful energy expenditure, fostering a more environmentally conscious blockchain ecosystem. Moreover, the requirement for substantial storage space to participate effectively in mining can serve as a deterrent to

malicious actors, raising the bar for executing a 51% attack, which is a concern in smaller or less-secured networks [139]. Despite its energy efficiency and resource consciousness, PoC is not without its challenges. The efficiency gains in energy consumption may be offset by the increased demand for storage space, potentially leading to resource intensiveness which might potentially slowdown the consensus throughput. Furthermore, the scalability of PoC, while advantageous for large-scale SCM implementations, prompts an examination of its long-term security implications. As the size of the network and the volume of stored solutions grow, the integrity and resilience of the storage-based mining process against evolving cybersecurity threats remains an ongoing area for rigorous scrutiny and research [62].

4.5.5 Proof of Importance (Pol)

Pol is a cutting-edge consensus technique specifically developed to enhance the security and efficiency of blockchain networks. Xiao and colleagues [140] found that the Pol model assigns weights to participants' qualitative contributions in the network, distinguishing it from other network validation models. This metric encompasses the total number of transactions, the execution of smart contracts, and the level of consistent network participation. Pol on the NEM blockchain surpasses mere token ownership by integrating stakeholder engagement into the consensus mechanism. The relevance of a node in the blockchain ecosystem can be better assessed by considering factors such as stake size, transactional activity, and network activity, which provide a more comprehensive evaluation. The concept underlying Pol aims to provide a fairer system in which the likelihood of validating transactions and creating new blocks is determined by the value of transactions and the allocation of resources, rather than by wealth or processing capacity.

The security features of Pol are noteworthy. The objective of Pol is to promote investment and active participation in order to establish a validator network that is both varied and resilient. Diversification serves as a safeguard against centralised control, hence potentially diminishing susceptibility to vector attacks that exploit the concentration of authority. Through incentivizing regular and significant engagement within the network, Pol diminishes the attractiveness of the network to malicious individuals who may be unwilling to participate in prolonged and advantageous endeavours to gain influence. The use of Pol as a consensus mechanism in SCM systems is now under investigation. The efficiency of Pol could be advantageous for SCM systems that prioritise transaction throughput and active network engagement. Nevertheless, the degree to which Pol may be seamlessly incorporated into SCM procedures and its relative advantage over PoW is still subject to empirical examination. Additional investigation is required to evaluate the

operational effectiveness and ability of Pol to withstand cybersecurity threats in the context of rising digital supply chain hazards in SCM scenarios.

4.5.6 Stellar Consensus Protocol (SCP)

SCP is a cutting-edge distributed ledger platform that provides decentralised control and a flexible trust mechanism. According to Mazieres [127], SCP is based on the Federated Byzantine Agreement (FBA) system, which allows network participants to choose trustworthy nodes to form quorums that can reach consensus without network-wide agreement. This architecture protects against forking and network validator collusion.

Blockchain networks are vulnerable to forks, thus SCP's cybersecurity measures focus on them. SCP guarantees fast and secure consensus by using quorums and quorum slices, portions of the network where each node chooses which nodes to trust for information. This quorum-based strategy ensures that the network can reach agreement even with malicious actors if the quorum slices overlap and the network is well-connected. Since confidence is acquired and granted by other nodes, the protocol guards against Sybil attacks, when a malevolent actor creates many pseudonymous identities to corrupt the network. Additionally, SCP's consensus method can swiftly establish agreement, enabling fast transaction settlement. SCM systems must be fast and reliable to handle the dynamic and time-sensitive nature of supply chain operations, therefore expedited transaction finalisation is ideal.

The SCP's novel distributed consensus method provides a promising model for secure, efficient, and scalable blockchain implementations. Its strong security and fast transaction processing make it a good alternative for SCM systems looking to use blockchain technology. To prove SCP's efficiency and resilience in a quickly changing cybersecurity ecosystem, more exploration is needed.

4.5.7 Ripple Consensus Protocol Algorithm (RCPA)

The RCPA, described by Schwartz et al., [141], is a notable progression in the realm of distributed ledger technology. This protocol functions inside a framework consisting of a network of validating servers, each of which plays a vital part in attaining consensus. The RCPA differs from conventional consensus algorithms by simplifying the process and prioritising transaction integrity and system-wide agreement above considerable computing effort. RCPA is highly resilient to typical cybersecurity risks in distributed networks, making it a notable attribute of the system. The validation procedure in RCPA entails the participation of numerous reliable servers working together to verify the legitimacy of transactions [142]. This approach

reduces the risk of fraudulent activities and guarantees the genuineness of each transaction. The use of this multiple validation mechanism significantly improves security by rendering the network impervious to a range of assaults, including as double-spending and network partitioning attacks.

In addition, RCPA's distinctive consensus approach greatly decreases the time needed for transaction confirmations, resulting in a highly scalable and efficient system. The efficiency is especially advantageous for SCM systems, which frequently deal with large numbers of transactions and require fast processing. The capacity of RCPA to efficiently process a substantial volume of transactions, while maintaining a high level of security, is very compatible with the operational requirements of SCM systems. RCPA's scalability, in addition to its cybersecurity benefits, makes it an attractive option for SCM operations that include managing large transaction volumes. The protocol's design guarantees that when the network expands and the number of transactions rises, the system may adapt and expand without a corresponding rise in complexity or a decline in performance.

The Ripple Consensus Protocol Algorithm is a highly advanced and reliable solution for blockchain-based SCM systems. The system's emphasis on ensuring the accuracy and reliability of transactions, along with its capacity to effectively handle a large number of transactions, makes it highly suitable for addressing contemporary SCM complexities. The protocol's strong cybersecurity measures, ability to handle substantial amounts of data, and fast transaction processing highlight its potential as a valuable tool in the changing field of blockchain technology and its use in supply chain management.

4.5.8 Wrap-Up

In the broader context of SCM, each consensus mechanism presents a unique amalgamation of strengths and weaknesses. PoW is acclaimed for its security but is often critiqued for its inefficiency and high energy consumption, rendering it less favourable for certain SCM applications. Conversely, mechanisms like DPoS, PoC, and PoI provide more energy-efficient alternatives but are not without potential security vulnerabilities and centralization concerns. PBFT, while excelling in security, encounters limitations in scalability. In comparison, the SCP and RCPA strike a more balanced chord, offering a harmonious blend of security, efficiency, and scalability, thereby suiting a diverse array of SCM requirements.

The selection of an optimal consensus mechanism for SCM is a multifaceted decision, necessitating a thorough consideration of various factors such as transaction throughput, transaction latency, security imperatives, and the overall projected scale of the supply chain network. This decision must be meticulously

aligned with the specific operational demands and strategic objectives of the SCM system to ensure the most effective utilization of blockchain technology.

4.6 Use cases of Blockchain in SCM

4.6.1 Provenance Tracking and Traceability

One of the primary applications of blockchain technology in supply chain management is provenance tracking and traceability [38], [143]. 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 [144]. Companies can create a tamper-evident and immutable ledger of product movements from origin to consumer. This application has been particularly transformative in industries where authenticity and origin are paramount, such as agri-food [145], pharmaceuticals [146], and luxury goods [147]. Furthermore, transparent nature of blockchain allows all stakeholders, including consumers, to verify the origin and authenticity of products, fostering trust and confidence in the supply chain [38]. In their 2019 publication, authors Tsang et al., [148], introduced BC-based food traceability systems and devised an innovative proof-of-supply-chain-share (PoSCS) consensus protocol. Validators, who are stakeholders in SCM, mine blocks in this consensus mechanism instead of miners. PoSCS employs a probabilistic method to choose the stakeholders (validators) responsible for validating and forging in the blockchain. PoSCS primarily emphasises factors such as volume, stakeholder analysis, transit time, and shipment, rather than giving priority to computational power and income. In addition, they conducted a comparison analysis of the proposed PoSCS consensus algorithm with existing consensus algorithms. This research focused on many aspects, including the function of block generation, selection of validator/miner, and processing capacity. They demonstrated and validated their performance by doing a case study for a retail e-commerce company. The authors also proposed that both PoW and PoS necessitate significant processing power, resources, and energy for decentralised networks. Therefore, the primary considerations for incorporating PoW and PoS into blockchain-based food traceability are the preservation of stability, scalability, and energy efficiency.

4.6.2 Smart Contracts for Automated Processes

Smart contracts are contracts that are written in code that automatically execute the conditions of the agreement between the buyer and seller. They are utilised to automate operations inside the SCM [41]. Smart contracts in supply chain management enable the automation of diverse procedures, including payment settlements, compliance checks, and dispute resolution. They can automatically verify

circumstances and carry out agreements, such as initiating payments upon the delivery of items, thereby diminishing the necessity for intermediaries and expediting transactions. Through the automation of these procedures, smart contracts have the ability to circumvent the necessity for manual involvement, lower transaction expenses, and mitigate the potential for human error or fraudulent activities [43]. Moreover, smart contracts can be customized to accommodate the specific requirements of different industries and supply chain scenarios, offering a flexible solution for streamlining operations [149].

4.6.3 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 [150]. 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 [151]. The traceability capabilities of blockchain allow consumers and companies to authenticate assertions regarding sustainability and ethical sourcing [39]. In their 2023 paper, Yusuf et al., [152] conducted a study to investigate the utilisation of a distributed ledger technology to tackle the difficulties encountered by a vegetable provider. Authors have highlighted that vegetable supply companies frequently face a restricted timeline to finalise their ledger due to the perishable nature of their items. As a result, this leads to a misunderstanding of information between the client and the supplier. The team established a network utilising blockchain technology, Kafka. This network resolves supplier problems by doing empirical analysis on the Hyperledger platform, employing varying channels and guaranteeing crash fault tolerance through the implementation of Kafka. The proposed blockchain network is verified using the crash fault-tolerant consensus algorithm, which is highly recommended to researchers as the most suitable and feasible consensus algorithm for the vegetable supply chain. Similarly, Haughton et al., [92] conducted a study on an Ethereum PoS consensus blockchain. The purpose was 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 different stakeholders, including suppliers, manufacturers, distributors, and retailers. Additionally, the blockchain would provide an open and unchangeable historical record for each transaction within the supply chain of this lifecycle. These platforms can improve coordination and information sharing among stakeholders in supply chains by

offering a reliable and widely accepted source of information, resulting in increased efficiency and resilience.

4.6.4 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 [153]. Blockchain's ability to provide a secure and unalterable record of transactions aids in counterfeit prevention [154]. 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 [155]. 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 [156]. In 2018, Y. Qian and Meng created a new framework for supply chain management called "DelivChain" which is based on a combination of aspects of PoS and 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 [157]. A hybrid consensus mechanism that combines elements of PoS and PoI could provide the DelviChain with the benefits of both mechanisms. PoS could provide the network with security and scalability, while PoI could provide the network with efficiency and fairness. So, combining fragments from different consensus algorithms can help to create a superior algorithm.

Each of these use cases represents a transformative potential for blockchain in SCM, underlining the technology's role in catalysing operational efficiencies and strategic value creation. The critical evaluation of these applications is essential for stakeholders contemplating blockchain adoption within their supply chain operations. The various applications of blockchain technology in supply chain management, such as provenance tracking, smart contracts, decentralized platforms, supply chain finance, and circular economy, have the potential to revolutionize the way businesses operate and collaborate. By leveraging the unique features of blockchain technology, stakeholders can achieve increased transparency, efficiency, and sustainability in their supply chains, ultimately enhancing their competitiveness in a rapidly evolving global market.

5 Simulation Modelling Tool, BlockSim

5.1 Background

This chapter delves into the scholarly exploration of simulation models in the context of blockchain systems as depicted in existing literature. The utilization of simulation methodologies to assess and quantify various attributes of blockchain frameworks has been a focal point of academic inquiry.

Neudecker et al., [158] and Schussler et al [159] introduce a simulation models aimed at dissecting and evaluating potential attack vectors and propagation delay within the Bitcoin network respectively. Their analysis contributes significantly to understanding the vulnerabilities inherent in such systems. Göbel et al., [160] went beyond that by utilising a discrete-event simulation approach to investigate the behavioural patterns of Bitcoin miners, particularly focusing on scenarios involving delayed information propagation and strategies such as selfish mining. This research was built upon by Shahsavari et al., [161] in a notable study that assessed architectural modelling coupled with simulation techniques employed to quantify the latency experienced in blockchain configurations under varying conditions. Continuing the trajectory of research on the propagation delay, another research by Aldweesh et al., develops a simulation model to scrutinize the dynamics of profit uncertainty within the Ethereum blockchain ecosystem [162]. Their findings reveal a critical insight: miners in the Ethereum network struggle with making optimal choices regarding transaction selections in block creation, thereby impeding their revenue maximization potential.

While these studies provide valuable insights, they tend to concentrate on facets of blockchain technology. For instance, Karame et al., [163] proposed a Bitcoin-centric simulator to analyse the security and performance implications across consensus and network layers. Other researchers, as cited in Aoki et al., [164] and Stoykov et al., [165] have also developed Bitcoin-like network simulators, however, a common limitation in these existing works is their focus on specific blockchain system elements, often neglecting a holistic integration of the technology's functional components such as transactions. To address this deficiency, Section 5.4 of this thesis presents BlockSim, a discrete-event simulator designed as a versatile tool for analysing blockchains. BlockSim is capable of handling a wide range of design and operational inquiries. BlockSim surpasses the limitations of prior models by incorporating a comprehensive framework for evaluating various sorts of blockchain systems. This encompasses a more thorough examination of

typical functional components and the fundamental mechanisms that are shared by many blockchain implementations. BlockSim is intricately designed and structured to navigate the many layers of blockchain technology, offering a comprehensive and detailed comprehension of its performance and security dynamics. Existing literature offers basic models for simulating certain features of blockchain systems. However, BlockSim marks a significant advancement in this field by providing a more comprehensive and multi-layered method for simulating blockchain systems. This progress enables a more detailed investigation of blockchain technologies, tackling important issues related to their design and implementation, and contributing to a more comprehensive comprehension of the technical aspects of blockchain systems in academic research.

5.2 Modelling and Simulation

5.2.1 Theoretical Foundations of Modelling

Modelling is the process of developing condensed abstract representations, or models, that replicate the characteristics of actual or hypothetical systems. It's a cerebral exercise in abstraction. These models carefully strike a balance between authenticity and simplification to represent the essential features of a system. The art of modelling lies in controlling the conflict between abstraction and realism to create a piece that accurately depicts the dynamics of the system while also being easily understood [166]. Often, achieving this balance necessitates an ongoing process of honing a foundational model and progressively introducing complexity in a controlled manner. As significant scholarly works have noted, models typically represent the behaviour and relationships of the system using mathematical constructions in conjunction with structural and logical frameworks.

5.2.2 Classification of System Models

System models are classified according to traits like determinism versus stochasticity and static versus dynamic natures, as illustrated in Figure 5.1 [167]. Probability is incorporated into stochastic models, as demonstrated by client arrivals in queuing systems. By contrast, non-random variables that have been predetermined define deterministic models. Unlike static models, which show a system at a single point in time, dynamic models show systems across time, such as industrial processes. In dynamic models, temporal aspects are crucial, while in static models, they are merely a minor consideration. Moreover, dynamic models split into discrete and continuous categories; discrete models represent changes at particular intervals, whereas continuous models are fluid.

By implementing these models to imitate system behaviours, simulations provide an opportunity for experimenting in settings when direct intervention is impractical or excessively costly [168]. To accelerate the evaluation of diverse designs and policy decisions, simulations offer an environment for testing various configurations and operational strategies. The primary advantage of simulation lies in its capacity to accurately forecast system reactions within a secure and regulated environment, encompassing various scenarios. This is particularly advantageous for conducting hypothetical "What if" scenarios that include speculation without producing actual disruptions in the real world [169]. There are two primary classifications of simulations: discrete-event and continuous-event, with the former being the specific emphasis of this thesis. Discrete-event simulation is particularly suitable for human-engineered systems, such as digital infrastructures, where it involves tracking the changes in state variables at certain time intervals. An excellent example of this is the 'BlockSim' tool, which adheres to the discrete-event simulation paradigm. This tool is discussed in more detail as the chapter progresses. One of the main objectives of this thesis is to investigate the concept that proposes a dynamic and stochastic nature characterised by the periodic change of state variables. This concept holds significant significance in systems that were devised by people, such as digital infrastructures. The 'BlockSim' tool, which is founded on the discrete-event simulation paradigm and is presented subsequently in this chapter, offers a demonstration of this concept.

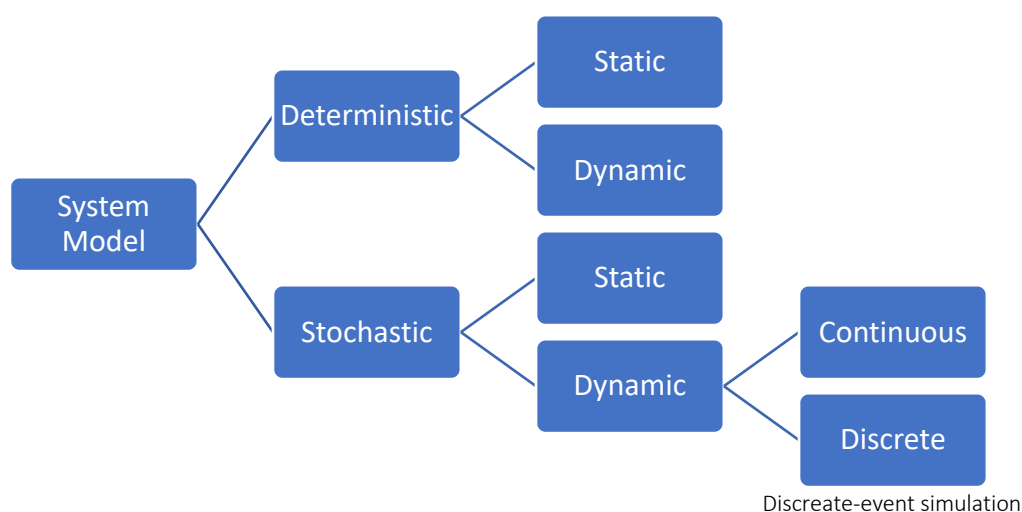


FIGURE 5.1: Figure illustrating system model taxonomy adopted from [167].

The utilisation of simulation models and tools can be categorised into two main approaches: the utilisation of general-purpose programming languages such as C++, Java, and Python, and the utilisation of specialised simulation languages such as Arena and GPSS [170]. The former option offers a wide range of applications and a familiar structure for writing code, while the latter choice provides a set of pre-existing features that streamline the process of building models. The existence of this paradox contributes to a continuous discourse about the most effective strategy for simulation endeavours. Furthermore, simulation

frameworks such as OMNeT++ [171] and SimPy [172] utilise general-purpose programming languages to provide a basis for the building of simulation models. This approach combines the versatility of the programming language with the specific simulation functionalities. In the present research, Python has been selected as the programming language used in the ‘BlockSim’ simulator because of its versatility and the extensive collection of libraries it offers for simulation-related purposes.

5.3 Steps of a Simulation Study

Simulation research mandates a series of methodological steps, as articulated in Figure 5.2, to navigate the complexity inherent in the study's design and execution [169]. These steps are sequentially structured yet dynamically interlinked, ensuring a robust and comprehensive exploration of the system under investigation.

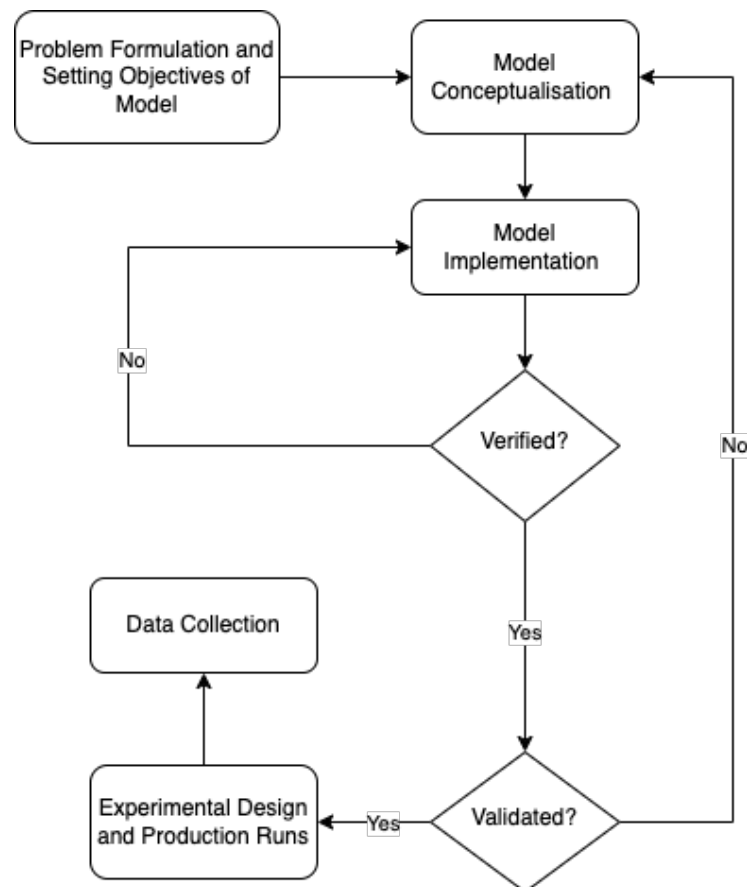


FIGURE 5.2: Figure illustrating the procedure for a Simulated Study (updated and reproduced after [169]).

- **Establishing the Problem and Objectives (Phase 1):** The initiation of a simulation research relies on the accurate formulation of the problem statement. All stakeholders must have a clear grasp of

the situation, together with a clear definition of the researches' goals, research questions, and objectives. This initial phase establishes the subsequent research direction and ensures consistency throughout the investigation process.

- **Conceptual Model Development (Phase 2):** Creating the Abstract Representation After identifying the problem, the next crucial step is to create a conceptual model. This abstraction functions as a substitute for the actual system, encapsulating its operating dynamics while simplifying its intricacies. The model's specification should include inputs, processes, and outputs, supported by clearly defined assumptions and limitations. The alignment between the model's intricacy and the research aims is crucial; it should be adequately comprehensive to provide valuable information, while avoiding excessive complexity that may confuse or overwhelm.
- **Model Implementation (Phase 3):** Transitioning from the conceptual stage to writing the actual code. To shift from a model to a simulation programme, one must decide between using specific simulation languages or general-purpose programming languages, as explained in Section 5.2. The use of a modular approach is recommended, gradually increasing the level of detail in the model to include all aspects of it.
- **Verification (Phase 4):** The model verification includes ensuring the accuracy and dependability of the model by making sure that the simulation code accurately represents the conceptual model. Consistency and error tests are employed to assess the model's resilience in different input scenarios and extreme conditions, respectively. The iterative nature of this phase allows for its integration at every stage of the model's gradual implementation.
- **Experimental Design and Execution (Phase 5):** Conducting the Simulation This pivotal step involves defining the simulation's experimental framework, stipulating conditions, and outlining the scenarios to be examined. Decisions regarding the duration of simulation runs, the number of replications, and the input variables form the crux of this phase. It is here that the simulation materialises into a tool for exploration and discovery.
- **Data Collection (Phase 6):** Executing the experiment would generate data from the model. The data collected relies on the model's parameters, and the interpretation of the results would subsequently require investigation through statistical analysis of the controlled experimentation.

Frequently, the data is included into theoretical distributions to facilitate the inclusion of stochastic aspects in the simulation.

- **Validation (Phase 7):** The concluding phase of a simulation involves examining and communicating the outcomes by verifying the precision of the model. Validation is the procedure used to verify the precision and genuineness of the simulation, guaranteeing that the program's outcomes faithfully depict the functioning of the real-world system it intends to reproduce. The approach involves conducting a triangulation analysis by comparing the model with facts and theoretical ideas. Any variation necessitates a re-evaluation of the model's construction and the data acquisition procedure. Validation is not a discrete phase, but a procedure that includes the complete range from conceptualising a model to its ultimate implementation.

The processes collectively form the framework for conducting simulation research, as implemented in the empirical investigations of this thesis.

5.4 BlockSim: An Extensible Simulation Tool for Blockchain Systems

Developing and deploying blockchain systems necessitates careful consideration of architectural, configurational, and parametric elements. Due to the limitations of actual testing via trial-and-error, it is necessary to utilise a model-based simulation such as BlockSim [173]. BlockSim is a precisely designed discrete-event simulation framework that allows for the exploration of how architectural complexities affect the behaviours of blockchain systems.

The architecture of BlockSim is cleverly designed to simplify simulation, by abstracting complex details and making it easy to manipulate. This architecture is specifically designed to handle a wide range of requests and scenarios related to blockchain design. BlockSim is an essential tool for professionals in blockchain construction, analysis, and academia due to its guiding principles of generality, extensibility, and simplicity. The main purpose is to help analyse and evaluate important performance measurements such as throughput and latency, as well as functional measurements like stale rates. It also investigates systemic features such as mining dynamics. BlockSim primarily emphasises performance evaluation rather than comprehensive security analysis or formal validation of consensus algorithms and smart contract mechanisms.

The core of BlockSim is the Base Model, which consists of three interconnected levels: the network, consensus, and application layers. The network layer encompasses the arrangement of nodes and protocols that form the foundation for data transmission between peers. The consensus layer comprises algorithms and governance rules that are crucial for attaining consensus among participants in a blockchain ledger. On the other hand, the application layer is responsible for overseeing the validation of transactions and other applications within the blockchain [174].

The Base Model of the blockchain encompasses several functional units, namely Node, Transaction, Block, Consensus, and Application. These units play a crucial role in the overall functioning of the blockchain and can be customised and expanded to meet the specific needs of the system being examined. The instantiation of these units is facilitated by Python modules, as elaborated in Section 6.5. Furthermore, the simulation engine is supported by supplementary modules such as event, scheduler, and statistics. The inherent transparency of permissionless blockchains presents significant prospects for verifying BlockSim by means of comparing it with established blockchain systems. Moreover, the functionality of BlockSim is showcased by conducting a simulated analysis that examines the rates at which blocks become stale, the throughput of the system, and the fairness of the mining process across a wide range of blockchain configurations. This research therefore goes beyond the configurations already present in existing blockchain systems.

5.4.1 BlockSim Base Model

The underlying framework of BlockSim is designed to encompass several types of blockchains, while also incorporating necessary adjustments to accommodate specific application-related factors. The design concepts that inform the development of BlockSim, namely generality, extensibility, and simplicity, are evident in the manner in which functional units are identified and organised inside each tier of the system, namely the Network tier, Consensus Layer, and Application Layer, as well as the operational dynamics in which they are involved.

5.4.1.1 Design Principles

The Base Model of BlockSim is meticulously tailored to fulfil its principal design goals:

- **Generality:** BlockSim is constructed to accommodate a diverse array of blockchain systems, configurations, and investigative queries.

- **Extensibility:** The framework is designed for ease of manipulation, enabling analysts to explore different facets of blockchain systems comprehensively.
- **Simplicity:** The objectives of this research are achieved while ensuring BlockSim's usability remains straightforward for simulation studies and subsequent expansions.

Striking a balance between generality, extensibility, and simplicity is the essence of BlockSim's design ethos. The Base Model is pivotal in this equilibrium, targeting optimal trade-offs within the blockchain domain. The Base Model's adaptability makes it an ideal simulation tool for the SCM context, wherein various blockchain phenomena, such as transaction propagation and consensus operations, are integral to the supply chain's fluidity and responsiveness. BlockSim's Network Layer allows for the exploration of SCM-specific network configurations, shedding light on the scalability and robustness of different blockchain solutions within the SCM framework.

The Base Model defines the fundamental components that are shared by all blockchain systems. It determines the range of simulation classes that BlockSim supports and the ease of developing models. The conversion of the Base Model into software modules is a crucial factor in determining the extensibility of BlockSim. This enables the creation of intricate models for blockchain processes.

5.4.2 BlockSim's Network Layer

The Network Layer in BlockSim is an essential component that enables the simulation of communication protocols and state management in blockchain systems. The system comprises two main components: the Node and the Broadcast protocol, as depicted in Figure 5.3. The Node entity plays a crucial role in managing and updating the system's state variables, specifically the blockchain ledger and the transaction pool. As a result, it serves as the central component for the operational state of the blockchain. Within the BlockSim framework, every Node is represented as an entity that possesses certain characteristics, such as a one-of-a-kind identification, a balance, and data structures for storing the local ledger and transaction pool. These structures have the ability to expand in real-time, allowing for the inclusion of additional transactions and blocks as they are distributed over the network. This architecture replicates the fundamental components seen in many blockchain implementations, providing a shared characteristic that enables the examination of system-wide behaviours and interactions.

