Bitcoin Core Call for Improvement

An Architecture Enhancement Report

CISC 322
Software Architectures
Professor Bram Adams

Group 34:
Sweet Home Ala-bram-a

Jean-Philippe Le Blanc - 20157203 - 18jpcl@queensu.ca (Team Leader)
Dallas Doherty - 20220683 - 19ded2@queensu.ca (Presenter)
Ethan Mah - 20224551 - 19ettm@queensu.ca (Presenter)
Ruairí O'Connor Clarke - 20235043 - 20rmoc@queensu.ca
Muhammad Ibrahim - 20218324 - 19mi22@queensu.ca
Mayy Mounib - 20230803 - 19mlm15@queensu.ca

Submitted on April 12th, 2023

Table of Content

Abstract 3
Introduction 3
Proposed Enhancement 3
Effects on Architecture and Interactions Between Features 6
Impacted Directories and Files 7
Current State of System Relative to Enhancement 8
Alternative Enhancement 8
Use Cases and Sequence Diagrams 11
Plans for Testing Enhancement 12
Potential Risk 13
Conclusion 13
Lessons Learned 14
Data Dictionary 14
References 15

Abstract

Bitcoin Core currently uses a proof-of-work consensus algorithm to validate transactions and preserve the integrity of the network. In recent years, the proof-of-work algorithm has been condemned for its massive energy consumption and centralization risks. This Architecture Enhancement Report explores the benefits and drawbacks of converting Bitcoin Core from using a proof-of-work to a proof-of-stake consensus algorithm. It examines the impact of this switch on the non-functional requirements, the stakeholders, the interactions with other features, and the internal and external effects of the enhancement. It also explores an alternative for implementation, where the concept of a hybrid model is explored. Lastly, this report includes plans for testing this enhancement along with the potential risks of the change.

Introduction

The world's first decentralized cryptocurrency, Bitcoin, has been operating on a proof-of-work [7] consensus algorithm since its inception. Miners around the world rely on this algorithm to secure and verify blockchain transactions by racing to solve computationally expensive cryptographic puzzles. These miners are rewarded with a bitcoin for every block added to the blockchain. It is the Bitcoin Core software that coordinates this large system and the flow of data and control. However, as the network grows and the demand for processing power increases, the energy consumption and associated costs of this proof-of-work algorithm have become a concern for the community and planet. Miners tend to set up operations in locations with the lowest electricity costs, but often these locations rely on energy sources with a significant carbon footprint. With the current state of the planet, it is important to mitigate carbon emissions and find alternatives that will help reduce Bitcoin Core's Carbon footprint. Furthermore, the issue of decentralization and security has arisen due to the accumulation of power by major stakeholders within the system. To address these concerns proposals have been made to convert Bitcoin from a proof-of-work algorithm to a proof-of-stake [6] consensus algorithm. Throughout this report, we will explore the potential benefits of converting Bitcoin from proof-of-work to proof-of-stake, and analyze the technical and economic considerations that must be taken into account when making such a transition. Alternatively, our report will investigate a hybrid model of the proof-of-work and proof-of-stake consensus algorithm. This hybrid version offers features of both consensus algorithms but also contains the drawbacks of both.

Proposed Enhancement

With the knowledge obtained by the process of deriving the conceptual architecture and by analyzing the concrete architecture of Bitcoin Core, we found that an area for improvement was the current consensus algorithm. Our team proposes that the consensus algorithm should be altered to implement a proof-of-stake (PoS) algorithm rather than a proof-of-work (PoW). Albeit this is a major change that would change the structure of Bitcoin Core it comes with many

advantages. This change would come with many adjustments to the non-functional requirements and to the positions of the stakeholders in Bitcoin Core. Due to the sheer size of the change, it is essential that there is a good project management team leading the transition. There are many moving parts and a lot of changes to be made, so keeping track of the current state of the software will be an absolute must. The actual architecture of the system will remain as a Peer-to-Peer system as the PoS implementation does not change the overall architecture, but rather how some subsystems interact.

