Department of Computer Science & Informatics
(CSIS6809)

Project Proposal

Blockchain: A Proof-of-Work Consensus Algorithm Implementation

Name: RC Lepeli
Student No.: 2018390157

13 March 2023

NATURAL AND
AGRICULTURAL SCIENCES
UFS

Abstract

This project aims to implement a Blockchain Proof-of-Work (PoW) consensus algorithm. A simple blockchain system will be created from scratch to create, validate, and complete transactions. The blockchain system implemented will include a data structure to record the transactions, the PoW consensus algorithm, a transaction, and a simple peer-to-peer network that simulates nodes or computers participating in the transaction; this includes the sender, receiver, and block proposers. PoW is one of the many consensus algorithms that add new blocks of transactions to a blockchain data structure by generating a hash that matches the target hash for the current clock. The block proposer who generates this hash wins the right to add a block to the blockchain and receives rewards (Daly, 2023). The general idea is to build a permissionless blockchain system allowing anyone who wishes to participate to participate in transactions. A permissionless blockchain system has five essential aspects: disintermediation, a peer-to-peer network, a distributed blockchain data structure, algorithmic trust, and open-source principles (Bezuidenhout, Nel, & Maritz, 2022). The Blockchain System will not have a central root of control but a network of nodes that decide on the final block of the distributed blockchain data structure. Since there is no central authority, PoW will be used for algorithmic trust to manage the blockchain's extension, security, and communication protocols. PoW will also provide the mechanism for constructing valid data to be transmitted on the peer-to-peer network and a means for verifying the validity of data received. It will ensure accessibility, immutability, and security through data validation of transactions, new transaction blocks, and the blockchain. This Blockchain System will allow any individual to create a transaction on the blockchain, e.g., sending Bitcoin from one user to another. PoW will handle the processing of the transaction. The recipient will then be notified that a transaction was made into their account. The Blockchain System developed for this project can be used as a data-capturing system for a new blockchain consensus algorithm called Proof-of-Publicly Verifiable Randomness (PoPVR) (Bezuidenhout, Nel, & Maritz, 2023). However, this will be done for future research and will not be focused on in this project.

Table of Contents

1. Introduction

Permissionless blockchain systems are distributed systems that utilise a combination of technologies such as distributed ledgers, cryptography, and consensus algorithms such that untrusted parties can agree on the state of decentralised transaction data. A blockchain system's purpose is to record immutable transactions on a distributed ledger that not be repudiated, secure, transparent, and accessible (Bezuidenhout, Nel, & Maritz, 2023). Meaning anyone can use the blockchain to execute or participate in transactions. However, blockchain systems face many challenges regarding algorithmic trust/ consensus algorithms. These include and are not limited to high energy consumption, centralised control, reliance on third parties for security, participation unfairness, non-deterministic inefficient solutions to security, and time-consuming processes (Geeks for Geeks, 2019) . This project aims to tackle this problem by building a blockchain system with the five aspects mentioned earlier for a permissionless blockchain system using a consensus algorithm that mitigates all the former challenges currently faced in the blockchain technology space. This system will fully implement the PoW algorithm and work as a proof of concept to simulate how a blockchain system functions. The PoW consensus algorithm was chosen for this project as it is a widely used algorithm for blockchain systems. Furthermore, it has high levels of security, allows block proposers to earn cryptocurrency rewards, and provides a decentralised method of verifying transactions (Chandler, 2022).

2. Problem Definition and Aims

2.1 Client needs and design criteria / Problem statement.

An entire blockchain system will be built from scratch. This includes implementing a Blockchain data structure that will act as a ledger for recording a collection of transactions taking place, the Proof-of-Work (PoW) consensus algorithm, a simple peer-to-peer network, and a transaction object that will be tracked in the system.

The Blockchain System developed in this project will be used for research and testing. It will simulate how a fully functional blockchain system works; however, it will require minimal human interaction as all the essential functions of a blockchain system will be

automated. This means multiple computers will not need to be set up to act as nodes that will participate in the blockchain. Again, all this will be automated.

In theory, the Blockchain System could be made accessible to anyone who wishes to participate; however, this could include challenges such as performance issues, limited flexibility, and high complexity. These issues heavily impact the use of blockchain technology. This is because security, transparency and fairness are entirely disregarded; thus, users are sceptical about using a system that cannot solve issues it stands against. It also makes it very hard for beginners to use the technology (Bloomberg, 2017).

