Lancaster University Leipzig School of Computing and Communications

PRIORITY-BASED CONSENSUS MECHANISM IN PRIVATE BLOCKCHAIN

Deven NavinPrakash Ramchandani

Date of Submission (22/03/2024)

Supervisor: Dr. Jiejun Hu-Bolz

B.Sc. (Hons) Computer Science

Number of words = 14,100
This includes the body of the report only

Declaration of Originality:

I declare that the content and material of this document are my own work and does not contain any unreferenced work and material. Additionally, no part of the implementation or any associated documentation are outsourced. I consent for this document to be electronically stored and copied for assessment purposes, including the university's use of plagiarism detection technologies in order to check the originality and integrity of my work.

I certify that my dissertation being placed in the public domain, with my name explicitly included as the author of the work.

Name: Deven Navin Prakash Ramchandani
Date: 22/03/2024

Abstract:

Priority-based consensus mechanism (PBCM) is a novel consensus mechanism proposed in the report to be used by an organisation as part of their internal transaction management system. The mechanism integrates Practical Byzantine Fault Tolerance (PBFT) with a dynamic grouping mechanism based upon the priority of the transactions in the system. The following paper analyses the predominant state-of-art consensus mechanisms that exist both in public and private domains and uses insights from the analysis to guide various design choices of the novel mechanism. To validate the proposed protocol, the project employs mathematical modelling, simulation of data and implementation within the Hyperledger Fabric platform to assess the mechanism's practicality and optimise performance in metrics including a transaction's size, latency and incentives for nodes. The outcomes of the analysis reveal a promising improvement in PBFT thereby enhancing the efficiency and meeting the requirements set by the organisation. PBCM provides innovative solutions to the organisation as it can manage transactions according to their significance to the company, whilst maintaining network throughput and aligned business objectives.

Table of Contents

Chapter 1 : Project Scope

Chapter 2 : Background and Related Work

Chapter 3 : Consensus Mechanism Review

Chapter 4 : Design of the Proposed Consensus Mechanism

Chapter 5 : Modelling of the Consensus Mechanism

Chapter 6 : Evaluation

Chapter 7 : Conclusion

CHAPTER 1: PROJECT SCOPE

1.1 INTRODUCTION

In today's world where every company across industries are going through a digital transformation, the emphasis is always on continuous improvement of technologies used. The relentless pursuit of adopting new and innovative technologies is not merely about competing with other companies; it's about refining paradigms and expanding horizons. This approach leads companies to offer their best services to their customers, optimise operations , increase productivity and foster greater value creation. In this context, we consider a representative multinational technology corporation that aims for continuous improvement and navigates the digital landscape to find solutions for their internal transaction organisation.

The corporation operates in a dynamic yet volatile technological environment where all processes are automated, providing their software solutions to internal and external clients instantaneously. Operating in a fast-paced industry with a global customer base, the company faces the dual challenges of preserving operational agility and ensuring the highest level of security and efficiency in transaction management. Additionally, it increases the pace of transaction processing for transactions that are time-sensitive and dynamic resource allocation where transactions with the least business cost are prioritised. For a technology company some of the transactions include policy decision-making, internal and external client verifications and payment authorisations. With these challenges, the company embarks on strategy to revolutionise their transaction management approach. This strategy has emerged as the organisation recognises that the traditional centralised systems are becoming inefficient and susceptible to security vulnerabilities. Reliance on a system having a centralised database or a hierarchical structure that requires multiple layers of authorisation and oversight, leads to security exposures and potential delays in transaction processing. Therefore, the corporation has chosen to harness the potential and transformative power of blockchain technology.

Since the birth of Bitcoin in 2008, the world has been introduced to cryptocurrencies - a financial technology introduced by Satoshi Nakamoto [1], it has challenged the traditional aspects of monetary systems, data storage and security. In the contemporary era, we entrust single centralised authorities to manage and conduct transactions. Some well known examples are banks, where individuals allow the enterprises to become custodians of their finances. Centralised transaction management has exposed limitations in transparency and control for individuals, reducing security and integrity.

Blockchain has challenged the established norms of centralisation, where a single authority stores and manages data, to a a decentralized platform where individuals or entities have a detailed overview of all transactions and flows within a network. As an implementation of Distributed Ledger Technology (DLT), blockchain allows multiple agents in a network to maintain an immutable list of transactions. This attribute is at the heart of blockchain's potential, ensuring data integrity and securing transactions. By transitioning their centralised transaction systems to a system based on a blockchain network, the company expects many advantages regarding transactional transparency and immutability. This technological shift promises to be a transformative endeavour poised to foster trust among stakeholders, streamline processes by eliminating intermediaries and mitigating the cyber security threats and malicious data manipulation. Moreover, the use of blockchain promises swift transaction processing, whether it's financial transactions, software licensing or policy voting.

Like any technology, blockchain's efficiency and security depend on how it is harnessed. In this dissertation, consensus mechanisms are reflected to be one of the pivotal components of blockchain applications. These mechanisms are protocols that enable participants to validate and come to an agreement regarding the contents of the blockchain. In many cases, they are also the mechanisms that incentivise nodes to participate in a network. Additionally, they incentivise not only participation but also foster trust.

The organisation requires a consensus mechanism to bolster efficiency and security in its private blockchain network across the decentralised system. This protocol has to be suitable and usable to accommodate their needs as a company. They decide to apply a blockchain network for one of their organisation branch located away from the headquarters as a test case. As mentioned before, this strategic approach is to shift from centralised systems where there is a single point of failure along with security vulnerabilities and efficiency bottlenecks. The company had decided to employ Practical Byzantine Fault Tolerance (PBFT) [2]. PBFT is a renowned consensus mechanism that functions in private networks. Unlike other mechanisms such as PoW [3], PBFT holds an advantage when it comes to energy consumption and authorisation. However, after careful consideration, the company had decided not to implement the idea. This is due to the scalability issues that PBFT is faced by, which result into increased transaction processing times.

In this dissertation, the organisation will be simulated as a small scale practicality test and will introduce a consensus mechanism that may suite the organisation and it's needs of efficiency, security and practicality of usage. A priority based consensus mechanism is proposed where nodes combine into smaller groups based on a transaction's priority before beginning the PBFT consensus process. The aim of the novel consensus is to limit the scalability issues that PBFT poses. The company is hoping that this approach would solve the problems of communication overhead and improve the latency of transactions processed, streamlining company operations.

Bitcoin, when it was formed, used the Proof of Work (PoW) consensus mechanism. Due to it's extensive resource demands, the landscape of consensus algorithms has evolved significantly. Many consensus mechanisms have been proposed, however, each mechanism brings trade-offs that affect the validation time, security and the efficiency of the network. In Chapter 3, we thoroughly discuss the most persistent state-of-art consensus mechanisms that exist in blockchain.

This project contributes to an ongoing quest to refine consensus mechanisms and seeks to implement an mechanism that would provide a balance to all the factors that contribute to the performance of blockchain networks and evaluate that mechanism at the corporation. The project combines conceptual analysis with the simulation of real-world scenarios to address challenges enterprises may face with blockchain technology. By conceptualising solutions and applying them to practical situations in the real-world, it aims to offer a novel perspective on blockchain research. This approach emphasises the critical role of consensus mechanisms in providing practical, applicable solutions for the industry.

1.2 AIMS AND OBJECTIVES

The primary aim of this project is to explore and contribute insights into the development of consensus mechanisms within the blockchain sector. The formal objectives of the project are as follows:

I. **Conducting a focused analysis of prevalent consensus mechanisms:** To gain a comprehensive understanding of consensus mechanisms, their key components, and the critical factors influencing the performance and factors that shape blockchain networks.

II. **Development of the Priority-based consensus mechanism, tailored for private blockchains:** Building on the foundation of Practical Byzantine Fault Tolerance (PBFT), propose a modified version that enhances efficiency and communication by prioritising transactions and effectively grouping nodes within the company's private networks.

III. **Perform simulation and mathematical modelling of the mechanism:** Evaluate the effectiveness of the proposed consensus mechanism through mathematical modelling and simulations.

IV. **Comparative analysis of the new mechanism and existing algorithms:** Compare the newly developed mechanism with existing consensus algorithms, integrating theoretical insights with practical outcomes to assess its relative performance and advantages.

1.3 REPORT OVERVIEW

The report is structured into several segments as outlined below. Each segment offers an overview of the subjects being addressed.

Background and Related Work chapter provides a broader context and essential background information on blockchain technology, categorises blockchain types, discusses their key characteristics and explores the application of the technology across industries. The chapter concludes with related works that are relevant to the project, highlighting the challenges and gaps identified in previous studies, illustrating how the proposed project aims to address and bridge those gaps.

Analysis of State-of-Art Consensus Mechanisms chapter provides a comprehensive review of prevalent consensus mechanisms in both public and private networks, including Proof of Work (Pow), Delegated Proof of Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT). For each mechanism, the chapter directs all the benefits it provides and the trade-offs it makes, attempting to achieve a balance. The essential objective of this chapter is to distill key insights from various mechanisms and leverage the findings in the development of the proposed consensus mechanism.

Design of the Proposed Consensus Mechanism chapter combines insights obtained from the previous chapter and introduces the proposed consensus mechanism. Moreover, the chapter describes the workflow, transaction lifecycle and fundamental characteristics that make the proposed mechanism unique.

Modelling of the Consensus Mechanism chapter consists of detailed mathematical modeling to predict performance, latency and relations between the components of the proposed consensus protocol. Moreover, it aims to provide a solid theoretical framework which will be used as a foundation for simulation and practical implementation.

Evaluation chapter provides simulation data using the equations derived from the modelling section of the report. Using the simulation data, the consensus mechanism's performance will be evaluated. Additionally, a short experiment using Hyperledger Fabric will be conducted as empirical evidence to supplement the modelling and simulations. Finally, a section conducting a comparative analysis between PBCM and other state-of-art solutions will be carried out.

Conclusion chapter summarises the report and revisits the objectives set for the project. It discusses if those objectives were met, what was not implemented as planned and provides recommendations for future work. Furthermore, the chapter includes a personal reflection from the author summarising learning outcomes, what skills and knowledge were acquired.

CHAPTER 2 : BACKGROUND AND RELATED WORK

This section introduces the fundamental concepts, terminologies, and current challenges relevant to the research. It provides a comprehensive background, setting the stage for the subsequent investigation. The purpose of this project is clearly outlined, demonstrating its relevance and goals within the context of blockchain technology. Through a detailed examination of the key developments and persistent issues in the field, this section places the research within a larger context, highlighting the critical gaps and emerging opportunities that the study aims to address.

2.1 PUBLIC AND PRIVATE BLOCKCHAINS

Blockchain can be categorised into four primary types: public, private, consortium and hybrid blockchains. Given the objectives of the report, this project will mainly focus on public and private blockchains. The distinction is critical to understand since each type has its intended use cases and access controls. Despite these differences, all blockchain types share fundamental similarities inherent to blockchain technologies.

Firstly, both public and private networks implement a Distributed Ledger Technology (DLT), allowing each node in the peer-to-peer to store records. DLT is the core technology that secures all records as tamper-evident and transparent to the entire network [4]. Unlike traditional databases, a DLT does not have any central data storage or administrative authority. In this broader context, each node has its own copy of the ledger, affirming security and transparency. The concept of immutability of records is shared on both public and private blockchains. Once transactions that are processed and validated on the blockchain, cannot be altered, manipulated or deleted. This characteristic is crucial for maintaining trust and integrity of the network. Additionally, the use of cryptography is cornerstone to all blockchain technologies. It provides the means for data encryption and secure transaction processing. The networks employ digital signatures and hash functions along with cryptographic algorithms to secure it against attacks and manipulative behaviour. [5]

Having explored the similarities between public and private blockchain networks, it becomes essential to evaluate the key differences that distinguish these types. A prominent example of public blockchain networks is Bitcoin, which embodies the fundamental characteristics of a public blockchain. It is a permission-less and an unlocked network allowing for unrestricted participation and decentralisation [1]. This openness supports cryptocurrencies as an alternative to financial applications, fostering innovation and encouraging participation. In contrast, private blockchains are restrictive and participation is limited to those who are granted access by the administrators of the network. These types of networks are suited for organisations who seek privacy in their operations. However, due to the networks not being available openly to the public, they are known for their efficiency, opportunity for internal collaboration and data confidentiality amongst the organisation. Regarding resource consumption, public blockchains are often resource-intensive. They require significant computational power and result in higher energy consumption [6]. For instance, Bitcoin is known for it's Proof of Work (PoW) consensus protocol, which results into participants, known as *miners*, to solve a mathematical problem and receive block accounting rights in the blockchain. This process is highly competitive and has led an "arms race" between participants to gain computational power [7] [8]. In contrast, private blockchains are typically known to handle transactions at a higher efficiency rate due to the limitation of participants. These networks are suitable if quick and efficient agreements are necessary for the network's administrators.

By examining these key similarities and differences, the section has highlighted the major factors that vary each networks' use case. In this project, due to simulations regarding the organisation, a private network is employed to simulate the proposed consensus mechanism. The rationale behind selecting a private network lies in the intention to apply conceptual solutions within an organisational context where we assume all devices are authorised. The network will provide an ideal and realistic framework to simulate the organisational environment and facilitate a more focused and efficient evaluation of the consensus mechanism.

2.2 CONSENSUS IN BLOCKCHAINS

Blockchains being a Distributed Ledger Technology is one of the main reasons of it's success. However, this notion of state replication brings upon many challenges. Consistency is key in decentralised technologies. It is not only desirable but critical in the context of blockchain. The integrity and the trust of a participant in a blockchain rests on the ability of the blockchain to accurately and reliably validate transactions and maintain a consistent state across all copies of the ledger. Therefore, to achieve consistency, consensus mechanisms play a pivotal role.

Consensus protocols are processes in which nodes in the blockchain agree on the current state of a ledger in a network. They also promote trust, efficiency and decentralisation ensuring transactions are recorded and available to all participants in the network [9]. Furthermore, it is a component that decides performance, security and latency of a network to a great extent. They are pivotal to balance transaction processing with the constant imperative of preventing fraudulent or malicious activities. However, the distributed nature of blockchain presents many challenges in implementing and tailoring consensus mechanisms depending on the objectives of the network. Some of these challenges include security risks and ensuring the system remains intact even if malicious nodes and attacks are happening in the blockchain network. Secondly, the consensus mechanism has to allow the blockchain to process under influx of rapid transaction while keeping the structure and the transaction properties consistent. This requirement poses a significant challenge in maintaining scalability and performance without sacrificing security or decentralisation. Thus, this rationale underpins the proposal of a new consensus mechanism.

As blockchain is being adapted in many industries, adapting consensus mechanisms to varied blockchain applications and ensuring that they align with the resources and the objectives of the application necessitates a delicate balance [10]. For example, in the healthcare industry where privacy and security critical and protection of sensitive patient data is paramount, consensus mechanisms that provide anonymity will involve trade-offs like scalability and performance. This is mainly due to increased layers of cryptography adding paradigms of encryptions and decryption which can slow down transaction processing and limit scalability [11]. In contrast, among finance applications, where performance and scalability is imperative consensus will be tailored to focus more on the networks performance demands and compromise security measures or limit participants based on resources.

The dissertation shall expand on the concepts introduced in this section. The novel consensus mechanism will be proposed according to the objectives of the organisation which involves lowering the network latency and ensuring incentivised participation. Consequently, the report will also evaluate the trade-offs that the proposed consensus mechanism will have to make to accommodate the needs of the company and it's participants.

2.3 BLOCKCHAIN ACROSS INDUSTRIES

In recent years, blockchain technologies have rapidly expanded into industries due to their potential benefits and innovative solutions beyond their initial financial sector origins. The transition has spanned across healthcare [12], logistics [13] , construction [14] , and energy management [15] among others. One of the main reasons for this adoption has been duty to the security threats that existing applications are vulnerable to. Blockchain solves those issues by introducing Distributed Ledger Technology for both transparency and data integrity along with eliminating the risks of single point of failure [16]. Moreover, blockchain provides an alternative to central client-server architectures or internet-based data transfers, both being notorious for their security exposures. Decentralisation of data storage and management not only solidifies the applications' security but also streamlines processes and optimises the overall efficiency of business operations.

Firstly, in the healthcare industry, the norms of storing patient's data in a centralised approach are a threat to privacy and a single point of failure, which in the healthcare industry, could be life threatening. Not gaining access to a patient's data during urgent needs is a serious challenge. Using blockchain technology, a patient's data can be stored on a ledger which would be held by all healthcare centres, ensuring prompt treatment. This would solve any privacy issues and the risk of data unavailability and promote data integrity [17]. Such applications are being proposed and are being contributed by individuals around the world. A paper by Akhilendra et al. [18] evaluates the prominence and potential of using distributed ledger technologies and proposes an application that consists of a decentralised healthcare record management system. Another example of such application is MedRec, a blockchain based record management system, proposed by Azaria *et al.* [19] which handles medical records, allowing patients to access their records at anytime without the vulnerabilities of a centralised database.

