Bitcoin Core Conceptual Architectural

CISC 322
Assignment 1 Report
Friday, February 17, 2023

Group 6: ArcProject
Chuyang Li (19cl98@queensu.ca)
Qintao Zhang (18qz28@queensu.ca)
Anthony Zhou (18zz172@queensu.ca)
Chang Xu (18cx19@queensu.ca)
Wenchu Xiao (19wx25@queensu.ca)
Xiaoran Zhang(19xz64@queensu.ca)

Abstract

Bitcoin core is a full-node implementation of the Bitcoin protocol, which is the backbone of the network and plays a crucial role in maintaining the security, reliability and decentralization of the Bitcoin network. Bitcoin core is now an open-source project, and collaborators can improve its security, and dependability or add new features by submitting change requests in GitHub. This article analyzes and discusses the conceptual architecture of Bitcoin Core, we summarize its derivation process and explain the interaction of the components and modules in the system. This article will discuss the following aspects: the interaction parts, the system's evolutionary, architectural style, subsystem, control and data flow among parts, concurrency, and possible use cases. We will also show the limitations we encountered and what we learned during the learning process.

Introduction and Overview

Cryptocurrency is a digital or virtual currency that, because it is protected using cryptography, makes it virtually impossible to counterfeit or re-consume. It’s a peer-to-peer system that enables anyone to send and receive payments anywhere. Instead of being physical money carried around and exchanged in the real world. (Kaspersky)

The rise of cryptocurrencies has had a major impact on the global financial system, not only disrupting traditional banking and financial models but also opening up new possibilities for financial innovation and investment. An added advantage of cryptocurrency is that it’s completely decentralized, which means that for citizens living in countries with currency instability, cryptocurrency allows them to trade freely across borders with citizens of more well-off countries, creating a level of economic equality. (PELICOIN)

Bitcoin Core is a full-node implementation of the Bitcoin protocol, the first and best-known cryptocurrency. Bitcoin Core connects to the Bitcoin peer-to-peer network to download and fully validate blocks and transactions. It also includes a wallet and graphical user interface, which can be optionally built. (Bitcoin GitHub) By running the Bitcoin Core node, individual users can participate in the verification process of transactions, contributing to the health and stability of the Bitcoin network and ensuring that the rules of the protocol are followed.

The purpose of this post is to provide a comprehensive overview of Bitcoin Core's conceptual architecture. This article provides an overview of the aggregation process, showing the principles and interrelationships of its components. The overall conceptual architecture is divided into six parts:

1. Derivation process
2. Architectural style
3. Subsystems
4. Control and data flow
5. Use cases
6. Limitations and lessons.

In addition, this report uses sequential, block and arrow diagrams to provide a quick overview of the Bitcoin Core system and to provide insights for our analysis. During our research, we found that the high-level architectural style of Bitcoin Core is peer-to-peer. In addition, a publish–subscribe architecture style is used in this subsystem.

This report provides detailed insights into the Bitcoin Core architecture as we examine its various components and functions. With a comprehensive description of the conceptual architecture of Bitcoin Core, this report provides basic theoretical knowledge and insights for those who wish to understand the fundamental workings of this revolutionary technology.

Derivation Process

In the early stages of the architectural analysis, we attempted to fully understand the design architecture of Bitcoin Core. To achieve this goal, we, therefore, conducted an extensive network study to gain insight into the system's infrastructure. This initial research gave us some basic understanding of its architecture but was not sufficient to support our detailed analysis of its conceptual architecture. Therefore, we realized that we needed to dig deeper into the conceptual architecture of the system to gain a more comprehensive understanding. This included reviewing available documentation, such as technical specifications and white papers, as well as analyzing the system's source code. We wanted to gain a deeper and fuller understanding of the system's architecture, rather than a basic understanding.