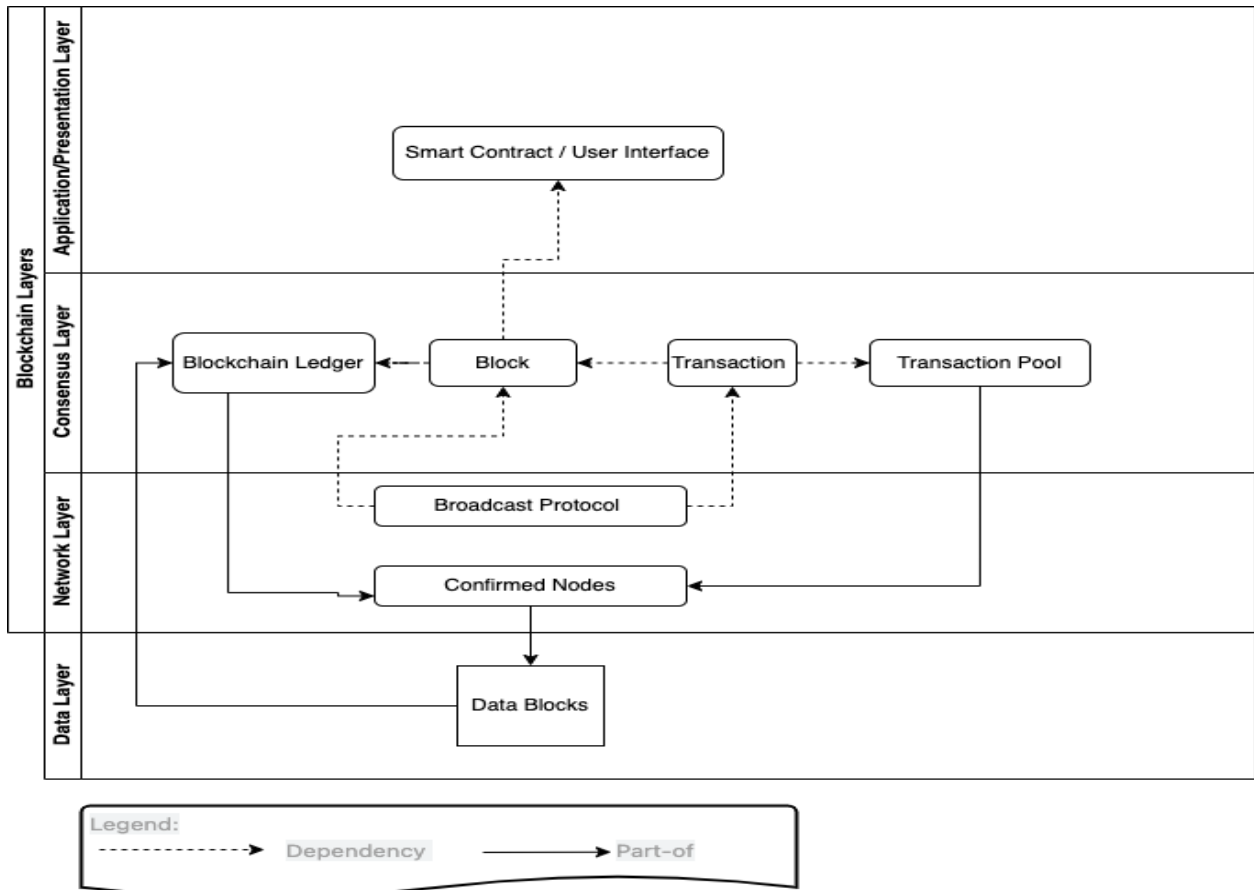


FIGURE 5.3: Figure illustrating the layers in the BlockSim Model.

The Broadcast protocol entity is a vital component in BlockSim, responsible for distributing blocks and transactions over the network. The protocol can be precisely defined, including aspects like as network topologies, geographical distribution of nodes, and intricate node-to-node communication. Nevertheless, in order to simplify and make the model more accessible, the protocol can also be abstracted to primarily emphasise the temporal dynamics of data propagation. The simplification of the broadcast process in this abstraction enhances the user-friendliness and manageability of the simulation environment, especially for individuals who do not need the intricate details of extensive network configurations [174].

By prioritising propagation delay as the main factor, BlockSim effectively optimises its performance, guaranteeing a user-friendly and efficient experience while maintaining the accuracy of its simulation results. This method aligns with BlockSim's fundamental idea of combining comprehensive analytical capabilities with a user-friendly interface that reduces unnecessary complexity. As a result, users have the freedom to interact with the simulation at different levels of complexity. Users can choose between exploring the detailed aspects of network setups for a more detailed study or using the simulator's broader, abstracted picture that is customised to their specific research requirements and skills [174].

5.4.3 BlockSim's Consensus Layer

One of the most important parts of the BlockSim architecture is the Consensus Layer, which is the layer of rules that a blockchain network's nodes use to synchronise on the state of the ledger. This is particularly relevant to SCM on blockchain, where shared data consensus and integrity are critical. As shown in Fig. 5.3, the layer consists of four fundamental entities: Transaction, Block, Transaction pool, and Blockchain ledger. These entities are maintained by every node, which updates continuously to guarantee the currency of the transaction pool and the accuracy of the ledger. Transactions in SCM blockchains can involve any movement or modification of products, services, or data along the supply chain, not just money exchanges. The BlockSim uses both "full" and "light" modelling approaches to simulate these transactions and how they spread throughout the network. The light technique concentrates on overall system throughput, a more appropriate approach when individual transaction details are less critical, whereas the full method tracks each transaction in detail, which is necessary for analysing granular transaction latency within SCM systems. The modelling of block formation and transaction propagation in BlockSim emphasises the need for both efficiency and accuracy in SCM systems. With modelling, the lifespan and timelines of each transaction in SCM can be tracked, whether the transactions are purchase orders, inventory updates, or delivery confirmations. On the other hand, the light technique provides a faster overview, which is advantageous for high-throughput analysis, which is frequently needed for strategic SCM decision-making. Grouped transactions are contained within BlockSim blocks, and when a new block is added to the ledger, it updates both the transaction pool (by eliminating completed transactions) and the ledger itself. This is similar to the SCM procedure, wherein the overall system state is updated upon the fulfilment of a batch of orders or deliveries.

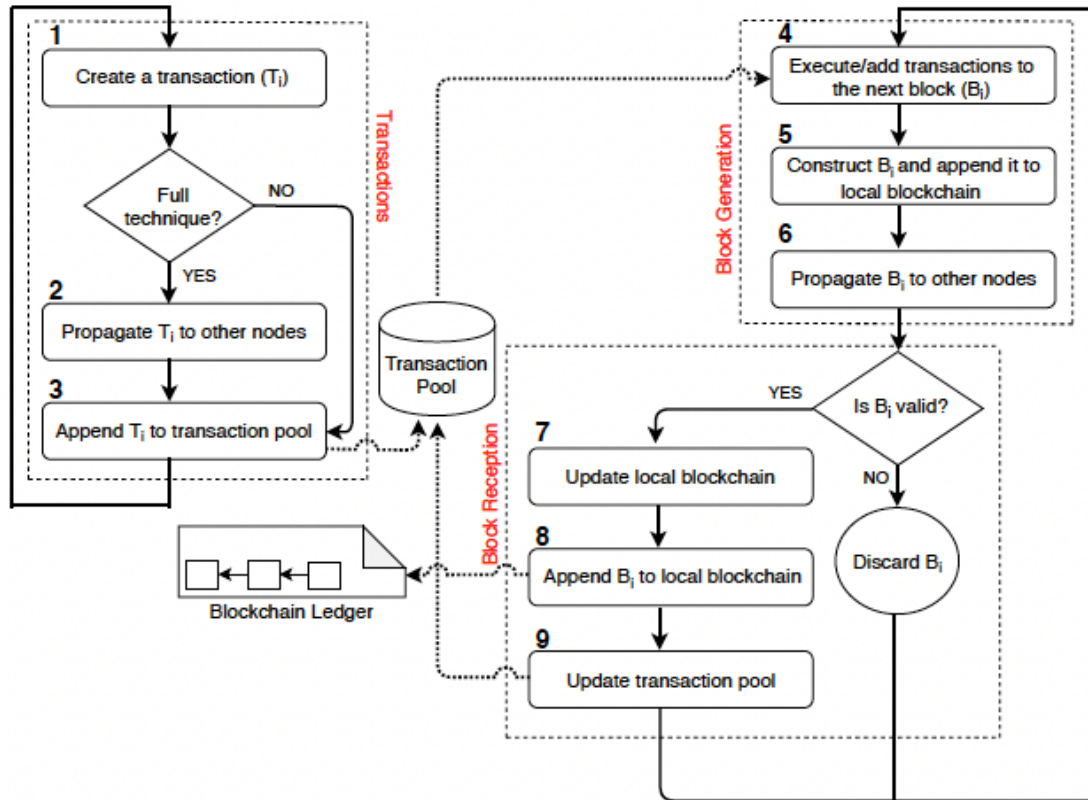


FIGURE 5.4: Figure illustrating the process flow for the consensus activities in BlockSim's Base Model [174].

The consensus process plays an essential part in BlockSim, especially in the context of Supply Chain Management (SCM). The process governs the way in which fresh data, similar to building blocks, is verified and included into the ledger. This process involves the verification and recording of items that are either being received or sent out in the supply chain management (SCM) system. By simulating this process, SCM practitioners can gain valuable insights into how various consensus techniques can impact the performance and reliability of an SCM blockchain. The consensus layer of BlockSim illustrates the two primary operations of block generation and receiving, as shown in Figure 5.4.

The process of block generation entails the identification of the appropriate timing and the selection of the authorised node responsible for creating and adding the subsequent block to the blockchain ledger. This process encompasses all conventional protocols that a miner undertakes, encompassing the execution of transactions within the block, the construction and addition of the block to the local blockchain, and the dissemination of it to other nodes in the network. On the other hand, the block reception procedure pertains to how nodes update their blockchain ledgers when they receive new blocks. This entails a sequence of operations commonly executed by a node upon receiving a freshly generated block. Upon receiving a valid block, the node will update its local blockchain if needed, integrate the new block, and update the transaction pool.

The consensus algorithm is tasked with the responsibility of choosing a miner to produce the subsequent block. The choice of this option is contingent upon the exact consensus protocol utilised in a certain blockchain system. After a miner is chosen to generate and add a new block, they execute a sequence of common activities, however certain blockchain systems might include additional stages. Miners initially arrange outstanding transactions, giving priority to those with higher related fees. Subsequently, they employ predetermined criteria to choose and carry out the most appropriate transactions, incorporating them into the block if there is enough space. This procedure persists until the block reaches its maximum capacity or there are no more transactions awaiting inclusion.

The protocol for updating the ledger in the event of forks: The blockchain ledger may be perceived differently by nodes at a given moment in time because of the propagation delay inside the network. The consensus layer plays a crucial role in establishing the guidelines that nodes can employ to effectively resolve forks. In SCM blockchain applications, handling forks, is crucial. BlockSim allows SCM stakeholders to simulate and evaluate the efficacy of various fork resolution strategies, such as the longest-chain rule employed in Bitcoin and Ethereum. This aspect of the simulation is critical for SCM systems where the rapid resolution of data discrepancies is essential to maintain operational continuity. BlockSim's consensus layer, therefore, not only simulates the foundational blockchain processes but also provides a versatile tool for SCM professionals to explore how different blockchain configurations may influence the performance and reliability of SCM systems. This exploration is crucial for designing SCM systems that are resilient, efficient, and scalable.

In the simulation environment, blocks are represented as objects with various features, including *block depth*, *blockID*, *previous blockID*, *date*, *size*, *miner ID*, and *transactions*. The block ID serves as a distinctive identifier for the block. The block depth refers to the position of a block within the blockchain of a node. The term *minerID* pertains to unique hash identification for the specific node responsible for generating a given block. Each block has the capacity to accept a set of transactions as its content. These attributes demonstrate similarities among different blockchain systems.

5.4.4 BlockSim's Application Layer

The Application Layer of BlockSim is crafted to architect the incentive mechanisms that are quintessential to the functioning of blockchain networks. It is in this stratum that the protocol delineates the criteria for economic rewards, such as block generation and transaction processing incentives, which motivate participant engagement in the network. This layer incorporates a reward entity intricately linked to the

Block entity, as outlined in Fig.5.3. In this system, incentives are distributed to miners based on their successful addition of new blocks to the blockchain ledger, which is an essential step inside the layer.

In the context of blockchain-based SCM, where incentivization can significantly influence the behaviour of various stakeholders, BlockSim offers a modular approach to reward modelling. The simulation framework is endowed with the ability to emulate the incentive structures prevalent in established blockchain systems, like Bitcoin, thereby providing a baseline for evaluating the efficacy of rewards in driving desired participant behaviours. BlockSim affords a block reward, reflective of the fixed cryptocurrency amount traditionally granted for block generation, and transaction fees, correlating to the transaction's size and the associated fees determined by the market dynamics. These parameters are user-configurable, offering the flexibility to simulate both fixed and variable incentive models.

Furthermore, the Application Layer's flexibility allows for an expansion beyond traditional reward mechanisms to encompass alternative incentivization strategies, such as rewards for uncle blocks, a feature particularly pertinent to Ethereum's blockchain, or innovative transaction fee models. This adaptability is crucial in a supply chain context, where the incentivization model may need to reflect the complex interplay between transaction volume, speed, and validation accuracy, which are pivotal in maintaining an efficient and trustworthy SCM system. BlockSim models the reward distribution process by incrementing the balance of miners in response to their contribution to ledger continuity, mirroring the real-world economic feedback mechanisms that underpin blockchain miner activities. In SCM applications, this modelling aspect could simulate incentive-based mechanisms for various supply chain actors, ensuring the integrity and promptness of updates to the shared ledger.

The design of the Application Layer in BlockSim, with its focus on modularity and extensibility, provides a scholarly yet practical framework for simulating and analysing the impact of different incentive structures on blockchain network behaviour. This is of particular importance in the domain of SCM, where incentive alignment across a diverse set of participants is a critical success factor for the adoption and effectiveness of blockchain technology.

5.5 BlockSim Implementation

In this segment, the implementation of the BlockSim simulator is described. The solution was implemented using Python 3.12 as the programming environment. The simulator's architecture is portrayed in Fig. 5.5,

showcasing the main modules that constitute its structure. Central to BlockSim is the Simulator Module, the heart of the simulator, encapsulating the event scheduler (elaborated in Section 6.5.1). The crux of this discussion orbits around the treatment of events and their granularity, a decisive factor influencing the simulator's performance. Complementing the Simulator Module is the Configuration Module (Section 6.5.2), offering users an interface to tailor the simulation environment. Additionally, Section 6.5.3 delves into the Base Model's implementation, dissecting it into three integral layers: Network, Consensus, and Application.

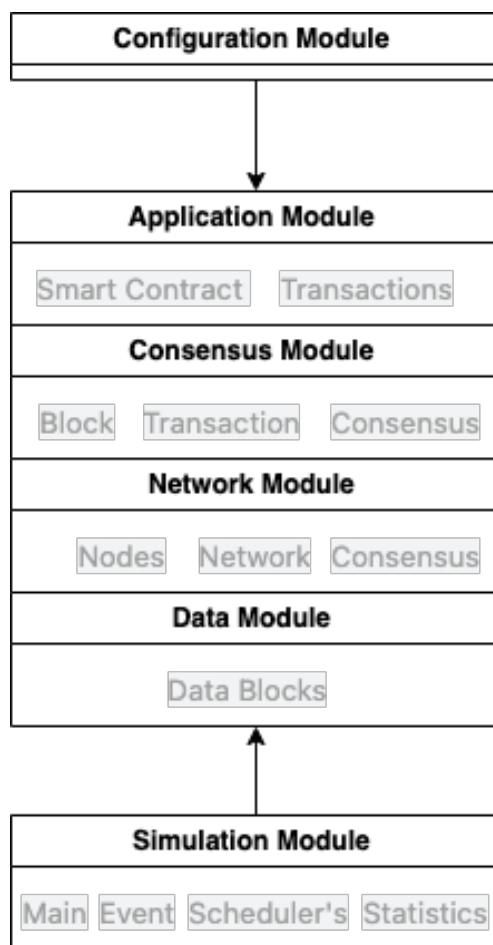


FIGURE 5.5: Figure illustrating BlockSim's Implementation Modules by layers.

5.5.1 BlockSim Simulation Layers

There are three essential classes, Configuration, Application/Incentive, Consensus, and Network classes are essential to the Simulation Module, as illustrated in Figure 5.5. Block-level events and transaction-level events are the two levels of abstraction that make up the event scheduling mechanism. The Network module specifies and arranges events; it has properties that are necessary for event management and processing, like type, *nodeID*, *time*, and *block information*. Future events are coordinated by the Consensus Module, which effectively manages them inside a dynamic Queue data structure. The Queue is updated

continuously by adding new events and removing processed events; it can be thought of as an array list. For instance, the Consensus Module schedules block reception events for additional nodes and initiates new block creation events following a block creation event. The Scheduler also chooses the miners who will work on creating the next blocks during this procedure. The Incentive module (Application layer) fulfils their respective anticipated functions. The simulation is initiated by the Application layer, which establishes the initial conditions and activates the Consensus to initiate event handling. The simulator sequentially processes events until the Queue is depleted or a predetermined simulation duration is reached. The Statistics course engages in the aggregation and analysis of findings from the simulation, with a specific emphasis on block statistics and throughput.

5.5.1.1 Configuration Module

The purpose of this module is to provide users with access to pick and configure different simulation parameters. The adjustment of settings related to nodes, blocks, transactions, consensus mechanisms, and the overall simulation configuration is possible for users. The primary configuration capabilities encompass the ability to modify the number of nodes, the duration of block intervals, and the volume of transactions. In addition, the module provides the capability to enable or disable transactional components, as well as the option to choose between complete or light transaction modelling methodologies. Additionally, the simulator has the capability to include new consensus methods and offer them as options for user selection.

5.5.1.2 Base Model Modules

The implementation of the Base Model, aligned with the structure outlined in Section 4.2, is dissected into three layers: Network, Consensus, and Application.

- **Network Module:** The Network Module consists of two classes: Node and Network. The Node class includes the distinct identifier and data structures for the local blockchain and transaction pool of each node. Notably, individual transaction pools are maintained only under the full transaction technique; otherwise, a shared pool is utilized. The Network class models network latency, currently implemented as a configurable time delay, though future extensions could incorporate specific broadcast protocols. Tailored for SCM, this module includes Node and Network classes, simulating different entities in the supply chain and their interactions. The modelling of network latency and information propagation is crucial in SCM for the realistic simulation of supply chain delays and information flow.
- **Consensus Module:** This module is divided into Transaction, Block, and Consensus classes. The Transaction module represents the characteristics of a transaction and provides support for both full and

lite transaction methods. The Block class defines the characteristics and procedures for generating and receiving blocks. The Consensus class is designed to facilitate the integration of different consensus protocols by implementing various consensus algorithms and fork resolution criteria in a systematic manner. This module is of paramount importance in SCM blockchain simulations. It includes classes for Transactions, Blocks, and Consensus mechanisms, allowing for the simulation of various consensus protocols relevant to SCM, such as proof of authority or PoS, which might be more applicable in a private SCM blockchain.

- **Application Module:** Responsible for the incentivization model, this module calculates and distributes rewards among participating nodes. It facilitates configuring reward structures, like block rewards, in the configuration module. In an SCM context, this module is crucial for simulating incentive mechanisms within the supply chain. It models rewards not just in terms of cryptocurrency but also in terms of SCM-relevant incentives like faster processing, improved trust, and better compliance with contracts.

6 Consensus Mechanism, Data Collection

6.1 Background and Context

The integration of blockchain and cryptocurrency into SCM has garnered considerable attention in recent literature, with influential works by Longo et al., [93], Kouhizadeh et al., [39] and Sarfaraz et al., [94] highlighting its diverse applications. Particularly, the private blockchain, as posited by Biswas et al., [95], emerges as an optimal choice for SCM, given its unique operational dynamics. This research proposes a mechanism fundamentally anchored in private blockchain technology. One of the most significant challenges in adapting blockchain to traditional SCM lies in the absence of bespoke consensus algorithms designed explicitly for SCM complexities, as noted by Xu et al. [96]. Within the blockchain paradigm, the consensus mechanism serves as the cornerstone for information validation, eliminating the need for intermediaries and ensuring data integrity and reliability [97]. Yet, prevalent blockchain technologies face critical limitations, such as inadequate transactions per second (TPS), high transaction latency, and issues with decentralization, as underscored by Zheng et al., [134]. The inefficiencies in throughput, primarily in public blockchains utilizing proof-of-work (PoW) mechanisms, primarily stem from the energy-intensive and time-consuming consensus process [175].

Given these limitations, the challenges posed by high consensus latency, limited throughput, and high energy consumption provide obstacles to conventional algorithms and prove them to be impractical and unsustainable for application in large or complex SCM systems. Given the many limitations seen in current consensus algorithms, it is imperative to develop a tailored and specialised consensus algorithm specifically built to address the common challenges encountered in SCM scenarios. This research identifies the necessity for a custom-designed consensus algorithm tailored for SCM, addressing the core issues of TPS, latency, and centralization. Current research focuses on refining mainstream consensus algorithms, with only a handful being directly relevant to SCM challenges (as explained in Chapter 2). Although the dynamic supply chain industry exhibits significant potential for growth, it still faces many challenges related to supply chain management, a gap this research aims to bridge. One such challenge is the Bullwhip Effect (BWE) in SCM, a phenomenon extensively examined by Jeong and Hong [176]. The BWE, typified by fluctuating order patterns along the supply chain, poses a significant challenge in SCM, leading to inefficiencies and increased costs. The Bullwhip Effect manifests through amplified order variances upstream in the supply chain. These

variances often result from demand forecast inaccuracies, order batching, price fluctuations, and rationing within the supply chain. Blockchain technology, with its inherent characteristics of transparency and real-time information dissemination, emerges as a potential mitigator of BWE. By enabling real-time information sharing and enhancing visibility across the supply chain, blockchain can significantly reduce the latency in information flow, which is a critical factor in the genesis of BWE. As posited by Kshetri [38], blockchain's capacity to provide a single source of truth can align the perceptions of demand among all stakeholders, thereby minimizing order forecast errors and improving efficiency.

In the preceding chapter, using a multilevel sharding technique similar to that proposed in Luu et al. [177], a novel consensus mechanism, termed the Proof-of-Efficiency (PoEf) is introduced, which amalgamates the strengths and addresses the weaknesses of existing systems. The PoEf mechanism employs a three-tier node structure separated into two networks: The first network, Authorization Network, contains one node structure which allows stakeholders to register, receive a trust level score and participate in the Stakeholders network. The second network, the Stakeholders Network, consists of two node structures (i) the first tier comprises high-authority nodes selected based on trust-level scores built upon a similar technique used in the Proof of Previous Transaction (PoPT) consensus layer, while (ii) the second tier consists of subordinate nodes organized in clusters, each led by a master node. This dual-layer approach, to be demonstrated in subsequent performance evaluations, significantly enhances blockchain efficiency by optimizing throughput, reducing latency, resolving centralization concerns, and fortifying security. The Proof-of-Efficiency (PoEf) mechanism, as proposed, stands as a potential paradigm shift in the realm of blockchain consensus algorithms, particularly tailored for SCM applications. This innovative approach aims to address the primary deficiencies observed in traditional blockchain systems, such as the limited transaction capacity and high latency, which are particularly problematic in dynamic SCM environments.

6.2 Data Collection

The accuracy of blockchain system simulations is highly dependent on the accuracy of data related to different system variables. This chapter presents a methodical strategy for gathering data, with the objective of obtaining empirically supported estimations that closely correspond to the actual distributions and dynamics of blockchain systems. The meticulous process of data collection is essential in the development of a simulation that effectively captures the many intricacies of blockchain processes. An essential component of the data-gathering method entails the thorough acquisition of data pertaining to consensus mechanisms. This comprises a range of variables that are crucial to the functionality of

blockchain, including, but not limited to, the types of consensus algorithms being utilised, their respective operational settings, and the diverse network conditions in which they operate. These variables are assessed through three (3) criteria namely (i) Transaction Throughput Efficiency, (ii) Transaction Consensus Latency and (iii) Consensus Scalability. The objective of this section is to get an understanding of the performance attributes of consensus methods and their influence on the broader blockchain network through the process of collecting and examining this data.

6.2.1 Throughput Efficiency

The metric known as throughput efficiency, sometimes represented as TPS, is a crucial measure of the operational effectiveness of a blockchain network. The calculation involves evaluating the total number of transactions that have been processed within a predetermined period. This metric functions as both an assessment of the network's present computing capabilities (i.e. how efficient the consensus mechanism is) and as a predicted gauge of its future scalability. An in-depth examination of TPS in many network settings provides crucial information into the resilience and effectiveness of the consensus algorithms being investigated. Defined as the rate of successful transaction executions per second, starting from the initial deployment time, throughput provides a lens through which the processing capacity of a system can be assessed and therefore stands as a quintessential metric in the evaluation of a system's efficiency. To calculate the average throughput, the total throughput is divided by the execution time. In the experimental series, the TPS value is measured and compared across various consensus algorithms.

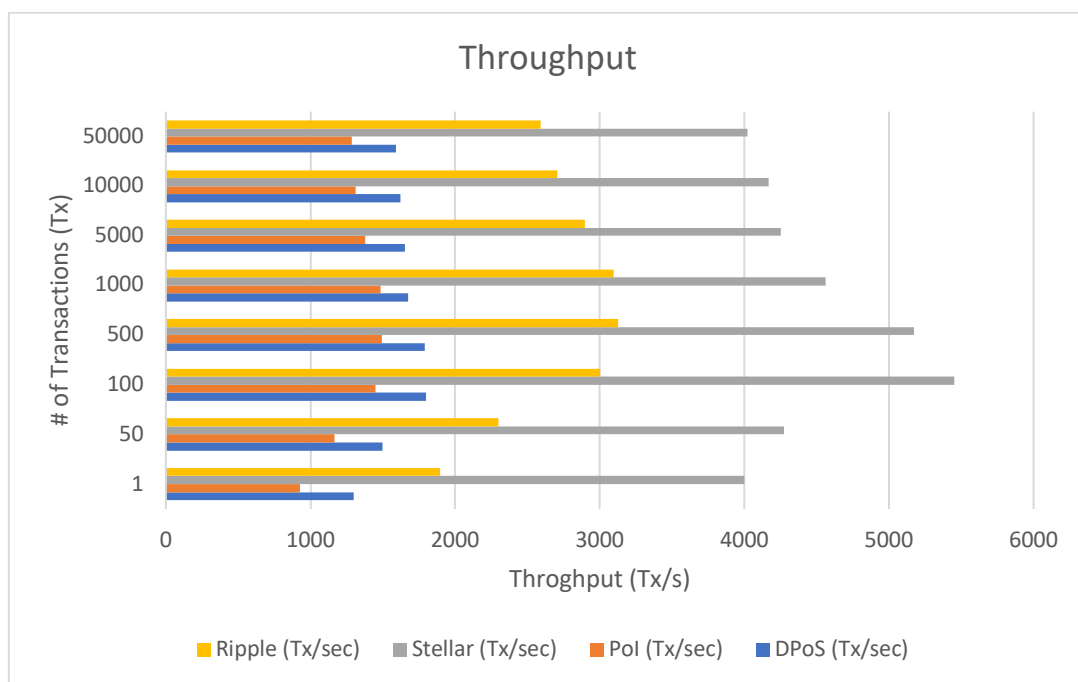


FIGURE 6.1a: Illustrating Blockchain Mechanisms throughput efficiency collected from the simulator.

The graph Figure 6.1a, illustrates the average transaction throughput for different consensus mechanisms, with higher levels of throughput, implemented in SCM. It shows that Stellar and Ripple offers the highest throughput, followed by DPoS and Pol respectively. Stellar offers the highest throughput consensus mechanism, with a throughput of over 5,000 TPS. The Stellar consensus mechanism uses an FBA algorithm, which relies on a set of trusted anchors to validate transactions. This makes Stellar a good choice for SCM cross-border payments and other applications that require high performance and trust. This mechanism allows for quick and efficient consensus without the intensive computational work found in PoW systems. Stellar, another consensus that uses the FBA has the second highest level of throughput and is specifically designed for high performance (efficiency) and scalability.