2.2 Existing work

Since the emergence of blockchain technology, many different consensus algorithms have been developed. This includes and is not limited to algorithms such as Proof-of-Stake (PoS), Proof-of-Luck(PoL), Proof-of-Burn(PoB), Proof-of-Space(PoSpace), Nonlinear Proof-of-Work(nlPoW) and Proof-of-Authority(PoA) (Awati, 2022). These algorithms are heavily used in the industry and support the top five most popular cryptocurrencies with a market cap of $692.45 billion US dollars as of 5 March 2023 (Nesbit, 2023). These cryptocurrencies include Bitcoin, which uses PoW; Ethereum, which uses PoS; Binance Coin, which uses PoA; Cardano, which uses PoS; and Polygon, which uses PoS plus PoA (Brenman & Asher, 2021). The focus of this project will be the PoW consensus algorithm.

There are three types of blockchain systems.

1. Public or Permission-less blockchain system, this blockchain network is public and allows for unrestricted participation by anybody. On a public blockchain that is managed by laws or consensus algorithms, the majority of cryptocurrencies operate (Oracle Corporation, 2020).

2. In a private or permissioned blockchain system, Organisations can restrict who has access to blockchain data using a private, or permission, blockchain. For example, certain data sets can only be accessed by users given permission. An example is the Oracle Blockchain Platform (Oracle Corporation, 2020).

3. A Federated or consortium blockchain is a network where a predetermined group of nodes or a predetermined number of stakeholders tightly regulates the consensus process (mining process) (Oracle Corporation, 2020).

The focus of this project will be on the public blockchain system.

2.3 Proposed solution

A complete blockchain system that will be built will include the following:

1. A distributed blockchain data structure. The blockchain data structure can be defined as an ordered, back-linked list of blocks containing transactions. It can be stored in a simple database or as a file. A hash-generated cryptographic hash technique on the block header identifies each block. For example, in the "prior block hash" field of the block header, each block refers to a preceding block called the parent block (Marin, 2018) . This ledger will be used to record all transactions in this system. The figure below shows what a general blockchain data structure looks like

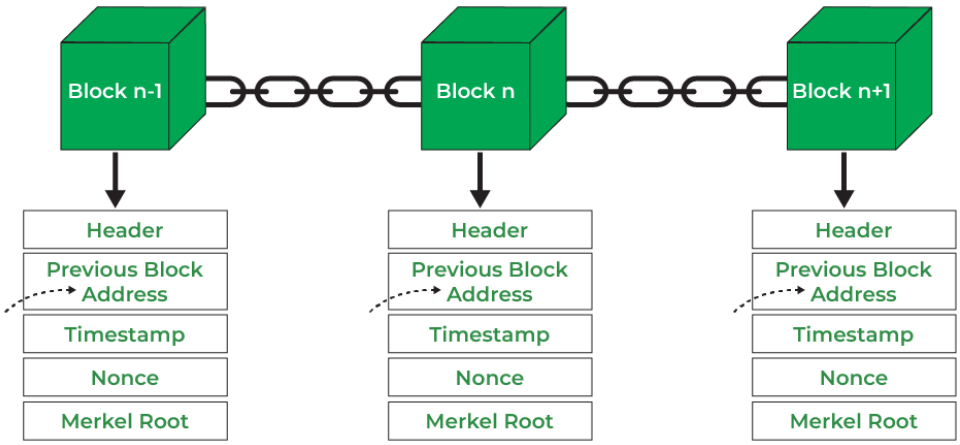
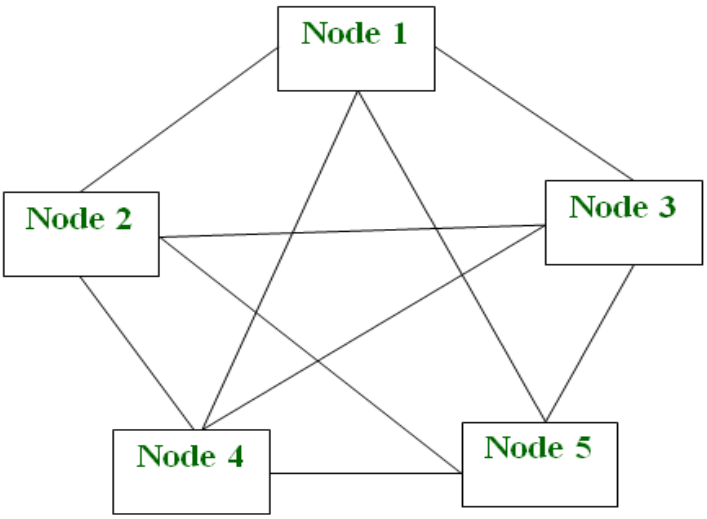