Beyond the healthcare industry, blockchain technology use has increased in the supply and logistics industries. Their main implementation has been in the realm of Supply Chain Management (SCM) [20], where blockchain can enhance the sustainability of such systems by introducing traceability, immutability and openness within supply chain agents and stakeholders [21]. This adaptation increases verification of products and traceability to their origins. Additionally, blockchain in SCM promotes ethical sourcing, registration of products and trust in consumers who can easily access data about products and their supply. Blockchain's capabilities extend to improving operational efficiencies, reducing counterfeit goods, and ensuring the authenticity of transactions.

Finally, a industry standing to benefit significantly from the distributed technology is the energy sector. Though 2016 to 2021, there was an observed reduction in fossil fuel usage amongst countries like Estonia (23.4%) and Denmark (14.2%) [22]. As the industry leans towards renewable energy due to shortage of fossil fuels and carbon emissions, it demands innovation solutions for both distribution and management of energy usage and production. Blockchain technology, with its unique characteristics, offers a compelling solution to these challenges. One of the primary use cases that blockchain has the most prominent potential in are the commodity trading platforms, where producers and consumers can trade their energy resources on a peer-to-peer basis [23]. This would allow for each participant in the trade to keep record of their transaction and allow for secure verification of entities on the network. Subsequently, similar to the supply chain industry, blockchain allows for traceability on energy origins and purchases, enabling for trust and verification in the wholesale energy markets. The use cases of DLT in the energy sector are increasing as more innovative solutions are presented.

This section in the project is a significant one as it underscores the relevance of blockchain technology's practical applications in the industry. The examination in this context is a pivotal one as we aim to evaluate the practical viability of the new consensus mechanism this paper will propose. It emphasises the necessity to bridge theoretical innovations with practical applications, ensuring that our proposed consensus mechanism can contribute to the advancements of blockchain in the industry.

2.4 RELATED RESEARCH

In the field of blockchain research, a multitude of significant contributions have surfaced, offering valuable insights and remedies to tackle pivotal challenges in consensus mechanisms, security and understanding the blockchain technology.

Wang et al. [24] delve into the limitations of PBFT and introduced an intriguing alternative known as Credit-Delegated BFT (CDBFT). The paper proposes a mechanism that includes having a credit evaluation system and introducing consistency and checkpoint protocols based on PBFT. The proposed mechanism utilises a rewards and punishment scheme to limit the presence of malicious nodes in the consensus process. They model reward and punishment along with the voting mechanism related to CDBFT. The outcome of the study was demonstration of a 5% reduction in abnormal node participation, accompanied by an increase in the efficiency and stability of the network due to the proposed mechanism. Nevertheless, despite the rigorous simulation and implementation of the novel consensus mechanism, the mechanism is yet to be assessed in real-world scenarios to assess its practical viability. Therefore, this project aims to propose a novel consensus mechanism and subjecting it to real-world application assessment, with the specific objective of practical viability and identifying its potential use.

Zhang et al. [25] provide a comprehensive review on blockchain technology, consensus mechanisms, particularly highlighting the aspect of security and privacy. The study aims for the readers to get an in-depth understanding of blockchain's security and privacy concepts including consensus algorithms, hash chained storage, mixing protocols etc. The article recognises the importance and the growth of blockchain technology in academia and industry whilst emphasising that only a small subset of blockchain platforms can achieve security goals in practice; which is an issue since security is one of the main fundamentals of the technology. Moreover, it positions security and privacy as the main sources of participant trust to engage in a blockchain network. The proposed project aims to go beyond security and privacy in its detailed review of consensus in Blockchain. Based on the comprehensive analysis, the project will propose a novel consensus mechanism that seeks to innovate and enhance the fundamental aspects of blockchain technology.

Another research by Guangxia et al. [26] introduces a novel Delegated-Proof-of-Stake (DPoS) mechanism by employing vague sets to mimic the voting model in the real world. Delegated PoS is a consensus mechanism in public blockchains. It is a variation of Proof of Stake (PoS), in which individuals or entities (stakeholders) who stake the most significant amount of a particular crypto asset are more likely to have the opportunity to validate a block and generate a reward only for themselves. DPoS combats the notion of a wealth gap by introducing a democratic approach. Nodes can stake their tokens to vote for other nodes that would do the work and share the rewards.

The authors of the paper suggest that the existing DPoS mechanism provides limited voting options to the nodes as they can only vote for a particular agent node. They claim that the mechanism does not reflect the complexity of such protocols in the real world such as in the United Nations, where permanent members can vote "yes", "no" or abstain against a proposal. Using this as inspiration, they propose an improved DPoS mechanism where additional voting options are given to the individuals. This allowed the entities to express disapproval and neutrality in the network which resulted into increased security, fairness and reducing the likelihood of malicious nodes becoming agent nodes.

Although the research presents a valid mechanism by drawing inspiration from a real-world scenario, it does not recognise the consequences that the added complexity of the proposed voting system could pose. Added options also mean added parameters and a more sophisticated decision making process which may impact the efficiency of the mechanism. In contrast, the consensus mechanism that is proposed in this dissertation will carefully consider and address all benefits and trade-offs associated with the novel approach.

These research efforts represent just a fraction of the work being done in the field of blockchain research. Many of the works are not only connected to consensus mechanisms but also in the field of IoT and AI, which underscored the versatility of blockchain technology. This paper aims to be a valiant contribution to the consensus mechanism sector of DLT research and to bridge gaps highlighted in the aforementioned analysis.

CHAPTER 3: ANALYSIS OF STATE-OF-ART CONSENSUS MECHANISMS

This section of the report dissects consensus mechanisms across both public and private blockchains. The aim of this section is to understand the workflows, benefits and trade-offs associated with various mechanisms. As this chapter concludes, the proposed consensus mechanism will integrate the insights from this section to guide the implementation, ensuring it is crafted to align with the benchmarks set by state-of-the-art solutions.

3.1 CONSENSUS IN PUBLIC BLOCKCHAINS

This part of the report discusses consensus mechanisms that reside in public blockchains and what are their fundamental characteristics. It aims to highlight how the mechanisms facilitate agreements between the distributed participants, within the networks that reside in the public domain. Additionally, the section seeks to unpack the comprehensive interplay between various consensus models like Proof of Work (PoW) and Proof of Stake (PoS), examining their impact on network security, scalability, and overall performance of the network.

3.1.1 PROOF OF WORK (PoW)

Overview: PoW is one of the earliest and most established consensus mechanisms used in public blockchains. It was introduced as the backbone to cryptocurrency applications like Bitcoin and initially Ethereum. In Bitcoin, Satoshi Nakamoto used cryptography hash functions to secure transactions. At it's core, PoW requires that individuals in the network need to expend a significant amount of computational power to achieve a goal. In this case, the goal is to find a solution to a complex mathematical problem that requires significant computational effort to solve. Through this concept, PoW enhances its security by catering those who possess the necessary computational resources to solve complex problems, thus discouraging malicious actors due to the high cost of participation [27]. Moreover, this concept encourages decentralisation and incentivises participants to invest into their computational power which would lead them to achieving more tokens.

Workflow: In cryptocurrency, tokens serve as digital assets that may have monetary value. These tokens are rewards for individuals who successfully solve the mathematical puzzle. The mathematical puzzles are required to validate transactions and add new blocks to the blockchain. The participants who take part in the process are called "Miners". **Figure 3.1** shows how blocks are linked to each other. Each block is linked to the previous block and contains information like when the block was created (Time stamp), the list of transactions in the block (Transactions), nonce, and the previous block's hash. Firstly, miners enter the network and listen to the transactions broadcasted to the miners **(1)** . Once a transaction is received, its the miners' turn to verify the transaction. Next, the miners in the pool create a block candidate which is due to be added to the block and begin to compete to the puzzle solving process, also known as "mining" **(2)**. In detail, the puzzle requires finding a nonce from the target values derived from the network's configurations. A value that when combined with the hash function, produces a hash value that is acceptable according to the difficulty criteria of the system **(3)**. Finally, when the result is accepted, the block is added to the chain of blocks by the miner who solved the puzzle **(4)** and is rewarded for generating the block **(5)**[28]. **Figure 3.2** encapsulates this process and the flow of transactions in Proof of Work consensus mechanism.

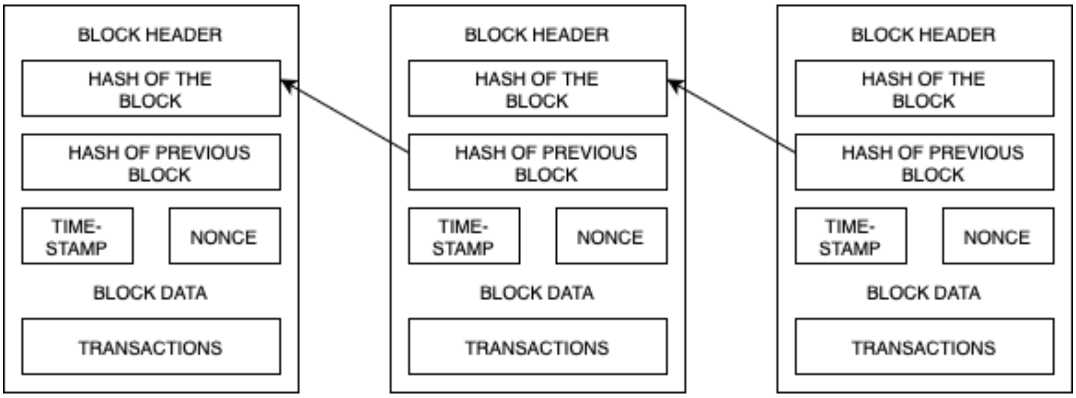


Figure 3.1 Block Composition

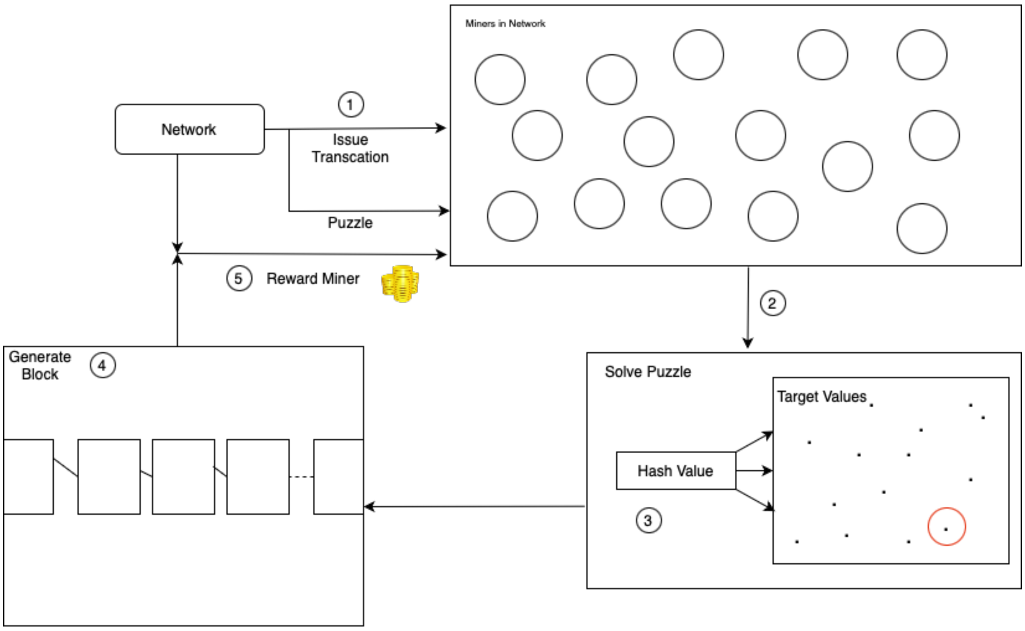


Figure 3.2 Proof of Work Workflow

Analysis: Although the mechanism raises it's security through it's higher barriers, it introduces challenges for it's participants. Proof of Work inherently demands for high computational power from its participants to gain rewards from their work. However, this demand has significant implications not only from economic aspects of the system, but also environmental. The miners in the network get involved in a competition for computational power which directly encourages them to invest into electrical devices that would allow them to gain any advantage possible. This "arms race" for hardware improvements leads to higher consumption of electricity, which is greatly sourced from non-renewable sources. As a result, the process leads to a significant carbon emission [29].

Economically, the process doesn't favour the miners. Despite each miner having access to all the transactions in the network and freedom to solve mathematical puzzles, only one miner can solve the puzzle and add a block to the chain at a time. The effort and the investment that other miners have expended into the process is ultimately wasted and discourages them to participate in the network [30]. Additionally, the price fluctuation in cryptocurrencies also cuts their profits comparing it to the value invested [31]. The constant race has led to some participants having more computational power than participants that cannot afford to invest more funds to hardware. The foundation of Bitcoin is to promote decentralisation. However, if wealthier participants are able to combine significant energies, they can form a coalition with other participants and threat the decentralisation aspect of the network. This is known as the "51% attack", where with majority control of the network's mining power can manipulate transaction confirmations [32]. Evaluating the performance of the consensus mechanism, the transactional efficiency of PoW is insignificant. Transactions need to be included in a block and sufficiently confirmed by subsequent blocks to be considered secure, leading to potential delays. Therefore, to mitigate these problems, the blockchain sector had been researching and developing more sustainable algorithms.

Table 3.1 summarises the shortcomings of PoW, particularly in the paradigms of efficiency, security, decentralisation and scalability. The table clearly depicts the need for innovation beyond Proof of Work. As a result of the analysis, the proposed consensus mechanism will function in the network where all participants within the network will have uniform computational power, fostering trust within the departments of the organisation and promoting cooperation and coordination rather than competition. The computational power may be increased if the organisation decides that it will accelerate processing and overall network performance.

ASPECT	STRENGTH	WEAKNESS
Efficiency		High computation power demands. Significant computational resources and redundant process cycles.
Scalability	Permissionless; allowing access to anyone without needing authorisation from an authority	Limit of block size and block validation time leads to bottlenecks and delays.
Decentralisation	Open access to the public and each participant keeps record of all transactions	Wealthier miners make the network vulnerable to 51% attack and make coalition to control the network.
Security	Required higher efforts of computation to make gains in the network. Discourages attackers due to the effort to reward ratio.	51% attack exposure

Table 3.1 PoW Performance Summary

3.1.2 PROOF OF STAKE (PoS)

Overview: To combat the challenges posed by Proof of Work, Proof of Stake (PoS) had been developed. PoS functions on the concept of "staking", where instead of competing for computational power to add blocks to the blockchain, participants are randomly selected to make changes to the blockchain. The only way for participants to make the random process more favourable for themselves is to stake their holdings. Entities which have more cryptocurrency to stake as collateral have more chances of being selected by the protocol itself [33].

Workflow: A flowchart in **Figure 3.3** is used to depict a simplified version of PoS where first, the transactions are gathered and a validator is selected based on a participant's stake. Once a validator is selected, a decision is made at random if they will be allowed to to create the block or not. This decisions depends on factors like how much stake the validator of the block has put up and randomness of the process [34]. The validator creates a block, attaches it to the hash of the previous block and then broadcasted to the network for validation. Once the network has validated the block, the block gets added to the blockchain and the validator is rewarded.

Analysis: If we evaluate Proof of Stake's performance, it does in fact solve some of the issues that PoW presents. The participants are no longer required to invest in hardware to gain more computational power, reducing the environmental impact [35] as well as economical impact of participating in a network. The selection process now depends on how much a participant is willing to stake to get a chance to validate a block, lowering the entry barrier. Having more participants and a lower demand from the network also increases the aspect of decentralisation in the network.

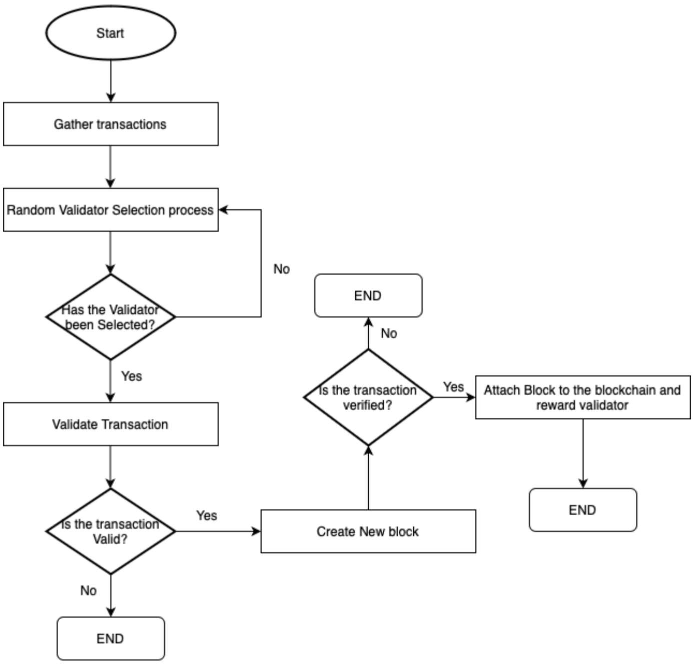

Start
Gather transactions
Random Validator Selection process
No
Has the Validator been Selected?
Yes
Validate Transaction
Is the transaction Valid?
Yes
No
END
Create New block
Is the transaction verified?
No
END
Yes
Attach Block to the blockchain and reward validator
END

Figure 3.3 Proof of Stake Sequential Flowchart

Additionally, PoS is considered to have reasonable security measures as the forger needs to stake a collateral before being able to commit a block into the blockchain, giving a guarantee that in an event of dishonest behaviour, their stake would be lost [36].