Changing Bitcoin Core from PoW to PoS would have significant implications for various stakeholders involved in the cryptocurrency ecosystem. The developers would be heavily impacted, as the transition and implementation would require a significant overhaul of the existing code and the development of new software tools to support PoS. The miners who currently play a pivotal role in securing and maintaining the Bitcoin network would be greatly affected. PoS would require a different method of validating transactions, which would result in miners becoming obsolete. This could lead to a significant shift in the distribution of wealth and power within the Bitcoin ecosystem. Owners of wallets and other third-party applications would need to adapt to the new proof of stake system, potentially requiring them to update their software and make other changes to their infrastructure. Regulators would also be affected by a switch to PoS, as it could alter the legal and regulatory landscape for cryptocurrencies. PoS could result in changes to tax laws, requirements, and other regulations governing the use of cryptocurrencies.

With a change of this magnitude on the Bitcoin Core architecture, many non-functional requirements would be affected. The list of NFRs that could be modified, created, and removed, is lengthy, however below are the most notable and important changes:

Environmental Effects: The current consensus algorithm consumes “around 110 Terawatt Hours per year — 0.55% of global electricity production” [1], which is an enormous amount of energy for a monetary system. Compared to Ethereum, a competing cryptocurrency that implements a PoS consensus, which only consumes “an estimate of 0.0026 TWh for the network’s annual electricity consumption” [2], which is a 42000% difference. By means of prediction, we can infer that Bitcoin Core would be in a similar range as Ethereum, which would have a significant and beneficial impact on the environment. This NFR primarily impacts regulators and miners, as regulators are concerned with the legal implications, and miners would become obsolete. However, it technically impacts everyone on the planet as the carbon footprint is reduced.

Security: This would be the top priority when implementing this transition from PoW to PoS. With a new consensus algorithm, it will be very important to thoroughly test and audit the system to make sure there are minimal vulnerabilities that attackers can exploit. New exploitations and challenges are always possible, so developers must consider edge cases to ensure the longevity of Bitcoin core. As mentioned, the security of the system primarily affects

the developers as they must keep this NFR in mind when designing and developing the new PoS system.

Performance: PoS has the potential to be more scalable and efficient than PoW, but it would still need to meet high standards for performance. The new system should be designed to process transactions quickly and with low latency. In addition, a PoS consensus algorithm decreases the hardware requirements that are required to perform PoW. This NFR affects the wallet owners and the developers. Owners will be directly affected when it comes to performance as they are the ones that will experience it. The developers also have a great deal to do with the performance of the system as they are in charge of creating fast and responsive code that performs to the highest standards.

Network Stability: In the face of changing conditions such as increases in user activity, changes in network topology, or the occurrence of unexpected events, the network must remain stable and resilient. This is crucial to maintain the availability and integrity of the system. If the new network is not stable, serious consequences such as transaction delays, lost funds, and decreased user trust can occur. The network stability affects many stakeholders. The wallet owners and third-party applications are affected as they need a reliable network in order to make transactions. The developers need to maintain and improve the network continuously, as a way to maintain its stability.

Scalability: The new consensus algorithm must be scalable to accommodate the potential increase in users, data, and transactions. With the PoS allowing for easier onboarding for users to participate, there will be increases in the amount of users staking their Bitcoin. In addition, with the growth of cryptocurrencies and its introduction to mainstream currencies, it must be able to handle massive volumes of traffic. The scalability affects nearly all stakeholders and developers must be ready for sudden increases in users, data flow, and transactions.

Accessibility: The new PoS algorithm must be designed to be easy for users to interact with. By creating an accessible way for users to interact with the consensus and stake their currency, there will be an increase in use and a lower barrier to entry. This will in turn cause more household computers and systems to be able to partake in the consensus, making it more accessible to the public. Accessibility is important for potential stakeholders.

Reliability: With a change of this magnitude, it is important that the system works reliably in all situations. If the system fails, crashes, or has significant downtime, then it will be harmful to the system and the stakeholders. It is important that the new consensus algorithm works smoothly and properly from the start. Ensures high-level security measures to protect stakeholders from exploitation attempts.

Evolvability: The change to a PoS algorithm would lead to a more centralized network as stakeholders would gain voting rights and the ability to help make decisions for the network. As a whole, this would lead to a more streamlined decision-making process and allow implementations and evolution of the network to become easier and more efficient than the governance power that PoW holds. This affects all the wallet holders as they would have more influence.

Maintainability: The maintainability of the Bitcoin network will greatly improve when considering the massive reduction in energy consumed by stakeholders and nodes on the Bitcoin network. With a lower barrier to entry and reduced reliance on the mining process, a shift to PoS would influence growth in users joining the Bitcoin network. As the currency simplifies in complexity and becomes more accessible to the general public the Bitcoin Network will continue to be maintainable for the foreseeable future ensuring stakeholders have a secure and reliable cryptocurrency to invest in.