Figure 1: General Blockchain Data Structure

2. A Peer-to-Peer network. Message passing on a blockchain network occurs over a peer-to-peer (P2P) network; P2P is a well-known network topology. P2P refers to a decentralised topology where nodes collaborate to share resources and services without a central authority to coordinate the processes (Blockchain Council, 2019). A simple P2P network will be developed to simulate how it would function in a blockchain system.

The figure below shows how a general P2P network looks like



P2P Architecture

Figure 2: Simple P2P Network

3. A consensus algorithm: Proof-of-Work (PoW) is the mechanism of choice for most cryptocurrencies (Geeks for Geeks, 2019) and in this project. The algorithm will verify transactions and add blocks to the blockchain data structure. The figure below shows the results of PoW, where the correct block proposer solves a hash calculation before other network participants.

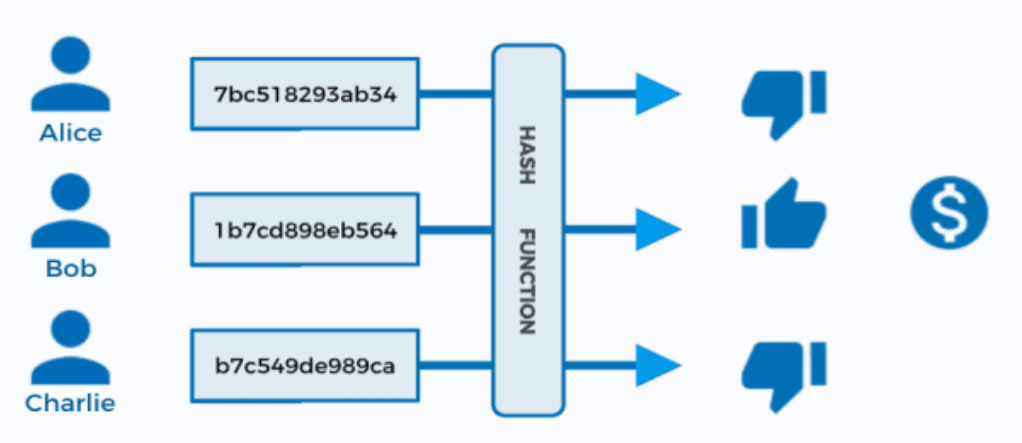


Figure 3: PoW Results

4. A transaction. This refers to a transfer or exchange of assets between two or more parties. The assets are usually cash or property (Vadapalli, 2022). For this project, a simple virtual currency will be used.

The system built in this project will fully simulate a fully functional permissionless blockchain system. This system will be used for benchmarking and to gain a deep and complete understanding of how blockchain systems function. It will heavily focus on the PoW consensus algorithm, its implementation and how it handles transactions. This gained knowledge can be used for future development in implementing a new algorithm Proof of Publicly verifiable Randomness (PoPVR).

PoPVR does not require large-scale computation, as is the case with Proof-of-Work and is not vulnerable to the exclusion of less wealthy stakeholders from the consensus process inherent in stake-based alternatives. It aims to promote fairness of participation in the consensus process by all participants and functions transparently using only open-source algorithms (Bezuidenhout, Nel, & Maritz, 2023, p. 14587). PoPVR randomly selects new block proposers from the participants in the blockchain system. This means no participant has the edge over others; thus, any participant who participates in the transaction verification can win the right to propose a new block (Bezuidenhout, Nel, & Maritz, 2023, p. 14601). The method uses verifiable random functions and hash functions to create a Blockchain Pseudo Random number generator that will produce the algorithm (Bezuidenhout, Nel, & Maritz, 2023, p. 14599). This algorithm will be a big step forward regarding computational power, fairness in the blockchain system, security, and transparency (Bezuidenhout, Nel, & Maritz, 2023, p. 14607).

This proposed method, however, will not be focused on in this project as it will be considered for a MSc degree in the future, where the system developed in this project will be used as a data-capturing system.