On the other hand, while the mechanism manages to propose solutions to the problems raised by PoW, there are some trade-offs that PoS has to make to accomplish them. A question is raised by the blockchain community if Proof of Stake is truly secure. This question is validated by the "Nothing at Stake" problem. This problem arises when validators support multiple forks in a blockchain simultaneously as it doesn't cost them anything and they receive transaction fees on each block validated [37]. This becomes a bigger problem as it leads to double spending.

ASPECT	STRENGTH	WEAKNESS
Efficiency	Improved efficiency from PoW as no complex computation processes are involved in PoS.	
Scalability	Allows for faster transaction processing and throughput.	As number of nodes increases, the number of validators also increases which can lead to slower consensus.
Decentralisation	Lower barrier of entry comparing to PoW as participants do not require expensive hardware which improves decentralisation in the network.	Participants who have accumulated higher currencies may have more influence in the network, forcing centralisation.
Security	Staking improves security and discourages dishonest behaviour, directly punishing malicious actors.	Nothing at stake problem leading to double spending. Wealth disproportionality.

Table 3.2 PoS Performance Summary

Despite Proof of Stake lowering the barrier for participants and incentivising them for participation by democratising the consensus process, the pure idea of staking can become a challenge overtime. As time goes on, participants with larger amounts of currencies could hold power in the blockchain and ultimately be favoured as forgers and validators. Wealth disproportionality could lead to an imbalance between participants, not allowing newer participants with lower currency holding to have any influence on the network. This also raises the threat of collusion between participants who hold a larger chunk of wealth in the network. **Table 3.2** summarises this section and concludes that: while PoS has some benefits over PoW, there is a need for refinement, increased security measures and toleration.

3.1.3 DELEGATED PROOF OF STAKE (DPoS)

Overview: Delegated Proof of Stake (DPoS) has been also introduced as an alternate by Larimer in 2014 [38] which attempts to address the main challenges associated with Proof of Work and Proof of Stake. Unlike PoW, DPoS does not have extensive power requirements since it abandons the concept of mining to a democratised process. Similarly to PoS, the algorithm is highly dictated through the stake of a participant. However, to mitigate the risk of centralisation, where the wealthiest participant could influence the network, DPoS introduces a voting-based validator selection process and methods of earning stake depend on their participation in the network.

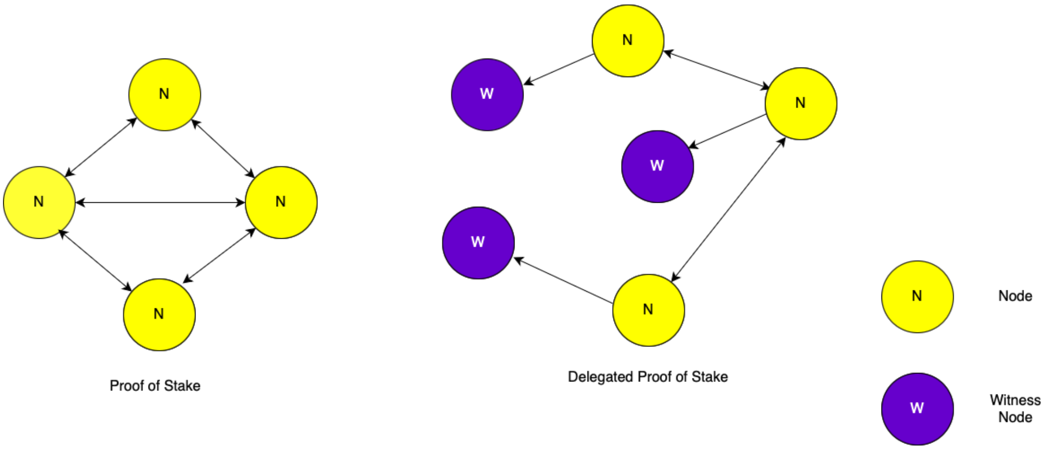


Figure 3.4 PoS and DPoS Node Communication

Workflow: In contrast to PoS's randomised process of selecting a validator, DPoS allows the participants to vote on a participant to become a "witness" or a "delegate". A witness, also known as "validators" or "block producers", is generally the participant responsible for validating transactions and adding blocks on the blockchain. Delegates are a part of the governance of the network where they do not directly impact the creation and validation of blocks but deal with general matters of the network such as network changes or transaction fee adjustments. **Figure 3.4** shows the difference of communication between PoS and DPoS, as each arrow represents the flow of communication, signifying how DPoS eases network pressure and allows for an efficient operation. In proof of stake's case, all nodes need to be in constant coordination with other peer nodes in the network. However, in DPoS delegate nodes vote only those witness nodes that they are selected to be final witnesses for block generation. Therefore, the network will not have significant communication complexity. Both these roles are of a fixed number and are assigned on voting basis by the stakeholders of the network. The importance of stake is emphasised on the voting process where the stakeholder's voting power is directly proportional to their stake in the network [39]. This ensures that the participants with the most significant investment in the network has a greater influence in the governance and operations of the network. Witnesses are in the block generation group at a rotational basis where if a witness misses to do their task of "witnessing", the block creation process, their turn will be handed over to the subsequent witness. As a result, witnesses have been observed to generating a block on an average every 3 seconds

on their turns which makes the consensus mechanism much more efficient in block generation than proof of work (10 minutes) and proof of stake (64 seconds) [40]. If a witness does not perform their obligations or is proved to be a malicious, they are

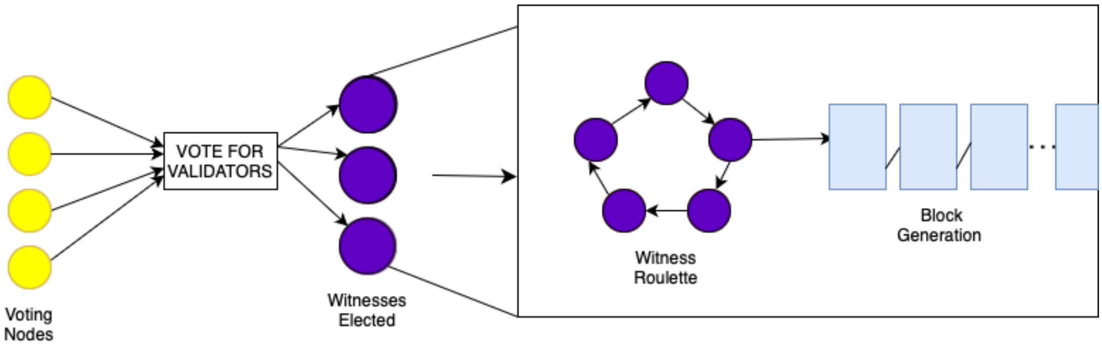


Figure 3.5 Delegated Proof of Stake Workflow

voted out by the stakeholders, keeping them accountable of their actions. Figure visualises the abstract network topology along with the sequence of activities taking place in DPoS.

Analysis: DPoS faces challenges despite the mechanism's efficiencies and benefits. Firstly, nodes have to vote and spend their time and energy on ensuring that they have some degree of influence on the network. This may not appeal to many nodes as they are not compensated for their work [41]. In DPoS, instead of a participant staking increasing amount of wealth, an attacker participant can convince other stakeholders to give them the majority voting power to influence the network for themselves. This creates vulnerabilities in the network and concluded DPoS to be susceptible to the 51% attack. Therefore, DPoS is also vulnerable to the 51% attack along with proof of work and proof of stake [42]. **Table 3.3** provides the performance summary of DPoS.

ASPECT	STRENGTH	WEAKNESS
Efficiency	Highly efficient due to limited number of delegates and witnesses who are held accountable.	
Scalability	Handles more transactions and block generations per second than PoW and PoS.	
Decentralisation	More democratic process compared to PoW and PoS as it allows participants to vote for validators.	Wealth imbalance could mean centralisation and make the application susceptible to 51% attack.
Security		Stakeholder collusion exposes security for participant influence.

Table 3.3 DPoS Performance Summary

3.2 CONSENSUS IN PRIVATE BLOCKCHAINS

This crucial section of the report turns the focus to consensus mechanisms that operate within private blockchains and how they distinguish from their counterparts in the previous section. The section dissects the core attributes that define these mechanisms, elucidating why they function most effectively in restricted applications where operational integrity and transaction confidentiality is of a paramount importance for an organisation. For this report, understanding what components may be adapted to the organisation at hand will be of utility as the organisation will also be employing a private application.

3.2.1 PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)

Overview: Practical Byzantine Fault Tolerance (PBFT) is an essential part of this project as it supports the proposed consensus mechanism for the organisation. Inspired by the Byzantine Generals Problem [43] , PBFT is renowned for being a technology that allows for consensus even with the presence of faulty or malicious nodes to ensure the reliability and integrity of an application.. PBFT is not only known for its fault tolerance features, but also for it's advancement of achieving increased efficiency and reduced complexity. PBFT being a consensus mechanism implemented in the private domain, the number of participants (nodes) is fixed in a permissions application. Therefore, a voting based consensus is suitable in that environment. The mechanism functions on a predicate that there are malicious nodes in the network. However, if the number of nodes does not exceed 1/3 of n, where n is the number of nodes [44] , majority vote is obtained and consensus is reached.

Workflow: In the application, there are two types of nodes: primary node and replica nodes. Primary nodes play a pivotal role in the consensus process as they are the ones who initiate the process and propose a new block or transaction to the network, are responsible for the order of transactions and are responsible to make sure all replica nodes receive messages regarding the transaction.Replica nodes are the core of PBFT as it is them who engage in the consensus process once they receive the proposed transaction. At first, they verify the transaction, making sure that no malicious blocks are being committed to the blockchain. When verification is complete, they engage with other nodes in rounds of communication to come to an agreement. What allows PBFT to be fault tolerance is the versatility of replica nodes. If there is a case that the primary node becomes redundant, malicious or faulty, replica nodes can replace the primary node to continue the functioning of the application and ensure the integrity of the application remains uncompromised. This process is also known as view change [39].
Figure 3.6 classifies each process into phases that the processes are typically described in the blockchain community:
Request (1) : Initial phase in PBFT where the client sends a request for a transaction to the primary node.
Pre-prepare (2): Primary node sends the transaction to all replica nodes.
Prepare (3): Replica nodes receive the transaction request. They verify it by making sure that they have not received other messages or if the message seems abnormal. Once verified, the prepare message is broadcasted to the rest of the network. Each node sends a prepare message and if the number of prepare message is equal or exceeds $2f + 1$, where f is the number of faulty or malicious nodes, all replicas will generate a prepared certificate and indicate that the process can move to the next stage.

Commit (4): In this phase, the replica nodes are prepared to execute the proposed operation. For this to happen, a node has to receive $2f + 1$ commit messages from its peers to signify that a consensus has been reached.

Feedback (5): Once the commit messages are received by a node, the nodes have executed the operation requested by the client. To provide feedback to the client that the operation has been successfully executed, the nodes provide feedback directly to the client. The client can choose to wait for a number of confirmations to be precise and ensure consistency amongst the node's feedbacks.

Analysis: Despite its strengths, PBFT similarly to other consensus mechanisms makes trade-offs. The mechanism provides many measures for fault tolerance amongst the nodes. However, to be able to do that means multiple rounds of communication between nodes to reach consensus. As seen in **Figure 3.6** the nodes are required to communicate with each other multiple times during multiple phases in the process to reach consensus. This poses a critical challenge for applications utilising PBFT as their consensus mechanism as they will face scalability, throughput bottlenecks and consensus delays as the network grows. However, PBFT's increased efficiency and commitment to system integrity, it remains a primary choice when it comes to private blockchains.

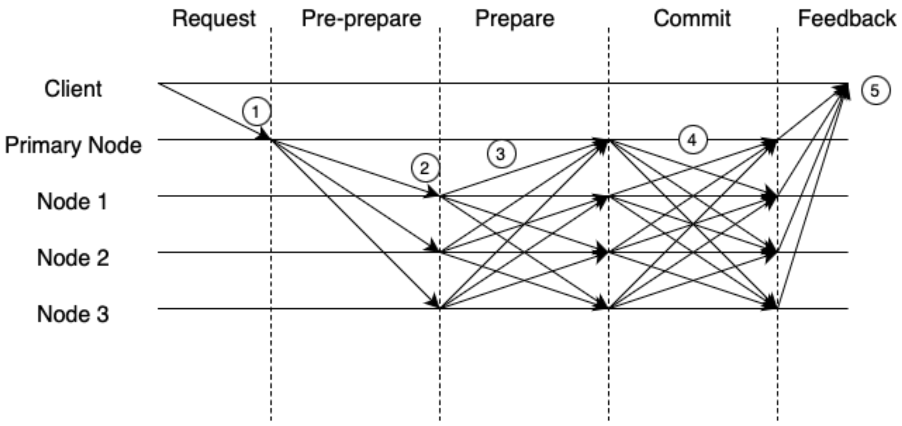


Figure 3.6 Phases of PBFT

it to mitigate the issues associated with PBFT's communication demands. **Table 3.4** summarises the section and encapsulates PBFT's performance in private blockchains, while the proposed changes haven't been applied to the mechanism. Although the consensus mechanism shows weaknesses in many aspects, the table proves that if the communication demand is lowered, PBFT is an optimal solution for its departments due to strengths in efficiency and security.

ASPECT	STRENGTH	WEAKNESS
Efficiency	High transaction throughput .	Communication overhead can significantly delay consensus.
Scalability		Suited for permissioned blockchains with limited participants. Mechanism is challenging to scale due to communication demands.
Decentralisation		More centralised since permissioned applications require authority to verify identities and carry out transactions.
Security	Resilient to faulty and malicious nodes.	

Table 3.4 PBFT Performance Summary

3.3 DESIGN CHOICES OF PROPOSED CONSENSUS

Designing a consensus mechanism involves forming a balance between efficiency, security and decentralisation. The preceding analysis of both public and private consensus mechanisms have provided valuable insights that can be extracted to justify the design choices made while constructing the consensus mechanism that is also tailored to the organisation's needs. Additionally, each design choice aims to mitigate weaknesses of a mechanism whilst capitalising on their strengths to form a more balanced algorithm.

Design Choice 1: PoW has challenges of participants competing for computational power to gain rewards. However, in an organisational setting, such circumstances will result into increased resource consumption and adverse environmental effects. Therefore, the proposed consensus mechanism is designed in an environment where all participants have uniform computational power to maintain resource consumption and increase fairness in the system.
Design Choice 2: The analysis of DPoS and PBFT revealed a gap in the rewarding concept where participants are not acknowledged for their voting and their participation in the consensus process. This has resulted for the proposed consensus mechanism to have an incentive system in place where participants are encouraged to perform operations no matter how meaningful and get rewarded for their cooperation.
Design Choice 3: The incentive mechanism in the proposed algorithm is instilled and refined in a way inherent to PoW, where the participants receive rewards exclusively once a transaction is processed, rather than merely participating in the network. This design choice encourages participants to make meaningful contributions in the network and enhance the systems's efficiency.
Design Choice 4: Public consensus mechanisms have highlighted the disadvantages of having systems that overly rely on a participants resources or staking which lead to centralisation including 51% attack, collusion and wealth disproportionality. Therefore, the mechanism will eliminate the concept of staking

or voting to ensure that all participants, regardless of their economic positions and past reputation, have equal opportunities in the application.

Design Choice 5: To mitigate PBFT's inherent communication overhead, the proposed mechanism adds a layer of grouping in the mechanism. The nodes are distributed into smaller groups to make the PBFT process more efficient amongst fewer nodes.

Design Choice 6: All nodes in the application are required to engage in every transaction during PBFT consensus process. However, an organisation where transaction processing is pivotal and resources are finite, this feature could lead to inefficiencies and unnecessary consumption of power.

CHAPTER 4: DESIGN OF THE PROPOSED CONSENSUS MECHANISM

Chapter 4 introduces the design of the proposed consensus mechanism, detailing its workflow, fundamental characteristics and components. Furthermore, this chapter includes a comprehensive analysis of its performance within the organisational context, evaluating its attributes similar to state-of-art mechanisms in Chapter 3.