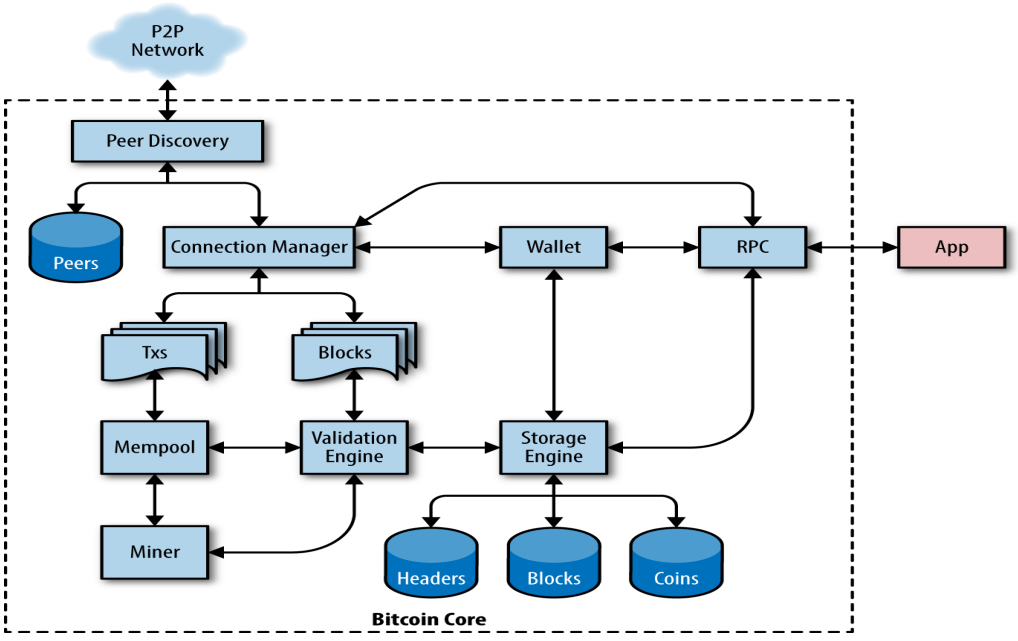

Figure 1. Bitcoin Core architecture (Source: Eric Lombrozo)
Source: Bitcoin open-source book, https://cypherpunks-core.github.io/bitcoinbook/ch03.html

After reading the Bitcoin Core open-source book and looking at its basic architecture diagram (Fig. 1), I found the network, login manager, wallet, RPC, GUI, mempool, validation engine, storage engine, and miner.

Further inspection of the developer manual on the Bitcoin developer's website reveals that some of the components shown in Figure 1 can be combined to provide a more accurate and complete classification of the architecture. In particular, it proposes components for the UI, transactions, scripts, wallets, mining, blockchain and individual parts of the network.

Based on the subsystem in Figure 1. Data and control flow in the Bitcoin system are important aspects of the overall system architecture. Interactions between various subsystems show how data and control flow through the Bitcoin network. Subsystems within the system work together to ensure that transactions are processed accurately and efficiently. For example, data flows from the transaction subsystem to the script subsystem, which evaluates transaction scripts and ensures their validity. Verified transactions are passed to the mining subsystem and added to the blockchain.

The monitoring process is also reflected in the mining subsystem, which decides which block to include the transaction in based on several factors, such as the value and priority of the transaction. The mining subsystem is responsible for creating new blocks and adding them to the blockchain. Network nodes also play a key role in the flow of data and management of the Bitcoin system, as they facilitate communication between subsystems and ensure the safe and efficient transfer of data. Data within transactions is made possible through communication between nodes in the network, allowing transactions to propagate across the network and be verified by multiple nodes.