3. Design considerations and specifications

The developed system will have a minimal user interface since the focus is on the backend and the PoW algorithm to be implemented. The system will be developed to allow the incorporation of the proposed algorithm (PoPVR) in future development. The system will be developed in such a way that takes into consideration that the end user already understands the purpose of the system, which is simulating transactions on the blockchain and using the proposed algorithm as a consensus for algorithmic trust.

Since most of the parts in the system will be automated, end users will not necessarily be the focus. This extends to the automated P2P network and wallets that do not require human interaction.

3.1 Technologies involved.

Technologies involved will include the C# programming language, The .Net Core framework, which will be responsible for the algorithm implementation, the distributed blockchain data structure, and the minimal user interface. The C# programming language is chosen as it has some built-in cryptography functions, which will be the biggest challenge in the project.

Visual Studio will be used as the primary development platform for this project; this will include installing packages and plugins and using the built-in Visual Studio methods. Visual Studio will also work well since it allows good integration with version control of the developed components. In addition, the tools will include using Git and GitHub for source control and backups.

3.2 Hardware and software limitations

The system will be able to run on any machine as it will be developed using the cross-platform .net core framework; however, it will only be limited to the Windows operating system for testing purposes.

The minimum requirements for running the system:

a. Windows 10 operating system

b. Intel core I5 7th gen / AMD 2nd and 3rd Gen CPU's

c. 8 Gb DDR4 Ram

d. 120Gb SSD

e. Access to the internet

3.3 Performance limitations

The system will be running on its own. Thus, It will not integrate with any existing blockchain systems. The system will be running locally on a single machine.

Individuals interested in simulating and understanding blockchain systems will only use the system. Since the user interface is minimal, the system will only output the critical parts of a transaction, including transaction creation, hash generation, block addition and block verification. The user should have prior knowledge of what a blockchain system is and the fundamentals of how it works theoretically. The processes will be executed in real-time. Since the system is for simulation and testing purposes, it will not handle large amounts of data; it will only use data stored in text files. This data will either be auto-generated or seed data used during the testing. The system will handle user errors, such as the tester might want to transfer assets from one account to another but not considering that the first account might have insufficient funds. The system will alert the user if they generate such familiar errors. These user errors will not affect the system's performance since the core of the system is handling, processing, and completing correct instructions; this means transaction creation, transaction validation, and transaction completion will only execute if the instructions provided are accurate and are validated by the user interface's error checking system.

4. Required skills.

The system requires skills and knowledge in Blockchain systems/technology, advanced data structures and algorithms, cryptography/hashing, and Object Orientated Programming. It also will require using the C# programming language and the .Net Core/Framework platform.

5. Design approach/methodology

5.1 Methodology

The Kanban software development methodology will be utilised for this project.

Kanban, like Scrum, is an agile framework that focuses on continuous product improvement throughout development. However, whereas the Scrum method emphasises the importance of scheduling and prioritising tasks that must be completed, Kanban does not have a time limit or a repetitive process; it is flexible when it comes to implementing tasks and relies on continuous delivery during the sprint (Nguyen, 2021).

The picture below shows the Kanban life cycle.