4.1 REVISITING THE SCENARIO

Revisiting the previous scenario outlined, the representative multinational technology corporation undertakes a strategic shift towards blockchain technology aiming to revolutionise its internal transaction management processes and further underline their commitment towards continuous improvement and evolution. The initial motivation for the decision is due to the limitations of centralised systems that already exist in the organisation, proving to be significantly impeding transactional processing due to its hierarchical structure and security vulnerabilities as the system has a single point of failure. The current architecture leaves the organisation at an elevated risk of disruptions and attacks. Blockchain's distributed nature and its consensus mechanism versatility presents itself as a transformative solution for the company.

By distributing data across a network of departments, the organisation mitigates the risks of single point of failure, introducing decentralisation, immutability of transactions and transparency amongst the employees. Moreover, through blockchain, it promotes cooperation amongst departments to reach agreements for transactions that require oversight. Some of the transactions include: policy decision making, access management and verification, contract signings etc. A distributed system with high level of cooperation not only boosts efficiency, but productivity and overall value offered to the internal and external customers who initialise the requests. As a result, the company has elected to conduct an assessment by implementing blockchain technology within a single branch as an initial test, with the intention that, if the trial proves to be successful and achieves the performance targets, there will be future plans set in place to scale it to other branches of the firm. Thus, the next step is to come to an agreement over the choice of consensus mechanism for the network.

As an organisation requiring authority for departments to participate in the network, choosing Practical Byzantine Fault Tolerance (PBFT) as their consensus mechanism was previously agreed upon. However, analysing the strengths and weaknesses of PBFT led the organisation to reassess this decision. The growing transaction processing times with a growing number of nodes proved to be the primary reason for its revaluation. Therefore a response in the form of technical modification of the consensus mechanism was necessary.

This chapter aims to provide an overview and the design of the proposed consensus mechanism which carries out the necessary restructuring of the consensus process to be better suited for the organisation addressing the communication overhead and latency issues that were impeding the initial implementation. By applying the consensus mechanism in the company's context allows for a feasibility assessment along with a clear roadmap of how the consensus mechanism can be altered in the future if the organisation decides to scale the solution.

4.2 PRIORITY BASED CONSENSUS

The proposed consensus mechanism is tailored for the organisation designed explicitly for a private, permissioned blockchain network prioritising efficiency of processing transactions, minimising communicational and computational latency and incentivising participants in the network which will contribute to the organisation's commitments and objectives. The mechanism's design is based upon PBFT at its core and an additional layer consisting of the principle of dynamic grouping according to a transaction's priority. The added layer further enhances PBFT, ensuring that transactions with higher priority to the organisation get processed in a prioritised manner, maintaining a consistent network throughput and fairness in the organisational context where departments feel incentivised and not resort to malicious activities. **Figure 4.1** illustrates the structure of the organisation and the blockchain network within the company branch, with each employee in the department acting as a node.

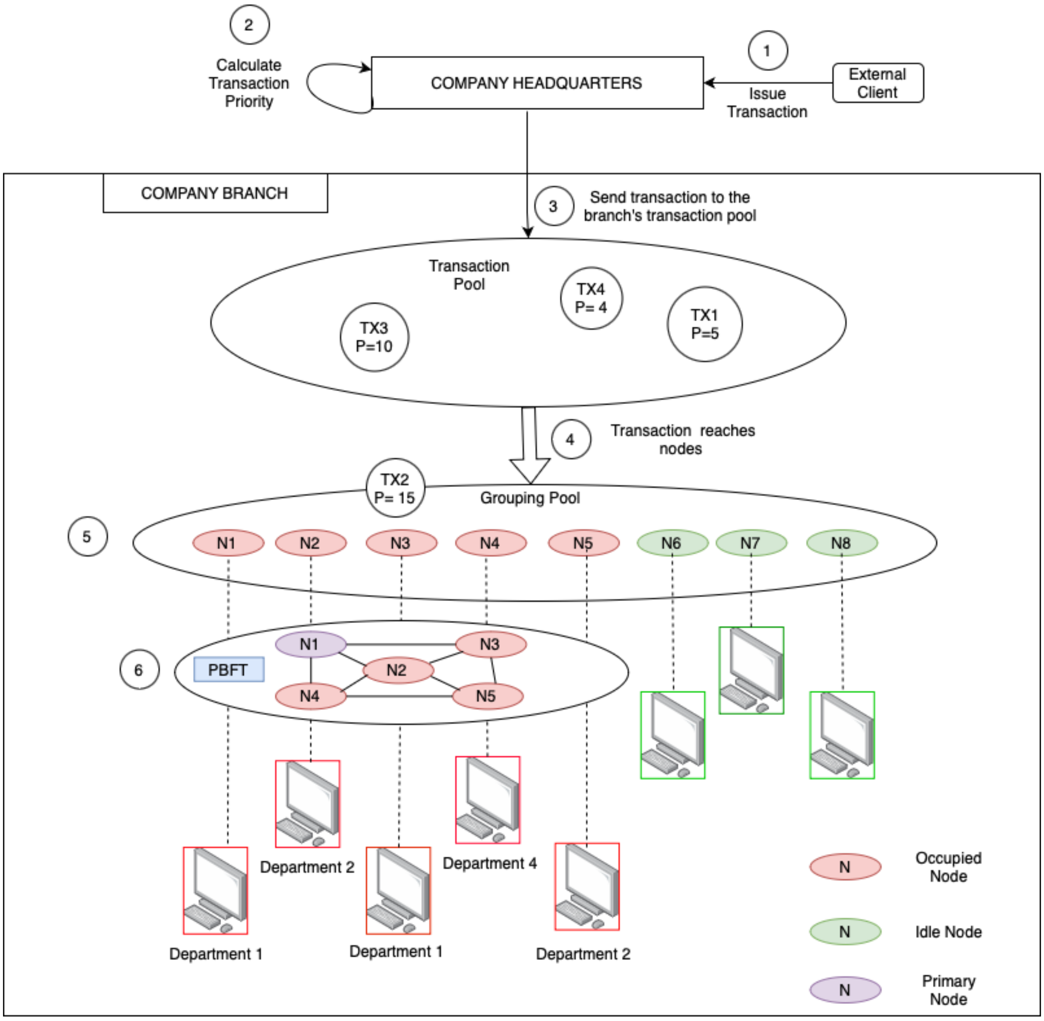


Figure 4.1 Proposed Mechanism Workflow

Workflow: The foundation of the network is set to respect a transaction's significance on their importance to the organisation's key performance metrics. **(1)** When the network receives a transaction from an internal or an external client, the transaction processing begins. Initially, the transaction is verified and authenticated. Once the verification is complete, the transaction is assigned a priority value which is primarily based upon the size of the transaction in kilobytes and the transaction's cost in dollars, indicating the priority level **(2)**.Transaction cost represents the financial measure of the resources and manpower needed to process a transaction, allowing the organisation to manage resource allocation and project completion management. This initial stage is pivotal to the overall workflow of the consensus mechanism as the transactional priority determines the group of nodes which are going to be tasked with its validation and addition to the blockchain. Moreover, the transactional priority specified the sequence in which transactions are going to be processed by the nodes in the network, ensuring a robust consensus process where significant requests receive the fastest feedback from the network back to the client. Following the assignment of priority, the transaction reaches the nodes in the network **(3)**. Before the consensus process, the network initiates the dynamic group formation process within the grouping pool, where nodes are in a neutral state, awaiting assignment **(4)**. Depending on the importance of the transaction, the number of nodes in a group are assigned to that request. Therefore, if the transaction's priority is quantified to be high, the number of nodes in the group are also going to be higher **(5)**. This is significant as the mechanism allocates resources accordingly increasing the efficiency of the organisation's operations and manage network throughput where smaller transactions which are quicker to process and within cost capacity, are assigned a group and added to the block.

The composition of the group purely depends on the transaction and no other factor. This is due to the insights that were obtained by analysing PoW, PoS and DPoS consensus mechanisms as computational power and staking led to applications becoming vulnerable to attacks and collusion between the participants. Within each group, a transaction is assigned and the groups begin processing the request. The PBFT algorithm commences and multiple rounds of communication are initiated particularly pre-prepare, prepare and commit **(6)**. The primary node is selected by the organisation in a predefined sequence ensuring all participants have a fair chance to act as a primary node. Due to PBFT's robust fault tolerance features, if the primary node suffers a failure, the other nodes in the group can replace the nodes to continue the workflow of PBFT. Moreover, due to the introduction of grouping, the group processing the transactions will only have a fraction of nodes depending on the transaction. Whereas, without dynamic grouping, any transaction would have to be processed by all departments in the organisation with no prior classification of a transition's priority. Therefore, even the least significant transaction would occupy all nodes in the system. As a result of the modification, a request is agreed upon in a productive manner without significantly exhausting the organisation's resources.

The analysis of DPoS consensus mechanism underlines that a consensus mechanism needs to appeal to its participants in order to be actively contributing to the blockchain regardless of their role in the organisation. Considering this, an incentive system is established for the proposed consensus mechanism. The incentive mechanism operates under a system where incentives are capped for a group based on the priority of a transaction. As the group receives the transaction, the max incentive is established and indicated to the nodes. However, to ensure efficiency, the available incentive diminishes based on the time that it takes to process a request. Therefore, it is in the nodes' best interest to process transactions at its earliest to maximise their potential earnings.

Consequently, the incentive mechanism ensures that the nodes reach agreements at a increased rate and demotes malicious behaviour. Additionally, if a node within a group deliberately slows down the consensus process, the PBFT mechanism is in place to ensure that the network functions effectively as it can withstand a certain amount of faulty nodes along with the view change protocol. Once the nodes have reached consensus, the transaction is added to the blockchain and incentives are distributed equally among the nodes in the group. The mechanism then returns nodes to the grouping pool, immediately available for reassignment for further transactions. **Figure 4.2** encapsulates a transaction's lifecycle and how nodes interact with it.

This fluidity in the consensus mechanism upholds the principle of fairness and productivity, providing all nodes with equal opportunities to participate in transaction processing. In conclusion, the workflow described is suitable for the organisation and its employees as the proposed consensus mechanism allows them to achieve their desired business and operational objectives while making a strategic shift towards DLT.

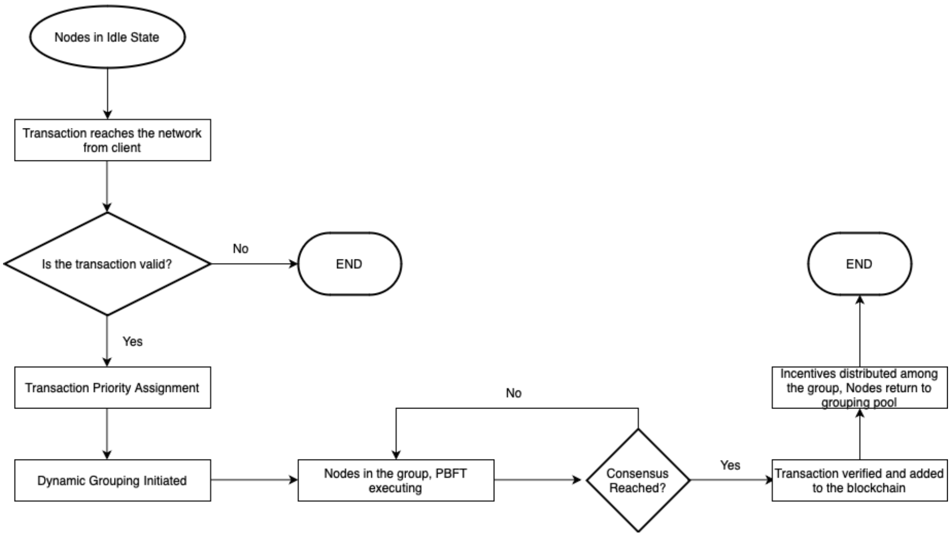

Nodes in Idle State
Transaction reaches the network from client
Is the transaction valid?
No
END
Yes
Transaction Priority Assignment
Dynamic Grouping Initiated
Nodes in the group, PBFT executing
No
Consensus Reached?
Yes
Transaction verified and added to the blockchain
Incentives distributed among the group, Nodes return to grouping pool
END

Figure 4.2 Sequential Flowchart of Priority-based Consensus

CHAPTER 5: MODELLING OF THE CONSENSUS MECHANISM

Chapter 5 provides an in-depth analysis into the proposed mechanism, employing a conceptualised modelling approach to evaluate its operational dynamics, how the components of the consensus mechanism interplay and at the end, how it impacts application performance. The focus of the modelling is the aspects of performance and incentives for its participants. Additionally, since the consensus is employing PBFT and introduces the concept of prioritising transactions based on their priority, it demands an analysis of how these innovations affect the organisation and its operations in blockchain.

5.1 SYSTEM MODEL

Let us define the organisation to have *N* nodes. As this is a conceptual model, we assume that the number of nodes in the organisation stay constant. We aim and consider that this consensus mechanism could be applied to any organisation which requires a dynamic transaction processing concept in addition to PBFT. When the departments (nodes) are in the grouping pool, they wait to receive a transaction from a client. **Table 5.1** presents an overview of the notations used in this chapter.

NOTATION	DESCRIPTION	NOTATION	DESCRIPTION
N	Number of nodes in the organisation	V	Communication Time
T_S	Size of a transaction	C_{min}	Minimum Communication Capacity
T_S^{Max}	Maximum possible size of a transaction	M	Computation Time
T_C	Cost of the transaction	α	Node Allocation Factor
T_C^{Max}	Maximum possible cost of a transaction	L_O	Optimal Latency
T_P	Priority of a transaction	m'	Minimum computational capacity
G	Number of nodes in one group	I	Incentives (Rewards) received by a group of nodes.
L	Latency	I_{max}	Maximum incentives possible
R	Transmission Rate	I_N	Rewards for a node in a particular group

Table 5.1 Notations and Descriptions

Once a transaction is obtained, the consensus mechanism begins its work by calculating the priority of the transaction since it is the basis of figuring how many nodes are going to be grouped to handle that particular transaction. We define the transaction priority to be a composition of the size of the transaction and the cost of the transaction defined as T_S (in kilobytes) and T_C (in dollars) respectively, while transaction priority is defined as T_P. The priority of a transaction can be computed as follows:

$$T_P = w_1 \frac{T_S}{T_S^{\text{Max}}} - w2 \frac{T_C}{T_C^{\text{Max}}} \tag{1}$$

The transactional priority is calculated as a normalised average of the two factors divided by maximum transaction size (in kilobytes) and maximum transaction cost (in dollars), where w_1 and w_2 are positive weights.The reason for these factors influencing the transaction priority is so that the organisation can classify requests to manage the transaction queue, ensure network throughput consistency and prioritise efficiency. Therefore, if transaction size increases and cost decreases, the priority assigned to it will also be higher as the transaction's importance will be quantified to be significant for the organisation and cost effective. Moreover, having maximum values constraints the factors where $T_S \in (0,T_S^{Max})$ and $T_C \in (0,T_C^{\text{Max}})$ ensures both variables have predefined upper bounds . Once a transaction priority is finalised, the number of nodes in a group handling the transaction are calculated as:

$$|G| = T_P \times N \tag{2}$$

where $|G|$ is the number of nodes rounded up and N is the total number of nodes in the organisation. According to equation (2), G is proportional to T_P and N. This step being applied before the nodes in the group engage in PBFT consensus allows the nodes to be significantly fractioned down. Minimising the number of nodes in PBFT groups results in lowered communication overhead. Now that the organisation have modelled the solution to improving the communication complexity, the added layers of processes threats to increase latency and therefore lower the transaction throughput. In conclusion, the objective is to minimise latency relative to the transaction processing.

The objective to minimise latency is of a significant importance as it dictates how long it takes for a transaction to be processed into the blockchain once it is requested. To effectively approach this problem, we need to direct what causes latency to increase at first.