Changing Bitcoin Core from a PoW to a PoS consensus algorithm is an enhancement that will come with many benefits. As previously mentioned, one of the biggest impacts that will positively affect stakeholders and non-stakeholders is the environmental impact. As the yearly power consumption is projected to decrease, the carbon emissions resulting from electricity production are expected to decline. With the current climate crisis, it is important that we decrease our carbon footprint whenever possible. In addition, the switch to a PoS lowers the barriers to entry, which makes its use more accessible to the public. If Bitcoin and Bitcoin Core want to be recognized and used on the same scale as FIAT currency, it is important that it is as simple to use. Removing the barrier that prevents the general public from taking part in the consensus will entice more stakeholders and more use of the Bitcoin network. This should further stabilize the system and protect it from attacks. PoS also has a reduced centralization risk; This means that the system will be more robust and secure from attacks trying to take control of the blockchain since users must stake Bitcoin in order to participate in the consensus. If a node is flagged for malicious intent there are economic penalties that can incur. These safeguards work to deter potential attackers since they risk losing their money.

Effects on Architecture and Interactions Between Features

As discussed previously, changing the consensus algorithm from Proof of Work to Proof of Stake in the Bitcoin Core architecture will lead to significant impacts on the entire system. Higher-level subsystems such as the wallet and user interface, along with the lower-level systems like the validation engine, mining, and RPC will all need important changes to their structure and codebase in order to support a PoS algorithm. The following effects of this change on the architecture and features of a blockchain network were identified through the help of two useful articles from the websites Block Geeks [3] and NerdWallets [4].

In order to verify transactions based on the amount of cryptocurrency held by the users, the wallet's architecture will need to be modified in addition to the consensus mechanism that takes into account the stake of validators in the network to maintain the integrity of the blockchain. To account for the updated block creation process and facilitate communication amongst the nodes with higher stakes, the lower-level networking subsystems will have to be modified as well. Furthermore, as one of the most important subsystems of the Bitcoin Core system, the user interface will also need to be updated to reflect the new functions and changes in

the PoS algorithm so that users can access and manage their accounts seamlessly. In addition to these modifications, the validation engine would also need to be altered to consider the new consensus algorithm and check for different types of transactions in order to determine their validity.

The switch from a PoW to a PoS mechanism would also result in the mining component losing its responsibility for validating transactions. The miners would instead be replaced by staking software that allows users to participate in the validation process by holding a specific amount of Bitcoin in a designated wallet or node. Similarly, the RPC would require an update in the possible commands that can be executed. More specifically, the new commands will likely need to account for actions such as staking, un-staking, checking staking rewards, and validating transactions.

In essence, each Bitcoin Core subsystem will need to adjust its architecture and features in order to accommodate the change in the consensus algorithm. While some of the components, such as the wallet, involve limited modifications to their codebase and structure, others like the validation engine require significant changes to their fundamental mechanisms. Overall, the switch to a PoS consensus algorithm will require careful consideration for each component to ensure the safety and success of the system.

Impacted Directories and Files

As mentioned previously in the report, Almost all of the subsystems in the Bitcoin Core Concrete architecture will be impacted. The most significant changes include the wallet, user interface, validation engine, mining, and RPC.

Here is a list of the impacted files and directories:

- bitcoin/src/wallet/: Add new subcomponents. Modify each file to accommodate new features. Modify to account for the stake of validators in the network to maintain the integrity of the blockchain.
- bitcoin/src/consensus/: Add new subcomponents. Modify each file to accommodate new features. Modify validation.h to consider the new consensus algorithm and check for different types of transactions in order to determine their validity.
- bitcoin/src/interfaces/: Modify files to reflect the new functions and changes in the PoS algorithm so that users can access and manage their accounts seamlessly.
- bitcoin/src/validation.cpp: Modify the file to accommodate the new algorithm.
- bitcoin/src/rpc/: Add a new subcomponent for staking software. Modify each file to accommodate new features. Modify for updated block creation process. Modify to facilitate communication amongst the nodes with higher stakes. Modify lower-level networking subsystems. Modify mining.h, mining.ccp, and mining_basic.py as a result of the mining component losing its responsibility for validating transactions.