Conceptual Architecture

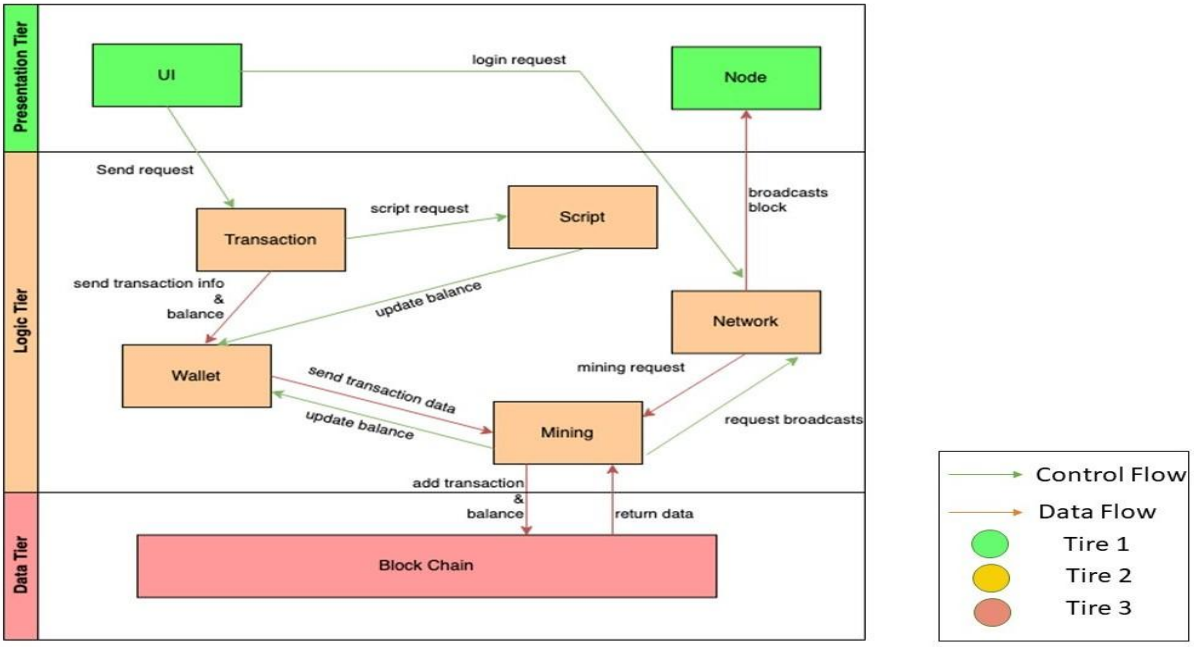

Figure 2. Conceptual Architecture

Architectural Style

The Bitcoin network is constructed with a peer-to-peer (P2P) architecture that employs a decentralized approach to network design. Within a P2P network, each node on the network is capable of operating as both a client and a server and assumes responsibility for the validation and propagation of transactions. Within the Bitcoin network, every node maintains a complete copy of the blockchain, which functions as a public ledger of all Bitcoin transactions that have taken place. When a new transaction is initiated, it is disseminated throughout the network, with each node employing cryptographic techniques to verify its authenticity and uniqueness. Upon successful verification, the transaction is appended to a block of transactions. Miners on the network use their computational resources to solve complex mathematical problems, with the successful solution resulting in the addition of a new block to the blockchain. Once a miner has added a new block to the blockchain, the transaction is deemed confirmed and irreversible.

The Bitcoin network's decentralized nature eliminates the need for a central authority or server to manage the network. Instead, the network is composed of numerous nodes, all of which possess the same level of authority concerning validating and confirming transactions. As a result, the network is remarkably resistant to censorship and control by any singular entity.

We considered whether it would be a pub/sub or repository style of architecture, but after further thought, we realized that the bitcoin core could not follow the standard structural model that is often used. Since the bitcoin core requires that each user be an independent node and be free to communicate with each other about transactions, each node can't communicate with a central database, which would lead to a decrease in data security and reliability. However, these structures could potentially be used in Bitcoin Core’s subsystems.

Overall, the Bitcoin network's peer-to-peer architecture establishes a trustless and decentralized system for securely transferring value without the need for intermediaries or third-party institutions. The decentralized nature of this architecture provides high resistance to any attempt at censorship or control by a single entity, hence guaranteeing the network's reliability and sustainability. With a distributed architecture, the network ensures that no single entity can exert undue influence or control, resulting in enhanced security and resilience.