Latency is dependent on how long nodes take to communicate to each other to achieve consensus, mainly how long does it take to propagate transaction related messages to other nodes. This may also relate to the geographical location of nodes. However, we assume that all nodes are at an identical geographical position. Therefore, communication latency can be be computed as:

$$f_1 = \frac{T_S}{R} \tag{3}$$

where R is transmission rate (in kilobytes/second) thus expressing communication time (V) in second(s). Moreover, computation is related to a transactions validation and verification. Thus, the latency is directly dependent on the computation power of a node as we need to know at what rate the transactions are being processed individually and as a group. A lower computation power may delay the transaction processing and as a result, increase latency. Note, we assume that the nodes have the same computational power and capacity. Thus, we have the computation time

$$f_2 = \frac{T_s}{m'} \tag{4}$$

where m' is computing capacity of a node (in kilobytes/second) and in turn, M is computation time (in seconds). As mentioned both communication time and computation time have direct impacts on latency and prove to be the essential formulas to help the organisation minimise latency. Therefore, we perform an addition function to communication and computation time to obtain latency L (in seconds)

$$L = V + M \tag{5}$$

However, the abstraction does not allow us to explore the intricacies of latency, which is essential to know if we are attempting to minimise it. A factor that is being omitted from the equation (5) is the number of nodes in a group G. This number is essential as it dictates how many nodes are working on a transaction together at a time to obtain latency within a group. Additionally, transaction size is a major factor for latency as well. Therefore, we can shift towards converting (5) into a functional form, acknowledging that latency is influenced by more factors other than just two components. We define communication time as a function f_1 signifying that C varies according to G and T_s. Similarly, computation time can be defined as function f_2 as a composition G and T_S varying M

$$C = f_1(G, T_s, R)$$

$$M = f_2(G, T_s, m') \tag{6}$$

Therefore, functions (6) can be substituted into the latency formula (5) and obtain a objective function

$$L = f_1(G, T_s, R) + f_2(G, T_s, m') \tag{7}$$

To solve the functional form of latency, we need to refine the model. This can be done by analysing communication time and computation time further. Communication time in PBFT involves $C = \frac{T_S}{R}$, but since PBFT required 3 phases of communication between the nodes to achieve consensus. Moreover, the number of nodes in a group impacts the communication time to increase quadratically as the complexity increases exponentially as the network grows. To minimise the latency, we can simplify the equation further by substituting accordingly:

$$f_1(G, T_s, R) = 3 \cdot \frac{T_S}{R} \cdot |G^2| \tag{8}$$

To obtain the final value of the function, we can substitute the equation that is used to calculated the number of nodes in a group (2) and from that equation, simplify the variable T_P to obtain the following equations

$$f_1(G, T_s, R) = 3 \cdot \frac{T_S}{R} \cdot (T_P \cdot N)^2$$

$$f_1(G, T_S, R) = 3 \cdot \frac{T_S}{R} \cdot \left[\left(w1 \cdot \frac{T_S}{T_S^{\text{Max}}} - w2 \cdot \frac{T_C}{T_C^{\text{Max}}}\right) \cdot N\right]^2 \tag{9}$$

Since the term $w1\frac{T_S}{T_S^{\text{Max}}} - w2\frac{T_C}{T_C^{\text{Max}}}$ suggests that both transaction size and transaction cost are relative to their maximums, the equation f_1 can be abstracted into:

$$f_1(G, T_S, R) = 3 \cdot \frac{T_s}{R} \cdot [N(\alpha T_s + \beta)]^2 \tag{10}$$

Where α is a constant relative of maximum transaction size $\frac{1}{T_S^{\text{Max}}}$ and β is the average transaction cost $-\frac{T_C}{T_C^{\text{Max}}}$. Now shifting the focus to function f_2 defining computation time as $f_2(G, T_s)$, the function can be defined as:

$$f_2(G, T_S, m') = 3 \cdot \frac{Ts}{m'} \cdot |G^2| \tag{11}$$

Similarly to f_1 we can substitute the equation (2) to simplify f_2

$$f_2(G, T_S, m') = 3 \cdot \frac{T_s}{m'} \cdot [N(\alpha T_s + \beta)]^2 \tag{12}$$

Thus, we can propose the final latency minimisation problem to be:

$$minf(T_s) = 3 \cdot \frac{T_s}{R} \cdot [N(\alpha T_s + \beta)]^2 + 3 \cdot \frac{T_s}{m'} \cdot [N(\alpha T_s + \beta)]^2 \tag{13}$$

$$min = 3N^2 T_s(\alpha T_s + \beta)^2 \cdot (\frac{1}{R} + \frac{1}{m'}) \tag{14}$$

Note, we assume $3N^2(\frac{1}{R} + \frac{1}{m'})$ as 'w' from this point onwards. Once expanding equation (14) we obtain a cubic polynomial as such:

$$f(T_S) = w\alpha^2 T_s^3 + 2w\alpha\beta T_S^2 + w\beta T_s \tag{15}$$

Since a cubic polynomial is obtained, we can proceed to performing derivation to obtain a quadratic equation

$$\frac{\partial f}{\partial T_S} = 3w\alpha^2 T_S^2 + 4w\alpha\beta T_S + w\beta^2 \tag{16}$$

This allows us to now obtain optimal values for T_S which would represent values that achieve minima and maxima latency

$$T_S^* = \frac{-4w\alpha\beta \pm \sqrt{(4w\alpha\beta)^2 - 4(3w\alpha^2)(w\beta^2)}}{2(3w\alpha^2)} \tag{17}$$

$$T_S * = -\frac{4w\alpha\beta \pm 2w\alpha\beta}{6w\alpha^2} \tag{18}$$

Thus, after simplification we obtain T_S1 and T_S2 as the optimal solutions

$$T^*_{S1} = -\frac{\beta}{\alpha} \tag{19}$$

$$T^*_{S2} = -\frac{\beta}{3\alpha} \tag{20}$$

Where if $\beta < 0$ then $T_{s1} > 0$ and $T_{s2} > 0$. Note, β being a negative in nature, equations (19) and (20) are both positive. Note, the optimal transaction size can be T^*_{S1} or T^*_{S2} to minimise the latency. Thus, we conclude the optimisation of transaction size with defining the optimal latency functions as

$$f * (T^*_{S1}) = L^*_1 \ or \ f * (T^*_{S2}) = L^*_2 \tag{21}$$

In the organisation, latency is not only significant for transaction processing, but it is also pivotal for the incentive system which yields rewards to the nodes for the transaction. The incentive system functions on a predicate that the nodes will only be rewarded when the consensus process is concluded and the request has been processed. However, their incentive has an incentive cap. Incentive cap is the maximum possible reward that a group can obtain on a transaction. When a group reaches agreement on a transaction and successfully generates the block, the reward for the group get equally distributed among the nodes in that particular group. Additionally, the rewards are contingent on the speed of consensus among nodes, as the incentive decreases with increased latency. Therefore we can define incentives as:

$$I = I_{max} - w_3 \cdot L \tag{22}$$

Where I is the rewards that the group processing a transaction obtains (in tokens) , I_{max} (in tokens) is the maximum possible incentives the group of nodes can claim and w_3 is the weight used as a conversion factor to translate the units. Additionally, according to the equation (21) we can optimise incentives based on the latency function $f(T_S)$ derived in equation (15) making the assumption that we can maximise incentives by minimising latency. Therefore, we can derive a function as such:

$$I = I_{max} - w3 \cdot [f_1(G, T_s, R) + f_2(G, T_s, m')] \tag{23}$$

Therefore, we can substitute the latency function in the equation (15) and express the optimisation problem of the incentive model as:

$$max\, I(T_s, w, \alpha, \beta) = I_{max} - w_3 \cdot (w\alpha^2 T_s^3 + 2w\alpha\beta T_S^2 + w\beta T_s) \tag{24}$$

This now allows us to find the critical points of I as a function of T_S using first order derivation, to indicate the points where I reaches its maximum or minimum

$$\frac{\partial I}{\partial T_S} = -(3w\alpha^2 T_S^2 + 4w\alpha\beta T_S + w\beta^2) \tag{25}$$

We can now solve the equation:

$$T^*_{S1} = -\left(\frac{-4w\alpha\beta + \sqrt{(4w\alpha\beta)^2 - 4(3w\alpha^2)(w\beta^2)}}{2(3w\alpha^2)}\right) \tag{26}$$

$$T^*_{S2} = -\left(\frac{-4w\alpha\beta - \sqrt{(4w\alpha\beta)^2 - 4(3w\alpha^2)(w\beta^2)}}{2(3w\alpha^2)}\right) \tag{27}$$

Thus, we can obtain our results as

$$T^*_{S1} = -\frac{\beta}{\alpha} \tag{29}$$

$$T^*_{S2} = -\frac{\beta}{3\alpha} \tag{30}$$

Note, similarly to the minimisation of latency problem, the optimal transaction size can be T^*_{S1} or T^*_{S2}. Optimal incentives are derived from the following equation:

$$I^* = I_{max} - w_3 \cdot f(T^*_S) \tag{31}$$

Furthermore, the optimal incentives received by a node in a group can be represented as

$$I_N = \frac{I^*}{N} \tag{32}$$

where I_N are the incentives received by a node (in tokens) in a group upon block generation.

The results of the optimisation reflect a correlation between latency, transaction size and incentives. The interconnection between the components is a product of system design and the effect that transaction size has on both the components of the consensus mechanism. In summary, the minimisation of latency and maximisation of incentives is aimed to be modelled in a way that an optimal T_S accomplishes both objectives simultaneously. In the next chapter, we will evaluate the changes in parameters linked and observe how transaction attributes, latency and incentives get affected.

CHAPTER 6: EVALUATION

Chapter 6 delves to simulate and evaluate the model that we have obtained in the previous chapter and dissect the results obtained from the process to contrast them again the optimisation objectives and anticipated outcomes. The analysis is mainly focused on transaction attributes like size and cost, latency and the incentive optimisation which are critical to understand the efficiency of the proposed consensus mechanism and the practicality of the conceptualised model. Additionally, a section is dedicated to conduct a comparative analysis between the proposed consensus mechanism and the existing mechanisms analysed in the previous chapters.

6.1 TRANSACTION PRIORITY RELATION TO SIZE

Transaction priority within our system is an integral part of the novel consensus mechanism as it determines the priority, thus the order in which the transactions will be processed in the organisation's blockchain application. It also has an impact on how many nodes will be grouped together to process a transaction based on its priority.

The nature of the transaction priority is determined by the size of the transaction (T_S) and cost of the transaction (T_C) to return a value, either positive or negative, which will be compared with other transactions' priority, forming an order of transactions.

To dissect the relationship between transaction priority and transaction size, we have conducted a simulation with varying transaction sizes, keeping other parameters as constants to isolate and highlight the effects of size on the priority of the transaction. **Figure 6.1** encapsulates the relation between transaction priority and transaction size. The x-axis represents the transaction sizes in kilobytes where $T_S^{\text{Max}} = 1000$. Inversely, the y-axis portrays the transaction priority that changes accordingly. The simulation plots the transaction sizes as: 200kB, 450kB and 800kB. $T_C = 10$ and $T_C^{\text{Max}} = 1000$. As shown on the graph, lines 1,2, and 3 vary in terms of the weight parameters w_1 and w_2. They are set as follows:

Line 1: $w_1 = 2, w_2 = 1,$
Transaction priorities: 0.36 (200kB), 0.86 (450kB), 1.59 (800kB)
Line 2: $w_1 = 1.5, w_2 = 1$
Transaction priorities: 0.28 (200kB), 0.67 (450kB), 1.19 (800kB)
Line 3: $w_1 = 0.5, w_2 = 1.5$
Transaction priorities: 0.08 (200kB), 0.21 (450kB), 0.38 (800kB)

The weights have been varied to allow how different factors influence the prioritisation of a transaction. This may also be done by the organisation when they need to change priorities based on their needs. For example, if the organisation has limited resources, they ought to choose a higher weight values that reflect their necessity in the transaction priority. Line 1 puts more emphasis on transaction size rather than cost, therefore it has the highest transaction priority. Line 2 decreases the transaction size's weight while keeping the weight on cost constant. This results at a flatter growth of transaction priority than

Line 1. Finally, in Line 3 a simulation where the weight on transaction's size was lower than its counterpart resulted in a depreciated transaction priority as transaction cost possessed higher influence. In conclusion, we observe an increase in transaction priority as transaction size increases. However, transaction cost counteracts that growth. The next section will simulate transaction costs' relation to priority.

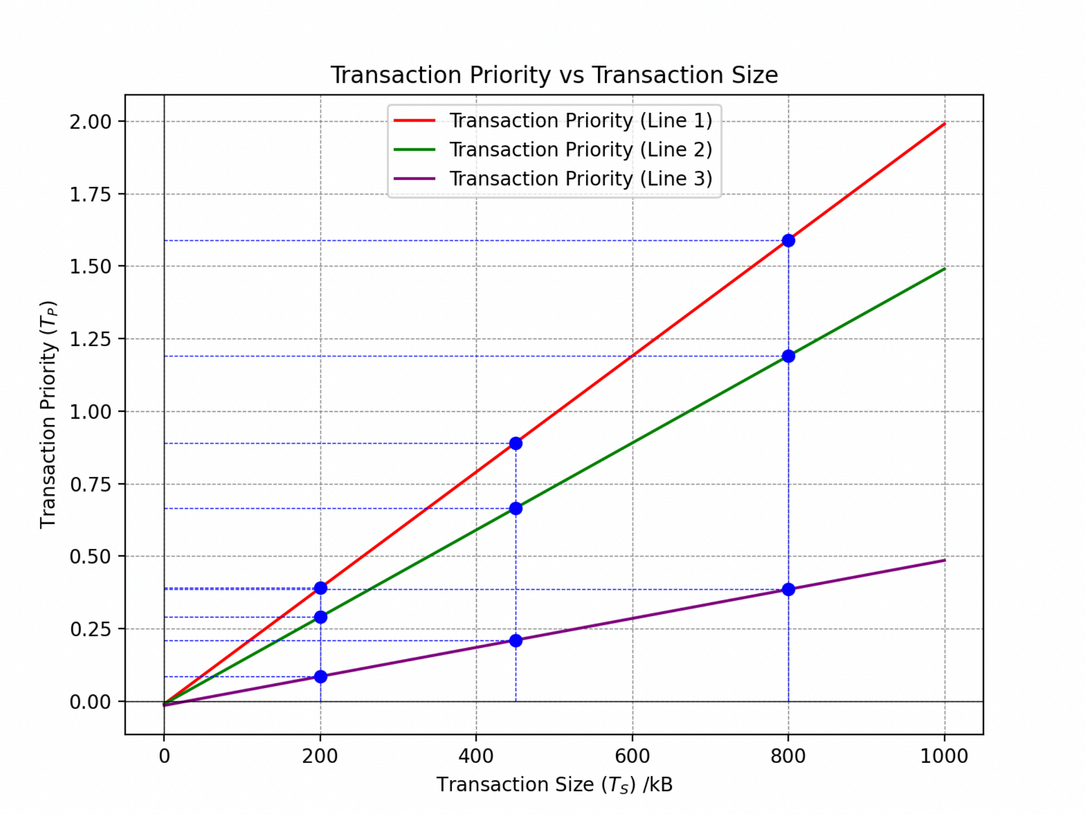


Figure 6.1 Relation Between Transaction Priority and Size

6.2 TRANSACTION PRIORITY RELATION TO COST

Transaction cost is pivotal to the calculation of transaction priority as it introduces a parameter that the organisation is able to manipulate according to their business needs. A cost of a transaction defines the amount of resources required to process a particular transaction. Therefore, it is important to evaluate the relation of transaction priority to cost. **Figure 6.2** displays the simulation results by plotting transaction cost on the x-axis and y-axis representing priority. Moreover, $T_C^{\text{Max}} = 1000$, $T_S = 500$, $T_S^{\text{Max}} = 1000$, and we plot transaction costs as: 200$, 450$ and 800$. Again, we vary the lines in terms of weight to simulate how cost affects priority as transaction size has the influence to increase it.

Line 1: $w_1 = 1, w_2 = 2,$
Transaction priorities: 0.10 (200), -0.40 (450), -1.10 (800)

Line 2: $w_1 = 1, w_2 = 1.5$
Transaction priorities: 0.20 (200), -0.23 (450), -0.70 (800)
Line 3: $w_1 = 1.5, w_2 = 0.5$
Transaction priorities: 0.65 (200), 0.53 (450), 0.35 (800)

Line 1 has the steepest slope among the lines indicating that that cost has a significant impact on priority as cost forces priority to rapidly decrease. This decrement is supported by the weight. Line 2 slope's comparison to Line 1 is a clear indication in change of weight as the decrease is not as significant. Lastly, Line 3 represents a scenario where transaction size is prioritised using weight. Simultaneously, the increase of priority may indicate that the organisation has acquired more resources and is prepared to process transaction that may be higher in cost.