Current State of System Relative to Enhancement

The conceptual architecture from the original conceptual architecture report is shown in (Figure 1) to illustrate the system before enhancement. The conceptual architecture of the high-level architecture of the Bitcoin Core system is changed by adding some new dependencies (Figure 2). Figure 2 shows the enhanced conceptual architecture from the proposed changes in the PoS algorithm. Relative to the new enhancement proposed to each subsystem, there are arrows in red to show the changes from the original architecture.

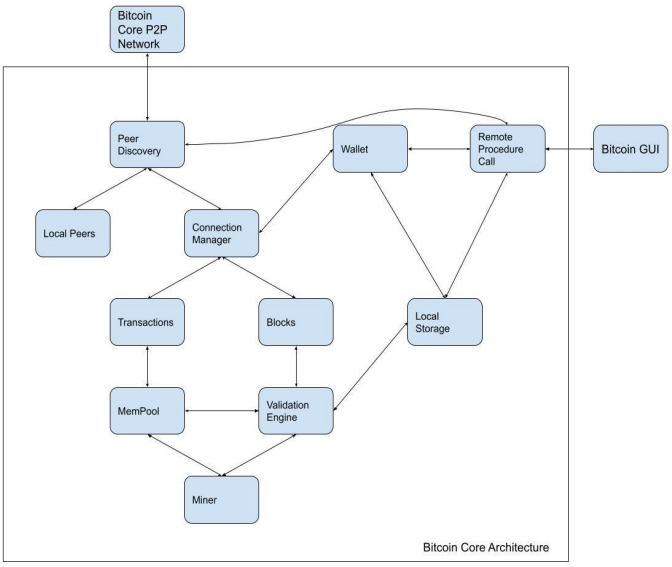

Figure 1: Bitcoin Core's Conceptual Architecture From Conceptual Architecture Report.

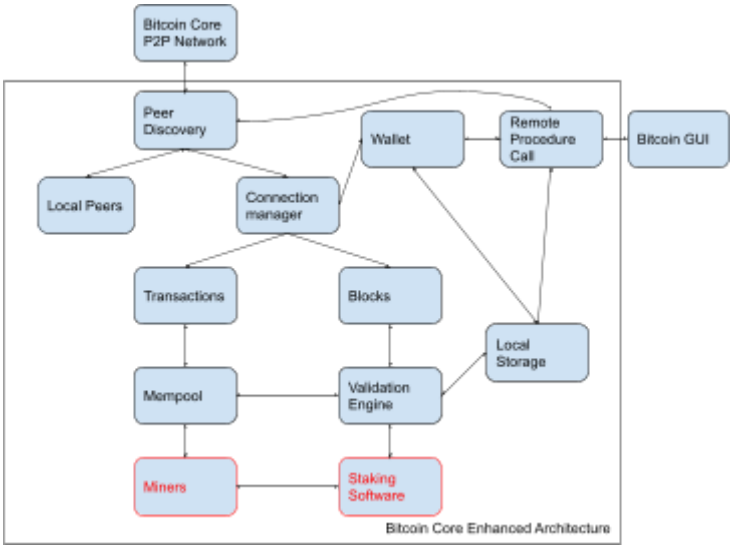

Figure 2: Bitcoin Core's Enhanced Conceptual Architecture.

Alternative Enhancement

Upon careful consideration and discussion, we have identified a potential alternative of a pure proof-of-stake consensus algorithm. Our initial approach is to completely convert the system from a proof-of-work to a proof-of-stake consensus algorithm. This involves restructuring many subsystems and will take lots of time and effort to do so. We find this feasible due to the benefits that will follow such restructuring. However, in the case that this implementation does that reach the requirements or performance desired, we have an alternative that will be able to perform. We propose a hybrid model consensus algorithm that implements both PoW and PoS styles to create what we call a Proof-of-Work-and-Stake (PoWaS). This alternative has benefits but also many drawbacks, as it carries the features of both types. This hybrid model would keep the Peer-to-Peer architectural style, as there is no change to the system's structure.