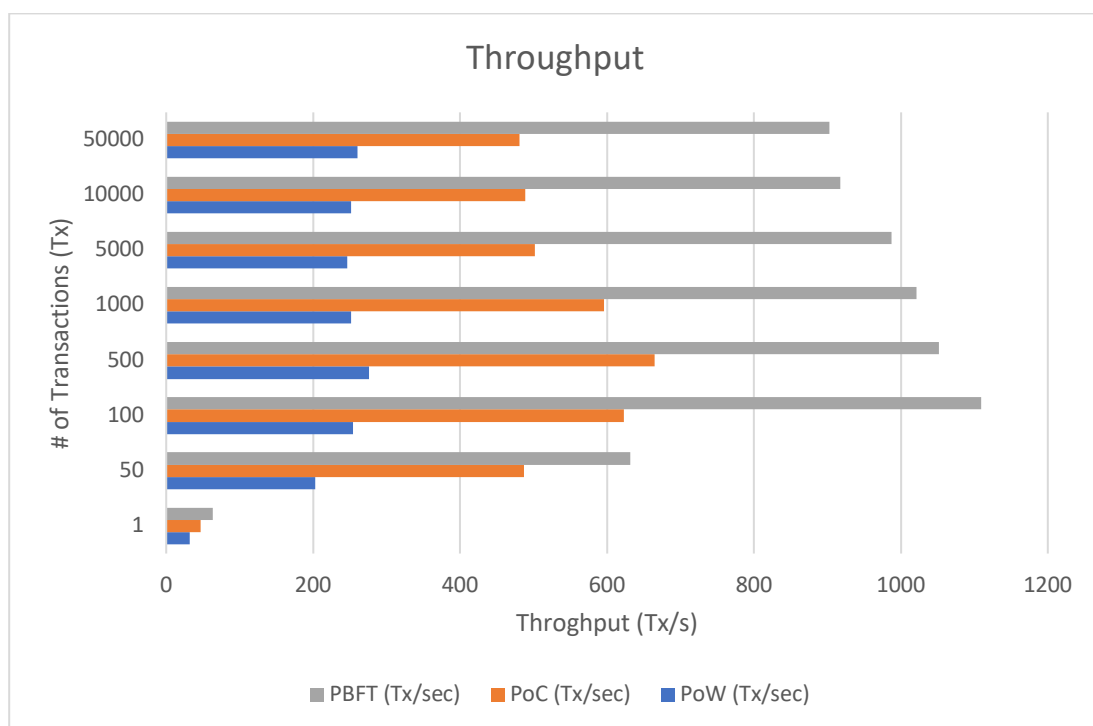


FIGURE 6.1b: Figure illustrating Blockchain Mechanisms throughput efficiency collected from the simulator.

The graph, Figure 6.1b, illustrates the average transaction throughput for different consensus mechanisms with lower throughput values. PBFT, PoC and PoW are all consensus with lower throughput values. For these values, the graph shows that PBFT offers the highest throughput with a value of approx. 1100, followed by PoC, and PoW. Because PBFT uses a Byzantine Fault Tolerance (BFT) algorithm similar to the consensus with the higher throughput levels, PBFT can tolerate up to one-third of faulty nodes making it an excellent choice for SCM applications that require medium performance and availability.

6.2.2 Consensus Latency

Consensus latency, sometimes referred to as block time or block delay, in the context of SCM, is the amount of time needed for a transaction to be approved and recorded to the blockchain, where it becomes an unchangeable and impenetrable record. The usefulness and efficiency of blockchain-based supply chain management systems are impacted by this delay, which is expressed in seconds or minutes. The algorithms that control the addition of new blocks to the blockchain, known as consensus mechanisms, are crucial in establishing consensus delay.

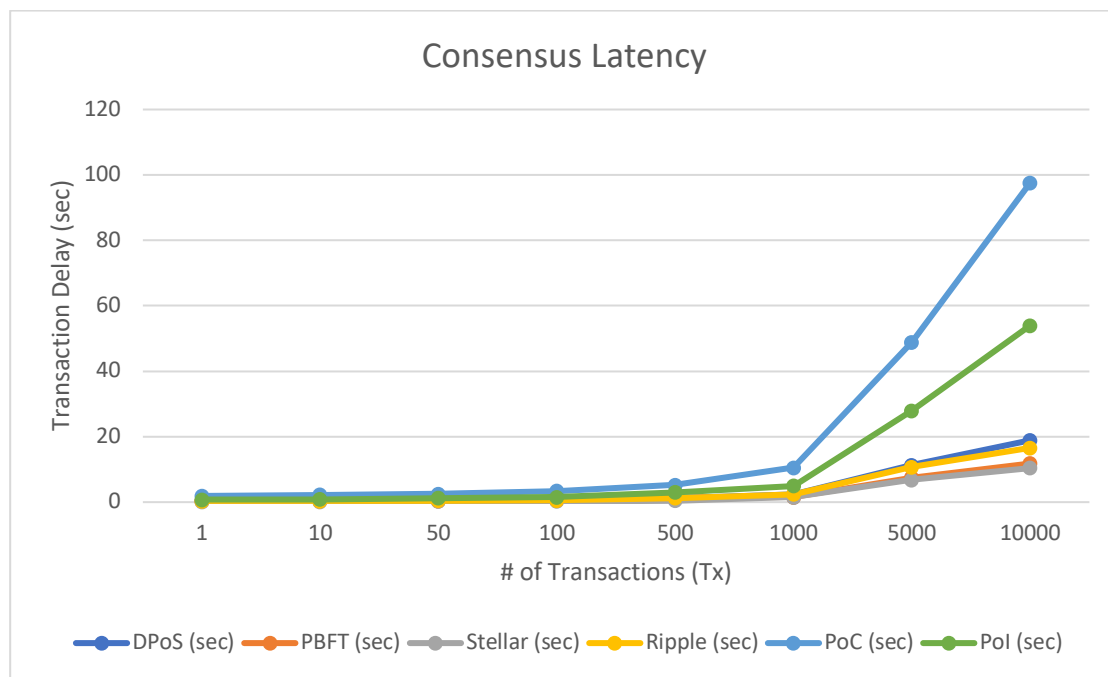


FIGURE 6.2a: Figure illustrating Blockchain Mechanisms consensus latency collected from the simulator.

The graph, Figure 6.2a, illustrates the average transaction latency for different consensus mechanisms implemented in SCM. It shows that PoC has the highest latency, followed by PoI. DPoS, Ripple, PBFT and Stellar all have low transaction delays with Stellar having the lowest latency depending on the number of transactions.

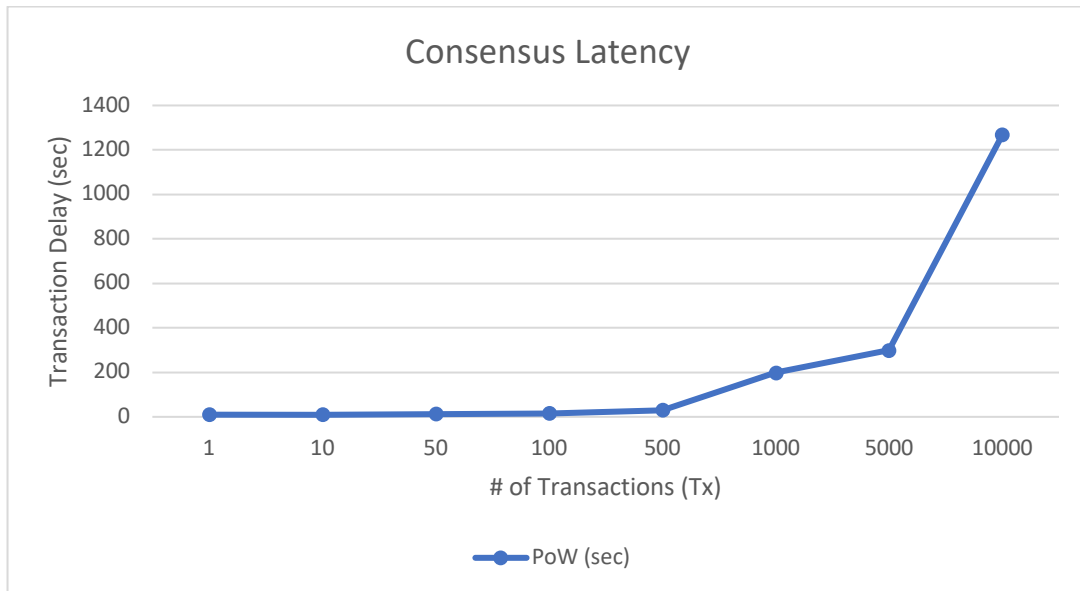


FIGURE 6.2b: Figure illustrating the PoW Mechanisms consensus latency collected from the simulator.

The graph, Figure. 6.2b, illustrates the average transaction latency for the PoW consensus mechanism implemented in SCM. PoW has the highest latency, up to 10 minutes per transaction. PoW was separated from the other consensus mechanisms because the transaction delay goes into the thousands.

6.2.3 Scalability Throughput

The "Scalability - Throughput" aspect of the research suggests how much the consensus mechanisms are maintaining a high rate of processed transactions even as the network expands. This characteristic is particularly vital for systems that anticipate high transaction volumes in SCM, where the ability to process numerous transactions rapidly is a benchmark of efficiency.

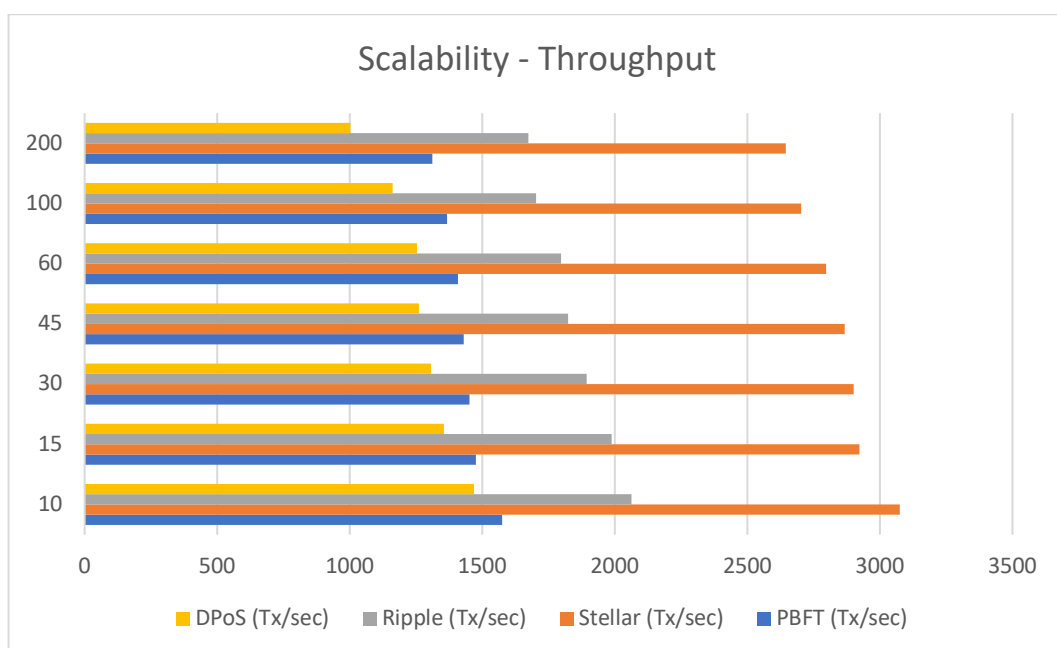


FIGURE 6.3a: Illustrating Scalability (from throughput) for various consensus mechanisms collected from the simulator.

The graph, Figure. 6.3a, illustrates the scalability of different consensus mechanisms implemented in SCM from the number of nodes available perspective. It shows that Stellar, Ripple and PBFT offer the highest scalability.

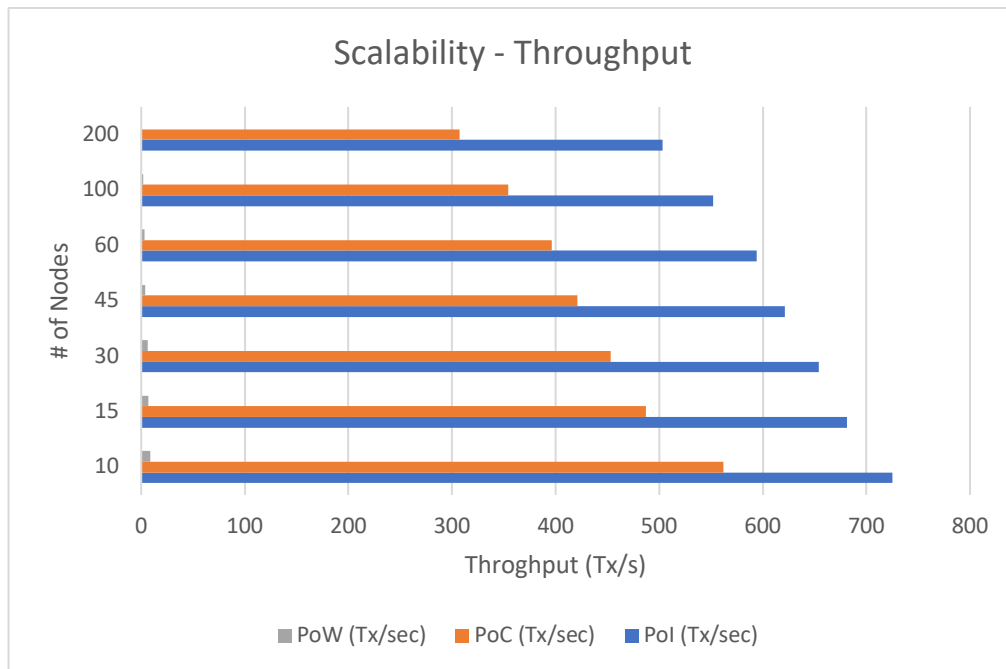


FIGURE .6.3b: Illustrating Scalability (from throughput) for various consensus mechanisms collected from the simulator.

The graph, figure 6.3b, illustrates the scalability of different consensus mechanisms implemented in SCM from the number of nodes available perspective. It shows PoW offers the lowest level of scalability. Overall, the graph shows that Stellar, PBFT, and Ripple are the best consensus mechanisms for SCM applications that require high performance and scalability. Pol is a viable choice for SCM applications that require a balance of security, performance, and scalability. DPoS is a good choice for SCM applications that require high performance and scalability, but it may be susceptible to centralization. PoC is a good choice for SCM applications that require energy efficiency and scalability, but it may be less secure than other consensus mechanisms. PoW is not a good choice for SCM applications that require high performance or scalability.

6.2.4 Scalability Latency

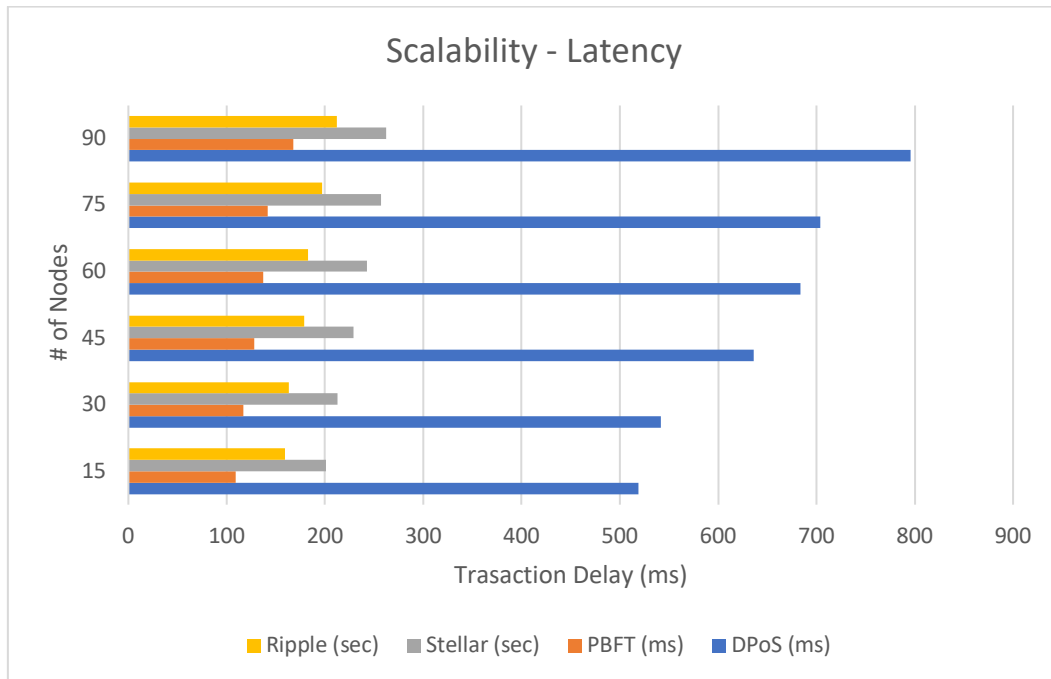


FIGURE 6.4a: Illustrating Consensus scalability (from latency) for various consensus mechanisms collected from the simulator.

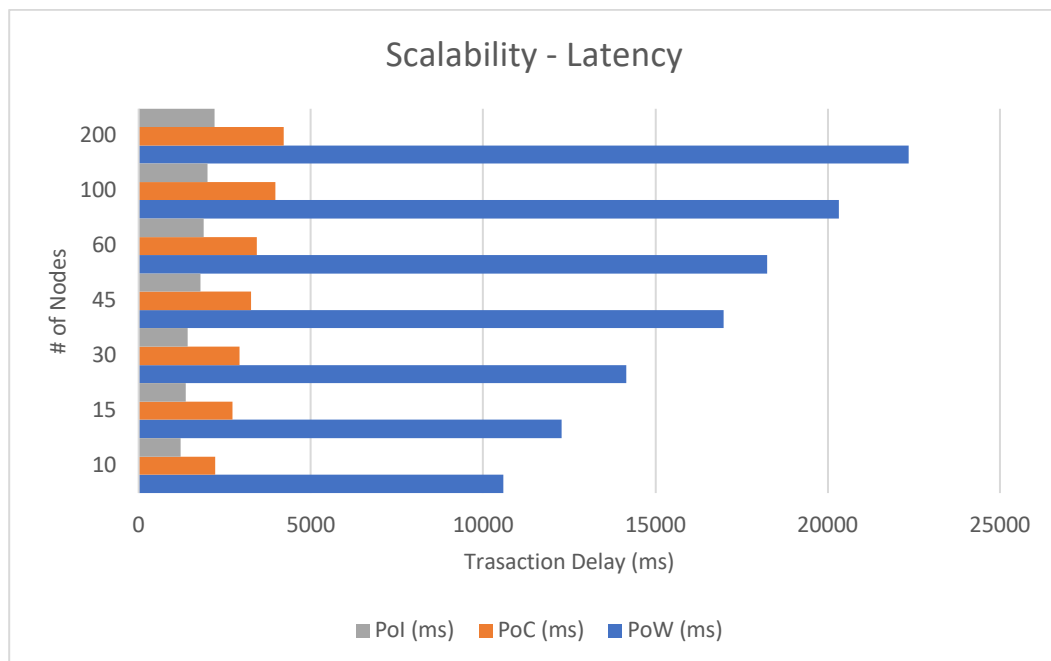


FIGURE 6.4b: Illustrating Consensus scalability (from latency) for various consensus mechanisms collected from the simulator.

The graphs, figure 6.4a and 6.4b, illustrate the scalability of various consensus mechanisms used in SCM from the standpoint of the number of nodes available. Lower transaction delays demonstrate that there is a higher potential for scalability. Each consensus mechanism reviewed here contributes distinct strengths and challenges to SCM. While PoW offers high security, its efficiency limitations reduce its suitability for certain SCM applications. Alternatives like DPoS, PoC, and PoI provide energy-efficient solutions, though

with concerns around security and centralization. PBFT is highly secure but less scalable, whereas SCP and RCPA offer a balanced mix of security, efficiency, and scalability, adaptable for various SCM requirements. Selecting the most suitable consensus mechanism for SCM hinges on specific criteria such as transaction volume, processing speed, security needs, and the scale of the supply chain network. This evaluation aims to guide stakeholders in aligning blockchain technology with the unique operational demands and strategic goals of SCM systems. The graphs demonstrate that the most scalable solutions are provided by PBFT, Stellar, and Ripple. DPoS is also relatively good for building scalable solutions but PoI, PoC, and PoW illustrate less potential for scalable solutions.

7 PoEf, an enhanced Blockchain-Coordinated SCM Architecture

In the realm of SCM, the implementation of the Proof-of-Efficiency (PoEf) mechanism is anticipated to serve as a catalyst for enhancing the core tenets of efficiency, security, and scalability within blockchain frameworks. PoEf's introduction is projected to precipitate the broader assimilation of blockchain technology into SCM practices, potentially leading to significant strides in the areas of transparency, traceability, and operational excellence. The mechanism's inherent flexibility and performance attributes are also expected to drive innovation within the broader spectrum of blockchain technologies, transcending the traditional boundaries of SCM.

This chapter delineates the integration of the Proof-of-Efficiency (PoEf) mechanism into the SCM infrastructure, particularly targeting the mitigation of the BWE. The BWE is a phenomenon that magnifies fluctuations in demand throughout the supply chain. The methodology for PoEf is founded upon a tripartite framework: (i) an authorization and authentication protocol that leverages blockchain technology to verify the credibility of suppliers and manufacturers, thereby ensuring that only trustworthy participants are involved in the supply chain; (ii) a knowledge-sharing infrastructure that is specifically designed to address the intricacies of supply chain management (SCM) operations, with the goal of minimising the BWE by improving the flow of information and coordination; and (iii) a threat model that thoroughly evaluates and prepares for various adversarial behaviours and their potential consequences.

Within the established algorithm, stakeholders first undergo an authorization procedure within the 'Authorization Network'. Successfully completing the authorization procedure, stakeholders are provided with cryptographic keys, namely a certificate containing a pair of public and private keys that would enable them to actively participate 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. The approach described in this thesis functions on many levels, namely the entrance barrier into the blockchain-driven SCM ecosystem, referred to as the Authorization Network, and the functional operationalization inside the SCM ecosystem, known as the Stakeholder Network.

7.1 Authorization Network

The Authorization network serves as the preliminary assessment stage for stakeholders seeking entry into the network. This phase entails a thorough verification of potential participants, utilizing 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.

Assumptions: The model assumes: (i) stakeholders (manufacturers and merchants) have been operating for a few years and are not new entrants to the market.

7.1.1 Stages of the SCM Authorization Network

Underpinning the authorization network, as illustrated in Figure 7.1, is the presumption that stakeholders, specifically manufacturers and merchants, possess established market tenure. The network's operational ethos is akin to the 'DelivChain' model, a blockchain-based novel framework for SCM developed by Y. Qian and Meng [157]. DelivChain advocates for a consortium blockchain environment, wherein trust is not a prerequisite for transactional engagement yet high-level security is ensured, as participants would need to register, based on previous experience through a registration contract, as illustrated in Figure 7.2. This trusted platform caters exclusively to authenticated participants across communicative organizations. The proposed framework for the Authorization Network is as follows:

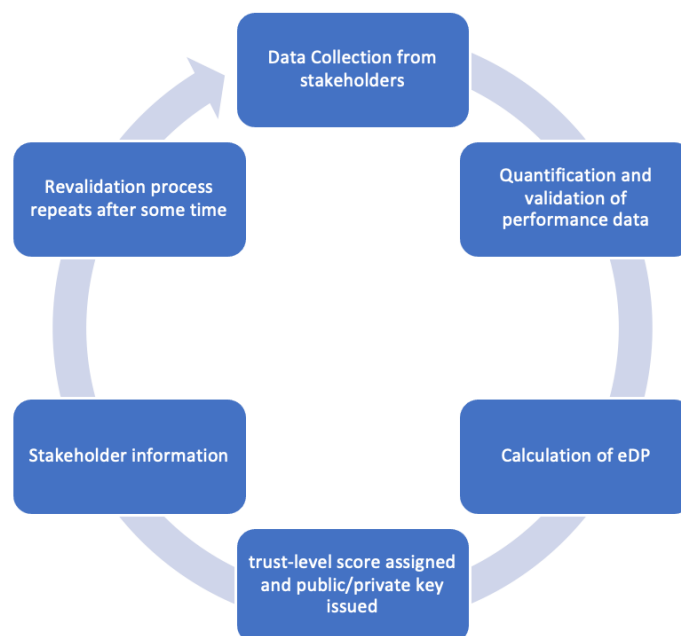


FIGURE 7.1: Figure illustrating the flow diagram proposed Authorization Network for this research.

- i. Critical data identification and collection: - Raw data is collected from potential suppliers. The raw data comes from both production and delivery happening in the supply chain.
- ii. Quantification of performance data. Raw data collected from the previous stage is checked and validated. The smart contract in this stage would convert the data into quantitative values with different weighting based on experience, turnover and customer base. These values are used in benchmarking an organization's performance of production and issuing a reputation-level score, R_l . For example, if the data implies manufacturing delays of one supplier, this will be converted to a risk percentage value on the expected production capability of that supplier, ultimately resulting in a lower reputation-level score.
- iii. Calculation of estimated delivery performance (eDP) (e. In this stage, the smart contract will use the supply chain assessment model On-Time In-Full (OTIF), to put all the quantitative values obtained in the previous stages into consideration 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. It is a percentage value used for the delivery key performance index (KPI) assessment of an organization. The formula of OTIF calculation could be presented as

$$OTIF = \frac{\text{number of deliveries OTIF}}{\text{total number of deliveries}} \times 100$$

- 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 "Authorization SCM blockchain ledger". The revalidation process happens on a yearly basis.

Registration Contract
Require { The stakeholder's password pw_S , The stakeholder's data D_S , The eDP value of function $Register(pw_S, P_B(D_S))$, } Execute { Set Stakeholder's Private Key $PK_S = Register(pw_S, P_B(D_S))$; } Output: Stakeholder's Private Key PK_S Stakeholder's Reputation ID R_l

FIGURE 7.2: Figure illustrating the proposed Registration Contract that is the Authorization Network algorithm for this research.

7.2 Stakeholder Network

The Stakeholder network, as illustrated in Fig. 7.3, is the actual network that facilitate SCM transactions among stakeholders. This phase entails two layers of confirmed participants (validator nodes and subordinate nodes) initiating and fulfilling transactions utilizing blockchain's inherent capabilities. Stakeholders would need to use their unique cryptographic keys and assigned an initial reputation score, from the authorization network to join the stakeholder network. This framework enables a transparent and efficient supply chain management system where all actions are recorded and validated on the blockchain, contributing to enhanced accountability and data integrity.

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 policy. This policy 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.

7.2.1 Stages of the SCM Stakeholder Network.

The proposed framework for the Stakeholder Network is as follows:

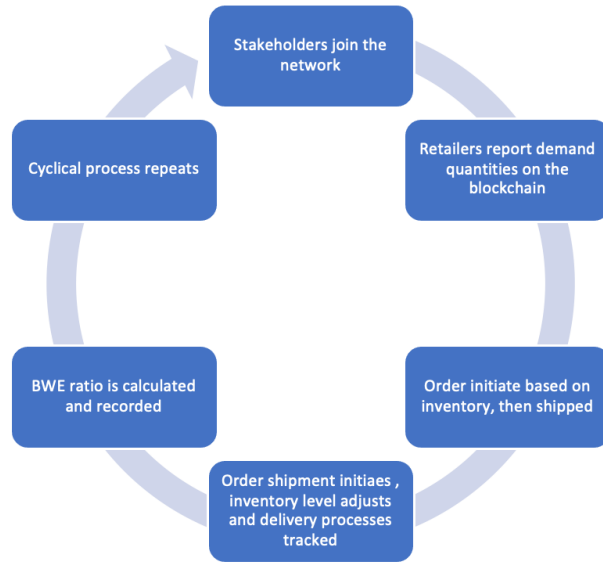


FIGURE 7.3: Figure illustrating the flow diagram of the proposed Stakeholder Network for this research.

- i. Stakeholders are authenticated and allowed to join the network using their keys for participation. As seen in Fig. 7.4, if the users are not authenticated then they will not be allowed to join the network.