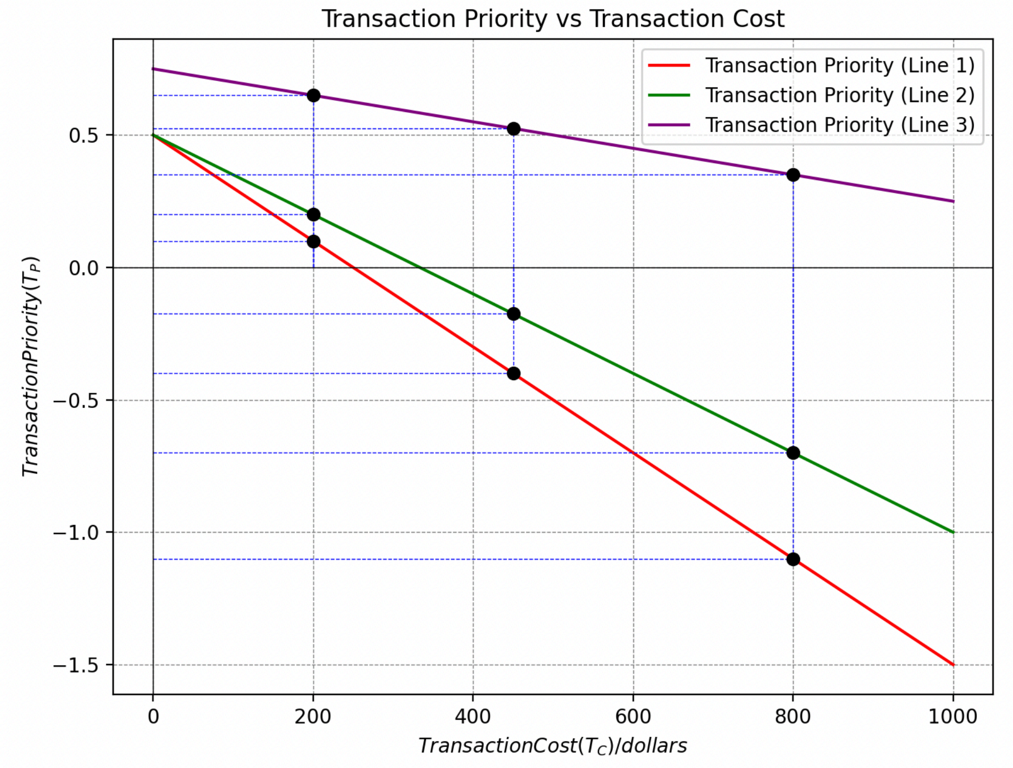


Figure 6.2 Relation Between Transaction Priority and Cost

Figure 6.2 may particularly interest stakeholders of the organisation when observing and analysing how resource allocation formula has been simplified by utilising the proposed consensus mechanism as it allows them to quantitatively adjust their operations simply manipulating values of the transaction priority equation. To conclude, the relation between the transactions' attributes, size and cost, each impact the urgency of a transaction. As transaction size increases, priority also increases. However, cost has an inverse effect by decreasing the urgency as the cost increases, and allows the organisation to plan for business costs when processing a transaction.

6.3 TRANSACTION SIZE AND LATENCY

The organisation's main objective was to minimise latency and increase the transaction throughput of which transactions are processed and added to the ledger in the company's private application. Through mathematical modelling, we proposed that transaction size plays a crucial role in the latency minimisation problem. **Figure 6.3** is a simulation of the equation

$$L(T_S) = w\alpha^2 T_s^3 + 2w\alpha\beta T_S^2 + w\beta T_s$$

under the parameters: $w = 1.25$, $\alpha = 0.068$ and $\beta = -0.90$ with x-axis being the transaction size in kilobytes and y-axis signifying latency in seconds. The function displays the latency curve obtained by the function, revealing critical points known as the local minima and maxima. These values are pivotal to understanding the simulation and the minimisation objective as they represent optimal transaction sizes for minimising latency in the system. However, the minima value at $T_S = 46kB$ could be either T^*_{S1} or T^*_{S2} . Due to the absence of direct computation, they represent theoretical optimal values.

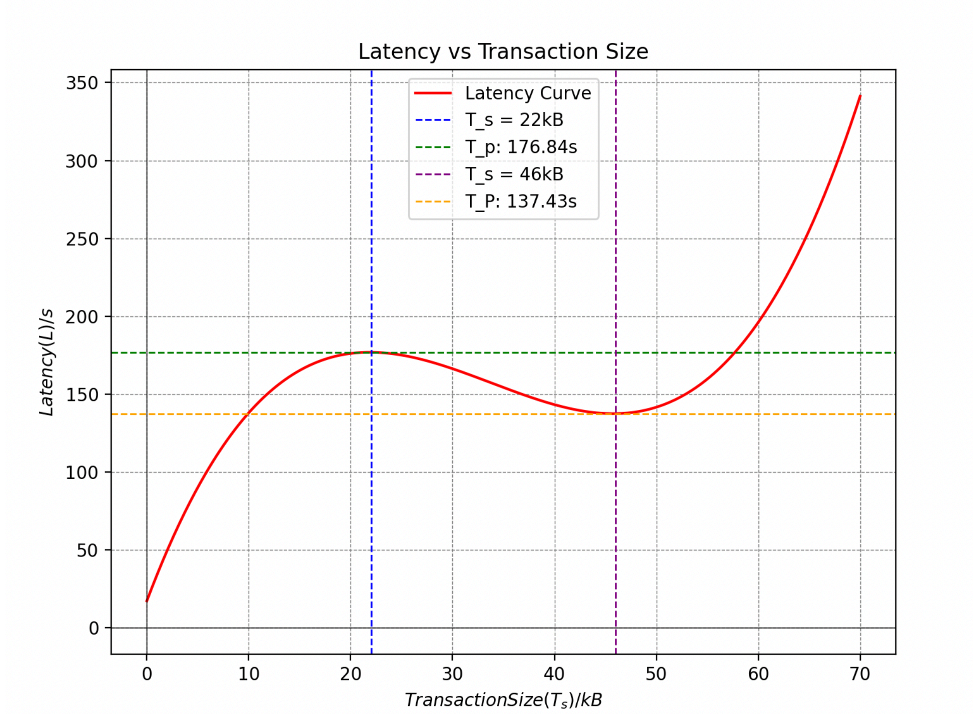


Figure 6.3 Relation between Transaction Size and Latency

We derive the following values from the simulation:
Transaction Size 1 = 22kB, **Latency 1** = 176.84s
Transaction Size 2 = 46kB , **Latency 2** = 137.43s

The results support the modelling as Transaction Size 2 does not follow the pattern of increasing size meaning increasing latency suggesting that this transaction size could be the local minima for the curve. This simulation is significant for the organisation as it allows the system admins to make informed decisions about adjusting transaction size and batch size of the blocks to be as close to the optimal values to mitigate inefficiencies.

6.4 INCENTIVES AND LATENCY

The result of modelling incentives indicated that there is a correlation between incentives and latency due to the system architecture. We then defined the solution to maximise incentives for the participants by minimising latency which means that if we find optimal values of transaction size, we can both minimise latency and maximise incentives.

Figure 6.4 simulates the equation and encapsulates the relation between incentives and latency. For simplicity, we set the parameters as $w = 1.25$, $\alpha = 0.068$, $\beta = -0.90$, $w_3 = 1$ and $I_{max} = 70$ to highlight the correlation between incentives and latency.

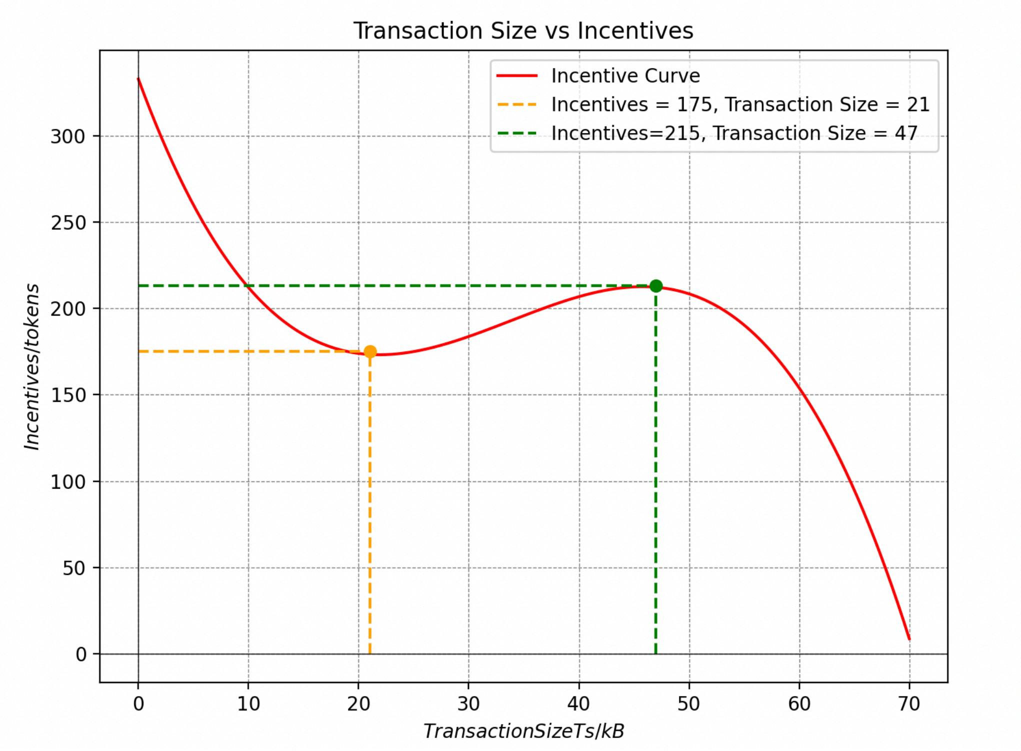


Figure 6.4 Relation between Transaction Size and Incentives

We obtain the following results from the simulation:

Transaction Size 1 = 21kb, **Incentive 1** = 175 tokens
Transaction Size 2 = 47 kb, **Incentive 2 =** 215 tokens

From the results, we can make the observation that the modelling of maximisation of incentives can be proven by simulation as a higher transaction size of 47kB yields higher rewards for the group of nodes.

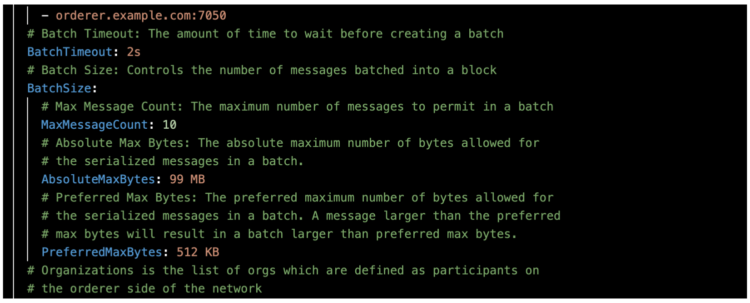
6.5 EXPERIMENTING RELATION BETWEEN TRANSACTION SIZE AND LATENCY

We use Hyperledger Fabric, a permissioned blockchain architecture hosted by the Linux Foundation to run an experiment to test the relation between transaction size and latency. Fabric is an open-source permissioned distributed ledger technology platform specifically designed for enterprises which makes it ideal for our experiment. Additionally, Hyperledger's modularity allows developers to configure various parameters that may influence the network throughput and latency.

To carry out this experiment, we will be configuring the **'test-network'** provided within the fabric-samples which includes:

- Two peer organisations: peer0.org1.example.com and peer0.org2.example.com. Peers are responsible for storing the blockchain ledger and validating transactions.
- One orderer organisation: orderer.example.com. Orderer organisation is a crucial service that uses single-Raft ordering service. Due to the test-network being a lightweight simplified network, a single orderer node exists. However, in production networks, multiple orderer nodes are in place to enhance security and fault tolerance.

Note, the number of nodes remain constant to underline communicational latency. In order to configure transaction size, we look to configure transaction batch size which is the size of transactions in a block. **Figure 6.5** depicts the configtx.yaml which is crucial for defining the initial channel configuration, particularly where the batch size values are provided.



```
  - orderer.example.com:7050
# Batch Timeout: The amount of time to wait before creating a batch
BatchTimeout: 2s
# Batch Size: Controls the number of messages batched into a block
BatchSize:
  # Max Message Count: The maximum number of messages to permit in a batch
  MaxMessageCount: 10
  # Absolute Max Bytes: The absolute maximum number of bytes allowed for
  # the serialized messages in a batch.
  AbsoluteMaxBytes: 99 MB
  # Preferred Max Bytes: The preferred maximum number of bytes allowed for
  # the serialized messages in a batch. A message larger than the preferred
  # max bytes will result in a batch larger than preferred max bytes.
  PreferredMaxBytes: 512 KB
# Organizations is the list of orgs which are defined as participants on
# the orderer side of the network
```

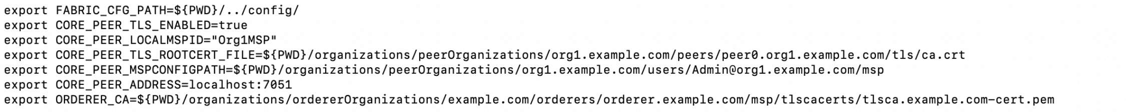
Figure 6.5 Initial Channel Configuration (Batch Size)

Among the batch size variables, the MaxMessageCount parameter plays a pivotal role to configure the batch size of transactions for the block to be committed. We aim to alter this parameter and test its impact on the network's latency. Firstly, we begin the experiment by installing fabric-samples to our system and running the test-network by using the command:

```
./network.sh up createChannel -ca
```

This command initialises the test network using the provided script and creates a new channel using the Certificate Authority (CA). A channel is a private communication path between specified organisations. CA in HyperLedger manages digital certificates to validate identities of the parties involved to ensure security in the network.

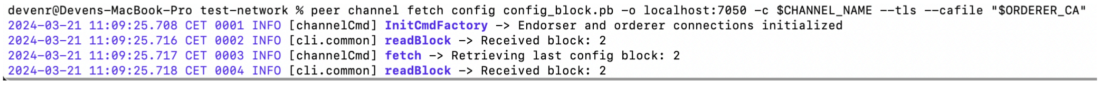
Once the network is initialised, the next step is to set up the environment variables which will allow us to interact with the peers, orderers and initialise paths to certificates including the Transport Layer Security (TLS) root certificate and the Member Service Provider (MSP) identification. These components in Hyperledger ensure security as TLS is used for data encryption and MSP ensures that each participant in the network is verified. **Figure 6.6** lists all the export commands used to set up the environment variables.



```
export FABRIC_CFG_PATH=${PWD}/../config/
export CORE_PEER_TLS_ENABLED=true
export CORE_PEER_LOCALMSPID="Org1MSP"
export CORE_PEER_TLS_ROOTCERT_FILE=${PWD}/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt
export CORE_PEER_MSPCONFIGPATH=${PWD}/organizations/peerOrganizations/org1.example.com/users/Admin@org1.example.com/msp
export CORE_PEER_ADDRESS=localhost:7051
export ORDERER_CA=${PWD}/organizations/ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem
```

Figure 6.6 Environment Variable Commands

In the subsequent phase, we fetch the current channel configuration block using the command "peer channel fetch config" and specifying the file in which the fetched configuration will be saved. **Figure 6.7** provides the complete command and its output.

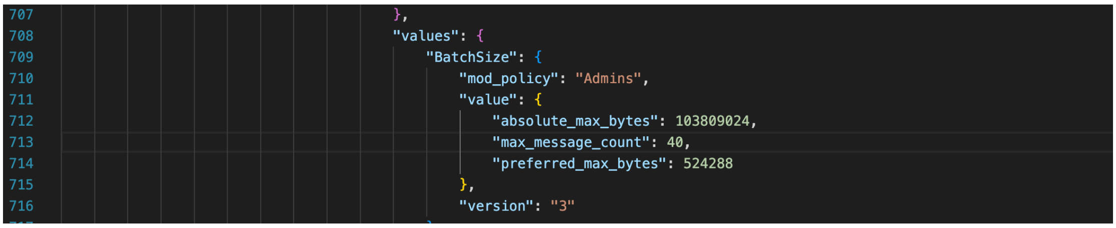


```
devenr@Devens-MacBook-Pro test-network % peer channel fetch config config_block.pb -o localhost:7050 -c $CHANNEL_NAME --tls --cafile "$ORDERER_CA"
2024-03-21 11:09:25.708 CET 0001 INFO [channelCmd] InitCmdFactory -> Endorser and orderer connections initialized
2024-03-21 11:09:25.716 CET 0002 INFO [cli.common] readBlock -> Received block: 2
2024-03-21 11:09:25.717 CET 0003 INFO [channelCmd] fetch -> Retrieving last config block: 2
2024-03-21 11:09:25.718 CET 0004 INFO [cli.common] readBlock -> Received block: 2
```

Figure 6.7 Fetch Channel Configuration Command

Additionally, the command tells the command line interface to fetch the configuration from the address of the orderer specified by '-o localhost:7050' and to save it in a protobuf file 'config_block.pb' which Hyperledger uses to serialise the data. The command outputs the 'Received block: 2' which means that the fetch was successful and the block 2 has been received and written to the file. Since the file is in a protobuf format, it is necessary to convert it into a JSON using the 'configtxlator' tool, a tool which allows for users to convert between data formats used in HyperLedger, so that the file could be updated by the user themselves.. Once we have converted the configuration into an editable config block JSON file, we can manually go to the file using an Integrated Development Environment (IDE) and edit the MaxMessageCount.