Converting Bitcoin Core from PoW to PoWaS would also have significant implications for the stakeholders involved. The developers would be heavily impacted, as the transition and implementation would require a significant overhaul of the existing code and the development of new software tools to support PoWaS. This hybrid model would also be more complex and require more effort to implement versus a pure PoS model. There would be a need for careful planning, communication, and management to make sure that the development is smooth and operating on schedule. This is also important so that all stakeholders are aware of the state of the system and what is happening in the development process. The miners who currently play a pivotal role in securing and maintaining the Bitcoin network, are in luck as they would still be a crucial part of the new system. The PoWaS model would keep the miners hard at work, but their role would be more focused on securing the network and validating transactions. Some hardware and software modifications would be required to accommodate this new system, so time and effort would have to be spent upgrading the miners. Wallet owners would have to deal with the new need to stake their currency in order to be a part of the consensus. Owners would find this beneficial rather than just having it in their wallet, as they can make a return from it. There would be a small learning curve for owners, but the system should help streamline the staking process. Certain conditions would need to be met in order to participate, such as having a certain amount of Bitcoin to stake. Third-party applications would need to adapt to the new PoWaS system. Systems would need to be updated to adhere to the new transaction protocols. They would also need to make sure that they modify their fees to reflect the new transaction method more accurately and fairly. Regulators would also be affected by a switch to PoWaS, as it could alter the legal and regulatory landscape for cryptocurrencies. Just like PoS, PoWaS's implementation could result in changes to tax laws, requirements, and other regulations governing the use of cryptocurrencies.

The NFRs that are affected by a change of this magnitude on the Bitcoin Core architecture are numerous. These requirements are modified, created, or removed based on the vision of this new PoWaS consensus algorithm. There are some that are more important than others; their effect on stakeholders and on the system are more significant. Below are the ones that are the most important in the development of the new system:

Scalability: The new consensus algorithm must be scalable to accommodate the increase in users, data, and transactions. With the PoS allowing for easier onboarding for users to participate, there will be increases in the amount of users staking their Bitcoin. In addition, with the growth of cryptocurrencies and its introduction to mainstream currencies, it must be able to handle massive volumes of traffic.

Network Stability: In the face of changing conditions such as increases in user activity, changes in network topology, or the occurrence of unexpected events, the network must remain stable and resilient. This is crucial to maintain the availability and integrity of the system. If the new network is not stable, serious consequences such as transaction delays, lost funds, and decreased user trust can occur. Since there is a PoW and PoS section, the intercommunication and stability of the network are crucial, as it crumbles when communication is not done properly.

Security: This would be the top priority when implementing this transition from PoW to PoWaS. With more interlacing subsystems and moving parts, there will be more vulnerabilities. Forms of attacks not possible in PoS styles, such as double-spending and 51% attacks would be possible as there is a PoW aspect. It is super important for the system to remain secure throughout the transitional period as we do not want anything to happen to the users and the blockchain.

Performance: PoWaS would perform better in some aspects than the original PoW model. Energy consumption and transaction processing are the sections of improvement. PoWaS requires less computational power and resources to validate transactions, as it relies on a smaller group of nodes rather than a large network of miners. It can also increase the transactional throughput and reduce the amount of time necessary to confirm. However, the performance increase causes a decrease in centralization.

The conversion of Bitcoin Core from a PoW to a PoWaS consensus algorithm is one that comes with many benefits. There is an incentivization to stake your currency, as you will get rewarded for doing so. This helps promote using the currency and will actually grow wealth over time, and secure the network at the same time. The PoW component of the hybrid model offers the same level of security as the traditional PoW-based version. Additionally, the PoS component offers an extra layer of security, making it harder for attackers to gain control of the network. Furthermore, the combination of both consensus algorithms means that it is harder for large miners to dominate the network, allowing for more security, and a more equitable distribution of the wealth generated.