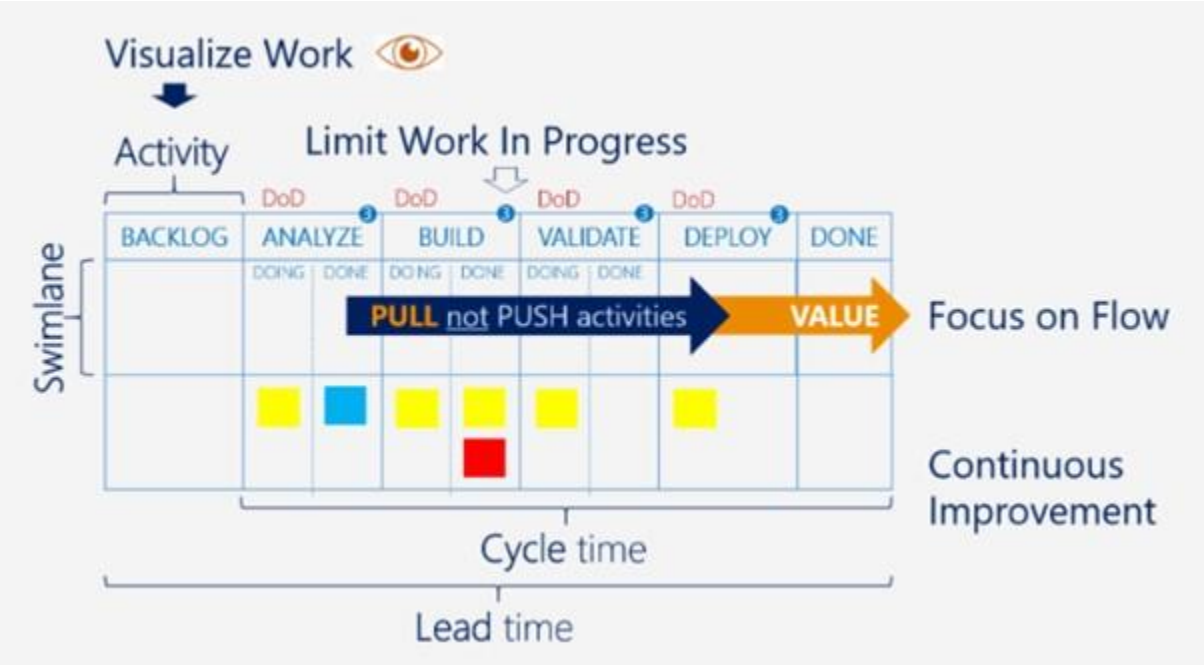


Figure 4: Kanban Lifecycle

Unlike other development methods, Kanban does not mandate specific team members or project management methods. Instead, the Kanban board is the essential element in this approach, used to list the tasks that need to be done in the product development process, also known as a to-do-list, categorises work that needs to be done or is in progress (Nguyen, 2021).

This method is a work management system that will help with visualising work, limiting work in progress and maximising efficiency. This method functions by building and using Kanban boards and kanban cards and setting up a work-in-progress limit. Kanban fits in perfectly with any schedule one might have and conforms to existing roles and responsibilities (Max, 2019), Meaning I can apply this methodology to how I currently work.

A Kanban board will be used to visualise all the tasks completed throughout the development of the system. Trello, a free digital platform, will be used create these kanban boards. The purpose is to categorise all the stages of work that a work item flows through, from something I have not started to something done. Each step in the workflow will have its column. These will include Tasks to complete, Tasks currently busy with and tasks that have been completed.

Kanban cards, in this project, will be used as work items—one card per task item. Cards will be made for all the tasks to be completed and placed in the appropriate workflow stage. Each card will have a title, a description, a checklist of task objectives, comments and a due date. These cards will be small enough to allow completion of tasks in a reasonable amount of time (Max, 2019).

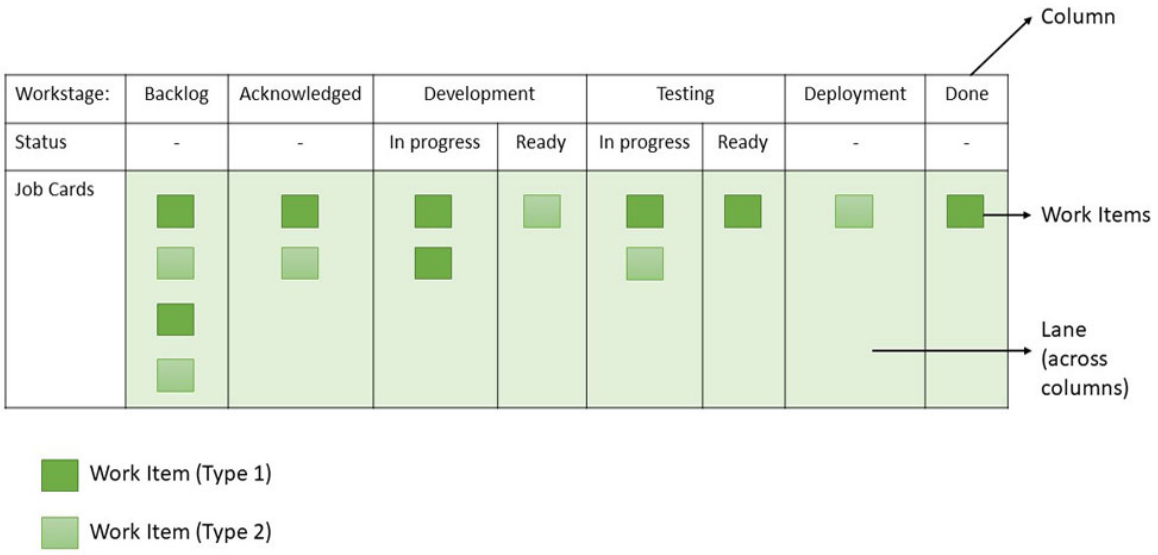


Figure 5: Kanban Simplified Version

One benefit of this methodology Is that it reveals early on the bottlenecks in any workflow and gives sense to what size a card should be such that tasks are completed on time. It is beneficial when working on solo projects. This helps move tasks from backlog to done (Max, 2019).