Stakeholder Authentication Contract
Require { The stakeholder's password pw_s , Stakeholder's Private Key PK_s Stakeholder's Reputation ID R_l The eDP value of function $Register(pw_s, P_B(D_s))$, } Execute { If (Stakeholder's Private Key, $PK_s ==$ $Register(pw_s, P_B(D_s))$ { Allow the user to access the blockchain; $T_x = 1$ } else { Forbid the user to access the blockchain; $T_x = 0$ } } Output: T_x

FIGURE 7.4: Figure illustrating the Authentication Contract as a part of the Stakeholder's Network algorithm.

- 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 is initiated once inventory is available. If the items are not available, order placement at the upper echelons is contingent on inventory levels relative to reorder points, with all transactional details recorded on the blockchain.
- iv. Order shipment and delivery processes are meticulously tracked, adjusting inventory levels accordingly. Continuous inventory analysis ensures alignment with reorder thresholds.
- v. Based on the delivery times of scanned inventory as they move along the supply chain, discrepancies in lead times are recorded and updated in the system.
- 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.

In the proposed blockchain network, a group of stakeholders denoted as $S = \{S_1, S_2 \dots S_n\}$. 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:

7.3 Design of the proposed PoEf algorithm

DPoS mechanism, while advantageous for scalability, inherently compromises the decentralized principle by concentrating authority within a select user base. This centralization of control poses a higher risk of network attacks due to the smaller number of actors involved in network maintenance. Similarly, other consensus methodologies like Ripple, PoC, and Pol grapple with centralization 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.

In the construction of the PoEf algorithm, these considerations have been paramount. As illustrated in Figure 7.5, the algorithm is delineated across three primary phases: (i) registration and verification (S_R), which leverages a reputation-based algorithm 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) , a node must hold a high trust-level score, substantiate its genuine identity and consent to disclose this identity across the network. Following registration and verification, the algorithm employs a reputation system to evaluate the node's credibility. Nodes that abstain from staking their identity, or nodes with a lower trust level score are relegated to a tertiary pool known as (S_L) . This tiered node selection strategy enhances the efficiency of the block addition process, allowing for immediate block incorporation post-verification. The overarching structure of the algorithm, depicted in Fig. 7.5, showcases a branched node system: (S_R) , (S_H) and (S_L) all operating in tandem for block generations. The (S_L) nodes are tasked with producing micro blocks, which are then dispatched to (S_H) nodes. Upon receipt, (S_H) nodes are responsible for validating these micro blocks and consolidating them into a singular, verifiable block.

At the crux of the PoEf algorithm is the nuanced and efficient selection of consensus nodes that function concurrently. The selection process is randomized, factoring in nodes' reputation scores, their commitment to transparency of identity, and a random selection algorithm that assembles a subset of nodes into clusters. This ensures a diverse and decentralized selection process, which is pivotal for maintaining network security and integrity. In essence, the PoEf algorithm seeks to strike a balance between decentralization and scalability while ensuring a secure, transparent, and efficient consensus process suitable for the demands of SCM blockchain systems. By fostering an equitable and dynamic consensus environment, the PoEf algorithm aims to fortify the blockchain against a multitude of potential security threats, thereby supporting a resilient SCM infrastructure.

7.3.1 Consensus node selection

In the field of blockchain architecture, a peer-to-peer network structure is commonly referred to as n , which signifies a set of nodes that are essential for the functioning of the network. The proposed approach for the “consensus block” introduces a categorization of n into two distinct tiers: (S_H) and (S_L) . The branching plays a crucial role in maintaining the operating efficiency and security of the blockchain, hence establishing a resilient and adaptable consensus process. The allocation of nodes into the layers of (S_H) and (S_L) requires a complex and subtle methodology. The algorithm effectively combines a dual-method approach by using a random number generation mechanism alongside a node reputation score system. The implementation of this dual approach plays a crucial role in attaining a well-balanced and merit-based distribution of nodes, which is essential for maintaining the integrity of the consensus process within the blockchain. Within this particular context, the method of generating random numbers of functions as a mechanism to incorporate stochasticity into the process of selecting nodes. This serves the purpose of

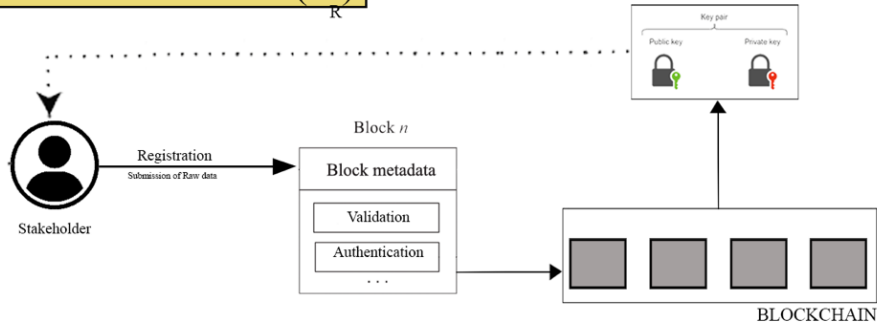
mitigating any potential systemic biases and guaranteeing a varied representation of nodes throughout the network. The inclusion of randomization plays a vital role in upholding the decentralised principles of blockchain technology, as it effectively prevents the emergence of centralization that could result from deterministic node selection methods.

Simultaneously, the reputation score of the node assumes a crucial role in this process of selection. The reputation score method assesses nodes by considering their past performance, dependability, and overall impact on the network. Nodes that possess better reputation scores are commonly preferred for inclusion in the (S_H) layer, where they undertake crucial responsibilities in upholding network consensus and validating transactions. The implementation of a merit-based allocation system not only serves to strengthen the security of the network but also fosters a sense of trust among its participants.

The integration of both stochasticity and reputation-based scoring mechanisms ensures a comprehensive and fair methodology for the selection of consensus nodes. The system effectively maintains a delicate balance between the need for unpredictability to discourage manipulation attempts, and the necessity to recognise and reward nodes that are dependable and demonstrate remarkable performance. An organised methodology for choosing nodes is essential in sophisticated blockchain networks, especially in situations where high-value transactions are handled and stringent security protocols are required. This phenomenon is commonly noticed in supply SCM applications. The suggested algorithm for selecting consensus nodes demonstrates the dynamic character of blockchain technology, where the strategic organisation of nodes is crucial for improving network stability and efficiency. The statement showcases an understanding of the complex demands of modern blockchain networks, skilfully integrating randomness and merit-based principles to create a robust and reliable consensus system.

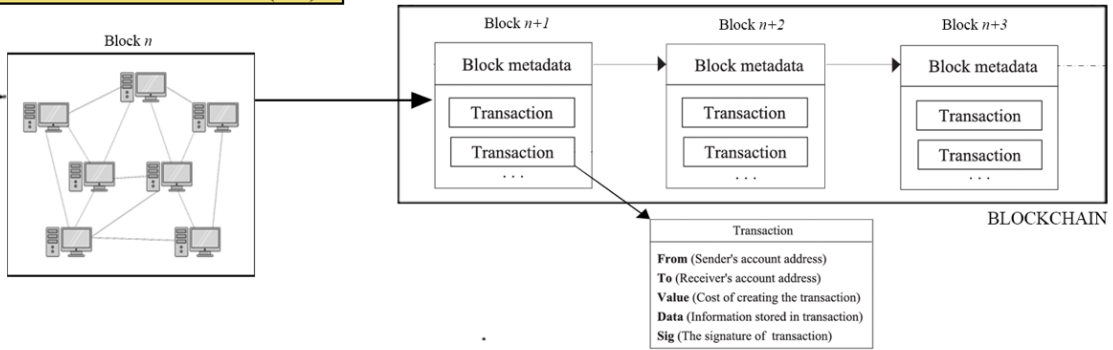
AUTHENTICATION NETWORK

Authentication Nodes (S_A)



STAKEHOLDER NETWORK

Validator Nodes (S_H)



Subordinate Nodes (S_I)

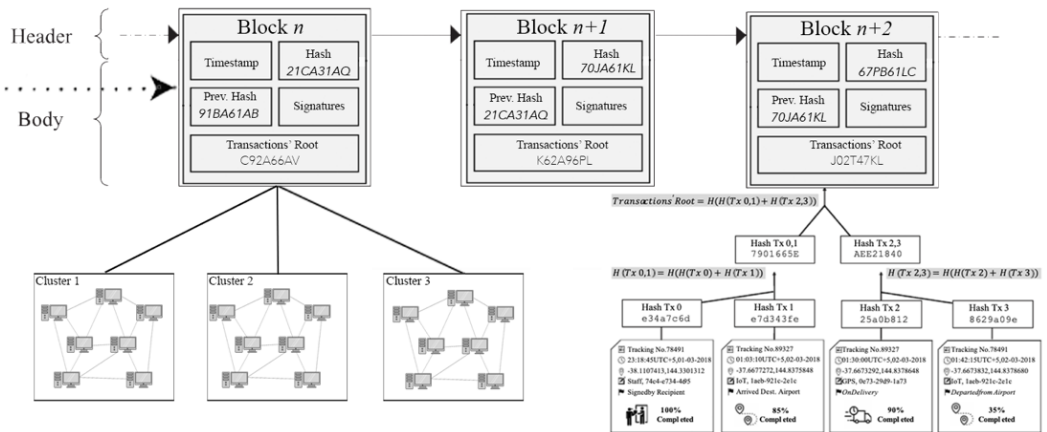


FIGURE 7.5: Figure illustrating the proposed Consensus Mechanism, PoEf

7.3.2 Transactions broadcasting

The Proof-of-Efficiency (PoEf) algorithm emerges as a paradigmatic shift toward a decentralized trust mechanism, pivotal for transaction validation and broadcast. As illustrated in Figure 7.5, the consensus process engenders a dual-role ecosystem, where stakeholders are segregated into “providers” -givers of a service and “raters”- receivers of a service. The provider, by virtue of their role, authenticates service data with their private key, thereby embedding security into the data transmission pipeline. In juxtaposition, the rater evaluates the service rendered and appends a reputation score, denoted by R_l , to the transaction, as illustrated in Figure 7.6, which is then promulgated across the network with digital signatures.

Transaction Contract
Require { The stakeholder's Address Add_{S_l} , The stakeholder's Address Add_{S_H} , Stakeholder's Private Key PK_{S_H} , Stakeholder's Private Key PK_{S_l} , Stakeholder's Reputation ID $R_{l(S_H)}$, Stakeholder's Reputation ID $R_{l(S_l)}$, The parameter $Data, D$, } Execute { Set From = Add_{S_l} , Set To = Add_{S_H} , Set Value = <i>Service expense</i> Set Data = $P_1(PK_{S_H}) \parallel P_1(D_{S_H}) \parallel P_1(D_{S_l}) \parallel P_1(PK_{S_l}) \parallel H \parallel$ <i>Tx</i> Output: $From \parallel To \parallel Value \parallel Data$;

FIGURE 7.6: Figure illustrating the Transaction Contract that happens inside of the Stakeholder's Network algorithm.

The reputation score, R_l , is quantitatively confined within the interval (0, 1). This metric affords a granular feedback mechanism, where a score of '1' connotes optimal satisfaction, and '0' denotes the antithesis of service satisfaction. In the PoEf construct, validator nodes, (S_H) , are discerned not merely by their cumulative reputation, a concept propounded by Gai et al., [178], but also by their validated identities, fostering a verifiable digital ecosystem. The integration of nascent stakeholders into the network, devoid of prior reputational metrics, invokes the assignation of an inaugural score, (R_0) , which predicates the minimal reputation requisite for engaging with the SCM network. Concurrently, an honesty parameter, H ,

is ascribed the value of '1' to signify initial trustworthiness, which is susceptible to devaluation of '0' in the event of misconduct, such as contradictory communications or transaction discrepancies.

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

As illustrated in the equation above, the aggregation of a stakeholder's reputation $R(\Delta_T)$ at a temporal juncture Δ_T is the synthesis of their primordial reputation $R_S(t_0)$ and the extant reputation $R_S(t_i)$. This composite score is dynamically recalibrated at intervals established by network governance, underscoring the imperative of sustained and ethical participation for reputational enhancement. In order to establish a strong reputation score, it is imperative for a stakeholder to maintain a consistent presence inside the system and adhere to principles of honesty and integrity.

Algorithm 1 (PLAINTEXT)

```

1: procedure ConsensusNodeSelection(NodesN, AuthThreshold)
2:   AuthorizedNodeList = [0] * len(NodesN)
3:   ClusterList = [0] * len(NodesN)
4:   MasterNodeList = [0] * len(NodesN)
5:   for i in range(len(NodesN)):
6:     AuthStatus = AuthenticateNode(NodesN[i])
7:     if AuthStatus == True and GetReputationScore(NodesN[i]) > AuthThreshold:
8:       AuthorizedNodeList[i] = NodesN[i]
9:     else:
10:      ClusterList[i] = SelectRandomNode(NodesN, AuthorizedNodeList)
11:    end if
12:  end for
13:  for i in range(len(ClusterList)):
14:    if len(ClusterList[i]) > 0:
15:      MasterNodeList[i] = SelectRandomNode(ClusterList[i])
16:    end if
17:  end for
18: end procedure

```

FIGURE 7.7: Figure illustrating the proposed Consensus Mechanism Algorithm 1 in plaintext.

Algorithm 1 (PYTHON)

```

1  import ConsensusNodeSelection
2
3  def authenticate_node(node):
4      # Placeholder for node authentication logic
5      return True if node['auth_status'] else False
6
7  def get_reputation_score(node):
8      # Placeholder for reputation score retrieval logic
9      return node['reputation_score']
10
11 def select_random_node(exclude_list):
12     # Select a random node that's not in the exclude_list
13     global nodes
14     return ConsensusNodeSelection.choice([node for node in nodes if node not in exclude_list])
15
16 def consensus_node_selection(nodes, auth_threshold):
17     authorized_node_list = [0] * len(nodes)
18     cluster_list = [0] * len(nodes)
19     master_node_list = [0] * len(nodes)
20
21     for i, node in enumerate(nodes):
22         if authenticate_node(node) and get_reputation_score(node) > auth_threshold:
23             authorized_node_list[i] = node
24         else:
25             cluster_list[i] = select_random_node(authorized_node_list)
26
27     for i, cluster in enumerate(cluster_list):
28         if cluster:
29             master_node_list[i] = select_random_node(cluster)
30
31     return master_node_list
32
33 # Example usage
34 nodes = [{'auth_status': True, 'reputation_score': 90}, {'auth_status': False, 'reputation_score': 70}, ...] # ... represents other nodes
35 auth_threshold = 75
36 master_nodes = consensus_node_selection(nodes, auth_threshold)

```

FIGURE 7.8: Figure illustrating the proposed Consensus Mechanism Algorithm 1 in Python.

The heart of the PoEf algorithm lies in its systematic node selection process, as described in Algorithm 1 (Figures 7.7 and 7.8). The aforementioned procedure methodically promotes nodes with prominent reputation scores to the S_H tier, so establishing the network's authority and scalability. Nodes that are not chosen for participation in S_H undergo a systematic process of consolidation, wherein they are grouped together into clusters. Within these clusters, a master node is autonomously elected based on its reputation, and this master node is responsible for overseeing the validation of transactions and the generation of micro blocks. In the event of a primary validator experiencing a failure, a node with a higher reputational score easily assumes the position, thereby guaranteeing continuous network functionality. It is crucial to acknowledge the dynamic nature of node responsibilities inside the PoEf framework. Nodes undergo role transitions in reaction to fluctuations in their reputation scores, thereby exemplifying a dynamic and merit-based infrastructure. The allocation of roles in the PoEf algorithm is designed to maintain agility and reflect the varying levels of trustworthiness across nodes. This allocation also strengthens the integrity of the blockchain network, particularly in the context of supply chain management operations. The PoEf algorithm therefore serves as a notable example of innovation within the realm of blockchain technology for supply chain management. It effectively establishes a consensus mechanism that prioritises security, transparency, and efficiency. The statement demonstrates a flexible strategy that aligns with a changing environment, where trust plays a crucial role in establishing strong supply chain management blockchain networks.

7.3.3 Consensus Block confirmation

The process of block confirmation within blockchain systems is a critical component for ensuring transaction integrity and network consensus. The following steps provide a detailed and scholarly expansion of the block confirmation mechanism:

- **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.
- **Cluster Node Verification:** Upon receiving the transaction, the cluster nodes first authenticate P_k and C_t . Successful verification leads to the transaction, now endorsed with the cluster node's private key $(T_x P_k, C_t)_{CPk}$ being relayed to the cluster's master node.
- **Master Node Validation:** The master node in each cluster is tasked with a critical validation process. The verification of the transaction is required to be conducted by this node. 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 $((T_x P_k, C_t)_{CPk})_M$.
- **Transaction Pooling:** Verified transactions by the Master node are pooled in a waiting area. Once a predetermined threshold of transactions is reached in the pool, the master node packages them into a smaller block, denoted as $((S_b)_{Tx})_M$, and broadcasts it to its peer nodes.
- **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.
- **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.
- **Continuous Transaction Processing:** Remaining transactions in the pool, not packed in the current small block, are prioritized in the next consensus round.
- **Validation by Higher Authority Nodes:** Nodes in the higher authority layer are responsible for validating the signatures and transactions within the received small block.
- **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.
- **Block Formation:** Successfully verified small blocks are sequenced chronologically. The compilation of a minimum of 10 small blocks leads to the formation of a larger block, which is then appended to the blockchain.

The module for achieving consensus on block verification, as detailed in Algorithm 2 (Figures 7.9 and 7.10), emphasizes the collective responsibility of nodes S_n in the network. By distributing transaction verification across all nodes, the proposed protocol not only boosts system throughput but also alleviates the computational burden traditionally placed on miners. In essence, this refined block confirmation protocol is designed to enhance the efficiency and reliability of transaction validation within blockchain networks, particularly in the context of Supply Chain Management. It ensures a democratic and distributed process of consensus, pivotal in maintaining the integrity and fluidity of the blockchain.

Algorithm 2 (PLAINTEXT)

```

1: procedure ReachConsensus(MasterNodeList, Author
1 1: procedure ReachConsensus(MasterNodeList, AuthorizedNodes)
2 2:   SmallBlockList = [0] * len(SmallBlock)
3 3:   AuthorizedSmallBlockList = [0] * len(SmallBlock)
4 4:   Blockchain = []
5 5:   CurrentBlock = None
6 6:   for i, masterNode in enumerate(MasterNodeList):
7 7:     SmallBlockList[i] = GenerateSmallBlock(masterNode)
8 8:     if AuthenticateProcess(SmallBlockList[i]):
9 9:       AuthorizedSmallBlockList[i] = SmallBlockList[i]
10 10:    if all(AuthenticateProcess(smallBlock) for smallBlock in
AuthorizedSmallBlockList):
11 11:      CurrentBlock = CombineSmallBlocks(AuthorizedSmallBlockList)
12 12:      Blockchain.append(CurrentBlock)
13 13:    end if
14 14:  end if
15 15: end for
16 16: end procedure
17

```

FIGURE 7.9: Figure illustrating the proposed Consensus Mechanism Algorithm 2 in plaintext.

Algorithm 2 (PYTHON)

```

PoEfBlockVerification.py x
1 #BlockGeneration
2 def generate_small_block(node):
3     # Placeholder for small block generation logic
4     return node['small_block']
5
6 def authenticate_process(block):
7     # Placeholder for block authentication logic
8     return True if block['is_valid'] else False
9
10 def combine_small_blocks(small_blocks):
11     # Placeholder for combining small blocks into a full block
12     return {'combined_block': small_blocks}
13
14 def reach_consensus(master_node_list):
15     small_block_list = [0] * len(master_node_list)
16     authorized_small_block_list = [0] * len(master_node_list)
17     blockchain = []
18
19     for i, master_node in enumerate(master_node_list):
20         small_block = generate_small_block(master_node)
21         if authenticate_process(small_block):
22             authorized_small_block_list[i] = small_block
23
24         if all(authenticate_process(small_block) for small_block in authorized_small_block_list if small_block):
25             current_block = combine_small_blocks(authorized_small_block_list)
26             blockchain.append(current_block)
27
28     return blockchain
29
30 # Example usage
31 master_node_list = [{'small_block': {'is_valid': True}}, {'small_block': {'is_valid': False}}, ...] # ... represents other nodes
32 blockchain = reach_consensus(master_node_list)

```

FIGURE 7.10: Figure illustrating the proposed Consensus Mechanism Algorithm 2 in Python.

7.4 The architecture of the PoEf Consensus Mechanism

The PoEf mechanism, central to this research, introduces a novel consensus approach tailored to bolster the throughput and scalability of blockchain in SCM. A blockchain's consensus algorithm is crucial, significantly impacting its security and efficiency. PoEf's design, featuring a dual-layer architecture, facilitates rapid consensus and scalability. By distributing mining operations across nodes, this layered approach reduces the workload on individual nodes, thereby enhancing consensus efficiency. The introduction of the PoEf mechanism within a blockchain-coordinated SCM architecture presents a paradigm shift in SCM operations. Its impact on enhancing scalability, security, and efficiency is poised to revolutionize SCM practices, aligning closely with the research objectives. This investigation not only scrutinizes existing methodologies at the intersection of blockchain, cybersecurity, and SCM but also innovates a distinct consensus mechanism that is finely attuned to the unique demands of SCM. Thus, this research contributes significantly to the discourse on leveraging blockchain technology to optimize SCM security and operational efficiency.

7.4.1 Network Model

This thesis argues that the network functions with partial synchronisation, which is consistent with the fundamental ideas outlined by Nakamoto in the influential Bitcoin whitepaper. In this network, there is a group of nodes that are authenticated and communicate with each other in a partially synchronous manner. They work together to maintain an agreement on updates to the system's state. The network is designed to guarantee strong connectivity between legitimate nodes, with minimal propagation delay and a well-defined bounded latency. This ensures that all state updates are reliably shared within this specified delay.

The system is designed to accommodate Byzantine faults, acknowledging the possibility that certain nodes may act maliciously or erratically, reflecting the real-world applicability of the proposed 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 as long as 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 further acknowledges the contributions of [140], whose rigorous analytical work provides the proofs and validations that bolster the proposed network's design.

against Byzantine faults. Their findings underpin the network's security model and are instrumental in the proof of concept for the proposed blockchain's operational framework. Hence, the system will not only draw upon established theoretical models but also incorporate previously simulated research to ensure a resilient, secure, and efficient blockchain network tailored for contemporary SCM challenges.

7.4.2 Security and Authenticity Model

The proposed security model of the Proof-of-Efficiency (PoEf) consensus algorithm is thoroughly scrutinised to establish its resilience within the context of the SCM blockchain network. The algorithm undergoes scrutiny to ensure its safety, which involves maintaining the integrity of the system against forks. Additionally, its authenticity is examined to guarantee the continual addition of blocks to the chain. The underlying assumption of this thesis is that the PoEf algorithm ensures a state of utmost security by disallowing forks, provided that the number of Byzantine nodes remains below a certain threshold denoted as f . This aspect has significant importance, particularly when no presumptions are made regarding the synchronisation of networks, hence emphasising the algorithm's robustness. In addition to incorporating the algorithm within the SCM framework, the research argues that the PoEf achieves authenticity in a partly synchronous network, which accurately represents the operating conditions of SCM. This particular attribute guarantees that, notwithstanding any network delays, fresh blocks will ultimately be added to the blockchain, hence supporting ongoing SCM operations.

In the proposed blockchain network, a group of stakeholders denoted as $S = \{S_1, S_2 \dots S_n\}$. 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:

- (i) From a security perspective, the blockchain ensures integrity. This means that there is an assurance that a transaction (denoted as T_x) is deemed genuine and comes only from an acknowledged and authenticated stakeholder (S_n) upon its formal inclusion in the blockchain. Furthermore, it is required that every transaction be documented just once on the blockchain, hence mitigating any occurrence of duplicate transactions. This is an essential feature for SCM operations where unique transactions (e.g., orders, shipments) are unchallengeable.
- (ii) From a security perspective, 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 critical for the immutable record-keeping required in SCM.

- (iii) From a security perspective, 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 mechanism guarantees consistency and consensus within the network with respect to the transactions documented in a certain block, thus maintaining consistency and reliability in the SCM ledger.
- (iv) From an authenticity perspective, central to SCM operations, the research delineates that for every transaction initiated by a stakeholder, if T_x is valid, it will eventually be committed by all stakeholder, assuring transaction throughput and the avoidance of system deadlock.

This security model is crucial in the SCM context as it not only ensures the proper functioning of the blockchain but also instils confidence among SCM stakeholders that the system will remain reliable and efficient despite adversarial attempts to disrupt it. The rigorous proofs of security provided within this research offer a concrete foundation for the implementation of the PoEf consensus algorithm, ensuring that it stands resilient against potential security threats while maintaining a high degree of throughput and scalability necessary for modern SCM solutions.

7.4.2.1 Breaking down the security of PoEf

The Proof-of-Efficiency (PoEf) consensus algorithm is meticulously crafted to guarantee network security, especially in situations where the communication network exhibits sluggishness and unreliability. The fundamental premise of its architecture is that when a truthful node, denoted as S , effectively adds a block to the blockchain, no other truthful nodes in the network will attach a competing block for the same round. The PoEf model's level of reliability and safety is highly dependent on the integrity and effectiveness of the Proof of Reputation (PoR) protocol, similar to that specified by Aluko and Kolonin [179]. The design of PoEf ensures network safety by preserving the trustworthiness and consistency of the blockchain, even in the face of potential obstacles arising from the performance of the communication network. The effectiveness and reliability of the PoEf consensus mechanism are intrinsically linked to the resilience of its underlying reputation-based protocol. Once a reputable node S , has published a block to the blockchain, no additional honest nodes S will be able to add a different block for that round.

- **Suggestion 1 (Security of PoEf):**

To explain the security 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_l , 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 safety and robustness in the consensus mechanism of 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:

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

where $R(\Delta_T)$ signifies the reputation score of individual stakeholders and $|S|$ represents the total number of stakeholders (validators). Ultimately assuming that an attacker is incapable of compromising the network's safety unless the conditions are not satisfied, establishing a robust safeguard against threats to the network's consensus integrity.

7.4.2.2 Breaking down the authenticity of PoEf

The Proof-of-Efficiency (PoEf) mechanism, which is integrated into a decentralised architecture, has been strategically developed to guarantee the integrity of transactions. The importance of authenticity in the system is crucial for maintaining its integrity. It requires the algorithm to function in a timely way and ensure that legitimate and genuine transactions are successfully executed. The network's capacity to maintain uninterrupted functioning, despite occasional disagreements, highlights its resilience and commitment to prioritising authenticity.

- **Suggestion 2 (Authenticity of PoEf):**

The authenticity of the PoEf framework 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 is received. If all stakeholders within the network receive T_x to validate, it is indicative of the network's capacity to maintain authenticity within an asynchronous environment, thereby validating the operational integrity for the node, S_H . (ii) the transaction is not received. If there is an absence of T_x , Such an event would occur under circumstances where is S_H either acting with malicious intent or experiences a failure during the transaction's transmission phase.

The verification process thus relies on a dual-pathway assessment where the receipt of a transaction by peer nodes is used as a metric for gauging 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 indispensable for the veracity and reliability of transactions within decentralized systems.

7.4.3 Proposed Encryption model

In the domain of blockchain security, public key cryptography serves as the bedrock for ensuring secure communications between entities. A prime example of such a cryptographic method is Elliptic Curve Cryptography (ECC), which employs a pair of keys for each user: a private key and a public key. The private key is a securely chosen random number, while the public key is a resultant point on an elliptic curve, derived by scalar multiplication of the private key with a predetermined generator point P_g on the curve. Each participant within the SCM blockchain is assigned a pair of keys: a private key, which is a secret random number known only to the owner, and a public key, which is 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 parties must concur on a specific elliptic curve and its associated parameters, namely, the curve coefficients a and b and the base point P_g . The curve itself 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.

The predilection for ECC in blockchain encryption protocols stems from its efficiency: it requires comparatively fewer resources, permits smaller key sizes, and assures reduced computational complexity. 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 overall robustness of the blockchain network, particularly under conditions of network delay or disruption. The resilience score may factor in the node's ability to handle such conditions without compromising the integrity and security of the blockchain.

ECC's cryptographic strength and efficiency manifested in lower CPU usage, minimal content utilization, decreased network consumption, and expedited encryption processes render it a superior choice for contemporary blockchain applications. This is substantiated by Sarfaraz et al. [94], who highlight ECC's advantages in an environment where security and performance are paramount. This measure of resilience is particularly relevant for the SCM environment where transaction security is critical yet must be balanced with system performance. The implementation of ECC in SCM blockchain not only aligns with the research's objective of fortifying data integrity and transactional security but also supports the efficiency required for high-volume, dynamic SCM operations. The adoption of ECC within the SCM blockchain encryption model is integral to achieving the research goals of creating a secure, resilient, and efficient supply chain architecture that can withstand the complexities of modern-day SCM challenges.