Initially, the MaxMessageCount is set to 10, but for the experiment we will update it to 40 to observe the changes that it may have. **Figure 6.8** displays the config_block.json file in Visual Studio IDE where the parameter is located . Next, after changing the parameter to 40, we can use the configtxlator tool again to encode the updated configuration back into protobuf format.



```
},
"values": {
    "BatchSize": {
        "mod_policy": "Admins",
        "value": {
            "absolute_max_bytes": 103809024,
            "max_message_count": 40,
            "preferred_max_bytes": 524288
        },
        "version": "3"
```

Figure 6.8 Batch Size Configuration

Now, we calculate the Delta between the initial configuration and the modified configuration to increase data efficiency since we need a way to only represent data that is being modified, which minimises the data needed to be processed.
We can use the configuration update as our transaction to be committed to the ledger. Our approach in doing that is to 'envelope' the Delta obtained which allows for changes, even configuration updates, to be formatted as transactions. Therefore, we can envelope the Delta using the command:

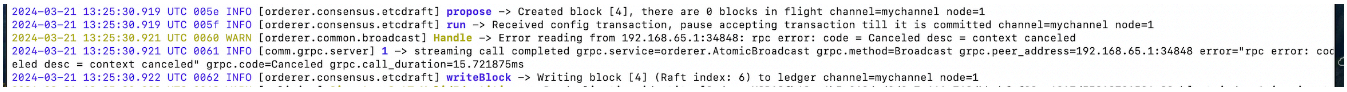
echo '{"payload":{"header":{"channel_header":{"channel_id":"<CHANNEL_NAME>", "type":2}},"data":{"config_update":'$(cat config_update.json)'}}}' | jq . > update_in_envelope.json

This command allows us to insert the contents in our update file into a new JSON file update_in_envelope.json using the jq JSON processor that formats the data to be appropriate for that file. Finally, we convert the JSON file containing the update into protobuf and it's ready to be signed and committed into the network.

To test if the updates were successfully configured we can utilise the following command:

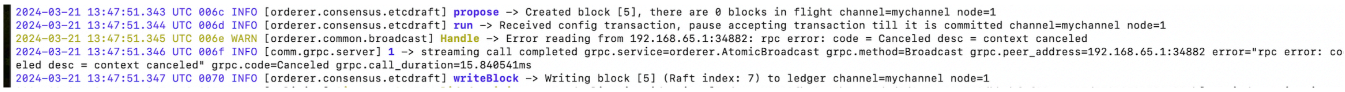
docker logs orderer.example.com

The command uses Docker containers that represent nodes in Hyperledger, which are useful to monitor network activity and updates. Furthermore, this gives us access to the logs of orderer.example.com as the orderer is responsible for block creation and distributing it to the peers. Figure 6.9 and Figure 6.10 shows the timestamps and the operations that the orderer performs to write a block to the ledger.



```
2024-03-21 13:25:30.919 UTC 005e INFO [orderer.consensus.etcdraft] propose -> Created block [4], there are 0 blocks in flight channel=mychannel node=1
2024-03-21 13:25:30.919 UTC 005f INFO [orderer.consensus.etcdraft] run -> Received config transaction, pause accepting transaction till it is committed channel=mychannel node=1
2024-03-21 13:25:30.921 UTC 0060 WARN [orderer.common.broadcast] Handle -> Error reading from 192.168.65.1:34848: rpc error: code = Canceled desc = context canceled
2024-03-21 13:25:30.921 UTC 0061 INFO [comm.grpc.server] 1 -> streaming call completed grpc.service=orderer.AtomicBroadcast grpc.method=Broadcast grpc.peer_address=192.168.65.1:34848 error="rpc error: coc
eled desc = context canceled" grpc.code=Canceled grpc.call_duration=15.721875ms
2024-03-21 13:25:30.922 UTC 0062 INFO [orderer.consensus.etcdraft] writeBlock -> Writing block [4] (Raft index: 6) to ledger channel=mychannel node=1
```

Figure 6.9 Processing transaction (maxmessagecount = 70)



```
2024-03-21 13:47:51.343 UTC 006c INFO [orderer.consensus.etcdraft] propose -> Created block [5], there are 0 blocks in flight channel=mychannel node=1
2024-03-21 13:47:51.344 UTC 006d INFO [orderer.consensus.etcdraft] run -> Received config transaction, pause accepting transaction till it is committed channel=mychannel node=1
2024-03-21 13:47:51.345 UTC 006e WARN [orderer.common.broadcast] Handle -> Error reading from 192.168.65.1:34882: rpc error: code = Canceled desc = context canceled
2024-03-21 13:47:51.346 UTC 006f INFO [comm.grpc.server] 1 -> streaming call completed grpc.service=orderer.AtomicBroadcast grpc.method=Broadcast grpc.peer_address=192.168.65.1:34882 error="rpc error: co
eled desc = context canceled" grpc.code=Canceled grpc.call_duration=15.840541ms
2024-03-21 13:47:51.347 UTC 0070 INFO [orderer.consensus.etcdraft] writeBlock -> Writing block [5] (Raft index: 7) to ledger channel=mychannel node=1
```

Figure 6.10 Processing Transaction (maxmessagecount = 100)

The timestamps signify that when maxmessagecount = 70, the time to process a transaction is 0.003ms but when maxmessagecount = 100, the time increases to 0.004ms. This signifies a relative 33% increase in latency which is due to increased batch sizes, leading to the system needing to handle more transactions concurrently. Since the test-network has limited, the increase in latency is 33%. However, in a bigger production network with multiple orderer nodes, this latency could increase exponentially.

6.6 COMPARATIVE ANALYSIS

PBCM is a consensus mechanism that integrates many strengths from all state-of-art mechanisms that exist in both public and private domain. Firstly, PBFT being PBCM's core consensus mechanism, the proposed protocol utilises its the efficiency, fault tolerance and versatility. The innovation of dynamic grouping, regrouping and priority based transaction processing allows PBCM to mitigate the communication issues and bottlenecks. Due to grouping, nodes no longer have to communicate to each and every node in the network to reach consensus. Instead, smaller numbers of nodes combine in groups to break PBFT's pattern of all-to-all communication and increase scalability potential of PBCM in the organisation. Moreover, the concept of prioritised block generation allows PBCM to allocate resources dynamically according to the business's needs so online PoW, this change significantly reduces energy consumption and increases energy efficiency as resources are allocated to the transactions that are most significant.

Regarding security and fault tolerance, PBCM promises to be more secure than DPoS and PoW. PoW encourages participants to invest in energy capacities and as a result, this leads to an arm race where wealthier participants have a larger chance of obtaining rewards. This attribute of PoW makes it susceptible to the 51% attack. However, PBCM having all nodes have uniform computational power, no participant can gain exploit the network, keeping the organisation secure. DPoS is dependent on the integrity of its delegates who control the protocols of the network. This dependency does not exist in PBCM as it uses PBFT for fault tolerance. Moreover, it resides in a private network so the proposed consensus mechanism is suitable for the organisation due to its security and privacy features. Despite PBCM being a consensus mechanism designed for the private domain, it has a democratised participation system. Participants in the novel consensus mechanism do not require a staking amount like PoS to have an influence on transaction processing.

In conclusion, PBCM promises to have significant advantages over state-of-art consensus mechanisms due to its resource and node allocation algorithms. Therefore, the organisation now can implement PBCM in their private application to achieve their objectives of revolution and optimisation.

CHAPTER 7: CONCLUSION

Chapter 8 summarises the report, reflecting on the project's overall success and reviewing the initial objectives outlined in the beginning. Moreover, the chapter includes a personal reflections on the report and the methodologies used along with suggestions on how the project can be further developed.

7.1 REVIEW OF THE PROJECT AIMS

Aim 1: *"Conducting a focused analysis of prevalent consensus mechanisms."*
This first aim of the project has been substantially achieved. The analysis conducted in Chapter 3 meticulously dissects the intricacies of the most prevalent state-of-art consensus mechanisms in both public and private blockchain domains which guided the design of the proposed consensus mechanism. Moreover, as highlighted in Chapter 4, the proposed mechanism mitigates many challenges posed by PBFT and introduces innovative features. Notably, dynamic grouping and the elimination of reputation systems along with staking which promise the organisation efficiency and fairness. The proposed consensus mechanism could further be refined by exploring less mainstream consensus mechanisms as the field of blockchain research is continuously expanding.

Aim 2: *"Development of the Priority-based consensus mechanism, tailored for private blockchains."*
Chapter 4 highlights the design of the Priority-based consensus mechanism that has been tailored specifically to meet the needs of the selected organisation. This organisation aimed to implement a private blockchain application for their internal departments. By adapting the Priority-based consensus, which is built upon PBFT, the organisation is supported to achieve its objectives in the private domain. Therefore, the overall aim has been achieved and sets a precedent for future implementation in similar contexts.

Aim 3: *"Perform simulation and mathematical modelling of the mechanism."*
This objective of the report has been successful as Chapter 6 and 7 provide mathematical modelling for the proposed consensus mechanism focusing on aspects such as latency, transaction size and incentives for participation. This modelling allowed the consensus mechanism to be optimised and set a solid foundation for practical implementation of the novel protocol. Moreover, a detailed experiment using Hyperledger Fabric was conducted to provide evidence that transaction size does influence the broadcast latency indirectly. Further improvement could include modelling for energy consumption and deploying a production network for the proposed consensus mechanism.

Aim 4: "*Comparative analysis of the new mechanism and existing algorithms."*
The final aim has been met as Chapters 3 and 6 benchmark the proposed consensus mechanism with the existing mechanisms, reflecting upon the key performance indicators such as security, transaction throughput and other blockchain characteristics. This objective could've been further enriched by comparing it to a wider range of mechanisms. Therefore, comparing PBCM to more consensus mechanism is a promising avenue for future work.

7.2 PERSONAL REFLECTION

Reflecting on the project as a whole, the entire process has been enlightening journey. I have learned about an industry that was previously unknown to me and the challenges faced in that industry. Before embarking on the project, I recognised the intensive reading, research and storytelling that would be required since this was a research oriented project. However, I have thoroughly enjoyed the entire process of research, from the detailed research, analysis and then actual writing the report. I've had the opportunity of learning new concepts and softwares such as mathematical modelling, Distributed Ledger Technology and Hyperledger among with others, that have opened up new perspectives in a domain that I had not been previously introduced during my computer science degree.

Blockchain has an extensive field of research as it transcends through industries. One of the most significant challenges of carrying out the project was understanding the details and the distinguishing between consensus mechanisms and their implications on cybersecurity and networking. Despite the challenge, I can affirm that it was an obstacle that I had overcame by extensive research, engaging with industry professionals and communities that have been in the field for a longer period of time. Moreover, finding current and reliable data to inform the project presented a challenge, as this was my first time engaging in a project that required reading journals and scientific papers. However, I addressed this challenge not merely reading papers, but by studying them in depth and engaging in modules within my degree that have taught me the process of academic writing and critical analysis. Finally, the most challenging aspect of the report itself was the simulation and mathematical modelling part of the report, especially the HyperLedger prospect. HyperLedger Fabric is a detailed software, the complexity of understanding the system which has numerous processes occurring in the background presented a significant learning curve. Due to time constraints, even after multiple trials and approaches, I was not able to implement those aspects in the detail as I would have liked. Nonetheless, I am satisfied with the outcomes of the project as it remains a testament to rigorous research and analysis. I have thoroughly enjoyed working on the project and I am keen on continuing to work on it with the aspiration of publishing my findings in the near future as the research has introduced me to the potential of blockchain technology and its real-world implications.

7.3 FUTURE WORK

An evident improvement to this project would be to implement the proposed consensus mechanism in a practical approach , utilising platforms such as HyperLedger Fabric or other similar software and unveil insights that theoretical work may not reveal. This could be done by designing a production network with a custom network configuration with multiple organisations, peers and orderer organisations to ensure security and fault tolerance whilst embodying a real-world enterprise network. Furthermore, deploying chain code to the that reflects the nature of PBCM and analysing its performance under various scenarios would provide insights to its effectiveness in a practical environment. Another significant improvement could be analysis of emerging and less documented consensus mechanisms that would encourage synergies similar to that of the proposed mechanism has with PBFT.

REFERENCES

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." *Decentralized business review* (2008).

[2] M. Castro et al., “Practical Byzantine fault tolerance,” in Proc. 3rd Symp. Operating Syst. Des. Implementation, 1999, pp. 173–186.

[3] Gervais, Arthur, et al. "On the security and performance of proof of work blockchains." *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 2016.

[4] Hawlitschek, Florian, Benedikt Notheisen, and Timm Teubner. "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy." *Electronic commerce research and applications* 29 (2018): 50-63.

[5] Zhai, Sheping, et al. "Research on the Application of Cryptography on the Blockchain." *Journal of Physics: Conference Series*. Vol. 1168. IOP Publishing, 2019.

[6] Jiao, Yutao, et al. "Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks." *IEEE Transactions on Parallel and Distributed Systems* 30.9 (2019): 1975-1989

[7] Houy, Nicolas. "The bitcoin mining game." *Available at SSRN 2407834* (2014).

[8] Gabison, Garry. "Policy considerations for the blockchain technology public and private applications." *SMU Sci. & Tech. L. Rev.* 19 (2016): 327.

[9] Zhang, Changqiang, Cangshuai Wu, and Xinyi Wang. "Overview of Blockchain consensus mechanism." *Proceedings of the 2020 2nd International Conference on Big Data Engineering*. 2020.

[10] Zhou, Sisi, et al. "A Systematic Review of Consensus Mechanisms in Blockchain." *Mathematics* 11.10 (2023): 2248.

[11] O'Donoghue, Odhran, et al. "Design choices and trade-offs in health care blockchain implementations: systematic review." *Journal of medical Internet research* 21.5 (2019): e12426.

[12] Hölbl, Marko, et al. "A systematic review of the use of blockchain in healthcare." *Symmetry* 10.10 (2018): 470.

[13] Hackius, Niels, and Moritz Petersen. "Blockchain in logistics and supply chain: trick or treat?." Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 23. Berlin: epubli GmbH, 2017.

[14] Perera, Srinath, et al. "Blockchain technology: Is it hype or real in the construction industry?." *Journal of Industrial Information Integration* 17 (2020): 100125.

[15] Miglani, Arzoo, et al. "Blockchain for Internet of Energy management: Review, solutions, and challenges." *Computer Communications* 151 (2020): 395-418.

[16] Bodkhe, Umesh, et al. "Blockchain for industry 4.0: A comprehensive review." *IEEE Access* 8 (2020): 79764-79800.

[17] Katuwal, Gajendra J., et al. "Applications of blockchain in healthcare: current landscape & challenges." *arXiv preprint arXiv:1812.02776* (2018).

[18] Singh, Akhilendra Pratap, et al. "A novel patient-centric architectural framework for blockchain-enabled healthcare applications." *IEEE Transactions on Industrial Informatics* 17.8 (2020): 5779-5789.

[19] Azaria, Asaph, et al. "Medrec: Using blockchain for medical data access and permission management." *2016 2nd international conference on open and big data (OBD)*. IEEE, 2016.

[20] Francisco, Kristoffer, and David Swanson. "The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency." *Logistics* 2.1 (2018): 2.

[21] Saberi, Sara, et al. "Blockchain technology and its relationships to sustainable supply chain management." *International journal of production research* 57.7 (2019): 2117-2135.

[22] Zastempowski, Maciej. "Analysis and modeling of innovation factors to replace fossil fuels with renewable energy sources-Evidence from European Union enterprises." *Renewable and Sustainable Energy Reviews* 178 (2023): 113262.

[23] Andoni, Merlinda, et al. "Blockchain technology in the energy sector: A systematic review of challenges and opportunities." *Renewable and sustainable energy reviews* 100 (2019): 143-174.

[24] Wang, Yuhao, et al. "Study of blockchains's consensus mechanism based on credit." *IEEE Access* 7 (2019): 10224-10231.

[25] Zhang, Rui, Rui Xue, and Ling Liu. "Security and Privacy on Blockchain." *ACM Computing Surveys* 52, no. 3 (2019): 1-34.

[26] Xu, Guangxia, Yong Liu, and Prince Waqas Khan. "Improvement of the DPoS consensus mechanism in blockchain based on vague sets." *IEEE Transactions on Industrial Informatics* 16.6 (2019): 4252-4259.

[27] Gu, Weiwei, Jianan Li, and Zekai Tang. "A survey on consensus mechanisms for blockchain technology." *2021 International Conference on Artificial Intelligence, Big Data and Algorithms (CAIBDA)*. IEEE, 2021.

[28] Gemeliarana, I. Gusti Ayu Kusdiah, and Riri Fitri Sari. "Evaluation of proof of work (POW) blockchains security network on selfish mining." *2018 International seminar on research of information technology and intelligent systems (ISRITI)*. IEEE, 2018.