5.2 Project components

- Developing the Blockchain Data Structure.
    - The design of the Data structure
    - Implementation
    - Test
- Developing The Transaction to take place.

    - Type of transaction design
    - Implementation
    - Integration
- Developing a small, simple logical peer-to-peer network.
    - Network Design
    - Network Implementation
    - Network Testing and Integration
- PoW Consensus Algorithm design and implementation.
    - Research
    - Implementation
    - Testing and Integration
- The testing will be done after each component to ensure they integrate well.
    - Test of the Entire System
- A Minimal User Interface design and implementation.

5.3 Planned timeline.

The table below provides a very rough estimate. This will heavily depend on the schedule I have + the Other Modules. However, the margin of error for {1 Week} will extend the length for each deliverable by one week. This will be avoided as much as possible.

Task	Start	Length	End	Dependent On	Type
A. Submit Project Proposal	Week 1[13 Mar]	2 Weeks	Week 2[24 Mar]		
B. Start Development of the Blockchain Data	Week 1[17 Mar]	4 Weeks {1 week}	Week 5[21 April]	A [While waiting for proposal feedback]	Parallel + Iterative

	Structure + Testing					
C.	**Developing and Integrating the Transaction + Project Proposal Presentation**	Week 5[24 April]	3 Weeks {1 week}	Week 8[8 May]	B [During the Finalising of project Deliverables and Proposal + An updated Proposal]	Parallel + Iterative
D.	**Developing Clients/Peer to peer Network {Should be Very Simple}**	Week 9[15 May]	3 Weeks {1 week}	Week 12[5 June]	C [Also Making sure the lit review, project schedule and Use cases and Descriptions are taken care of]	Parallel + Iterative
E.	**Developing The Consensus Algorithm**	Week 13[12 June]	4 Weeks {1 week}	Week 17[20 July]	D [During the Database Design, Motivation]	

Below is a complete Kanban Trello board for the above table.