Use Cases and Sequence Diagrams

Use Case 1 - Adding a block to the blockchain

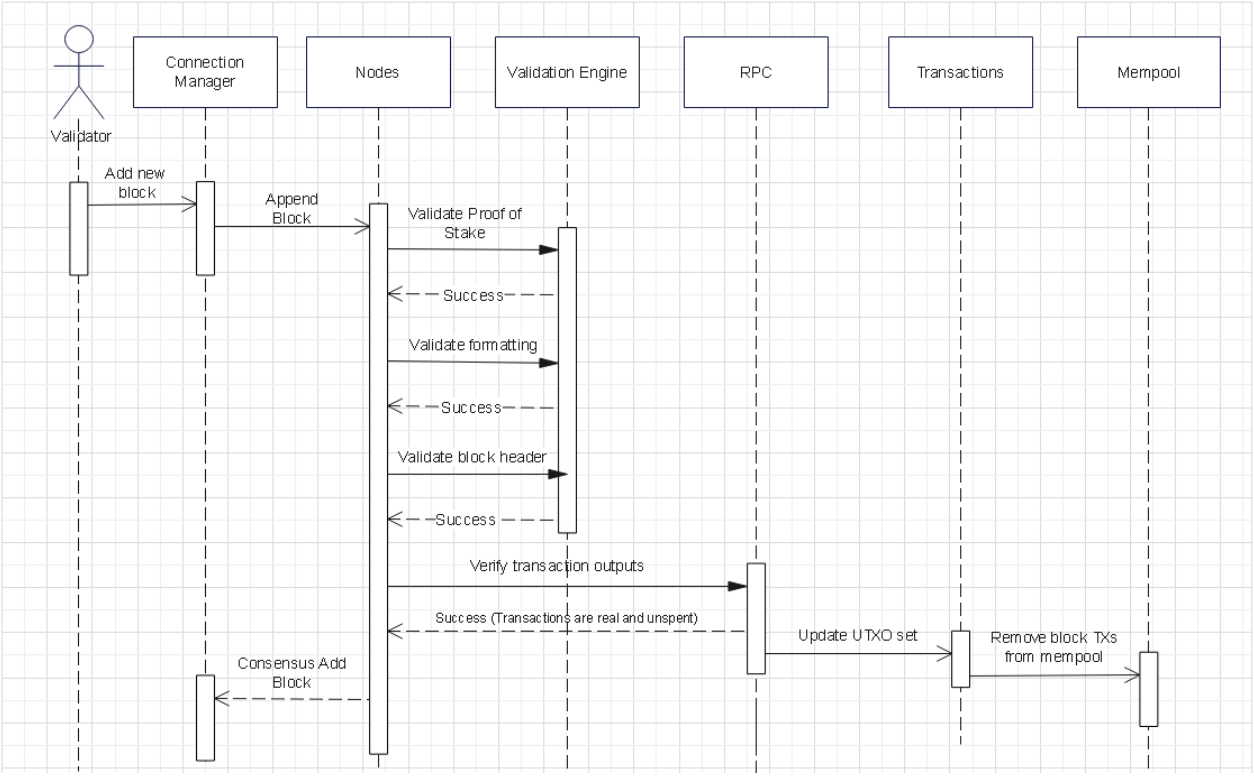

Figure 3: Use Case Diagram for adding a block to the blockchain

Adding a block to the blockchain with proof of stake looks very similar in terms of subsystem interactions to the process with proof of work with a few key differences. The block can now be created by anyone (known as validators) and miners are not needed in the process. The block is then broadcast to the peer-to-peer network by the connection manager which appends the block to each Node's local storage. The node then makes calls on the validation engine to verify aspects of the block. First, it checks if the block has a valid proof of stake by checking that the Bitcoin staked by the initial validator is enough to add it to the blockchain. Next, the formatting including inputs, outputs, and fees of transactions within the block are validated. Finally, the header of the new block is checked against the header of the previous one to ensure it is added correctly. The nodes then call on the RPC to verify the transaction outputs in the block are all real and currently unspent. On success, RPC removes the transaction outputs from the UTXO set by making a call to the transactions subsystem and removes the block's transactions from the local mempool. The nodes then broadcast the block's validity and it can be added by consensus meaning that the majority of nodes in the network must agree that the block is valid. If the majority agrees the block is then added to the blockchain.