[29] Sapra, Nishant, Imlak Shaikh, and Ashutosh Dash. "Impact of proof of work (PoW)-Based blockchain applications on the environment: a systematic review and research agenda." *Journal of Risk and Financial Management* 16.4 (2023): 218.

[30] S. King and S. Nadal, “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake,”

[31] Wei, Yunkai, et al. "Block mining or service providing: A profit optimizing game of the PoW-based miners." *IEEE Access* 8 (2020): 134800-134816.

[32] Han, Runchao, Nikos Foutris, and Christos Kotselidis. "Demystifying crypto-mining: Analysis and optimizations of memory-hard pow algorithms." *2019 IEEE international symposium on performance analysis of systems and software (ISPASS).* IEEE, 2019.

[33] Saleh, Fahad. "Blockchain without waste: Proof-of-stake." *The Review of financial studies* 34.3 (2021): 1156-1190.

[34] Sheikh, Husmeara, Rahima Meer Azmathullah, and Faiza Rizwan. "Proof-of-work vs proof-of-stake: a comparative analysis and an approach to blockchain consensus mechanism." *International Journal for Research in Applied Science & Engineering Technology* 6.12 (2018): 786-791.

[35] Sriman, B., S. Ganesh Kumar, and P. Shamili. "Blockchain technology: Consensus protocol proof of work and proof of stake." *Intelligent Computing and Applications: Proceedings of ICICA 2019.* Springer Singapore, 2021.

[36] Saad, Sheikh Munir Skh, Raja Zahilah Raja Mohd Radzi, and Siti Hajar Othman. "Comparative analysis of the blockchain consensus algorithm between proof of stake and delegated proof of stake." *2021 International Conference on Data Science and Its Applications (ICoDSA).* IEEE, 2021

[37] Feng, Xiaoqin, et al. "Regulatable and hardware-based proof of stake to approach nothing at stake and long range attacks." *IEEE Transactions on Services Computing* (2022).

[38] Fan, Xinxin, and Qi Chai. "Roll-DPoS: a randomized delegated proof of stake scheme for scalable blockchain-based internet of things systems." *Proceedings of the 15th EAI international conference on mobile and ubiquitous systems: computing, networking and services*. 2018.

[39] Zhang, Peng, et al. "Consensus mechanisms and information security technologies." *Advances in Computers* 115 (2019): 181-209.

[40] Yang, Fan, et al. "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism." *IEEE Access* 7 (2019): 118541-118555.

[41] Zhang, Wang, and Yunsheng Ge. "Improvement of DPoS consensus based on block chain." Proceedings of the 4th International Conference on Intelligent Information Processing. 2019.

[42] Akbar, Nur Arifin, et al. "Distributed hybrid double-spending attack prevention mechanism for proof-of-work and proof-of-stake blockchain consensuses." *Future Internet* 13.11 (2021): 285.

[43] Zhong, Weiyu, et al. "Byzantine Fault-tolerant consensus algorithms: a survey." *Electronics* 12.18 (2023): 3801.

[44] Yao, Wei, et al. "A survey on consortium blockchain consensus mechanisms." *arXiv preprint arXiv:2102.12058* (2021).

[45] Saini, Poonam, and Awadhesh K. Singh. "Proactive and reactive view change for fault tolerant byzantine agreement." *Journal of Computer Science* 7.1 (2011): 101.

APPENDIX

A. PROJECT PROPOSAL

PRIORITY-BASED CONSENSUS MECHANISM IN PRIVATE BLOCKCHAIN

ABSTRACT

The proposed project reported in this paper aims to conduct a comparative analysis of the existing blockchain consensus mechanisms and proposing a new consensus mechanism that is based on managing transactions based on priority and incentivise participants in a private blockchain to contribute without bias towards those with higher computational power or token holdings. This is pivotal to understand the importance of consensus mechanisms in blockchain and how new consensus mechanisms can be developed to encourage more users on the technology.

The initial phase of the study involves identifying the most commonly used consensus mechanisms in today's blockchain world; specifically Practical Byzantine Fault Tolerance and recognising their advantages and disadvantages. The outcome of the first stage will contribute to the analysis of the new consensus mechanism. Thirdly, incorporating game theory and model optimisation to allow further enhancement of the novel consensus mechanism.

The project will conclude by examining the new consensus mechanism through simulation which can be done via implementation on the HyperLedger Fabric platform and via game theory/optimisation modelling. The mechanism will be put through different scenarios and assumptions to guide changes and refinements and assess the practicality of the proposed consensus mechanism.

1. INTRODUCTION

The word 'Blockchain' has resonated with many individuals throughout the recent years, not only due to it's impact on technology and academia but also financial technology and cryptocurrency. Its noteworthy feature is having a distributed system that you can trust and communicate without having a central authority to control data flows [1]. Some blockchains are public, while others require permission to join. Blockchains such as Bitcoin are public and can be accessed by anyone and can handle several transactions at once [2]. Naturally, this creates opportunities for malicious actors to take advantage of the technology. It is susceptible to attacks such as Sybil attacks [3] , where an attacker can create numerous fake identities and manipulate network's decision-making process. This is one of the bigger issues when it comes to blockchain technology.

Due to it's rapid adaptation and demand, to combat such activities consensus mechanisms have been introduced. Consensus mechanisms not only incentivise participants for cleaner behaviour and secure participants from attacks, but also influence the performance of a blockchain network [4]. Consensus methods play a pivotal role in how a certain blockchain performs. Aspects like consensus in validation of blocks, scalability of the network (Public or private) and measures against malicious actors are linked to the effectiveness of a consensus mechanism. On the contrary, Consensus mechanisms have their drawbacks, such as communication overhead in PBFT, energy overhead in Proof of Word, risk of collusion in Delegate Proof of Stake (DPoS) etc. Mitigating these limitations is essential for making a blockchain consensus mechanisms as efficient and safe as possible.

The proposed project will investigate how consensus mechanisms are linked to the blockchain's network performance in both public and private settings. How mechanisms such as Proof-of-work

(PoW) function in the Bitcoin blockchain [5] and what are some of their features that enable Bitcoin to process numerous transactions concurrently while motivating miners to invest in expensive computational resources for access and participation. With the help of theoretical research, the priority-based consensus mechanism; which is combined with PBFT, this project aims to achieve a better performing algorithm that will be measured against state-of-art solutions, pinpointing it's strengths and weaknesses allowing for a improved simulation fidelity at the latter stages of the project. The study will also involve introducing a real-life scenario of a company in which a private blockchain exists to encourage inclusion of all ranks of employees and enhance the decision making process in the company. The blockchain network in the company will be using the proposed consensus mechanism to justify the algorithm's use in the real world.

The project proposal is as follows: background; which will contain background information on the related research that has been done regarding blockchains and consensus mechanisms, the proposed project; containing the aims and objectives of the project along with the methodology of how data and evidence will be gathered. Additionally, a programme of work is constructed to describe the plan of action and the task schedule to complete the project in a 18 week timeframe. A Gantt chart is provided to visualise the programme of work undertaken to the production of this project on the last page of the proposal on Figure 1. Finally, resources required and references used for the project are also provided in this document.

2. BACKGROUND

The previous work that relates to the project consist of proposing new consensus mechanisms [6] as it discusses the limitations of Practical Byzantine Fault tolerance and introduce a new consensus mechanism Credit-Delegated BFT (CDBFT) which proposes a mechanism that includes having a credit evaluation system and introducing consistency and checkpoint protocols based on PBFT. The results of this mechanism show a 5% reduction in abnormal node participation and a rise in efficiency and stability of the network. Despite the rigorous simulation and implementation of the novel consensus mechanism, it was not put into a real-life scenario to portray it's practicality. Therefore, the proposed project using a real-world scenario and pinpointing it's use cases would generally be a intriguing perspective.

Another study that relates to the project [7] provides a comprehensive review on blockchain technology, particularly the aspect of security and privacy. It aims for the readers to get an in-depth understanding of blockchain's security and privacy concepts including consensus algorithms, hash chained storage, mixing protocols etc. The article recognises the importance and the growth of blockchain technology in academia and industry whilst emphasising that only a small subset of blockchain platforms can achieve security goals in practice; which is an issue since security is one of the main fundamentals of the technology. Moreover, it positions security and privacy as the main sources of participant trust to engage in a blockchain network. The proposed project also aims to provide a detailed survey on blockchain technology but not only the aspect of security and privacy. Performance, incentive mechanisms and decentralisation concepts in the technology will be analysed in both public and private blockchains. Using that, a new novel consensus mechanism will be proposed to direct fundamentals into innovation.

3. THE PROPOSED PROJECT:

3.1. AIMS AND OBJECTIVES:

The proposed projects main aim is to propose a new consensus mechanism that is made for private blockchains. It consists of a priority-based mechanism that groups nodes based on the priority of a transaction and then use a PBFT approach to come to a consensus between the nodes.

Through theoretical research and literature reviews, the project seeks to explore the existing consensus mechanisms in both, Public and Private blockchains in order to find out which factors and features of a consensus mechanism influence: performance of the blockchain network; specifically speed of block creation and validation, incentive mechanisms that encourage participation in the network and ways of reaching consensus that also protects the network from adversity. Since PBFT (Practical Byzantine Fault Tolerance); a private blockchain consensus mechanism known for it's security and finality, [8] is a crucial component of the new consensus algorithm, it will be subjected to a more thorough examination compared to other mechanisms. This particularly will help make changes and adjustments to the new consensus mechanism so that the simulation phase does not have any anomalies and unexpected roadblocks.

The study will continue to examine it's practicality through a collection of experiments, simulations, and mathematical game theory models. This will provide substantiating evidence for the effectiveness of the mechanisms' approach. Subsequently, the project will carry out an evaluation and analysis phase to determine the practicality of the algorithm and assess it's strengths and weaknesses in comparison to existing consensus algorithms.

3.2. METHODOLOGY:

The methodology of this project is an experimentation one where certain hypothesis and assumptions will be made to carry out experiments to test the practicality of the priority-based algorithm that has been proposed for the project. How this will be done in terms of week split is described in the programme of work in the next section.

In the experimental phase, the open-sourced HyperLedger Fabric platform will be used along with game theory being integrated to work as an iterative process to conduct thorough experimental analysis. Game theory will allow for developing of models that will simulate the interactions between the participants, enabling to gain an insight on behaviours of agents and their decision-making. The use of game theory is pivotal to this experiment as it will also help examine the practicality of the method in a real-world scenario.

HyperLedger is specifically built for private enterprise blockchain use which is ideal as the priority-based consensus mechanism is also primarily intended to be used in private consortium networks [9]. The experimentation phase involves the design of a series of experiments that emulate various blockchain network conditions and user behaviours. Assumptions such about the node's computational capacity, throughput of the transactions and constraints like the number of devices will be made to tailor the scenario in order to gain insightful data about the feasibility of the algorithm in comparison to others. Game theory models become a crucial aspect of the methodology as they allow for formation of the hypothesis and the preliminary scenario to be made before HyperLedger is used for the collection of data.

4. PROGRAMME OF WORK:

- Literature Review: This is the first stage of the project where a comprehensive literature review of prior works related to the analysis of consensus mechanisms and blockchain metrics in both private and public networks. This is pivotal to the project as it will help pinpoint what are the main components of a consensus mechanism allowing for adjustments to be made to the proposed algorithm before it is simulated. This will take 2 weeks.

- Developing a Theoretical Foundation: This process comes after the literature review in which key components and operations are underlined of the consensus method and adjustments are made according to the output of the literature review. A detailed description is expected from this process, making it simpler to construct simulations and experiments. This process will take around 2 weeks.

- Initial Simulations and Testing: Setting up a simulation and doing preliminary tests to outline obvious faults and fix them before testing practicality of the mechanism in an experimental environment. This will take around 4 weeks.

- Experimentation and performance analysis: Experiments in different scenarios and use cases will be conducted to verify if the consensus mechanism is practical in each scenario and how does it influence factors such as: performance, speed of consensus etc. Platforms such as HyperLedger

Fabric will be used during this process. All data will be recorded, collected and visualised.

Moreover, assumptions under which the consensus method was under will also be taken into account in the experimental phase. This will take 5 weeks.

• Incorporate game theory mathematical models: Along with experimentation, mathematical models involving game theory will be done along side to explore different scenarios and form hypothesis. This incorporation may add 2 weeks to the project.

• Evaluation: This stage consists of drawing up conclusions from all scenarios and results of the experiments. This stage will also act as a buffer for the previous stages to make any corrections. The evaluation is estimated to take 2 weeks.

• Conclusion and Documentation: Final summaries and conclusions will be made in this part of the project along with recommendations. This process is an extension of the evaluation stage, therefore will take only 1 week.

The schedule is set for the years 2023-2024 and is visualised in the Gantt chart on the final page of this project proposal. (Figure 1)

5. RESOURCES REQUIRED:

No resources are required for this project.

6. REFERENCES:

[1] Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016) Where Is Current Research on Blockchain Technology?—A Systematic Review. PLoS ONE 11(10): e0163477. https://doi.org/10.1371/journal.pone.0163477

[2] Xie, M., Liu, J., Chen, S. and Lin, M. (2023), "A survey on blockchain consensus mechanism: research overview, current advances and future directions", *International Journal of Intelligent Computing and Cybernetics*, Vol. 16 No. 2, pp. 314-340.

[3] Sayeed S, Marco-Gisbert H. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Applied Sciences*. 2019; 9(9):1788. https://doi.org/10.3390/app9091788

[4] W. Wang *et al*., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," in *IEEE Access*, vol. 7, pp. 22328-22370, 2019, doi: 10.1109/ACCESS.2019.2896108.

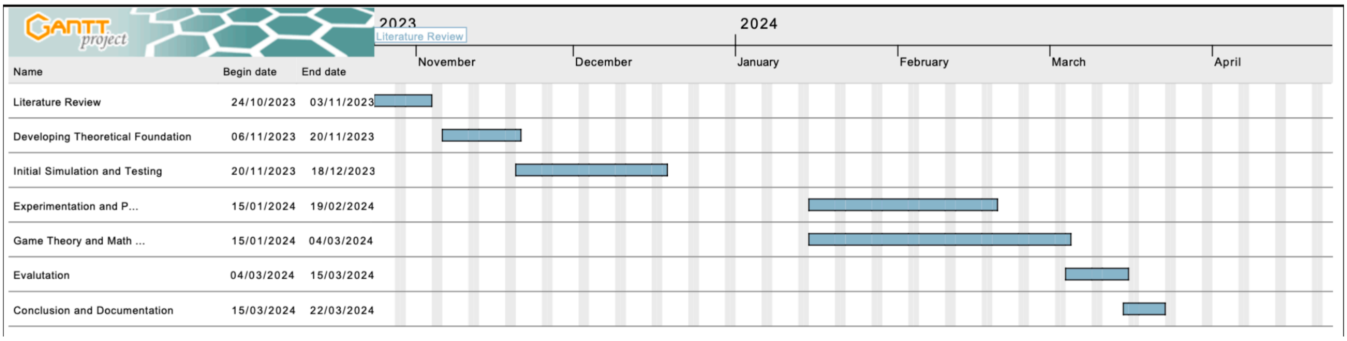
[5] Shi, N. A new proof-of-work mechanism for bitcoin. *Financ Innov* **2**, 31 (2016). https://doi.org/10.1186/s40854-016-0045-6

[6] Wang, Yuhao, Shaobin Cai, Changlong Lin, Zuxi Chen, Tian Wang, Zhenguo Gao, and Changli Zhou. "Study of Blockchains's Consensus Mechanism Based on Credit." *IEEE Access* 7 (2019): 10224-0231.

[7] Zhang, Rui, Rui Xue, and Ling Liu. "Security and Privacy on Blockchain." *ACM Computing Surveys* 52, no. 3 (2019): 1-34.

[8] K. Lei, Q. Zhang, L. Xu and Z. Qi, "Reputation-Based Byzantine Fault-Tolerance for Consortium Blockchain," *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*, Singapore, 2018, pp. 604-611, doi: 10.1109/PADSW.2018.8644933.

[9] Qassim Nasir, Ilham A. Qasse, Manar Abu Talib, Ali Bou Nassif, "Performance Analysis of Hyperledger Fabric Platforms", *Security and Communication Networks*, vol. 2018, Article ID 3976093, 14 pages, 2018. https://doi.org/10.1155/2018/3976093



Name	Begin date	End date
Literature Review	24/10/2023	03/11/2023
Developing Theoretical Foundation	06/11/2023	20/11/2023
Initial Simulation and Testing	20/11/2023	18/12/2023
Experimentation and P...	15/01/2024	19/02/2024
Game Theory and Math ...	15/01/2024	04/03/2024
Evalutation	04/03/2024	15/03/2024
Conclusion and Documentation	15/03/2024	22/03/2024

Figure 1 (Gantt Chart)