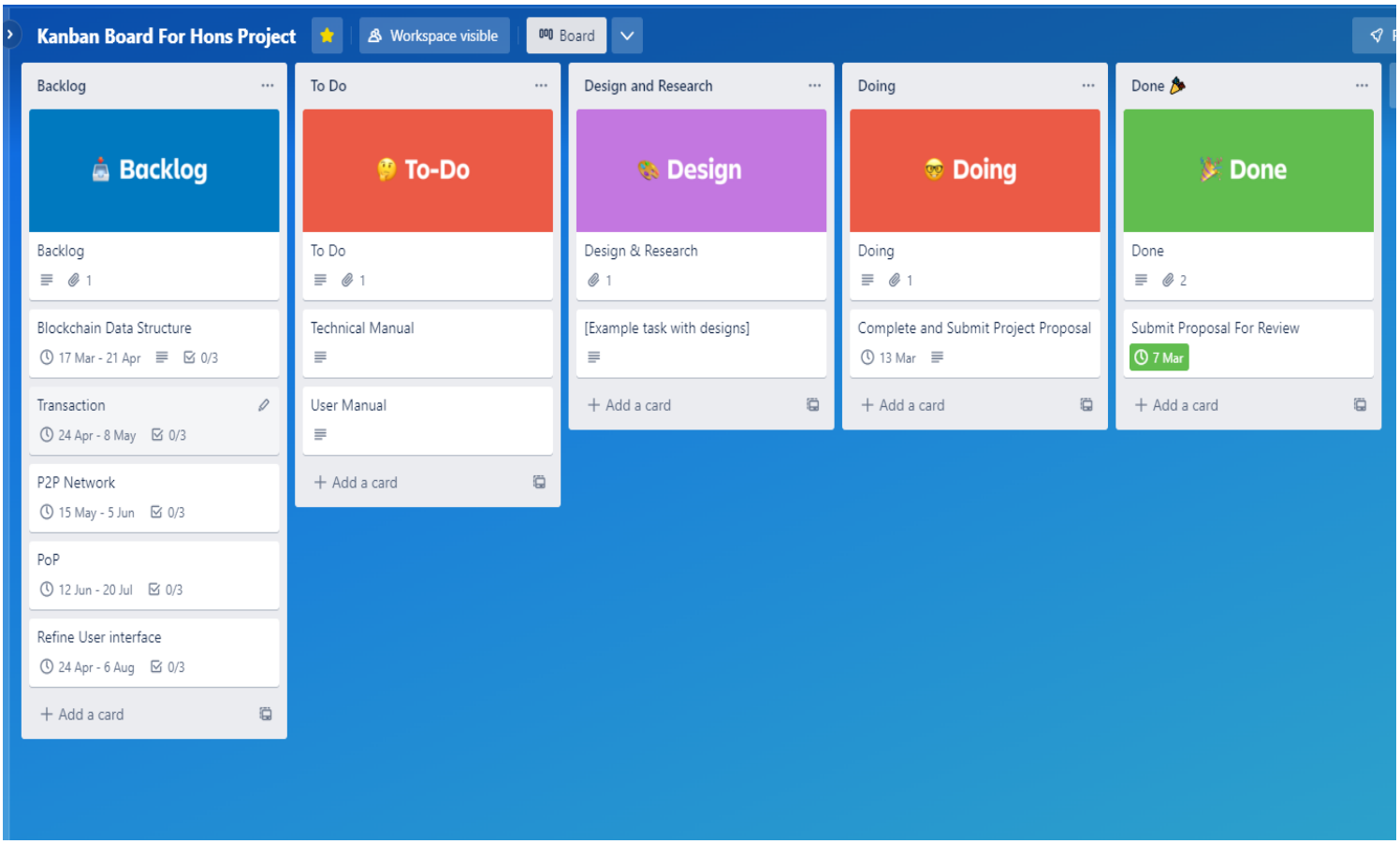


Figure 6: Development Schedule

6. Environmental Impact

The Blockchain System will not be used by any user unfamiliar with the project. It will only be for testing purposes. No sensitive data will be handled, and even if crashes happen, they will not affect the user in any way.

The program should only work on the machine containing the system's source code. Blockchain's ethical issues stem from its three promises: immutability, disintermediation (distributed verification), and automation. Immutability results in a permanent record and raises ethical issues such as privacy and transparency concerns (Hofmann et al., 2017). However, these will not be a concern since the Blockchain system developed in this project does not require any user data to function. The data will be auto-generated, and the system will not be deployed as a blockchain system. It does not interact in any way with existing blockchain systems and will run as its system for testing purposes.

All resources used during this Blockchain system's development, including books, articles, academic resources, and any other resources used, will be heavily referenced and documented.

7. Evaluation of solution

The Blockchain system developed will be regarded as a success if it can create, verify, and complete blockchain transactions. This includes:

1. The Distributed Blockchain data structure can enable the untrusted network of participants to agree on a single transaction record. In addition, the data structure acts as a tamper-proof distributed ledger with cryptographically linked sequential blocks where each block contains a set of transaction data.
2. A usable Transaction entity. The transaction should be able to be recorded on the data structure. In this project, the transaction will be a simple virtual currency sent to other accounts participating in the system.
3. A simple functional Peer-to-Peer(P2P) network: The system should generate a scalable network of virtual computer nodes participating in the blockchain system.
4. A Functional Proof-of-Work Consensus algorithm. The PoW algorithm should be able to verify transactions and add a new block on the blockchain on a timely basis that the tester or user will set. It should also be able to adjust the mining difficulty depending on how quickly participants add blocks. If mining is happening too fast, the hash computations get harder. If it is going too slowly, they get easier. It should also be able to allow block proposers to earn rewards after solving hash computations.
5. A simple Minimal interface. The interface should allow the user to set the number of network nodes, start a transaction and display notifications when transactions are completed or created.

The complete Blockchain system should be able to be used as a data gathering system for a Proof of Publicly Verifiable Randomness (PoPVR) consensus algorithm in the future for an MSc degree.

8. Conclusion

The system developed in this project will be a permissionless blockchain system that utilises the Proof-of-Work consensus algorithm. This system will simulate a functional blockchain system that maintains a decentralised and secure record of blockchain transactions that are temper resistant, transparent and accessible to all the participants in the blockchain system.