Subsystem Decomposition

Bitcoin Core is a full-node implementation of the Bitcoin protocol that provides a robust and secure foundation for the Bitcoin network. developed by a group of volunteers, Bitcoin Core is an open-source software project that allows all developers to contribute to the ongoing development and improvement of the protocol. Its flexibility and reliability make it an essential part of the Bitcoin ecosystem, enabling users to conduct transactions in a decentralized and hassle-free manner.

Transaction

The transaction subsystem of Bitcoin Core processes, validates, and broadcasts transactions to the network. It verifies transaction authenticity and compliance with network consensus rules. It checks for unused transaction inputs and sufficient user funds, as well as verifies digital signatures. Validated transactions are broadcasted to the network and added to the blockchain by the mining subsystem.

Script

The Scripting subsystem in Bitcoin Core is responsible for executing transaction scripts to determine whether they are valid and authorized by the bitcoin owner. It interprets the script's instructions that establish the conditions for spending the bitcoin being transferred. If the script is valid, the transaction moves to the next validation stage, but if it is invalid, the transaction is rejected.

Wallet

The Bitcoin Core wallet subsystem is an important part of managing user funds in the Bitcoin network. Its main function is to facilitate the sending and receiving of Bitcoin transactions and store the private keys required to sign and verify those transactions. The wallet subsystem is also responsible for keeping an accurate record of a user's transaction history and balance and can generate new addresses for receiving funds. It also includes advanced features such as coin control, which allows users to select specific entries and exits for trades, and rate estimation, which makes trade processing more efficient.

Mining

Mining is a core aspect of the Bitcoin network, the link responsible for the creation and validation of new transactions on the blockchain. In the Bitcoin core, the mining subsystem is responsible for generating new blocks containing transaction data, which are then added to the existing blockchain while verifying the validity of the transactions. To achieve this, miners must compete with each other to solve complex mathematical puzzles that are designed to be difficult enough to ensure that only one miner can solve them at a time. In the end, the first miner to solve the puzzle is rewarded with newly created bitcoins as well as a transaction fee paid by the user.

Block Chain

The blockchain is the core component of the Bitcoin network, which is a decentralized and trustless ledger of all transactions on the network. At the Bitcoin core, the blockchain is maintained by a network of nodes that work together to validate and add new transactions to the blockchain. The blockchain is composed of a sequence of blocks, each of which contains a collection of verified transactions, a timestamp, and a reference to a previous block in the chain. This structure ensures that all transactions on the blockchain are

linked together in a tamper-evident manner, such that any attempt to modify any one block will invalidate all subsequent blocks. The blockchain at the core of Bitcoin is secured through the use of cryptographic hash functions and proof-of-work consensus mechanisms, which ensure that the network can withstand attacks and provide a high degree of security and untrustworthiness. The blockchain is the backbone of the Bitcoin network, providing a transparent, immutable and secure record of all transactions on the network.

Network

The network subsystem in Bitcoin Core is responsible for establishing and maintaining connections to other nodes on the Bitcoin network. This is achieved through the use of peer-to-peer protocols, which allow nodes to share transaction data and block data with each other. The network subsystem is critical to ensuring the security and reliability of the Bitcoin network, as it allows nodes to exchange information and synchronize copies of their blockchains. Not only that, but it also facilitates the propagation of new transactions and blocks throughout the network, which allows users to transact with each other in a decentralized and trustless manner. In addition, the network subsystem includes advanced features such as the ability to run Bitcoin nodes on the Tor network, which can help protect the privacy and security of users.