7.4.4 Threat model

Within the complex realm of blockchain-enabled SCM systems, the threat model plays a crucial role in defining the system's defensive measures against Byzantine adversaries. The model classifies prospective antagonists into two main categories. 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 arise from within a system, wherein nodes that have been authenticated may exhibit hostile behaviour because of malware penetration or other types of cyber-attacks. This can occur even when the nodes possess valid credentials, leading to abnormal actions. According to the findings of Hassan et al. [180], the main goal of an adversary is commonly centred around the process of introducing and spreading false transactions within the ledger of a blockchain. This scenario exemplifies a blockchain assault, which primarily seeks to undermine the integrity of the transactional ledger. This can be achieved by impeding valid transactions or by assuring the inclusion of deceitful transactions.

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 important to acknowledge that the reputation-based processes governing these blockchains are susceptible to manipulation, as shown by Aluko and Kolonin [179]. In order to mitigate these weaknesses, the proposed protocol utilises modern public key infrastructure (PKI) for the purpose of managing cryptographic keys, in addition to employing state-of-the-art encryption techniques to ensure the security of data transfer.

Within the system's threat model, the process of systematically identifying and analysing a range of potential threats that have the capability to undermine the integrity and security of the blockchain network is assessed:

- Attack 1: An adversary conducts concurrent transactions with distinct nodes, attempting to double-spend within the network.
- Attack 2: Persistent Byzantine conduct is exhibited by an attacker through repeated subversive actions within the system.
- Attack 3: An entity fabricates multiple identities, ostensibly to enhance network resilience but with the ulterior motive of diluting the system's security posture.
- Attack 4: Distributed DDoS attacks are orchestrated against specific nodes, inundating them with spurious transaction requests to erode their availability.
- Attack 5: The consensus process is targeted by an attacker aiming to co-opt network nodes to sway decision-making.
- Attack 6: 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.

Within the framework of the threat model, it is postulated that the adversary is constrained by computing limitations that prevent them from compromising cryptographic protocols. Furthermore, the approach deliberately excludes terminal attacks and key hijacking from its scope, prioritising instead the more common dangers that exist within the context of the supply chain management blockchain. The threat model presented in this thesis offers a strong basis for the construction of secure and resilient supply chain management blockchain systems. The statement not only acknowledges many potential security risks but also emphasises the importance of employing modern cryptographic methods and maintaining watchful network administration to anticipate and reduce adversary acts.

7.5 PoEf, Experimentation Results

PoEf's Throughput

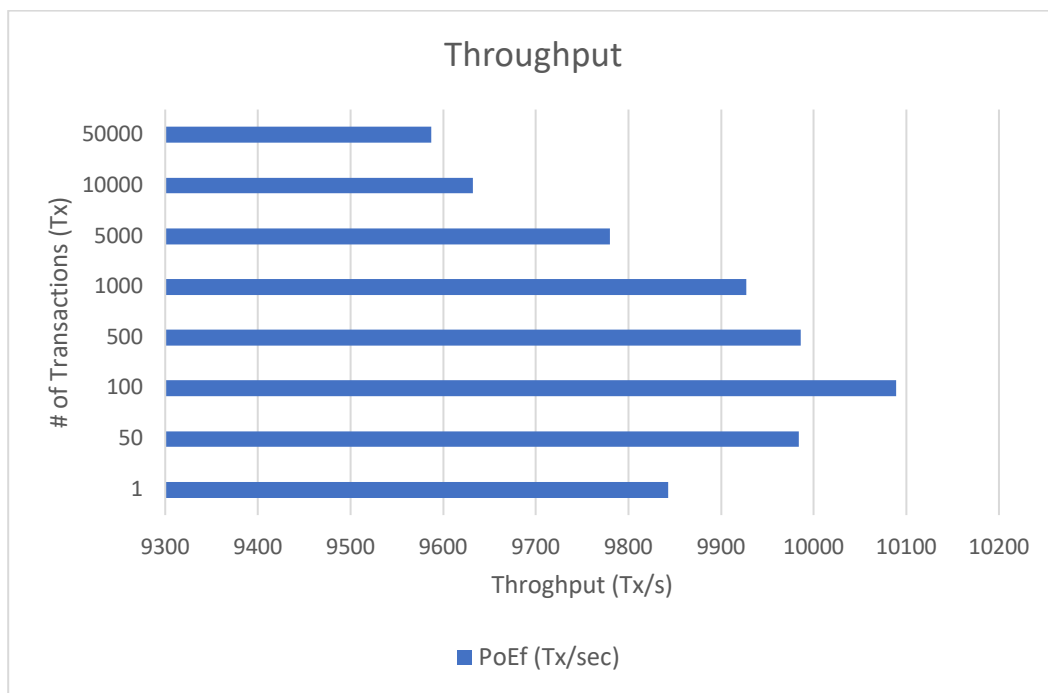


FIGURE 7.11: Figure illustrating PoEf's consensus throughput results from simulation.

The graph, Figure 7.11, illustrates the throughput of the newly proposed consensus algorithm PoEf. Throughput is measured in transactions per second (Tx/s) on the horizontal axis, and the number of transactions is shown on the vertical axis, using a logarithmic scale (as indicated by the '1x', '10x', '100x', etc.). The logarithmic scale on the vertical axis is used to display a wide range of values, allowing for better visualization of data that vary exponentially. Each bar on the chart represents the throughput of the PoEf consensus mechanism at different transaction volumes.

Based on the figure, it is clear that there is an inverse relationship between the number of transactions and the throughput, measured in transactions per second. This phenomenon is prevalent in numerous systems, wherein an increase in transaction volume generally results in a decrease in the processing capacity measured in transactions per second.

PoEf's Latency

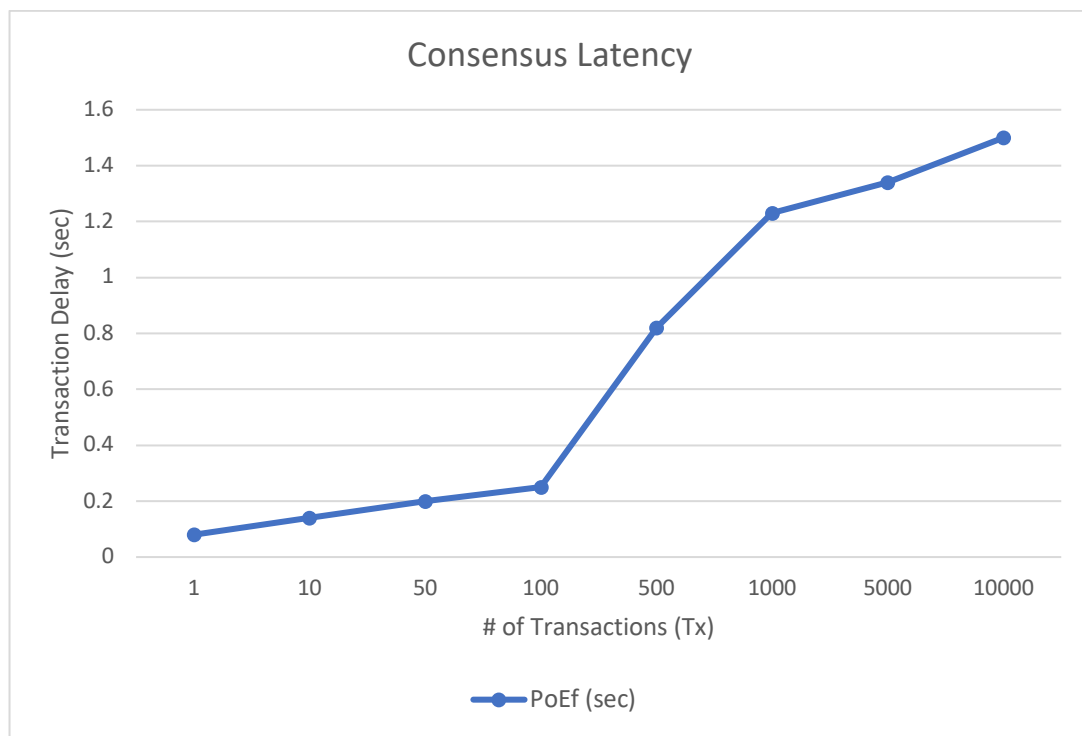


FIGURE 7.12: Figure illustrating PoEf's consensus latency results from simulation.

The graph, Figure 7.12, depicts the consensus latency, measured in seconds, for the PoEf consensus algorithm as the number of transactions increases. The horizontal axis represents the number of transactions on a logarithmic scale, and the vertical axis represents the transaction delay in seconds.

Here's how to interpret the graph:

Low Transaction Volumes (1 to 100 Tx): The latency remains relatively low and stable as the number of transactions increases from 1 to 100. This suggests that the PoEf algorithm can efficiently handle low to moderate numbers of transactions with minimal impact on latency.

Moderate Transaction Volumes (100 to 1000 Tx): As the transaction count goes from 100 to 1000, there is a noticeable increase in latency, although it remains below one second. This indicates that while PoEf starts to experience higher delays, it still maintains sub-second latency at these volumes.

High Transaction Volumes (1000 to 10000 Tx): There is a more pronounced increase in latency as the number of transactions grows from 1000 to 10000. The delay more than doubles, climbing from just below 1 second to approximately 1.5 seconds. This shows that the PoEf algorithm’s performance degrades more significantly under high transaction loads, which is a critical factor for scalability.

PoEf’s Scalability (throughput)

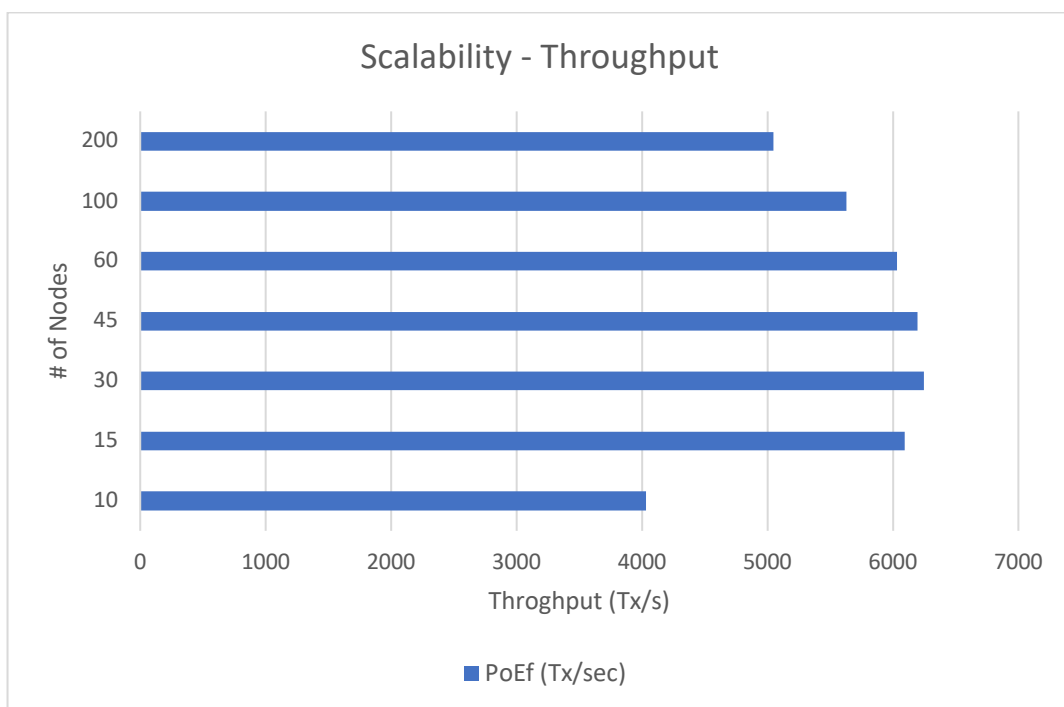


FIGURE 7.13: Figure illustrating PoEf’s Scalability throughput results from simulation.

The graph, Figure 7.13, showcases the scalability of the PoEf consensus algorithm in terms of throughput, which is measured as transactions per second (Tx/s). The vertical axis represents the number of nodes in the network, while the horizontal axis shows the throughput.

The graph presented provides an insight into the scalability of the PoEf consensus algorithm, showcasing how it performs as the network expands. It indicates that the PoEf's throughput, or the number of transactions it can process per second, does not suffer significantly as more nodes join the network. This stability in transaction processing speed with the increase in nodes highlights the algorithm's capability to scale efficiently, a critical factor for blockchain-based SCMs that need to support growing user bases

without compromising on performance. Furthermore, the graph demonstrates a consistent level of performance across a network size ranging from 10 to 200 nodes. This consistency suggests that the PoEf algorithm is adept at managing higher loads, maintaining a steady transaction rate without performance degradation. While the throughput is consistently high, suggesting that PoEf is a high-performance mechanism, there's an indicated upper boundary to its capacity. This plateau in throughput is likely due to inherent limitations common in distributed systems, such as constraints on bandwidth, delays in message propagation, and the computational overhead involved in reaching consensus.

The data collected shows that PoEf's design allows for scaling up the number of nodes without experiencing a significant drop in throughput, which is a strong indicator of the algorithm's efficiency and robustness against increased loads.

PoEf’s Scalability (Latency)

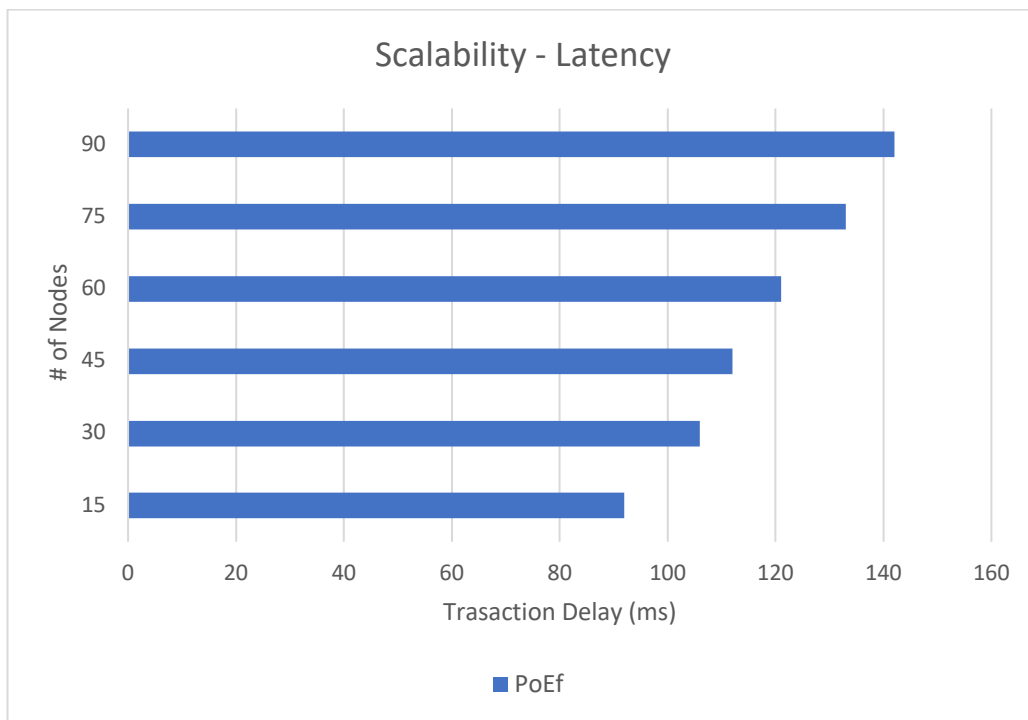


FIGURE 7.14: Figure illustrating PoEf’s Scalability latency results from simulation.

The graph, Figure 7.14, represents the relationship between the number of nodes in a network utilizing the PoEf consensus algorithm and the corresponding transaction delay, measured in milliseconds (ms).

From the graph, it is evident that as the number of nodes in the network increases, the transaction delay (latency) also increases. This is a typical behaviour in distributed systems as more nodes can mean more coordination and communication is required, which can increase the time it takes to achieve consensus

and thus process transactions. The transaction delay is relatively low for smaller numbers of nodes; however, as the network grows beyond 30 nodes, the increase in delay becomes more pronounced. For example, with 90 nodes, the delay approaches 140 ms, which suggests that the PoEf algorithm may face challenges maintaining low latency in larger networks.

It's important to note that the latency does not increase linearly. The graph shows a more gradual increase up to around 45 nodes, after which the increase in delay becomes steeper. This could indicate that the PoEf algorithm is quite efficient in smaller networks but may not scale as well in terms of latency in larger networks. Overall, the graph suggests that while the PoEf consensus algorithm demonstrates efficiency in handling transactions with lower latency in smaller networks, its performance in terms of latency may degrade as the network scales up. This information is crucial for understanding the potential limitations of the PoEf algorithm in large-scale applications.

8 Evaluation and Discussion

This thesis involves a comparative analysis of experimental findings obtained from simulations of various consensus algorithms, namely PoW, DPoS, Ripple, PBFT, PoI, and PoEf. The results reported in this thesis are the mean outcomes derived from a set of 15 individual simulation runs. At the core of this analysis lies the investigation of the PoEf consensus algorithm, with a particular emphasis on three crucial performance metrics: throughput efficiency, latency, and scalability.

8.1 An Evaluation of Throughput Efficiency

The efficiency of consensus algorithms in SCM is crucial, particularly in terms of transaction throughput. Figures 8.1 illustrates a graphical representation of the average throughput across different consensus algorithms, delineated against varying transaction volumes. The graph shows that outside of the proposed PoEf, Stellar and Ripple and PBFT are the best consensus mechanisms for SCM applications that require high performance. PoI is a good choice for SCM applications that require a balance of security, performance, and scalability. DPoS is a good choice for SCM applications that require high performance and scalability, but it may be susceptible to centralization. PoC is a good choice for SCM applications that require energy efficiency and scalability, but it may be less secure than other consensus mechanisms. PoW is not a good choice for SCM applications that require high performance or scalability. It's performance, in terms of transaction throughput (efficiency), is limited by this intensive computational work. the energy-intensive nature and slower throughput of PoW pose practical constraints for SCM applications, making it less suitable for SCM which sometimes require high throughput (Croman et al., 2016), where real-time data recording and energy efficiency are essential.

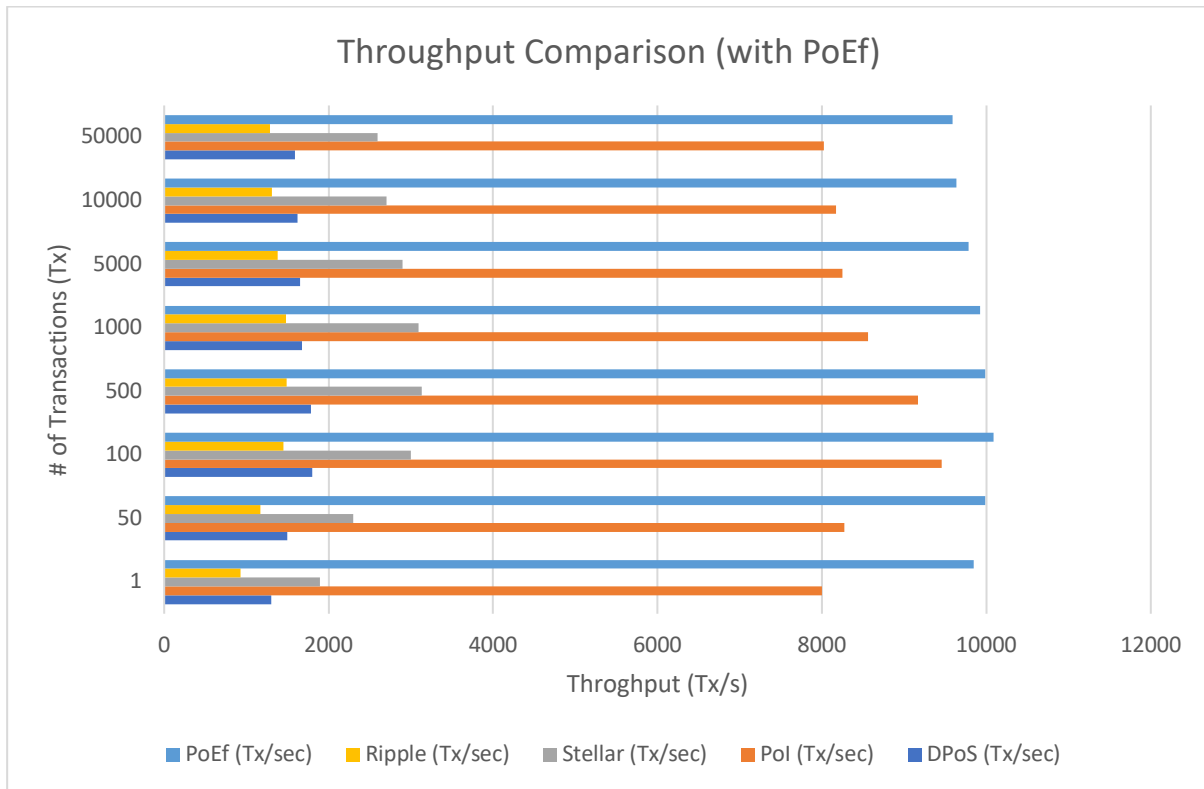


FIGURE 8.1: Figure illustrating Blockchain Mechanisms consensus throughput comparison including PoEf algorithm.

Notably, as the transaction count (T_x) incrementally rises from 1 to 100, there is an observable increase in the average throughput for all algorithms. Under the condition of 100 T_x , algorithms such as Pol, DPoS, and PoEf demonstrate superior throughput. Conversely, PoW, Proof of Contribution (PoC), PBFT, and Ripple exhibit lower throughput rates. A noteworthy trend is observed wherein the average throughput for all algorithms diminishes post the 500 T_x mark, as depicted in Figure 8.1. A comparative analysis of DPoS, Pol, and PoEf with an increasing number of T_x reveals that PoEf consistently maintains a higher average throughput compared to DPoS, Pol, Stellar and Ripple. Even as the number of transactions increases, two of the established algorithms with the highest through (Pol and Stellar) still could not match up to the proposed PoEf. The TPS for Pol ranged between 8000 and 9000, Stellar fluctuated from 1000 to 3000, and PoEf varied notably between 9000 and 10000.

The underlying algorithm that controls the process of adding new blocks to the blockchain, known as the consensus mechanism, has a major impact on throughput. The consensus process used by Bitcoin, known as PoW (Proof-of-Work), is renowned for having a low throughput, usually ranging from a few TPS to a maximum of about seven TPS. This restriction results from the energy-intensive mining procedure needed to validate transactions, solve intricate mathematical riddles, and add new blocks to the chain.

Another consensus method called DPoS provides higher throughput, usually in the range of tens to hundreds of TPS. This improvement can be because it streamlined the consensus process, increased transaction processing capacity, and delegated validation obligations to a small group of pre-selected validators.

The throughput of more sophisticated consensus methods, like Stellar, Ripple, and PBFT, is sometimes far higher, reaching tens of thousands or even millions of TPS. Through the use of the BFT algorithm in PBFT, performance can be maximised, and parallel transaction processing is made possible even in the event of faulty nodes. Stellar and Ripple employ effective algorithms as well, utilising a distinct consensus process and a FBA technique, respectively, to handle massive transaction volumes and attain high throughput. The needs of the supply chain determine which consensus mechanism is best for SCM applications. Consensus methods with high throughput, like PBFT, Stellar, or Ripple, may be advantageous for applications that prioritise high transaction volumes, including cross-border payments or real-time tracking of products and services. These methods make it possible to handle a lot of transactions quickly, which makes supply chain operations more effective and scalable.

Nevertheless, despite its lower throughput, PoW might be a better option for applications that value security and immutability, such as maintaining sensitive supply chain data records or guaranteeing the authenticity of high-value commodities. PoW's lengthy block duration and energy-intensive mining procedure offer a strong degree of security and tamper-proofness, protecting vital supply chain data and guaranteeing the integrity of priceless items.

In conclusion, a key component in assessing the efficiency and scalability of blockchain-based supply chain management systems is throughput or transaction throughput. The consensus mechanism selected has a major effect on 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, careful analysis of the requirements of the SCM application and the trade-offs between security, efficiency, and throughput is necessary. The proposed PoEf mechanism emerges as a notably efficient solution, providing higher throughput compared to traditional and contemporary consensus algorithms. Its integration into SCM systems can potentially enhance the overall efficiency and scalability, accommodating the evolving needs of modern supply chains.

8.2 An Evaluation of Latency

Latency is a critical metric inside the blockchain ecosystem that quantifies the duration between the commencement of a transaction and its ultimate inclusion into the ledger. This thesis focused on doing a comparative evaluation of the timestamps recorded at the commencement of transactions with those at the stages of validation and integration into the ledger. The significance of this statistic resides in its capacity to assess the agility and efficiency of the blockchain network, offering an illustration of the dynamics involved in transaction processing.

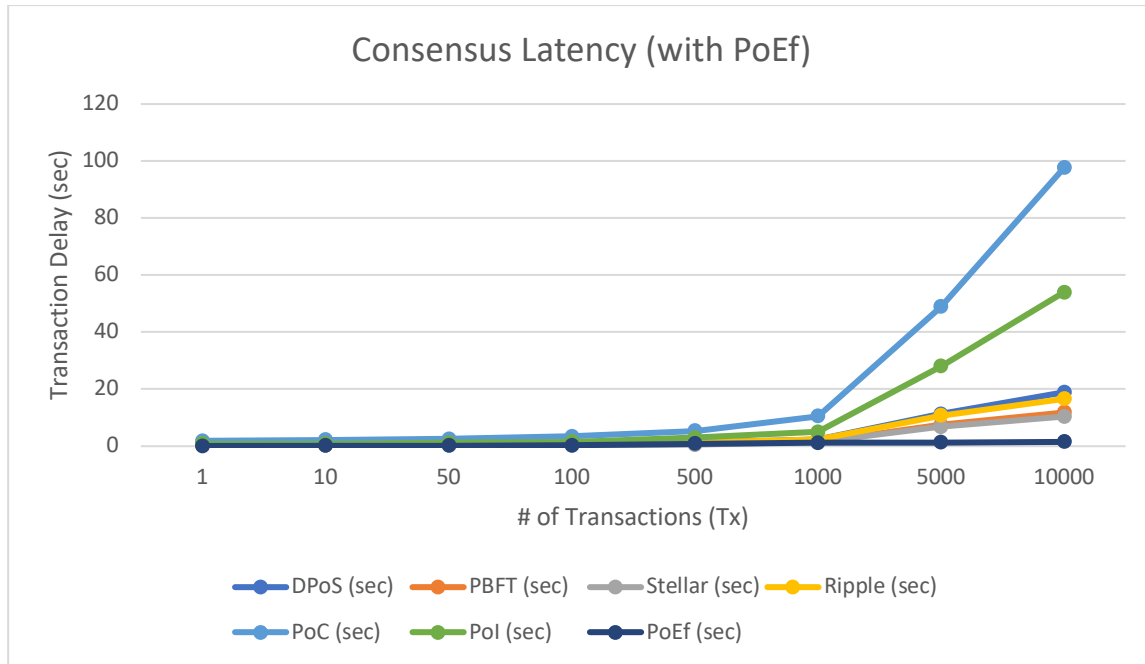


FIGURE 8.2: Figure illustrating Blockchain Mechanisms consensus latency comparison including PoEf algorithm.