Use Case 2 - Staking process of a transaction

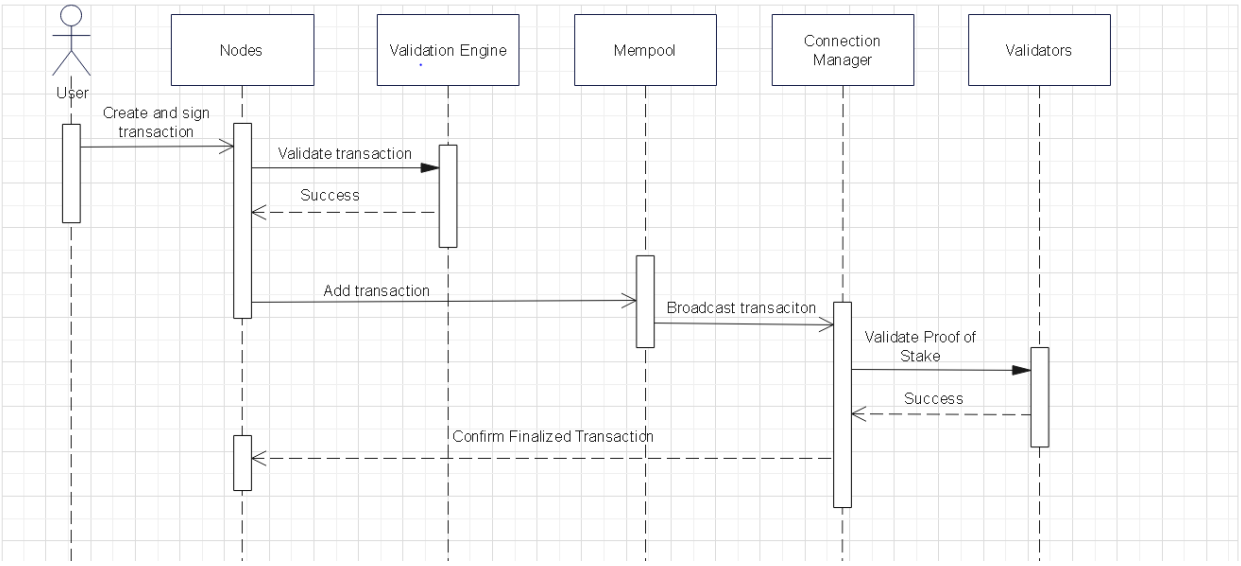

Figure 4: Use Case Diagram for the staking process of a transaction

A transaction is created by a user and signed with their own private key. The user specifies an amount they're willing to pay to a validator and a base amount of bitcoin as the stake for the transaction. The transaction is then broadcast to the user node's validation engine to ensure that the user has enough Bitcoin to complete the transaction and that it has been signed with the correct key. Once validated, the user adds it to their local mempool and it is broadcast across the network of nodes to be added to all mempools. Once broadcast to the entire network, a validator is chosen by the connection manager pseudo-randomly to validate that the transaction has a valid proof of stake, meaning the proposing user of the transaction has staked a certain minimum amount of Bitcoin on the transaction. The verified proof of stake will then be communicated to the validation engine to store that its proof of stake is valid, to be used when the transaction is in a block to be added to the blockchain. The transaction is then considered in a finalized state which is communicated to the original user node and remains in the mempool until the time comes that it is to be added to a block.

Plans for Testing Enhancement

Testing the PoS algorithm will involve several steps to ensure its proper function and security. Our first step will be to implement a test environment that mirrors the real network as closely as possible. This environment will include multiple nodes running our Bitcoin Core software, as well as a testnet [10] that can be used to simulate network conditions. Our second step will be to test the consensus mechanism. The core of the PoS algorithm is the consensus mechanism that determines which node will create the next block. We will have to test this mechanism thoroughly to ensure that it is secure and works as expected by simulating different network conditions and testing the algorithm's ability to select a node to create the next block. Thirdly, we will test for security vulnerabilities. Our PoS algorithm is designed to be secure,

however like anything it is not immune to attack. We will be sure to test our algorithm for potential vulnerabilities, such as 51% attacks [8], double-spending attacks, and other types of attacks that can compromise the security of the network. These will be discussed later in potential risks. We will also test the transaction processing as our PoS algorithm must process transactions quickly and efficiently. In order to test this we will have to simulate a variety of network conditions and ensure it can handle a high volume of transactions without compromising performance. In addition to testing the transaction processing, it is imperative that we ensure the integrity of our economic model is sustained. Our economic model must incentivize node operators to act in the best interest of the network. The last stage of our testing will involve comprehensive testing. Comprehensive testing will include testing our algorithm in real-world conditions. The testing will simulate a range of unique scenarios and edge cases to ensure that the algorithm is secure, reliable, and performs well under all conditions.

Potential Risk

While a proof of stake algorithm is beneficial over a proof of work algorithm, it is not immune to risks. Let's start with two theoretical security issues facing PoS; the long-range attack problem and the nothing-at-stake problem. The nothing at stake [5] problem may arise when there is no cost to creating multiple forks of the blockchain. In a PoS algorithm, a node that creates a fork can create blocks on the forked and original chain, with no cost involved, leading to a lack of consensus and the potential for double-spending. As for long-range attacks, in a PoS algorithm, an attacker who gains control of a large amount of stake can theoretically rewrite the entire blockchain history. This type of attack can be difficult to detect and prevent. However, it would require quite a bit of coordination on the attackers part. Another risk unique to the PoS algorithm is stake-grinding attacks. In a PoS algorithm, an adversary can attempt to manipulate the consensus mechanism by strategically dividing their stake into smaller portions to gain a higher probability of them being selected to create the next block. Which, like long-range attacks, can be difficult to prevent and detect. Lastly, we can not discuss risks without security vulnerabilities. Like any other computer program, PoS algorithms can have security vulnerabilities that can be exploited by hackers. These vulnerabilities can lead to the loss of funds or compromise the security of the network. Some common security vulnerabilities include sybil attack [6], eclipse attack [9], and time-based attack. Although PoS algorithms can be vulnerable, many of the risks discussed above can be mitigated through vigilant design and testing of the algorithm, as well as continuous monitoring and maintenance of the network.