Control and data flow

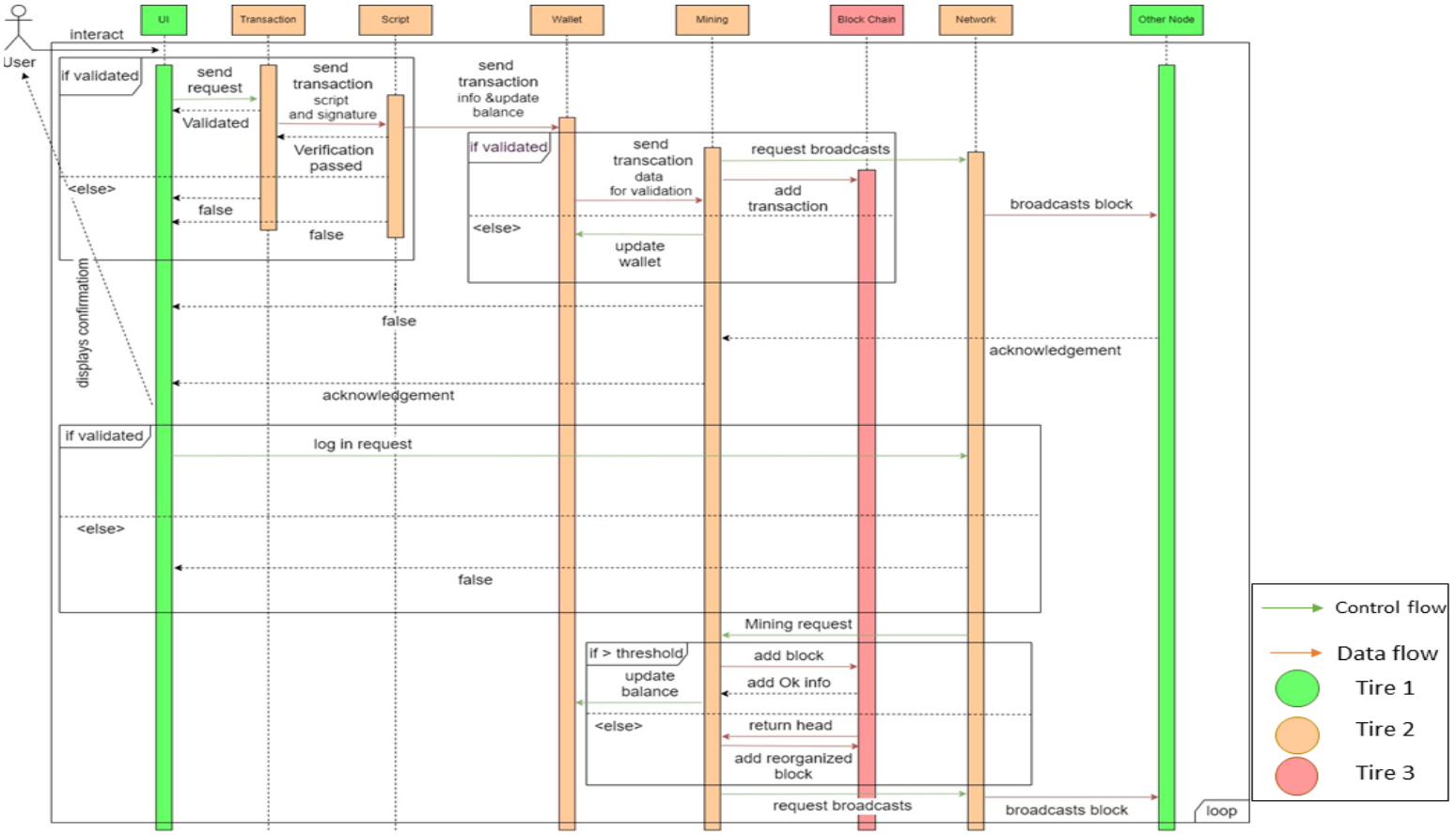

Figure 3. Sequence diagram with control and data flow

By analyzing the main components of the conceptual architecture, we created a sequence diagram (Figure 3.). As shown in the figure, the user first engages and interacts with the UI, and then the user can choose between two activities.

We assume that the user first selects a transaction, and the user sends a transaction request to the transaction subsystem through the UI. The transaction subsystem then determines whether the request is valid, and if it is not, the transaction subsystem will reject the request and display it on the UI, and if it is valid, the request is sent to the script subsystem. At this time, the script subsystem that receives the request from the transaction subsystem will further verify whether the request is valid and verify the signature, if the verification fails, the result will be returned to the UI, and if successful, the transaction information will be sent to the wallet subsystem, the wallet subsystem needs to wait for the mining subsystem to verify the data, if successful, the wallet will be If successful, the balance of the wallet will be updated and the new transaction will be added to the blockchain and board cast to the network subsystem so that other users will know about the blockchain update.