The consensus process used by Bitcoin, known as PoW (Proof-of-Work), is infamous for having a long latency, frequently lasting hours, or minutes. The energy-intensive mining procedure needed to solve challenging mathematical riddles, validate transactions, and add new blocks to the chain is the cause of this prolonged wait. Another consensus method called DPoS provides better latency, usually in the range of seconds to minutes. This improvement is credited to the fact that it streamlined the consensus process and decreased transaction latency by assigning validation duties to a small group of pre-selected validators. Stellar, Ripple, and PBFT are examples of more sophisticated consensus systems that achieve decreased latency, often ranging from milliseconds to seconds. By ensuring consensus even in the face of malfunctioning nodes, PBFT's BFT algorithm speeds up transaction processing and reduces transaction latency. To achieve low latency and minimise transaction delay, Stellar and Ripple also make use of effective algorithms, utilising a FBA approach and a distinct consensus mechanism, respectively. The supply chain's unique requirements determine which consensus mechanism is best for SCM applications. As seen in Figure

8.2a, Stakeholders that value quick transaction processing, like international payments or real-time inventory tracking, could profit from low-latency consensus methods like PBFT, Stellar, or Ripple. By reducing transaction latency, these methods enable a timely and smooth flow of goods and services across the supply chain. Though PoW has a higher latency, it might be a better option for applications that value security and immutability, including maintaining track of important supply chain data or verifying the legitimacy of high-value commodities. PoW's lengthy block duration and energy-intensive mining procedure offer a strong degree of security and tamper-proofness, protecting vital supply chain data and guaranteeing the integrity of priceless items. To sum up, consensus latency, also known as transaction latency, plays a crucial role in determining the efficacy and efficiency of blockchain-based supply chain management systems. The consensus mechanism selection has an enormous impact on transaction processing times, which affects supply chain operations' overall speed, responsiveness, and security. To choose a consensus mechanism that best fits the demands of the supply chain, careful analysis of the requirements specific to the SCM application and the trade-offs between security, efficiency, and transaction delay are necessary.

8.3 An Evaluation of Scalability.

Scalability, as a metric for evaluating performance, examines the algorithm's capacity to sustain or improve its operating efficiency in response to changes in size or volume, sometimes involving an increase. The measurement holds significant importance in assessing the adaptability and resilience of the consensus algorithm, particularly in situations characterised by increasing transaction volumes or network expansion. The metric of scalability serves as an indicator of the flexibility and resilience of a consensus algorithm, playing a crucial role in determining its applicability for a wide range of blockchain applications. Each of these indicators offers a nuanced perspective through which the performance of consensus algorithms can be analysed and comprehended. Throughput provides valuable information regarding the network's processing capacity, latency signifies the system's level of responsiveness, and scalability denotes the network's ability to accommodate growth and heightened demands. By collecting and analysing these metrics, this thesis assessed the PoEf algorithm in comparison to other algorithms and determined its effectiveness and applicability within the field of blockchain-based SCMs.

Scalability, which is frequently measured by transaction throughput in the dynamic and always changing field of SCM, is the capacity of a blockchain-based system to manage a growing number of transactions without sacrificing effectiveness or performance. This metric, which is commonly expressed in terms of

TPS, is essential for assessing how resilient and adaptive SCM systems are as they manage increasing transaction volumes and expanding supply chains.

The selection of the consensus mechanism has a major impact on scalability. The consensus process used by Bitcoin, known as PoW (Proof-of-Work), is renowned for having a restricted capacity to scale, usually extending from a few TPS to a maximum of approximately 7 TPS. This restriction results from the energy-intensive mining procedure needed to validate transactions, solve intricate mathematical riddles, and add new blocks to the chain. An alternate consensus method DPoS has better scalability and can often handle tens to hundreds of TPS. This improvement can be due to the fact that it streamlined the consensus process, increased transaction processing capacity, and delegated validation obligations to a small group of pre-selected validators. Higher scalabilities are often achieved by more sophisticated consensus processes, such as Stellar, Ripple, and PBFT, which can reach tens of thousands or even millions of TPS. Through the use of the BFT algorithm in PBFT, performance can be maximised, and parallel transaction processing made possible even in the event of faulty nodes. Stellar and Ripple employ effective algorithms as well, utilising a distinct consensus process and an FBA technique, respectively, to handle massive transaction volumes and attain high throughput. The supply chain's unique requirements determine which consensus mechanism is best for SCM applications. Consensus methods with high scalability, like PBFT, Stellar, or Ripple, may be advantageous for applications that prioritise high transaction volumes, including cross-border payments or real-time tracking of products and services. These methods make it possible to handle a lot of transactions quickly, which makes supply chain operations more effective and scalable. Nevertheless, despite its lower throughput, PoW might be a better option for applications that value security and immutability, such as maintaining sensitive supply chain data records or guaranteeing the authenticity of high-value commodities. PoW's lengthy block duration and energy-intensive mining procedure offer a strong degree of security and tamper-proofness, protecting vital supply chain data and guaranteeing the integrity of priceless items.

In summary, the ability to handle large volumes of transactions at a fast pace is a crucial component of blockchain-based supply chain management systems' flexibility and durability. The consensus mechanism selected has a major impact on transaction processing rates, which in turn affects the supply chain's overall capacity and ability to manage an increasing volume of transactions and adjust to the needs of a dynamic ecosystem. A suitable consensus mechanism that fits the changing needs of the supply chain requires careful evaluation of the requirements of the SCM application and the trade-offs between security, efficiency, and throughput.

8.4 An Evaluation of Scalability Dynamics

Scalability, within the realm of distributed systems, is an essential characteristic that facilitates the system's ability to adjust flexibly to varying operating factors. The adaptability of the system is mostly dependent on how the consensus mechanism allows for the seamless integration and disengagement of nodes. The present thesis conducted an empirical investigation to explore the scalability dimension by investigating the influence of manipulating the number of nodes on the functioning of diverse consensus algorithms. The primary emphasis was placed on assessing the consequences of these modifications on the system's TPS and transaction latency. The present research systematically investigated the PoI, DPoS, and PoEf algorithms.

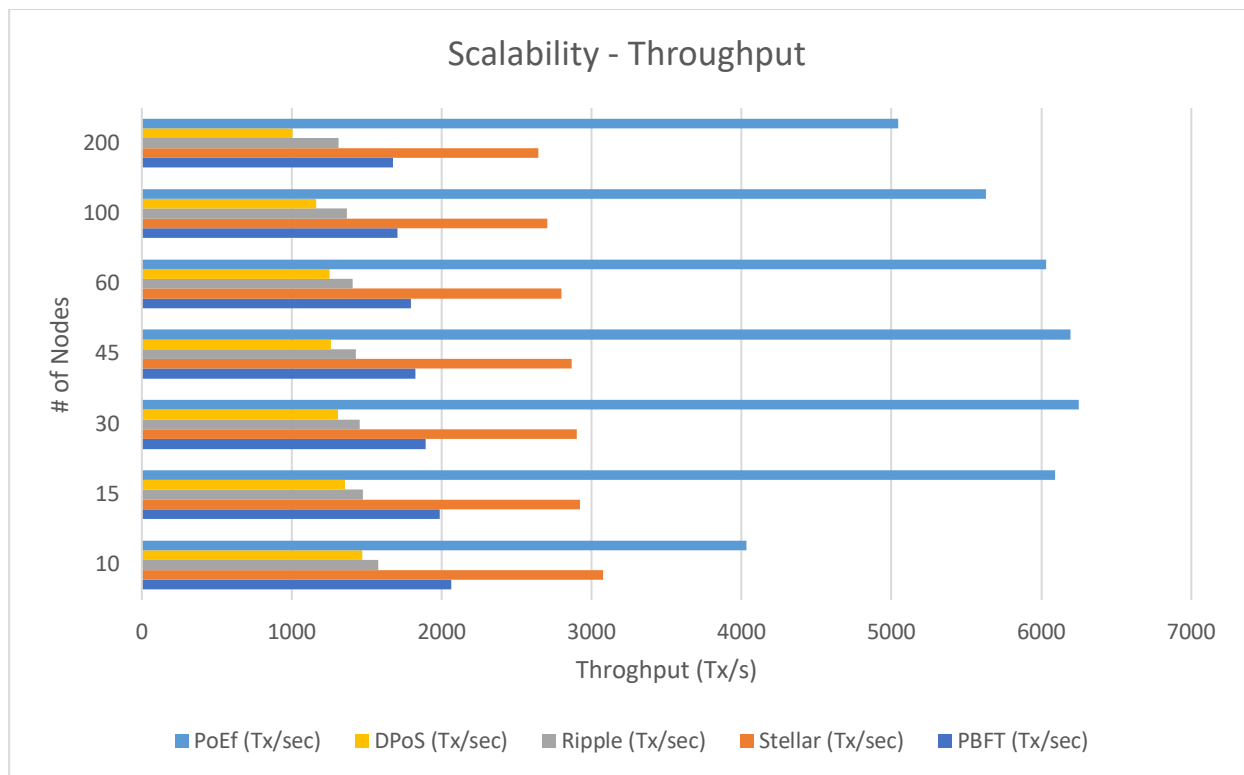


FIGURE 8.3: Figure illustrating Blockchain Mechanisms Scalability (throughput) comparison including PoEF algorithm.

Figures 8.3 and 8.3 displays an illustration of transaction processing performance across several algorithms, considering varied numbers of nodes. The graphical representation illustrates that as the number of nodes increases, both the DPoS and PoI algorithms demonstrate a decrease in performance. It is worth mentioning that the TPS for the Stellar algorithm with approximately 3000 transactions when the network consists of 200 nodes is the best performing established algorithm for scalability. Stellar is a consensus mechanism that is designed to be fast and efficient. It can process thousands of transactions per second, and it is very scalable. Stellar is a good choice for SCM applications that require high performance and

scalability, such as cross-border payments. However, in comparable circumstances, the suggested PoEf method demonstrates a substantial improvement over these established algorithms results, achieving around 5047 TPS for 200 nodes.

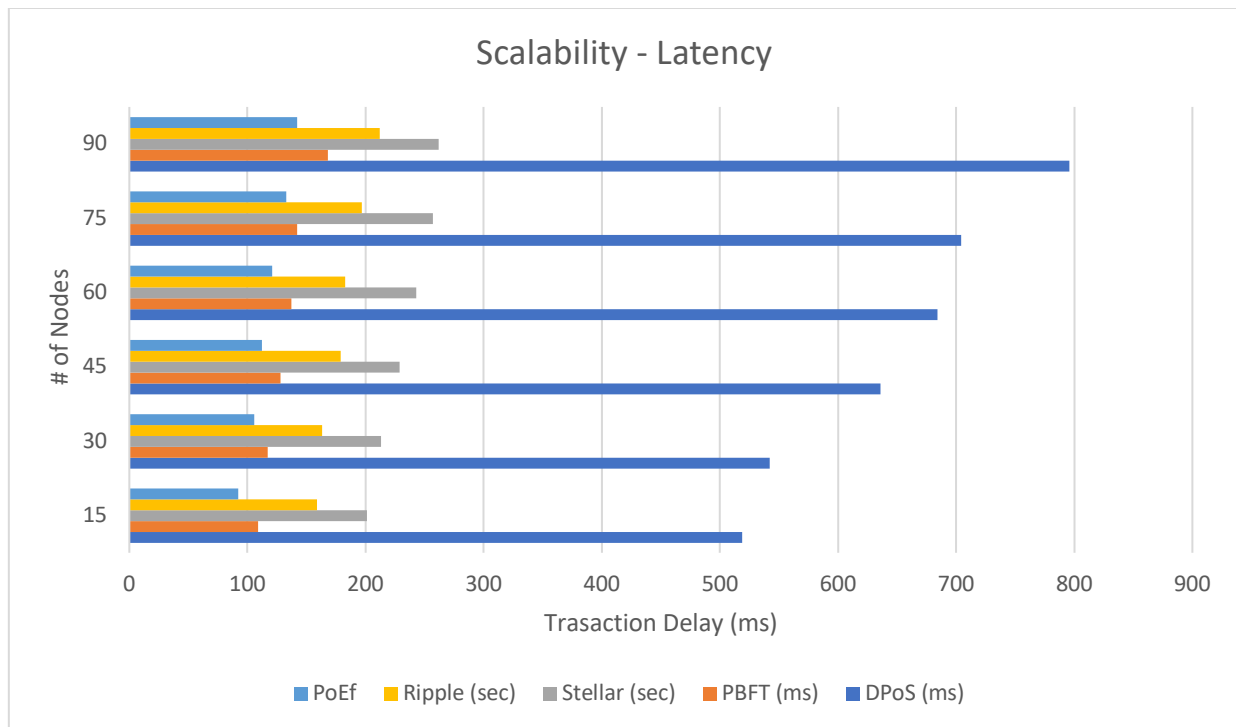


FIGURE 8.4: Figure illustrating Blockchain Mechanisms Scalability (latency) comparison including PoEf algorithm.

Moreover, Figures 8.4 presents a comparison of the average latency metrics for Stellar, Ripple, PBFT, DPoS and PoEf algorithms, while keeping the node counts constant. A noticeable pattern is found whereby the average delay for each algorithm increases in parallel with the rise in the number of nodes. When starting with a minimum of 15 nodes, the PBFT and the PoEf techniques demonstrate similar latency measurements. Nevertheless, when the number of nodes increases, the latency for PBFT and the others experiences a more significant increase compared to PoEf. The rate at which the average latency increases from 45 to 90 nodes is approximately twice as fast for the established algorithms as compared to PoEf.

In the conducted trials, the Stellar, Ripple, PBFT and the suggested PoEf algorithm exhibited noteworthy performance, as they shown low-efficiency disruption despite the increase in the number of nodes. Nevertheless, it has been found that the DPoS method has comparatively lesser scalability, whilst Stellar, Ripple PBFT and PoEf maintain better levels of scalability. In some circumstances, the efficacy of PoI and DPoS methodologies closely approximates that of PoEf. It is important to acknowledge that DPoS are consensus algorithm that rely on lotteries. These algorithms are specifically designed to encourage the circulation of coins, which is highly beneficial for cryptocurrency applications that prioritise active coin

circulation rather than hoarding. In supply chain environments, the selection of a suitable consensus algorithm becomes critical significance due to the essential importance placed on trust and reliability within the network. The findings of this thesis indicate that algorithms such as DPOS may be suitable for applications that prioritise coin circulation. However, in scenarios that require high levels of trust and resilient scalability, like in SCM, it is suggested that algorithms like PBFT or the proposed PoEf may be most beneficial.

8.5 Additional validation of the PoEf Model with similar models

Building upon the comparative analyses previously presented, the PoEf algorithm can be compared other to consensus methods based on reputation of the nodes. The Proof-of-X-Repute (PoXR) and the Reputation Proof of Cooperation (RPoC) techniques, as described by Wang et al. (2020) and Sarfaraz et. Al 2023 respectively, serves as a comparative benchmark to the PoEf algorithm. Both the PoXR and the RPoC protocols employ a consensus technique that is 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 that there is 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, while the PoXR comprises a conventional protocol resembling PoW, supplemented by an additional layer of reputation and 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 the reputation of a node. Consequently, this process inherently exhibits an iterative nature. Furthermore, PoXR has challenges in upholding user privacy due to the capacity of users to obscure their identities, hence potentially dodging accountability for participating in hazardous behaviours.

To validate the PoEf algorithm and establish a fair comparison, a side-by-side analysis of PoEf, PoXR and RPoC would need to be done. Neither the PoXR and RPoC are a widely recognized or standard consensus mechanism in the blockchain community. This means that specific data regarding the maximum throughput of them is not readily available.

From the limited publicly available data for PoXR and RPoC that were evaluated in a standardised operating environment, specifically a public network context. 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 give an average of ~5900 TPS.

The comparative throughput performance of each is similar, though each has a significant differentiation in reaching consensus: PoEf does not require resource-intensive block mining, in contrast to PoXR and PoEf has separated the calculating reputation through a sharding technique, as opposed to RPoC that does the calculation in the same blockchain consensus layer. Simulating each algorithm under similar conditions, with particular emphasis on resilience, should prove notable outcomes comparing each algorithm. In conclusion, the research supports the notion that the PoEf model displays a slight advantage over PoXR and RPoC in terms of throughput efficiency. The extensive validation could not only strengthen the effectiveness of PoEf in real-world scenarios but also establish it as a more feasible option in situations when both high throughput efficiency and strong security are of utmost importance.

8.6 Security Vulnerability analysis

This section provides a thorough examination of the security analysis of the PoEf algorithm in relation to various types of malicious attacks, as outlined in part 3.5. The assumption is made that advanced safe encryption measures are implemented, hence making them resistant to any attempts by attackers to penetrate them. In this analysis various danger vectors are examined.

8.6.1 Safety and Authenticity

The consensus algorithm's BFT characteristic relies on its intrinsic properties of safety and authenticity. In the context of PoEf, potential attackers are effectively prevented from utilising their mining capability to undermine the integrity of the system. In contrast, individuals are required to establish and nurture a favourable standing, thereby making a constructive contribution to the integrity of the blockchain. Theoretical research and empirical observations indicate that in a network where reputable miners have a substantial presence, an external attacker without a reputation score is fundamentally unable to join the consensus group. This ensures the safety and liveness of the system.

8.6.2 Double spending attack

One aspect that is crucial for the security of a digital currency system is its ability to resist double spending attacks. Within the framework of the PoEf protocol, the occurrence of a double spending attack, characterised by the deliberate reutilization of previously validated transaction data by an attacker (referred to as At_k), is effectively addressed through the inherent design of the system. The triple-layer consensus mechanism of PoEf, in conjunction with the decentralised nature of blockchain, automatically provides protection against such attacks. During the process of block verification, the network's validators promptly detect any instance of a double-spend transaction. Consequently, the validator responsible for the double spend transaction, referred to as At_k , is removed from the validator list. Additionally, a notification is sent to the Authorization Network and reputation score updated.

8.6.3 Resilience against Consensus Group Attacks

When examining situations in which malevolent nodes infiltrate both consensus layers, exerting influence over block production and validation, the PoEf protocol demonstrates resilience. If the proportion of attacks in a cluster remains below one-third, the influence on block generation remains insignificant. In situations where the At_k component represents a majority of two-thirds within a lower-tier cluster, their ability to create smaller blocks is countered by the higher authority nodes, which assure the proper construction of larger blocks. The technique serves to strengthen the inclusion of solely valid mini-blocks into the blockchain, a process further supported by the reputation-based selection of validators in the PoEf consensus algorithm.

8.6.4 Sybil attack.

To mitigate the risks posed by Sybil attacks, various defensive measures can be implemented. These measures aim to detect and prevent the creation of multiple fake identities by a single malicious entity. One approach is to employ reputation systems, which assign trust values. The prevention of Sybil attacks, which include an attacker operating numerous identities, is achieved in the PoEf system by implementing a distinctive two-layer consensus process. The individual identity of each node, which is verified by the Authorization Network, along with transparent and verifiable identities, reduces the likelihood of Sybil assaults. Furthermore, the allocation of a low default reputation score to newly established accounts serve to further undermine the competitiveness of any rogue accounts created by At_k .

8.6.5 Denial-of-service attacks

The structure of PoEf automatically provides protection against DoS assaults. The allocation of block-generating privileges exclusively to nodes that possess the ability to survive such attacks, together with the pre-authentication process that networks nodes undertake, serves to bolster the system's resilience. Additionally, the decentralised structure of the blockchain provides additional support to the system in mitigating DoS attacks.

8.6.6 Under 51% attack

The mitigation of 51% attacks is a crucial aspect to consider in the realm of blockchain security. In the specific context of permissioned blockchains, such as the PoEf protocol, the potential for a 51% attack is significantly diminished in comparison to public blockchain networks. The task of an attacker to gain control over most nodes within this context is amplified, hence safeguarding the network's integrity. The durability of PoEf is further explored through experimental scenarios that involve different proportions of malicious nodes. This investigation highlights the superiority of PoEf over traditional consensus protocols, which primarily depend on computational power or basic validator selection methods that do not take reputation into account.

8.6.7 Fault Tolerance in PoEf

Fault tolerance in the PoEf consensus algorithm is attained by the collaborative process of several validators adding blocks at the higher authority layer. The validators are chosen in a random manner, considering their reputation scores, to maintain fairness and resilience within the system. In the event of a master node failure inside a subordinate tier, the system rapidly reassigns the verification process to a high-reputation node within the same cluster, therefore mitigating the adverse effects on transaction processing. The adoption of a multi-layered approach to safety and liveness significantly improves the overall dependability and resilience of the network. The PoEf protocol, therefore, exhibits robust resilience against several security vulnerabilities, encompassing double spending, consensus group assaults, Sybil attacks, DoS attacks, and 51% attacks. The PoEf blockchain platform is characterised by its novel two-layer consensus mechanism, which is based on reputation-based validator selection and robust fault tolerance. This unique approach makes PoEf a highly secure and efficient solution for blockchain applications that prioritise safety, authenticity, and operational integrity.

8.7 So... Which Consensus then?

The ideal consensus mechanism depends on specific needs such as transaction volume, processing speed, growth expectations, operational costs, and security requirements. Though PoEf appears to offer a balanced and superior performance across all criteria, potentially making it the most suitable option for a wide range of SCM applications. However, the specific context of the SCM system, such as the value of goods, the sensitivity of data, and the required speed of transactions, must be considered when selecting a consensus mechanism. The evaluation of varying blockchain deployments through the lens of security robustness and operational efficacy is pivotal for the integration of blockchain within SCM frameworks. The consensus mechanisms outlined each impart distinct influences on the security and efficiency of blockchain-integrated SCM systems.

8.7.1 Proof of Work (PoW)

PoW is renowned for its robust security framework, making it a cornerstone of blockchain technology where data integrity and resistance to tampering are paramount. However, its low throughput and scalability, coupled with high latency, render it less conducive for SCM systems demanding high transaction volumes and rapid processing times. The energy-intensive nature of PoW, while providing a formidable security foundation, poses sustainability and cost-efficiency challenges for SCM systems, necessitating careful consideration of its application in scenarios where environmental impact and operational expenditure are of significant concern. PoW, while exhibiting very high security due to its energy-intensive and computationally demanding mining process, is beset by low throughput and poor scalability. This renders it suboptimal for SCM applications that require high transaction volumes and rapid scalability, despite its exemplary tamper-resistance and data integrity. The operational inefficiency and high latency may lead to bottlenecks in supply chain processes, thus hindering real-time tracking and inventory management that are critical in SCM.

8.7.2 Delegated Proof of Stake (DPoS)

DPoS emerges as a consensus mechanism that aptly balances efficiency and performance, with a medium-high throughput and low latency conducive for SCM systems with moderate to high transactional demands. The high scalability of DPoS aligns with the dynamic nature of SCM systems, facilitating expansion and adaptation with minimal performance degradation. However, the medium security rating suggests a trade-off, where the risk of centralization and governance challenges may necessitate additional safeguards for SCM systems requiring stringent security protocols. DPoS offers an improved transaction rate and lower

latency, enhancing the operational efficacy of SCM systems. However, its security is rated medium due to the potential risks associated with delegate centralization. While DPoS provides a more efficient flow of transactions, which is beneficial for SCM systems with high transaction demands, the security risks must be mitigated through robust delegate selection processes and governance models to prevent any central point of failure or manipulation.

8.7.3 Practical Byzantine Fault Tolerance (PBFT)

PBFT's architecture presents a high-throughput, low-latency solution that addresses the critical need for rapid transaction processing in SCM systems. The medium scalability of PBFT indicates a potential to accommodate growth within SCM networks, albeit with limitations in very large-scale environments. The balance of performance and resource utilization in PBFT, denoted by its medium efficiency, alongside its high security, suggests its suitability for SCM systems that prioritize data integrity and system robustness, especially in environments where trust levels among participants vary. PBFT is recognized for its high security and is suited for SCM applications that require a reliable transaction consensus in the presence of potentially untrustworthy nodes. However, its medium scalability could be limiting in the face of rapid expansion and high-volume transactions, common in large-scale SCM operations. The challenge lies in balancing the inherent security benefits of PBFT with the need for scalability, which is essential for evolving SCM networks.

8.7.4 Stellar and Ripple

Stellar and Ripple both exhibit high throughput and low latency characteristics, positioning them as viable choices for high-demand SCM systems that require swift and efficient transaction processing. Their high scalability and efficiency metrics further underscore their potential to support extensive SCM operations. However, the medium security rating necessitates a consideration of the specific security needs of the SCM system in question, particularly when handling sensitive information or transactions of significant value. Stellar and Ripple, known for their high throughput and low latency, are conducive for SCM systems that demand efficiency. They provide scalable solutions for handling a large volume of transactions. Nonetheless, the medium security rating suggests that while they offer adequate protection against common vulnerabilities, they may not be as resilient as PoW or PBFT against sophisticated attacks. This necessitates additional security measures or hybrid models that combine the efficiency of these protocols with enhanced security mechanisms.

8.7.5 Proof of Importance (PoI) and Proof of Capacity (PoC)

PoI and PoC offer a diverse range of applications within SCM systems, providing medium to high throughput and efficiency. Their scalability and latency metrics indicate a capability to serve SCM systems with varying requirements for transaction volume and speed. However, the low security rating of PoC may raise concerns for SCM systems that necessitate robust security measures, and thus, its application should be aligned with risk assessment and mitigation strategies. PoI and PoC present a medium level of security, indicating a need for additional safeguards within SCM systems. While PoC offers high efficiency due to less energy-intensive mining based on storage space, its security may not suffice for SCM systems handling sensitive data or requiring high trust levels. PoI, considering network participants' behaviour and stakes, offers a nuanced approach to security but may require further empirical validation to ensure reliability in diverse SCM contexts.

8.7.6 Proof of Efficiency (PoEf)

The PoEf mechanism distinguishes itself with exemplary performance, characterized by very high throughput and efficiency. This makes PoEf particularly suitable for expansive SCM operations where high transaction volumes and rapid processing are critical. Its low latency and high scalability suggest that PoEf is well-equipped to support the burgeoning needs of modern SCM systems, while its high security rating provides the reassurance necessary for safeguarding against potential cyber threats, affirming its place as a potentially transformative solution in the domain of blockchain-based SCM systems. PoEf, characterized by very high throughput and efficiency, coupled with high security, stands out as an advanced solution that can significantly enhance both the security robustness and operational efficacy of SCM frameworks. Its architecture appears to address the efficiency issues present in PoW while providing a secure and scalable environment that is crucial for contemporary SCM systems.

The integration of these consensus mechanisms into SCM systems has profound implications for the adoption of blockchain technology. Table 8.1, simplifies and categorize the experimental findings in an effort to draft the selection Framework. SCM systems are increasingly facing demands for higher transaction volumes, real-time data processing, and robust security to protect against fraud and cyber-attacks. By critically assessing the strengths and weaknesses of each mechanism, organizations can select the most suitable blockchain configuration that aligns with their specific SCM needs.

Algorithm	Throughput	Latency	Scalability	Efficiency	Security
PoW	Low	High	Low	Low	Very High
DPoS	Medium-High	Low	High	High	Medium
PBFT	High	Low	Medium	Medium	High
Stellar	High	Low	High	High	Medium
Ripple	High	Low	High	High	Medium
Pol	Medium-High	Medium	Medium	Medium	Medium
PoC	Medium	Medium	Medium	High	Low
PoEf	Very High	Low	High	Very High	High

TABLE 8.1: Table illustrating the properties of each Consensus Algorithm assessed.

The table assesses each algorithm in terms of Throughput (the number of transactions processed per second), Latency (the time taken from the submission of a transaction to its inclusion in the blockchain), Scalability (the ability to maintain performance with an increasing number of transactions), Efficiency (the overall performance considering resources used), and Security (resistance to attacks and system integrity). The insights drawn from this evaluation can guide the development of hybrid or customized consensus mechanisms, like PoEf, that leverage the strengths of existing protocols while addressing their limitations. This could lead to the adoption of more secure and efficient blockchain configurations in SCM systems, enhancing their capacity to support complex supply chains, ensure data integrity, optimize logistics, and reduce costs. Thus, the continuous evolution of consensus mechanisms, with a focus on meeting the specific demands of SCM systems, is essential for the broader adoption and optimization of blockchain technology in this space. The proposed PoEf algorithm stands out with 'Very High' throughput and efficiency, and 'High' scalability and security, making it a potentially superior choice for SCM systems requiring robust performance across these criteria.

8.8 Developing a Methodology Framework for Consensus Mechanism Selection in SCM

The advent of blockchain has introduced a paradigm shift in SCM, where the selection of an appropriate consensus mechanism is not merely a technological choice but a strategic business decision. This section aims to develop and recommend a methodology for the judicious selection and application of the most suitable blockchain consensus mechanism for SCM, taking into account the size and demand of the supply chain.

8.8.1 Foundation for Consensus Mechanism Selection

The need for a robust methodology is underpinned by the theoretical understanding that the choice of consensus mechanism directly impacts the scalability, efficiency, and security of a blockchain network. As SCM systems vary in size and complexity, a one-size-fits-all approach to consensus mechanism selection is inadequate. The methodology, as illustrated in Figure 8.5, proposes a synthesis of the experimental simulation findings from various consensus algorithms, including PoW, DPoS, Ripple, PBFT, PoI, and the newly proposed PoEf to incorporating their consensus throughput, latency and scalability.