Conclusion

Overall, this report explores a potential enhancement to the Bitcoin Core system by changing the current Proof of Work (PoW) algorithm for validating transactions on the blockchain by consensus to a Proof of Stake algorithm (PoS). The structural style of the architecture would remain the same with a peer-to-peer implementation and the RPC handling certain pub-sub aspects. This would be a big change that would require a lot of time and effort.

Security and stability would have to be tested consistently to maintain the safe and steady reputation of Bitcoin Core. The PoS algorithm would have a far smaller environmental impact than PoW as PoW takes a lot of computing power, therefore expending massive amounts of energy.

Lessons Learned

Upon researching and learning more about proof-of-stake algorithms, we learned a lot about the negative sides of Bitcoin Core. Even when researching for the previous reports, we never realized the sheer amount of energy being consumed in order to maintain the system. Its energy use is talked about but it's only when you get a better understanding of the entirety of the system that you realize the importance of building environmentally friendly software. The concept of Bitcoin is awesome and has already changed so much, but if it comes at the cost of pollution, it is crucial to find alternatives.

Data Dictionary

Proof-of-Work (PoW): A blockchain consensus algorithm that uses computing power to authenticate and add transactions to the blockchain.

Proof-of-Stake (PoS): An alternative to proof-of-work, where cryptocurrency owners validate block transactions based on the number of staked coins. This staked currency then acts as collateral that can be destroyed if the validator behaves dishonestly or lazily.

Proof-of-Work-and-Stake (PoWaS): A hybrid model that combines the functionality of PoW and PoS into one.

Non-Functional Requirements (NFR): The characteristics of a system that are not directly related to the actual functionality of the system.

51% Attacks: When a staker takes control of 51% of a proof-of-stake network's coins.

Sybil Attack: When someone tries to get an unfair advantage by creating many nodes.

Eclipse Attack: Targets particular nodes in a network by surrounding them and obscuring their view of the entire network.

Time-Based Attack: If the amount of stake a node holds is multiplied by the time it has been held, an attacker can accumulate a significant amount of stake and then sell it just before it loses its value, in an attempt to manipulate the network.

References

[1] Koomey, J. G. (2021, May 18). How Much Energy Does Bitcoin Actually Consume? Harvard Business Review. https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume

[2] Ethereum Foundation. (2021, August 5). Energy Consumption. Ethereum. https://ethereum.org/en/energy-consumption/#:~:text=Ethereum%20is%20a%20green%20blockchain,across%20the%20entire%20global%20network.

[3] BlockGeeks. (n.d.). Proof of Work vs. Proof of Stake: Basic Mining Guide. BlockGeeks. https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

[4] NerdWallet. (2021, July 8). Proof of Work vs. Proof of Stake: What's the Difference? NerdWallet. https://www.nerdwallet.com/article/investing/proof-of-work-vs-proof-of-stake

[5] Coinmonks. (2018, June 3). Understanding Proof of Stake & The “Nothing at Stake” Theory. Medium.https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027

[6] Ethereum. (2022, January 25). Proof of Stake (PoS). Ethereum Developer Documentation. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

[7] Ethereum. (n.d.). Proof of Work (PoW). Ethereum Developer Documentation. https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/

[8] NBX. (n.d.). What is a 51% Attack? Crypto 101. https://nbx.com/crypto101/what-is-a-51-attack#:~:text=Both%20proof%2Dof%2Dwork%20and,%2Dof%2Dstake%20network's%20coins.

[9] River Financial Corporation. (n.d.). Eclipse Attack. River Learn. https://river.com/learn/terms/e/eclipse-attack

[10] BitDegree. (n.d.). What is Testnet? Learn Cryptocurrency. https://www.bitdegree.org/crypto/learn/crypto-terms/what-is-testnet