If the user chooses a mining operation, the user will first login via the network and send a mining request to the mining subsystem after success. After the mining subsystem completes the operation, if a new block is successfully mined, it will send an update request to the wallet to update the balance of the wallet. If it fails, the head of the current block will be added to the blockchain, and the result of mining will be sent to other users via network broadcast

Evolution of the System

The 0.1.0 Version of Bitcoin was released in 2009. This version allowed users to send and receive Bitcoin transactions using a peer-to-peer network. However, it had limited functionality and was primarily used by early adopters and enthusiasts. From version 0.1.0 to 0.9, the Bitcoin system underwent several significant updates and improvements. The system allows for more complex transactions, including the ability to send bitcoins to multiple addresses at once, and also introduced the concept of mining, which involves using computing power to verify transactions and add them to the blockchain. In addition, the system's security was enhanced by introducing a new feature called "BIP 0030," which required users to sign all of their transactions.

Bitcoin Core version 0.9.0 was released in 2014, and a major security flaw was discovered(transaction malleability bug). This flaw allowed an attacker to modify a Bitcoin transaction ID before it was confirmed on the blockchain, which could lead to issues with transaction processing and confirmation. Bitcoin Core development team quickly addressed the issue by introducing a new feature called "BIP 0065," which made transaction verification more accessible and more secure. This fix helped improve the system's overall reliability and restore confidence among Bitcoin users and investors.

From version 0.10.0 to 0.18.0, the Bitcoin system introduced the concept of the Lightning Network, which is a layer-2 protocol that enables near-instant and low-cost Bitcoin

transactions. The Bitcoin system underwent a major upgrade with the introduction of "SegWit," which stands for "Segregated Witness." This upgrade increased the system's block size limit and improved its scalability, allowing more transactions to be processed faster.

Bitcoin version 0.18.0 was released in 2019, which introduced several new features, including support for the Bech32 address format, a more efficient method of transaction verification, and support for multi-part payments, which allows for larger transactions to be split into smaller parts for increased privacy.

In 2021, Bitcoin version 0.21.0 was released, and the Bitcoin system underwent a significant upgrade with the release of Taproot, a new type of transaction that enhances Bitcoin's privacy and fungibility.

In summary, the Bitcoin Core system has evolved through several updates and upgrades since its inception, with a focus on improving functionality, security, and scalability. The future of Bitcoin is expected to continue to evolve, driven by growing adoption and acceptance in the mainstream.

Concurrency

Bitcoin's design leverages the power of concurrency to realize its decentralized ambitions. Four critical concurrency aspects feature in the architecture of Bitcoin. The first of these aspects concerns how concurrency accelerates transaction processing. By concurrently processing multiple transactions, Bitcoin can validate transactions and create blocks in record time, with no undue delays or interruptions.

The second aspect focuses on the use of a multi-threaded architecture to manage incoming network traffic and validate transactions. By employing multiple threads to receive and process incoming data, Bitcoin ensures that the system can handle large numbers of transactions without experiencing any blocking or delays. This enables Bitcoin to process transactions in real time while keeping the blockchain secure and reliable.

The third concurrency aspect pertains to the consensus algorithm that Bitcoin relies on. Achieving consensus among network nodes demands high levels of concurrency and real-time communication. Concurrency enables nodes to communicate and verify transactions, ultimately ensuring the blockchain's accuracy and security.

Forth, the Bitcoin core uses a peer-to-peer network architecture to facilitate communication between nodes, necessitating significant concurrency. In this architecture, nodes need to exchange blockchain state, transaction data, and other vital information in real time, a task that demands high levels of concurrency.