8.8.1.1 Throughput Efficiency and SCM Scale

In evaluating throughput efficiency, the methodology considers how the consensus mechanism supports transaction volumes reflective of the SCM's size. For smaller SCM operations, where transaction loads are moderate, mechanisms such as DPoS and PoI offer a balance of performance and security. However, for larger SCM systems with high transaction volumes, mechanisms like PBFT, Stellar, Ripple, and particularly PoEf, exhibit superior performance, maintaining high throughput rates even as transaction counts escalate.

8.8.1.2 Latency Considerations Based on Demand Urgency

Latency is another pivotal factor in the methodology, especially for SCM systems that prioritize real-time tracking and rapid transaction processing. The proposed methodology recommends consensus mechanisms with lower latency, such as PBFT, Stellar, and Ripple, for SCM applications requiring promptness. Nonetheless, for SCM networks where security and immutability outweigh the need for speed, a mechanism like PoW, despite its higher latency, may be more appropriate.

8.8.1.3 Scalability Aligned with Supply Chain Growth

The methodology's scalability assessment acknowledges the need for a consensus mechanism to adapt to the expanding scope of supply chains. It highlights that while PoW may struggle with scalability due to its computationally intensive nature, algorithms like Stellar and Ripple excel in this regard. Yet, the standout in scalability, as the data suggests, is PoEf, which not only copes with increased node counts but also maintains an optimal balance between throughput efficiency and latency.

8.8.2 Methodology Recommendations Based on SCM Characteristics

The consensus selection methodology for Blockchain-based SCM:

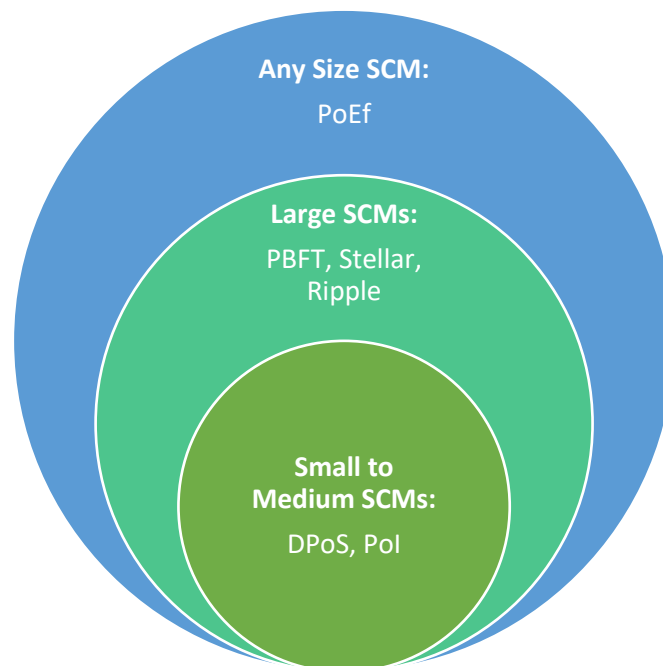


FIGURE 8.5: Figure illustrating the consensus selection methodology for Blockchain-based SCM.

- For small to medium-sized SCM systems with moderate transaction volumes and demand for balance in security and efficiency: DPoS or Pol.
- For large SCM systems with high transaction volumes and a necessity for rapid processing: PBFT, Stellar, or Ripple.
- For SCM systems across all sizes that are evolving or anticipate significant growth: PoEf for its scalability and balance of throughput and latency.

The methodology illustrates the implementation strategy that guides the selection of the right consensus mechanism for varying SCM's deployments. It provides guidelines for piloting the selected mechanism, evaluating its performance, and ensuring that it aligns with the SCM's operational goals and security requirements. In essence, this methodology serves as a strategic tool for businesses to evaluate and select a blockchain consensus mechanism that aligns with their SCM size, demand, and operational priorities. It emphasizes the need for an informed approach that considers the nuanced requirements of SCM systems, advocating for solutions like PoEf, which promise to enhance the efficiency and adaptability of supply chains in the digital era.

8.9 Chapter Summary

The chapter introduces the Proof of Efficiency (PoEf) algorithm as a notable progress in blockchain consensus methods, specifically designed for enhancing SCM efficiency and security. PoEf differentiates itself from traditional blockchain consensus mechanisms by eliminating the requirement for validators to solve intricate computational problems before appending blocks, therefore simplifying the process. The distinctive attribute of PoEf establishes it as a highly effective and adaptable agreement methodology. The system implements a dynamic method of choosing agreement nodes, encouraging widespread involvement throughout the network. An essential innovation of PoEf is its method of decentralising the transaction confirmation process across the network. This distribution greatly diminishes the burden on individual nodes, resulting in improved overall efficiency in achieving agreement. Nevertheless, PoEf's technique is not exempt from constraints. The project faces difficulties related to the 'blockchain scaling trilemma', which entails finding a balance between security, scalability, and decentralisation. An important concern is the system's dependence on node trust values, which has the potential to impact the decentralisation of the system. In addition, the current iteration of PoEf lacks comprehensive methods for identity supervision, which are crucial for the efficient functioning of a reputation-based system.

The chapter also examines and compares PoEf with existing consensus approaches, emphasising its superior performance in important aspects. Thorough investigation reveals that PoEf surpasses conventional consensus approaches in terms of Transactions Per Second (TPS), latency, and scalability. The features mentioned are crucial for blockchain applications in SCM, where the rapidity and effectiveness of transaction processing are of utmost importance. The increased data processing speed and decreased time delay of PoEf greatly enhance the efficiency of blockchain systems, making it an attractive option for SCM applications. In addition, the chapter recognises the persistent difficulties in attaining an optimal equilibrium in the blockchain scaling trilemma. The statement highlights that PoEf prioritises scalability and efficiency, but it also faces the challenge of balancing security and decentralisation. This observation highlights the intricate nature of blockchain technology, where enhancements in one element frequently necessitate thoughtful evaluation of their effects on other essential characteristics. The chapter highlights the capabilities of the PoEf algorithm and its significance in the wider context of blockchain-based supply chain management (SCM) systems. It contributes to the ongoing discussion on the most effective implementation of blockchain technology in SCM.

9 Conclusion, Recommendation and Future Directions

9.1 Introduction

The emergence of blockchain technology signals a pivotal transition in SCM, heralding an era where enhanced transparency, efficiency, and security are within grasp across complex global supply networks. This thesis journeyed through the heart of blockchain-integrated SCM systems in Industry 4.0, unpacking cybersecurity challenges, and charting paths toward innovative operational enhancements. In the preceding chapters of this thesis, a ground-breaking consensus method was meticulously designed, constructed, and evaluated within a blockchain simulator environment. This novel method, tailored for enhanced security and efficiency in blockchain systems, represents a significant stride in advancing blockchain technology, particularly within the domain of SCM. This concluding chapter aims to succinctly summarize the entire thesis, shedding light on the pivotal contributions and breakthroughs of the research undertaken.

The journey of this research has been marked by several notable achievements, each contributing to the broader understanding and application of blockchain in SCM. The development of the novel consensus method, a centrepiece of this thesis, stands as a testament to the innovative approach and technical prowess exhibited in the research. This method, through rigorous simulation and analysis, has demonstrated promising potential in overcoming some of the critical challenges faced by traditional blockchain systems, such as scalability issues, latency, and energy consumption. However, the path to these achievements was not without its challenges. Throughout the research process, several hurdles were encountered, ranging from technical complexities in the design and implementation of the new consensus method to analytical challenges in assessing its performance against existing systems. These challenges not only tested the resilience and adaptability of the research approach but also provided valuable learning opportunities, shaping the course of the thesis.

Looking forward, this chapter will also outline a series of recommendations for future research in this field. These recommendations are aimed at building upon the foundation laid by this thesis, exploring new horizons in blockchain technology, and addressing the evolving needs of SCM systems. Potential areas for future work include further optimization of the proposed consensus method, exploration of its applicability

in diverse SCM scenarios, and the integration of emerging technologies to enhance blockchain efficiency and security. The insights and outcomes of this research open new avenues for innovation and advancement in blockchain-enabled SCM, setting the stage for future explorations and discoveries.

9.2 Conclusions: The Tripartite Review

Adopting a triangulated multifaceted mixed-methods methodology, this research integrated an extensive literature review, relevant case studies, and experimental simulations to obtain a holistic understanding of the security challenges and opportunities to improve the inherent efficiency in blockchain-based SCM systems.

The literature review methodically canvassed existing academic works, providing a detailed view of the current state of blockchain technology in SCM. It critically examined a variety of themes, ranging from consensus mechanism vulnerabilities to smart contract flaws, offering a broad spectrum of insights into the cybersecurity challenges facing blockchain SCM systems. The inclusion of case studies provided a practical perspective, illustrating the real-world application and implications of blockchain technology in SCM. These case studies enriched the research by demonstrating practical examples of blockchain deployment in SCM, highlighting both successes and challenges. They served as a bridge between theoretical research and practical application, adding depth and contextual relevance to the thesis. The experimental simulations, conducted using the BlockSim tool, were a cornerstone of the research methodology. They allowed for the empirical testing of various blockchain consensus mechanisms, providing quantifiable data on key performance metrics such as throughput efficiency, latency, and scalability. These simulations offered a controlled environment to assess the performance of traditional and newly proposed consensus mechanisms, contributing significantly to the development of the novel PoEf mechanism.

Together, these methods formed a triangulated approach that balanced theoretical depth with practical insights and empirical evidence. This multifaceted methodology ensured an exploration of the cybersecurity challenges and efficiency opportunities in blockchain-based SCM systems, underpinning the thesis's contributions to the field.

9.2.1 Literature Review

At the outset, a comprehensive systematic mapping of academic research combining Security, Blockchain, and SCM was conducted. Conducting the SLR offered several key benefits that align directly with the overall

objectives of the research, particularly in a field as complex and evolving as blockchain in SCM. One of the primary objectives of this research was to identify and address technological inefficiencies and security vulnerabilities in SCM systems based on blockchain technology. The SLR methodically collated and analyzed existing literature, helping to categorize the research that was previously done into thematic areas and pinpoint areas that had not been adequately addressed in previous studies, thus directing the focus of the research towards these gaps. The insights gained from this SLR guided the development of research methodologies and frameworks. Understanding the strengths and weaknesses of various approaches used in existing studies informed the design of more robust and effective research methods for this research. This systematic literature review, therefore, not only illuminated the current state of blockchain technology in SCM but also provided a critical baseline from which the thesis could advance.

This initial phase of the research (Chapter 2) was crucial for laying a solid foundation, as it methodically identified and categorized the prevalent cybersecurity issues inherent in blockchain-based SCM systems. Key areas such as failures in consensus mechanisms, vulnerabilities in smart contracts, the susceptibility of networks to various levels of cyber-attacks, and the intricacies of cryptographic challenges were analysed. Given the depth and complexity of each thematic area found from doing the SLR, the proposed research area was broken down into different stages, prioritizing the exploration of consensus mechanisms, because they are considered the crux of a blockchain's efficiency and security. Although the thorough academic research mapping laid the groundwork for the four thematic areas, segueing into a nuanced exploration of diverse consensus mechanisms, each spotlighted for its distinct features and limitations.

9.2.2 The blockchain and its use-cases

Having decided to explore the consensus layer as an initial phase, it was then important to understand the entire architecture of the blockchain (Chapter 4), to discern the complexities of the consensus layer. The second phase involved the research delving into the core fundamentals of blockchain technology, offering an exploration of its architecture and multiple layers. By exploring the architecture and layers of blockchain, the chapter ensures that readers and researchers have a clear grasp of the technical underpinnings and operational dynamics of blockchain technology. The chapter also highlighted various use cases of blockchain in SCM, underscoring the transformative potential of this technology in enhancing supply chain operations. It critically examined a diverse array of consensus mechanisms used within SCM, evaluating their significant impact on both security and operational efficiency. This analysis was particularly vital in understanding how different blockchain deployments could influence the robustness and efficacy of blockchain-integrated SCM frameworks. These findings were crucial in the context of this research as they

provided a nuanced understanding of how blockchain technology can be relatively applied in SCM. Each consensus mechanism, with its unique characteristics, impacts the efficiency, scalability, and security of a blockchain network. Understanding these differences is key to identifying the most suitable blockchain applications for SCM, aligning with the research's aim to enhance security and operational efficiency in SCM systems. This understanding was pivotal in developing recommendations for the adoption of more secure and efficient blockchain systems in SCM, aligning with the overarching aim of enhancing both the security and operational efficiency of SCM frameworks. This methodology is a key contribution of the research, aiming to facilitate the adoption of more secure and efficient blockchain configurations in SCM systems.

9.2.3 Simulation Modelling Tool, BlockSim

After examining the technological foundations of the blockchain and evaluating various types of consensus mechanisms. It became crucial to conduct tests on them. Chapter 5 of the research focused on investigating the simulation tool, BlockSim. Blocksim was crucial in the thesis since it played a vital part in assessing different blockchain consensus algorithms. BlockSim is a versatile and advanced simulation tool specifically created to imitate the functionality and operations of blockchain networks. It provides a regulated setting in which various consensus mechanisms can be replicated and studied without the complications and dangers involved with real-world experiments. Understanding how different consensus algorithms function under various settings and configurations is essential for assessing and improving the efficiency and security of blockchain technologies in SCM.

The chapter methodically details the technical foundations of modelling, the classification of system models, and the steps involved in the simulation study. It delved into and highlighted the inner workings of BlockSim, including its base model and various layers such as the network layer, consensus layer, and application layer. By doing so, it provided an in-depth understanding of how blockchain networks can be modelled and simulated for research purposes. The necessity of creating simulations in this research lies in the ability to meticulously analyse different consensus mechanisms, such as PoW, DPoS, and the newly proposed PoEf, in a controlled and measurable manner. The simulations facilitated the assessment of key performance metrics like throughput, latency, and scalability, which are crucial in determining the suitability of consensus mechanisms for SCM systems. Furthermore, by employing BlockSim, the research was able to test hypotheses and explore scenarios that would be difficult or impractical to recreate in a real-world setting. This includes stress-testing the systems under high transaction loads, examining the impact of network size on performance, and understanding the resilience of the proposed consensus

mechanism, PoEf, to various types of cyber threats. The insights gained from the BlockSim simulations are essential in guiding the development of more efficient and secure blockchain configurations, directly contributing to the overarching aim of enhancing SCM systems through blockchain technology.

9.2.4 The Data Collected

Blocksim facilitated the collection of datasets to evaluate the different consensus mechanisms to understand the practical implications and performance efficiencies of different consensus models used the realm of SCM. This phase of the research (Chapter 6) presented the data collected from simulations, which serve as a foundation for a comparative analysis of various consensus mechanisms. The key performance metrics evaluated were throughput efficiency, latency, and scalability.

- Throughput efficiency assessment is crucial as it determines the transaction processing capacity of the blockchain. For SCM systems, where large volumes of transactions occur, a high throughput is essential to maintain operational fluency and real-time data processing.
- Latency evaluation focuses on the time taken by the consensus mechanism to process and validate a transaction. In SCM, reduced latency is vital for ensuring timely decision-making and maintaining the flow of operations, particularly in environments requiring real-time data analysis.
- Scalability analysis addresses the ability of the consensus mechanism to maintain or enhance performance in response to an increase in transaction volumes or network expansion. This is particularly relevant for SCM, as supply chains are dynamic entities that often experience fluctuations in transaction volumes and network size.

By collecting and analysing data on these performance metrics, the author was able to identify which consensus mechanisms are most suited for different types of Supply Chains. The findings are crucial for making informed decisions about the integration of blockchain technology into SCM systems, ensuring that the selected consensus mechanism aligns with the specific operational needs and scalability requirements of particular SCM systems.

9.2.5 Experimentation: The novel PoEf Consensus Algorithm

The final stage of the research (Chapter 7) presented the novel PoEf mechanism which stands out for its bespoke design and is a beacon of innovation in this research. The PoEf consensus mechanism was designed specifically to address the limitations of existing blockchain consensus mechanisms in the context of SCM by enhancing the operational aspects of blockchain of how the blockchain process requests. Its

design focuses on optimizing throughput efficiency, minimizing latency, and improving scalability, all key factors that influence the performance and applicability of blockchain technology in SCM systems. In comparison to traditional consensus mechanisms such as PoW, PoS, and various other proof-based and voting-based systems, PoEf exhibits several distinct advantages to meet SCM's intricate demands with precision. Primarily, its layered structure allows for parallel processing, significantly improving transaction throughput and reducing latency. This is a critical enhancement over existing systems, where the consensus process often becomes a bottleneck, impeding the blockchain's overall performance. Additionally, the PoEf mechanism's focus on efficiency addresses one of the most pressing criticisms of conventional blockchain technologies, especially those reliant on PoW. By reducing the energy requirements and computational intensity, PoEf not only enhances environmental sustainability but also makes the blockchain application more viable and cost-effective for SCM scenarios. The proposed PoEf consensus mechanism marks a significant advancement in blockchain technology, specially tailored to address the specific challenges in SCM. By balancing efficiency, security, and scalability, PoEf offers a promising solution to the limitations of existing blockchain consensus algorithms.

The development and testing of PoEf have already made major advancements in blockchain research, particularly in improving efficiency and security in consensus methods. To further enhance the algorithm's capabilities, further investigations could enhance the existing research by doing alternative simulation studies on the PoEf algorithm. These investigations could concentrate on increasing the transactions volumes and frequency in an effort to analysing the performance of PoEf in high-volume transaction settings for extended durations. This essentially would provide insights into its long-term operational effectiveness. Moreover, the implementation of PoEf in real-world pilot projects in SCM could reveal realistic applications and concrete effects in genuine business scenarios. To fully comprehend the adaptability of PoEf, it is essential to include a wide range of industries and operational scales in this expansion. Future researchers have the potential to expand the utilisation of the PoEf mechanism in different scenarios within SCM. They can also explore the compatibility of PoEf with other blockchain platforms and existing SCM systems, such as those in hybrid blockchain setups or those integrated with legacy systems. Performing a thorough vulnerability analysis, which includes rigorous stress testing under various circumstances and possible attack scenarios, might also yield fascinating findings regarding the resistance of PoEf against sophisticated cybersecurity attacks. All these investigations could yield valuable insights into future development of the PoEf algorithm.

PoEf is an innovative concept in the field of Blockchain-based Supply Chain Management that has the capacity to address technological inefficiencies that have previously impeded the broader acceptance of

blockchain technology in SCM. The implementation of PoEf is expected to significantly transform SCM methods, resulting in supply chains that are not only safer and more efficient but also more flexible in meeting changing business requirements. Any progress made in blockchain technology is crucial, as the technology grows, innovations such as PoEf has the potential to be a turning point in the wider adoption and improvement of blockchain applications in supply chain management. This, in turn, will have a knock-on ripple effect in enhancing the durability and efficiency of global supply networks.

9.2.6 Key Contributions of thesis

In conclusion, this thesis contributes a layered and multifaceted perspective on blockchain in SCM that successfully addresses the primary aim of scrutinizing and assessing the cybersecurity challenges and efficiency considerations in blockchain applications within SCM systems. It underscores the need for robust, scalable, and sustainable SCM systems, leveraging the full potential of blockchain technology to meet the burgeoning demands of modern trade and commerce. The journey from conceptual analysis to practical application recommendations encapsulates a wide-ranging approach to blockchain in SCM, setting the stage for future academic discussions and technological advancements. Through comprehensive research and analysis, the thesis critically evaluated how different blockchain deployments impact the security robustness and operational efficacy of blockchain-integrated SCM methodologies. Key achievements of this research include:

- **Cybersecurity Challenges and Efficiency Considerations:** The thesis provided an in-depth analysis of cybersecurity challenges in blockchain-based SCM systems. This included a systematic literature review that identified key areas of concern such as consensus mechanism failures, smart contract vulnerabilities, network-level attacks, and cryptographic challenges. The analysis highlighted the critical need for enhanced security and efficiency in blockchain deployments for SCM.
- **Evaluation of Blockchain Deployments:** A thorough examination of various blockchain consensus mechanisms was conducted, assessing their implications for SCM systems. This evaluation involved innovative simulations using the BlockSim tool, providing empirical evidence on the performance of different consensus mechanisms in terms of throughput efficiency, latency, and scalability.
- **Introduction of PoEf Consensus Mechanism:** A significant contribution of this research was the development of the PoEf consensus mechanism. PoEf was designed to optimize the performance of blockchain deployments in SCM, focusing on improving throughput, reducing latency, and

enhancing scalability. The simulations demonstrated that PoEf outperforms traditional consensus mechanisms like PoW, DPoS, and PBFT in these aspects.

- **Methodology for Consensus Mechanism Selection:** The research culminated in the development of a methodology for selecting the most suitable blockchain consensus mechanism for SCM. This methodology guides practitioners in choosing the most appropriate blockchain configuration based on specific SCM requirements, thereby facilitating more secure and efficient blockchain implementations. By improving latency, throughput, and scalability, blockchain technology can significantly enhance both efficiency and security across various stages of SCM, from procurement and logistics to inventory management and customer service.

Overall, this thesis makes a substantial contribution to the field of blockchain in SCM. It not only provides a critical evaluation of current challenges and inefficiencies but also establishes a foundation for subsequent exploration, development and innovations that will pave the way for more secure and efficient supply chain operations in the digital age. The insights and methodology developed in this research have the potential to significantly influence the adoption and optimization of blockchain technology in SCM systems, ultimately enhancing the resilience, transparency, and effectiveness of global supply networks.

9.3 Challenges

- Initially, it was planned to complete all the stages presented in Table 6.1 as part of this PhD research. As the research advanced, it became evident that the scale of this project exceeded the capacity of a single PhD and required division into smaller, more manageable stages. At this juncture, the decision was made to concentrate solely on a single phase of the entire research endeavour. It was also a valuable lesson in avoiding the pitfall of a PhD being overly expansive by attempting to accomplish too many objectives and ensuring that the research remains focused to clearly demonstrate its benefits.
- Due to the scarcity of prior studies integrating these distinct disciplines, there was a dearth of existing work upon which this research could be based. While there was some degree of freedom in determining the routes to pursue, having a more extensive corpus of prior work that integrates several disciplines would have instilled better confidence in making these judgements.

- This thesis integrated the three domains of Blockchain, security, and supply chain management. The researcher, whose background was in computer science, explored the latter subject, which was previously unfamiliar to them. This led to the difficulty of finding a balance between a knowledge domain that was highly familiar and another that was relatively unfamiliar to the researcher. Nevertheless, despite the difficulties, it also sparked curiosity about the integration of these three distinct fields and showcased the significance and attractiveness of interdisciplinary studies. In essence, if there is a genuine interest in one field, it is conceivable to have excitement for both, as the curiosity to explore how that expertise might be utilised in other areas is always present.

9.4 Future Directions

The exploration of the Proof-of-Efficiency (PoEf) mechanism provides a foundation for future research endeavours, particularly in the realm of blockchain application within SCM. The potential of PoEf extends beyond immediate operational improvements, suggesting a transformative impact on the broader landscape of blockchain technology. There are still numerous possibilities for further expanding this research. As discussed earlier in Chapter 1, the work presented in this thesis is just the initial phase of a multi-stage endeavour, as indicated in Table 9.1. As illustrated in the table, future research (Stages 2-4) should focus on further refining this mechanism, exploring the other layers (network and data layers) of this blockchain its application in various SCM scenarios, using different types of hardware and investigating its potential broader impacts on the blockchain ecosystem. This is important to get to an all-round “close to real-world” adoption and aligns with the research objectives of critically 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.

Stage 1	Stage 2	Stage 3	Stage 4	Stage 5
Assessment, evaluation, and testing of different types of Consensus Mechanisms in SCM systems	Assessment, evaluation, and testing of different types of Smart Contract deployments in SCM	Assessment, evaluation, and testing of different Network-Level attacks of Blockchain-based in SCMs	Assessment, evaluation, and testing of different Cryptographic Techniques used Blockchain-based in SCMs	Development of a computational framework for designing blockchain-based SCMs

TABLE 9.1: Table illustrating research stages.

This thesis has effectively accomplished the initial phase of this thesis endeavour. The following are explicit suggestions for future endeavours, along with their respective impact on each phase.

9.4.1 Stage 2: Assessment, evaluation, and testing of different types of Smart Contract deployments in SCM

Exploring the application/presentation layer that houses smart contracts, and understanding the vulnerabilities inherent in these smart contracts, is crucial for advancing this research and achieving its aim. This approach is vital for several reasons:

- **Integration with Consensus Mechanisms:** Smart contracts operate in tandem with consensus mechanisms, executing predefined rules upon achieving consensus. Understanding how smart contracts interact with different consensus mechanisms can significantly influence the overall security and efficiency of blockchain applications in SCM. By examining this interplay, the research can offer more holistic solutions that consider both the execution layer (smart contracts) and the agreement layer (consensus mechanisms).
- **Critical Role in Automation and Efficiency:** Smart contracts are pivotal in automating and streamlining SCM processes. They facilitate trust-less agreements and transactions, thereby enhancing the efficiency of supply chains. However, vulnerabilities within these contracts can undermine these benefits. By identifying and addressing these vulnerabilities, the research contributes to developing more reliable and efficient blockchain-based SCM systems.
- **Complex and Subtle Vulnerabilities:** The vulnerabilities in smart contracts are often not apparent and require detailed analysis. These vulnerabilities can range from programming errors to design flaws. Exploring these vulnerabilities is essential to ensure the integrity and reliability of SCM systems. It helps in understanding the depth and breadth of potential risks and in developing strategies to mitigate them.
- **Real-World Impact on SCM Systems:** Vulnerabilities in smart contracts can lead to significant disruptions in SCM operations, including financial losses and reputational damage. By analysing case studies and real-world incidents, the research gains insights into the practical implications of these vulnerabilities and how they can affect SCM systems. This understanding is crucial for developing robust and resilient blockchain solutions for SCM.

Exploring the application/presentation layer and vulnerabilities in smart contracts is essential for advancing the development of this research. It ensures a complete understanding of both the technical and human aspects of blockchain technology, leading to the development of more secure, efficient, and resilient blockchain-integrated SCM systems. By addressing this area, the research moves closer to its aim of enhancing the all-round security robustness and operational efficacy of blockchain deployments in SCM.

9.4.2 Stage 3: Assessment, evaluation, and testing of different Network-Level attacks of Blockchain-based SCMs.

Exploring the network layer and analysing network-level attacks in blockchain applications are fundamental steps in advancing this research and fulfilling its primary aim. Focusing on these aspects is crucial due to the following reasons:

- **Inherent Vulnerability of Networked Infrastructure:** Blockchain's reliance on networked infrastructure inherently exposes it to various network-level attacks. Understanding these vulnerabilities is essential to ensure the security and robustness of blockchain SCM systems. By identifying and addressing these vulnerabilities, the research contributes to the creation of more secure and resilient blockchain networks. The exploration of network attack vectors and their specific relevance to blockchain SCM provides a focused understanding of the risks involved. This is crucial for developing targeted countermeasures that cater to the unique needs and structures of blockchain SCM systems.
- **Countermeasures and Resilience:** Presenting and assessing various countermeasures such as network segmentation, secure routing protocols, and real-time monitoring systems are vital in enhancing the security posture of blockchain SCM systems. This research aspect aims to identify effective strategies that can be implemented to mitigate network-level threats.
- **Reliability and Timeliness of SCM Operations:** Network-level attacks can significantly impact the reliability and timeliness of SCM operations. Analysing the implications of these attacks helps in understanding how they can affect the supply chain's performance and in devising measures to maintain operational continuity.

- **Holistic Security Approach:** After exploring consensus mechanisms and smart contracts, focusing on the network layer completes the holistic approach to blockchain security. It ensures that all potential vulnerabilities are addressed, contributing to the development of a security framework for blockchain SCM systems.

Exploring the network layer and network-level attacks is imperative for advancing this research towards achieving its aim. It enriches the understanding of the security challenges faced by blockchain SCM systems and fosters the development of robust, secure, and efficient blockchain solutions for SCM. This approach aligns with the research's aim of scrutinizing and enhancing the cybersecurity robustness and operational efficacy of blockchain-integrated SCM frameworks.