Software Deliverable Summary

- *A distributed Blockchain Data Structure*
    - *Will record transactions taking place in the system.*
    - *It will dictate the security and communication protocols.*
- *A transaction entity*
    - *It will be a transference of virtual currency.*
    - *It will be recorded/Kept on the data structure.*
- *Simple Peer to Peer Network (P2P)*
    - *The network includes the Sender and Recipient*
    - *Participants in the Blockchain system/ Block Proposes*
- *Consensus algorithm*
    - *It will dictate how blocks/records are added to the data structure.*
    - *Manages how clients participate and how they can trust each other.*

Complexity/difficulty component(s) of my project

The following aspects will bring the desired complexity to the project to ensure that it is on the Honours level:

- *Cryptography*
- *Advanced-Data Structures*
- *Blockchain technology*
- *Advanced algorithms*
- *Space and time complexity for the algorithms*

9. References

Appelbaum, B. (2019, March 12). *Pan View*. Retrieved from Top 6 Software Development Methodologies: https://blog.planview.com/top-6-software-development-methodologies/

Awati, R. (2022, August 15). *Consensus Algorithm*. Retrieved from Tech Target: https://www.techtarget.com/whatis/definition/consensus-algorithm

Bezuidenhout, R., Nel, W., & Maritz, J. M. (2022). Defining Decentralisation in Permissionless Blockchain Systems. *The African Journal of Information and Communication (AJIC)*(29), 1-24. doi:https://doi.org/10.23962/ajic.i29.14247

Bezuidenhout, R., Nel, W., & Maritz, J. M. (2023). Permissionless Blockchain Systems as Pseudo-Random Number Generators for Decentralized Consensus. *peer-reviewed open-access scientific journal, 11*, 14587-14611. doi:10.1109/ACCESS.2023.3244403

Blockchain Council. (2019, 13 November). *What is Peer-to-Peer Network, and How Does It Work?* Retrieved from Blockchain Council: https://www.blockchain-council.org/blockchain/peer-to-peer-network/

Bloomberg, J. (2017, 31 May). *Eight Reasons To Be Skeptical About Blockchain*. Retrieved from Forbes: https://www.forbes.com/sites/jasonbloomberg/2017/05/31/eight-reasons-to-be-skeptical-about-blockchain/?sh=58a98f2d5eb1

Brenman, C., & Asher, M. (2021, May 27). *Consensys*. Retrieved from Analysing Polygon's Proof of Stake Network: https://consensys.net/blog/blockchain-explained/analyzing-polygons-proof-of-stake-network/

Chandler, S. (2022, November 22). *Proof of work is at the core of the system that manages bitcoin transactions and secures the network*. Retrieved from Business Insider: https://www.businessinsider.com/personal-finance/proof-of-work#:~:text=Proof%20of%20work%20enables%20bitcoin,mechanisms%20like%20proof%20of%20stake.

Daly, L. (2023, 9 February). *What Is Proof of Work (PoW) in Crypto?* Retrieved from The Motley Fool: https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/proof-of-work/

Geeks for Geeks. (2019, 9 January). *Blockchain - Proof of Work (PoW)*. Retrieved from GeeksForGeeks: https://www.geeksforgeeks.org/blockchain-proof-of-work-pow/

Marin, J. (2018, 27 July). *Blockchain as a data structure*. Retrieved from Medium: https://medium.com/@juliomacr/blockchain-as-a-data-structure-3bd125d8ddda

Max. (2019, 3 April). What is Kanban? - Agile Coach (2019). Sydney, New South Wales, Australia. Retrieved from https://youtu.be/iVaFVa7HYj4

Nesbit, J. (2023, March 6). *Go Banking Rates*. Retrieved from 8 Best Cryptocurrencies To Invest In for 2023: https://www.gobankingrates.com/investing/crypto/best-cryptocurrency-to-invest-in/

Nguyen, P. A. (2021, 9 October). *wear from*. Retrieved from The Best Software Development Methodologies for Small Teams: https://wearefram.com/blog/software-development-methodologies/

Nikolaieva, A. (2019, June 13). *Up tech*. Retrieved from 8 Best Software Development Methodologies: https://www.uptech.team/blog/software-development-methodologies

Oracle Corporation. (2020, 12 March). *Oracle*. Retrieved from What is Blockchain: https://www.oracle.com/middleeast/blockchain/what-is-blockchain/

Vadapalli, P. (2022, September 12). *upGrad*. Retrieved from What is Blockchain Transaction? How Does it Work?: https://www.upgrad.com/blog/what-is-blockchain-transaction/#:~:text=on%20the%20network.-

,What%20is%20a%20blockchain%20transaction%3F,computers%20in%20a%20blockchain%20system.