Developer Contributes

Technical leaders, software developers, software testers and collaborative contributors are involved in the main development of the Bitcoin core architecture. Technical leaders are required to manage the development team, specify the roadmap for development and ensure the stability of the network. Software developers are responsible for front-end and back-end network development. Software testers are also needed to perform testing to verify the reliability and security of the software. Collaborative contributors are responsible for submitting bug reports, feature requests, and code contributions to improve the network.

The Bitcoin Core development team is an open-source project that focuses on improving the scalability, security, and reliability of the network. Developers ensure that the network remains stable and free of bugs and defects, and contribute significantly to the development of Bitcoin.

Use Cases

Transaction

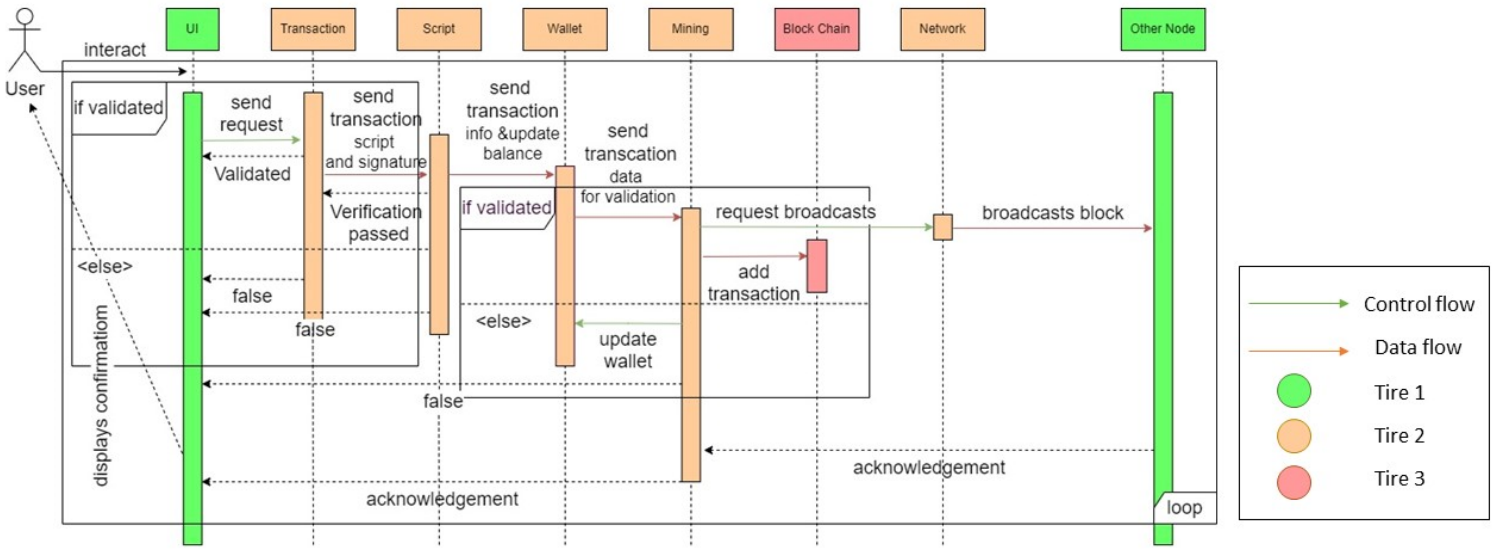

Figure 4. Transaction sequence diagram

The Bitcoin transaction process begins with a user providing the required details through a Graphical User Interface (GUI), such as the recipient's address, the amount of Bitcoin, and the transaction fee. These details are then transmitted to the Transaction subsystem, where the system validates the legitimacy of the transaction and checks whether the user has sufficient funds in their wallet to complete the transaction. Assuming the transaction is verified as valid, the Transaction subsystem forwards the transaction data to the Scripting subsystem for additional validation. Here, the script and signature are checked to ensure that the user has the necessary authorization to complete the transaction. If the script and signature are both valid, the Scripting subsystem passes the information to the Wallet

subsystem, which updates the user's wallet balance by deducting the amount of Bitcoin and transaction fee from their wallet. The updated balance is then transmitted to the Mining subsystem for processing.