9.4.3 Stage 4: Assessment, evaluation, and testing of different Cryptographic Techniques used Blockchain-based in SCMs.

Exploring the data layer and addressing cryptographic challenges in blockchain applications is a crucial next step for this research to achieve its aim. This stage is vital for several reasons:

- **Foundation of Blockchain Security:** Cryptography is the cornerstone of blockchain security. Exploring cryptographic challenges is fundamental in ensuring the robustness and integrity of blockchain SCM systems. As the research moves from examining smart contracts and the network layer, focusing on the data layer's cryptographic aspects helps in comprehensively securing the blockchain from multiple angles.
- **Vulnerabilities in Cryptographic Primitives:** Understanding vulnerabilities in cryptographic primitives such as hash functions, digital signature algorithms, and encryption methods is essential. These are central to the functioning of blockchain technology, and any weakness in these areas could compromise the entire SCM system. Analysing these vulnerabilities will help in identifying and addressing potential security flaws. Cryptographic failures can also significantly impact data integrity and non-repudiation in SCM systems. Since supply chain management heavily relies on the authenticity and integrity of data, ensuring the robustness of cryptographic methods is imperative to enhancing trust and reliability in blockchain-based SCM systems.
- **Holistic Security Approach:** By examining cryptographic challenges after exploring smart contracts and the network layer, the research adopts a holistic approach to blockchain security. It ensures

that all aspects of security, from application to network to data, are broadly covered. Addressing cryptographic challenges aligns with the research's aim of scrutinizing and enhancing the cybersecurity robustness of blockchain-integrated SCM frameworks. It contributes to developing and recommending comprehensive frameworks for selecting suitable blockchain technologies, focusing on security and efficiency.

Exploring cryptographic challenges in blockchain SCM systems is the next critical stage in this research. It is essential for advancing the development of the research and achieving its aim of creating secure, robust, and efficient blockchain SCM systems. This approach ensures that the research meticulously addresses all layers of blockchain technology, contributing significantly to the field of blockchain in SCM.

9.4.4 Stage 5: Development of a computational framework for designing secure blockchain-based SCMs

After an exhaustive analysis of the consensus, application, network, and data layers in blockchain SCM systems, the insights would be used to propose an integrated security framework. The essence of this framework lies in its layered security measures, designed to holistically address each category of risk identified in previous chapters. The proposed framework would adopt a multi-layered security strategy, ensuring that each aspect of the blockchain SCM, from data integrity and smart contract execution to consensus process and network resilience, is robustly protected. This involves implementing tailored security protocols at every layer, creating a cohesive and fortified defence mechanism against potential breaches. By integrating insights from each critical area of blockchain SCM systems, the framework serves as a blueprint for secure implementations. This ensures a balanced focus not only on the present challenges but also on future developments in the field of blockchain and cybersecurity.

This research journey has meticulously dissected the various facets of blockchain technology as applied to SCM, highlighting the opportunities and challenges it presents. The culmination of this research in the development of a computational framework marks a significant contribution to the field, providing a roadmap for the secure and efficient implementation of blockchain in SCM. The framework proposed in this thesis is not just a response to current cybersecurity challenges but also a proactive step towards future proofing SCM systems. It embodies a holistic approach to security, considering the interconnected nature of blockchain technology, and offers practical, actionable strategies for organizations looking to leverage blockchain in their SCM operations. Finally, the thesis emphasizes the need for collaborative efforts between technologists, industry experts, and policymakers to foster the development of robust, secure,

and efficient blockchain SCM systems. This collaborative approach is crucial for realizing the full potential of blockchain technology in transforming SCM practices, making them more transparent, efficient, and secure.

10 References

- [1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: www.bitcoin.org
- [2] C. Devecchi *et al.*, "Blockchain Educational Passport: Decentralised Learning Ledger (DLL)," *Development Heads: Sajin Abdu (Technology)*, (DII). 2017.
- [3] M. Swan, *Blockchain: Blueprint for a new economy*. "O'Reilly Media, Inc.," 2015.
- [4] N. Upadhyay, "Demystifying blockchain: A critical analysis of challenges, applications and opportunities," *Int J Inf Manage*, vol. 54, Oct. 2020, doi: 10.1016/j.ijinfomgt.2020.102120.
- [5] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthcare (Switzerland)*, vol. 7, no. 2. MDPI, Jun. 01, 2019. doi: 10.3390/healthcare7020056.
- [6] O. Ali, M. Ally, Clutterbuck, and Y. Dwivedi, "The state of play of blockchain technology in the financial services sector: A systematic literature review," *International Journal of Information Management*, vol. 54. Elsevier Ltd, Oct. 01, 2020. doi: 10.1016/j.ijinfomgt.2020.102199.
- [7] 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>.
- [8] G. J. Katuwal, S. Pandey, M. Hennessey, and B. Lamichhane, "Applications of Blockchain in Healthcare: Current Landscape & Challenges," *arXiv preprint arXiv:1812.02776*, Dec. 2018, [Online]. Available: <http://arxiv.org/abs/1812.02776>
- [9] 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.
- [10] 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.
- [11] 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.
- [12] M. Torky and A. E. Hassanein, "Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges," *Computers and Electronics in Agriculture*, vol. 178. Elsevier B.V., Nov. 01, 2020. doi: 10.1016/j.compag.2020.105476.
- [13] 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," *IEEE Access*, vol. 8. Institute of Electrical and Electronics Engineers Inc., pp. 32031–32053, 2020. doi: 10.1109/ACCESS.2020.2973178.
- [14] 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.
- [15] 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.
- [16] J. Heppelmann, "How the Internet of Things could transform the value chain," *McKinsey & Company*, vol. 92, no. 11, Nov. 2014.
- [17] 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.
- [18] 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.
- [19] 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.

- [20] M. Casey and P. Wong, "Global Supply Chains Are About to Get Better, Thanks to Blockchain," *Harvard Business Review*. Accessed: Aug. 24, 2022. [Online]. Available: <https://hbr.org/2017/03/global-supply-chains-are-about-to-get-better-thanks-to-blockchain>
- [21] K. Toyoda, P. Takis Mathiopoulos, I. Sasase, and T. Ohtsuki, "A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain," *IEEE Access*, vol. 5, pp. 17465–17477, Jun. 2017, doi: 10.1109/ACCESS.2017.2720760.
- [22] 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.
- [23] M. Attaran, "RFID: An enabler of supply chain operations," *Supply Chain Management*, vol. 12, no. 4, pp. 249–257, 2007, doi: 10.1108/13598540710759763.
- [24] F. Thiesse, T. Staake, P. Schmitt, and E. Fleisch, "The rise of the 'next-generation bar code': An international RFID adoption study," *Supply Chain Management*, vol. 16, no. 5, pp. 328–345, Aug. 2011, doi: 10.1108/13598541111155848.
- [25] T. Papadopoulos, A. Gunasekaran, R. Dubey, N. Altay, S. J. Childe, and S. Fosso-Wamba, "The role of Big Data in explaining disaster resilience in supply chains for sustainability," *J Clean Prod*, vol. 142, pp. 1108–1118, Jan. 2017, doi: 10.1016/j.jclepro.2016.03.059.
- [26] G. Büyüközkan and F. Göçer, "Digital Supply Chain: Literature review and a proposed framework for future research," *Comput Ind*, vol. 97, pp. 157–177, May 2018, doi: 10.1016/j.compind.2018.02.010.
- [27] V. J. Morkunas, J. Paschen, and E. Boon, "How blockchain technologies impact your business model," *Bus Horiz*, vol. 62, no. 3, pp. 295–306, May 2019, doi: 10.1016/J.BUSHOR.2019.01.009.
- [28] E. Hofmann and M. Rüsch, "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.
- [29] 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.
- [30] U. Agarwal *et al.*, "Blockchain Technology for Secure Supply Chain Management: A Comprehensive Review," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2022.3194319.
- [31] 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.
- [32] 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.
- [33] 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.
- [34] 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.
- [35] H. Treiblmaier, "The impact of the blockchain on the supply chain: a theory-based research framework and a call for action," *Supply Chain Management*, vol. 23, no. 6, pp. 545–559, Nov. 2018, doi: 10.1108/SCM-01-2018-0029/FULL/PDF.
- [36] 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.
- [37] 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.
- [38] 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.
- [39] 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.

- [40] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A Comprehensive Survey of Blockchain: From Theory to IoT Applications and beyond," *IEEE Internet Things J*, vol. 6, no. 5, pp. 8114–8154, Oct. 2019, doi: 10.1109/JIOT.2019.2922538.
- [41] S. F. Wamba and M. M. Queiroz, "Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities," *Int J Inf Manage*, vol. 52, p. 102064, Jun. 2020, doi: 10.1016/J.IJINFOMGT.2019.102064.
- [42] M. M. Queiroz, S. C. F. Pereira, R. Telles, and M. C. Machado, "Industry 4.0 and digital supply chain capabilities: A framework for understanding digitalisation challenges and opportunities," *Benchmarking*, vol. 28, no. 5, pp. 1761–1782, 2019, doi: 10.1108/BIJ-12-2018-0435/FULL/XML.
- [43] 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.
- [44] 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.
- [45] 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.
- [46] 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.
- [47] 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.
- [48] J. Webster and R. T. Watson, "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *Quarterly*, vol. 26, no. 2, pp. xiii–xxiii, 2002.
- [49] C. Okoli and K. Schabram, "Working Papers on Information Systems A Guide to Conducting a Systematic Literature Review of Information Systems Research A Guide to Conducting a Systematic Literature Review of Information Systems Research," 2010.
- [50] P. Brereton, "A study of computing undergraduates undertaking a systematic literature review," *IEEE Transactions on Education*, vol. 54, no. 4, pp. 558–563, Nov. 2011, doi: 10.1109/TE.2010.2090662.
- [51] F. M. , L. M. J. Jesson. Lacey, *Doing your literature review: Traditional and systematic techniques*. Doing Your Literature Review , 2011.
- [52] 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.
- [53] 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.
- [54] 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.
- [55] 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.
- [56] 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.
- [57] B. A. Kitchenham, "Systematic review in software engineering," pp. 1–2, Sep. 2012, doi: 10.1145/2372233.2372235.

- [58] 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.
- [59] 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.
- [60] 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.
- [61] 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.
- [62] I. Eyal and E. G. Sirer, "Majority is Not Enough: Bitcoin Mining is Vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, Jun. 2018, doi: 10.1145/3212998.
- [63] 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.
- [64] 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.
- [65] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (SoK)," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10204 LNCS, pp. 164–186, 2017, doi: 10.1007/978-3-662-54455-6_8/FIGURES/1.
- [66] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies," *Proc IEEE Symp Secur Priv*, pp. 375–392, Jun. 2017, doi: 10.1109/SP.2017.29.
- [67] M. Saad *et al.*, "Exploring the Attack Surface of Blockchain: A Systematic Overview," Apr. 2019, Accessed: Dec. 19, 2023. [Online]. Available: <https://arxiv.org/abs/1904.03487v1>
- [68] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, Jun. 2020, doi: 10.1016/J.FUTURE.2017.08.020.
- [69] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things," *IEEE Wirel Commun*, vol. 25, no. 6, pp. 12–18, Dec. 2018, doi: 10.1109/MWC.2017.1800116.
- [70] E.-R. Latifa, E. L. Kiram, and M. Y. Ahemed, "Journal of Internet Banking and Commerce BLOCKCHAIN: BITCOIN WALLET CRYPTOGRAPHY SECURITY, CHALLENGES AND COUNTERMEASURES," *Journal of Internet Banking and Commerce*, vol. 22, no. 3, 2017, Accessed: Dec. 19, 2023. [Online]. Available: <http://www.icommercecentral.com>
- [71] S. Singh, A. S. M. S. Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021, doi: 10.1109/ACCESS.2021.3051602.
- [72] P. Myers, *Knowledge Management and Organizational Design*, vol. 1. Routledge, 2009. doi: <https://doi.org/10.4324/9780080509839>.
- [73] J. W. Creswell, R. Shope, V. L. Plano Clark, and D. O. Green, "How interpretive qualitative research extends mixed methods research," *Research in the Schools*, vol. 13, no. 1, pp. 1–11, 2006.
- [74] N. K. Denzin, "Triangulation 2.0," *J Mix Methods Res*, vol. 6, no. 2, pp. 80–88, Feb. 2012, doi: 10.1177/1558689812437186.
- [75] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and the PRISMA Group*, "Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement," *Ann Intern Med*, vol. 151, no. 4, pp. 264–269, 2009.
- [76] M. Easterby-Smith, R. Thorpe, and P. (Paul R.) Jackson, *Management Research*, 4th ed. 2012.

- [77] G. G. Gable, "Integrating case study and survey research methods: an example in information systems," *European Journal of Information Systems* 1994 3:2, vol. 3, no. 2, pp. 112–126, Jan. 1994, doi: 10.1057/EJIS.1994.12.
- [78] J. Collis and R. Hussey, *Business Research: A Practical Guide for Students*, 4th ed. Palgrave Macmillan, 2014. Accessed: Mar. 30, 2022. [Online]. Available: https://books.google.co.uk/books?hl=en&lr=&id=NnhkEAAQBAJ&oi=fnd&pg=PT12&dq=Collis,+J.+and+Hussey,+R.&ots=Qb641F0cOz&sig=JedGkGrmi_fRAchiJDfFFkNKx_0#v=onepage&q=Collis%2C%20J.%20and%20Hussey%2C%20R.&f=false
- [79] R. K. Yin, "Designing case studies," *Qualitative research methods*, vol. 5, no. 14, pp. 359–386, 2003.
- [80] J. Popay *et al.*, "Guidance on the conduct of narrative synthesis in systematic reviews," *A product from the ESRC methods programme Version*, vol. 1, no. 1, p. b92, 2006.
- [81] G. Dodig-Crnkovic, "Scientific Methods in Computer Science," *Proceedings of the Conference for the Promotion of Research in IT at New Universities and at University Colleges in Sweden*. Skövde, Suecia, pp. 126–130, Apr. 2002.
- [82] Hevner, March, Park, and Ram, "Design Science in Information Systems Research," *MIS Quarterly*, vol. 28, no. 1, p. 75, 2004, doi: 10.2307/25148625.
- [83] 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)*, 2022, pp. 1–5. doi: 10.1109/ICBC54727.2022.9805504.
- [84] 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, 2018, doi: <https://doi.org/10.1016/j.cie.2018.09.054>.
- [85] 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: <https://doi.org/10.1046/j.1365-2575.2000.00088.x>.
- [86] 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.
- [87] T. Edgar and D. Manz, *Research methods for cyber security*. Syngress, 2017.
- [88] K. E. Wegrzyn and E. Wang, "Types of Blockchain: Public, Private, or Something in Between." Accessed: Dec. 11, 2022. [Online]. Available: <https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between>
- [89] 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.
- [90] 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.
- [91] 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.
- [92] 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.
- [93] F. Longo, L. Nicoletti, A. Padovano, G. d'Atri, and M. Forte, "Blockchain-enabled supply chain: An experimental study," *Comput Ind Eng*, vol. 136, pp. 57–69, Oct. 2019, doi: 10.1016/J.CIE.2019.07.026.
- [94] 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.

- [95] K. Biswas, V. Muthukkumarasamy, and W. L. Tan, "Blockchain based wine supply chain traceability system," in *Future Technologies Conference (FTC) 2017*, The Science and Information Organization, 2017, pp. 56–62.
- [96] 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.
- [97] 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.
- [98] N. El Ioini and C. Pahl, "A review of distributed ledger technologies," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11230 LNCS, pp. 277–288, 2018, doi: 10.1007/978-3-030-02671-4_16/COVER.
- [99] 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.
- [100] M. Singh and S. Kim, "Blockchain Based Intelligent Vehicle Data sharing Framework," Jul. 2017, Accessed: Dec. 19, 2023. [Online]. Available: <https://arxiv.org/abs/1708.09721v1>
- [101] J. A. Kroll, I. C. Davey, and E. W. Felten, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries," *Proceedings of WEIS*, vol. 2013, no. 11, 2013.
- [102] M. Vasek and T. Moore, "There's no free lunch, even using bitcoin: Tracking the popularity and profits of virtual currency scams," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8975, pp. 44–61, 2015, doi: 10.1007/978-3-662-47854-7_4/COVER.
- [103] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9603 LNCS, pp. 515–532, 2017, doi: 10.1007/978-3-662-54970-4_30/COVER.
- [104] 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.
- [105] V. Buterin and V. Griffith, "Casper the Friendly Finality Gadget," Oct. 2017, Accessed: Dec. 20, 2023. [Online]. Available: <https://arxiv.org/abs/1710.09437v4>
- [106] Y. Sompolinsky and A. Zohar, "Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains," *Cryptology ePrint Archive*, 2013.
- [107] 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.
- [108] 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.
- [109] 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.
- [110] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Portfolio, 2016.
- [111] 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.
- [112] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, "BlockChain Technology: Beyond Bitcoin," *Applied Innovation Review*, no. 2, Jun. 2016.
- [113] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The Blockchain as a Decentralized Security Framework [Future Directions]," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, Mar. 2018, doi: 10.1109/MCE.2017.2776459.

- [114] 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.
- [115] S. , Bano, M. , Al-Bassam, and G. Danezis, "The Road to Scalable Blockchain Designs Functional Components of a Blockchain," *USENIX; magazine*, 2017. [Online]. Available: www.usenix.org
- [116] Eye For Transport, "2017 Supply Chain Trends Recap ," 2017. Accessed: Dec. 26, 2023. [Online]. Available: <https://www.reutersevents.com/supplychain/content/2017-supply-chain-trends-recap>
- [117] R. Azzi, R. K. Chamoun, and M. Sokhn, "The power of a blockchain-based supply chain," *Comput Ind Eng*, vol. 135, pp. 582–592, Sep. 2019, doi: 10.1016/J.CIE.2019.06.042.
- [118] S. King and S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," *Self-published Paper*, vol. 1, Aug. 2012.
- [119] V. Buterin, "A next-generation smart contract and decentralized application platform," *White Paper*, vol. 3, no. 37, pp. 1–2, 2014, Accessed: Jun. 22, 2023. [Online]. Available: https://docs.nem.io/pages/Whitepapers/NEM_techRef.pdf
- [120] A. Litke, D. Anagnostopoulos, and T. Varvarigou, "Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment," *Logistics 2019, Vol. 3, Page 5*, vol. 3, no. 1, p. 5, Jan. 2019, doi: 10.3390/LOGISTICS3010005.
- [121] 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.
- [122] A. Nember, "NEM Technical Reference," Feb. 2018.
- [123] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8975, pp. 528–547, 2015, doi: 10.1007/978-3-662-47854-7_33/COVER.
- [124] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10401 LNCS, pp. 357–388, 2017, doi: 10.1007/978-3-319-63688-7_12/FIGURES/6.
- [125] D. Ongaro and J. Ousterhout, "In Search of an Understandable Consensus Algorithm (Extended Version)," in *2014 USENIX annual technical conference (USENIX ATC 14)*, 2014.
- [126] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *OsDI*, 1999, pp. 173–186.
- [127] D. Mazières, "The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus," Jul. 2015.
- [128] X. Fu, H. Wang, and P. Shi, "A survey of Blockchain consensus algorithms: mechanism, design and applications," *Science China Information Sciences*, vol. 64, no. 2, pp. 1–15, Feb. 2021, doi: 10.1007/S11432-019-2790-1/METRICS.
- [129] R. Beck, C. Müller-Bloch, and J. King, "Governance in the Blockchain Economy: A Framework and Research Agenda," *J Assoc Inf Syst*, vol. 19, no. 10, Oct. 2018, Accessed: Dec. 23, 2023. [Online]. Available: <https://aisel.aisnet.org/jais/vol19/iss10/1>
- [130] M. Montecchi, K. Plangger, and M. Etter, "It's real, trust me! Establishing supply chain provenance using blockchain," *Bus Horiz*, vol. 62, no. 3, pp. 283–293, May 2019, doi: 10.1016/J.BUSHOR.2019.01.008.
- [131] S. S. Kamble, A. Gunasekaran, V. Kumar, A. Belhadi, and C. Foropon, "A machine learning based approach for predicting blockchain adoption in supply Chain," *Technol Forecast Soc Change*, vol. 163, p. 120465, Feb. 2021, doi: 10.1016/J.TECHFORE.2020.120465.
- [132] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2018 - Proceedings*, pp. 1545–1550, Jun. 2018, doi: 10.23919/MIPRO.2018.8400278.
- [133] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy*, 2015, pp. 104–121. doi: 10.1109/SP.2015.14.

- [134] P. Zheng, Z. Zheng, X. Luo, X. Chen, and X. Liu, "A detailed and real-time performance monitoring framework for blockchain systems," *Proceedings - International Conference on Software Engineering*, pp. 134–143, May 2018, doi: 10.1145/3183519.3183546.
- [135] H. Vranken, "Sustainability of bitcoin and blockchains," *Curr Opin Environ Sustain*, vol. 28, pp. 1–9, Oct. 2017, doi: 10.1016/J.COSUST.2017.04.011.
- [136] 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.
- [137] G. I. Navaroj, E. G. Julie, and Y. H. Robinson, "Adaptive practical Byzantine fault tolerance consensus algorithm in permission blockchain network," *International Journal of Web and Grid Services*, vol. 18, no. 1, pp. 62–82, 2022, doi: 10.1504/IJWGS.2022.119273.
- [138] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9216, pp. 585–605, 2015, doi: 10.1007/978-3-662-48000-7_29/FIGURES/1.
- [139] L. Ren and S. Devadas, "Proof of space from stacked expanders," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9985 LNCS, pp. 262–285, 2016, doi: 10.1007/978-3-662-53641-4_11/TABLES/3.
- [140] 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," *ACM International Conference Proceeding Series*, pp. 510–513, Dec. 2021, doi: 10.1145/3498851.3499007.
- [141] D. Schwartz, N. Youngs, and A. Britto, "The Ripple Protocol Consensus Algorithm," *Ripple Labs Inc White Paper*, vol. 5, no. 8, Sep. 2014, Accessed: Dec. 23, 2023. [Online]. Available: <https://arxiv.org/abs/1802.07242>
- [142] I. Amores-Sesar, C. Cachin, and J. Micic, "Security Analysis of Ripple Consensus," *Leibniz International Proceedings in Informatics, LIPIcs*, vol. 184, Nov. 2020, doi: 10.4230/LIPIcs.OPODIS.2020.10.
- [143] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things," *14th International Conference on Services Systems and Services Management, ICSSSM 2017 - Proceedings*, Jul. 2017, doi: 10.1109/ICSSSM.2017.7996119.
- [144] 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.
- [145] 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>.
- [146] 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/ASSET/IMAGES/LARGE/10.1177_14604582211011228-FIG3.JPEG.
- [147] G. M. Hastig and M. 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.
- [148] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, and H. Y. Lam, "Blockchain-Driven IoT for Food Traceability with an Integrated Consensus Mechanism," *IEEE Access*, vol. 7, pp. 129000–129017, 2019, doi: 10.1109/ACCESS.2019.2940227.
- [149] J. Mendling *et al.*, "Blockchains for Business Process Management - Challenges and Opportunities," *ACM Trans. Manage. Inf. Syst.*, vol. 9, no. 1, Feb. 2018, doi: 10.1145/3183367.
- [150] 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.

- [151] 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.
- [152] 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.
- [153] 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.
- [154] J. Parra Moyano and O. Ross, “KYC Optimization Using Distributed Ledger Technology,” *Business and Information Systems Engineering*, vol. 59, no. 6, pp. 411–423, Dec. 2017, doi: 10.1007/S12599-017-0504-2/FIGURES/6.
- [155] 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, 2019, doi: <https://doi.org/10.1016/j.compind.2019.04.002>.
- [156] 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.
- [157] M. H. Meng and Y. Qian, “A Blockchain Aided Metric for Predictive Delivery Performance in Supply Chain Management,” *Proceedings of the 2018 IEEE International Conference on Service Operations and Logistics, and Informatics, SOLI 2018*, pp. 285–290, Sep. 2018, doi: 10.1109/SOLI.2018.8476723.
- [158] T. Neudecker, P. Andelfinger, and H. Hartenstein, “A simulation model for analysis of attacks on the Bitcoin peer-to-peer network,” *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, pp. 1327–1332, Jun. 2015, doi: 10.1109/INM.2015.7140490.
- [159] F. Schussler, P. Nasirifard, and H. A. Jacobsen, “Demo abstract: Attack and vulnerability simulation framework for bitcoin-like blockchain technologies,” *Middleware 2018 - Proceedings of the 2018 ACM/IFIP/USENIX Middleware Conference (Posters)*, pp. 5–6, Dec. 2018, doi: 10.1145/3284014.3284017.
- [160] J. Göbel, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor, “Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay,” *Performance Evaluation*, vol. 104, pp. 23–41, Oct. 2016, doi: 10.1016/J.PEVA.2016.07.001.
- [161] Y. Shahsavari, K. Zhang, and C. Talhi, “A Theoretical Model for Block Propagation Analysis in Bitcoin Network,” *IEEE Trans Eng Manag*, vol. 69, no. 4, pp. 1459–1476, Aug. 2022, doi: 10.1109/TEM.2020.2989170.
- [162] A. Aldweesh, M. Alharby, E. Solaiman, and A. Van Moorsel, “Performance Benchmarking of Smart Contracts to Assess Miner Incentives in Ethereum,” *Proceedings - 2018 14th European Dependable Computing Conference, EDCC 2018*, pp. 144–149, Nov. 2018, doi: 10.1109/EDCC.2018.00034.
- [163] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, “Misbehavior in Bitcoin,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 18, no. 1, pp. 1–32, May 2015, doi: 10.1145/2732196.
- [164] Y. Aoki, K. Otsuki, T. Kaneko, R. Banno, and K. Shudo, “SimBlock: A Blockchain Network Simulator,” *INFOCOM 2019 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2019*, pp. 325–329, Apr. 2019, doi: 10.1109/INFCOMW.2019.8845253.
- [165] L. Stoykov, K. Zhang, and H. A. Jacobsen, “VIBES: fast blockchain simulations for large-scale peer-to-peer networks: demo,” *Proceedings of the 18th ACM/IFIP/USENIX Middleware Conference: Posters and Demos*, pp. 19–20, Dec. 2017, doi: 10.1145/3155016.3155020.
- [166] H. Huang, W. Kong, S. Zhou, Z. Zheng, and S. Guo, “A Survey of State-of-the-Art on Blockchains: Theories, Modelings, and Tools,” Jul. 2020, doi: 10.1145/nnnnnnnn.nnnnnnnn.

- [167] E. Babulak and M. Wang, “Discrete event simulation,” *Aitor Goti (Hg.): Discrete Event Simulations. Rijeka, Kroatien: Sciyo*, p. 1, 2010.
- [168] D. R. Anderson, D. J. Sweeney, T. A. Williams, J. D. Camm, and J. J. Cochran, *An introduction to management science: quantitative approach*. Cengage learning, 2018.
- [169] J. Banks, *Discrete event system simulation*. Pearson Education India, 2005.
- [170] L. M. Leemis and S. K. Park, *Discrete-event simulation: A first course*. Pearson Prentice Hall Upper Saddle River, 2006.
- [171] A. Varga, “Discrete event simulation system,” in *Proc. of the European Simulation Multiconference (ESM’2001)*, 2001, pp. 1–7.
- [172] N. Matloff, “Introduction to discrete-event simulation and the Simpy language,” *Davis, CA. Dept of Computer Science. University of California at Davis. Retrieved on August*, vol. 2, no. 2009, pp. 1–33, 2008.
- [173] M. Alharby and A. Van Moorsel, “BlockSim,” *ACM SIGMETRICS Performance Evaluation Review*, vol. 46, no. 3, pp. 135–138, Jan. 2019, doi: 10.1145/3308897.3308956.
- [174] M. Alharby and A. van Moorsel, “BlockSim: An Extensible Simulation Tool for Blockchain Systems,” *Frontiers in Blockchain*, vol. 3, p. 459097, Jun. 2020, doi: 10.3389/FBLOC.2020.00028/BIBTEX.
- [175] 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.
- [176] K. Jeong and J.-D. Hong, “The impact of information sharing on bullwhip effect reduction in a supply chain,” *J Intell Manuf*, vol. 30, pp. 1739–1751, 2019.
- [177] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, “A secure sharding protocol for open blockchains,” *Proceedings of the ACM Conference on Computer and Communications Security*, vol. 24-28-October-2016, pp. 17–30, Oct. 2016, doi: 10.1145/2976749.2978389.
- [178] F. Gai, B. Wang, W. Deng, and W. Peng, “Proof of reputation: A reputation-based consensus protocol for peer-to-peer network,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10828 LNCS, pp. 666–681, 2018, doi: 10.1007/978-3-319-91458-9_41/COVER.
- [179] 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.
- [180] 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.