The Mining subsystem authenticates the transaction and adds it to a newly created block, which is then added to the blockchain. After the block is verified and added to the blockchain, the Network subsystem broadcasts the new block to all other nodes on the Bitcoin network. Other nodes on the network then verify the block's information and the validity of the transaction, sending acknowledgments to the Network subsystem to confirm that the block has been added to their local copies of the blockchain. Once the Mining subsystem receives an acknowledgment that the block has been added to the network, it sends an acknowledgment to the GUI, which displays a confirmation message to the user.

Solo Mining

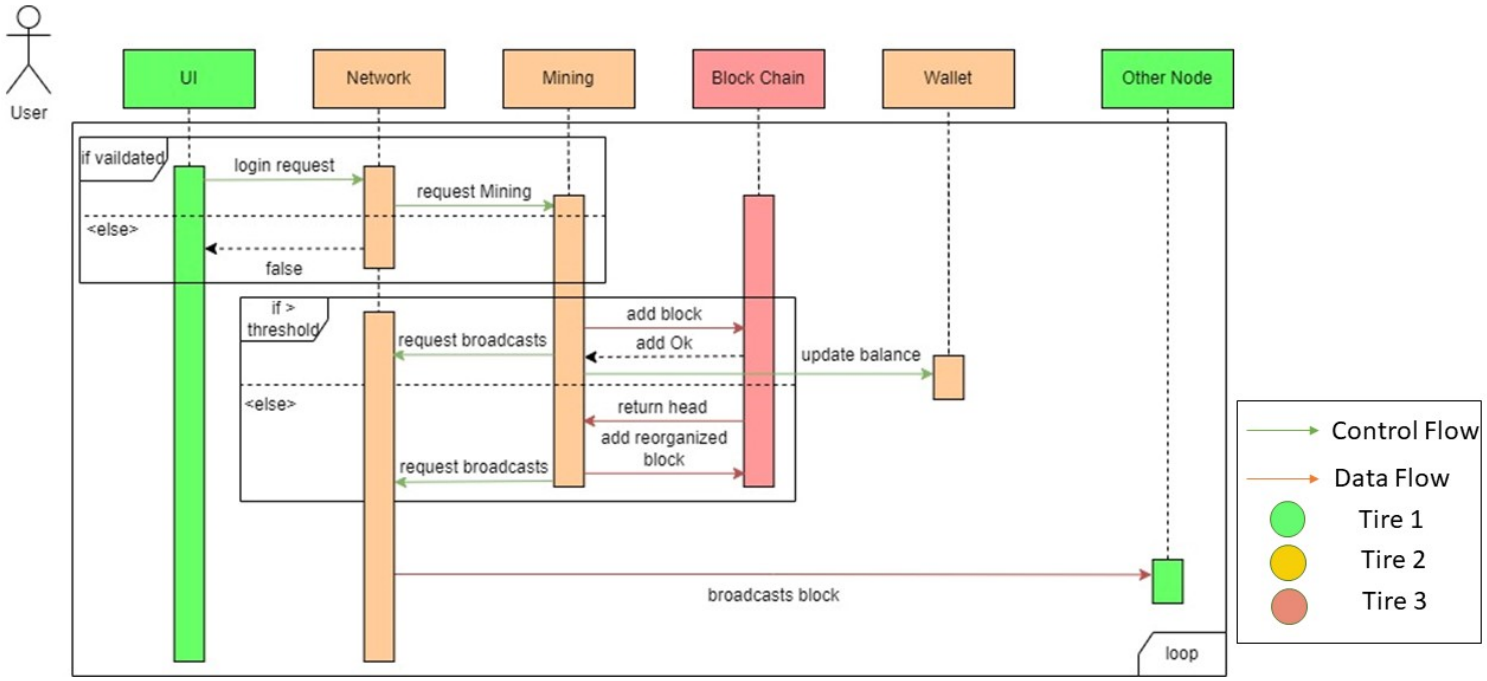

Figure 5. Solo mining sequence diagram

After the mining node creates the ready block, it sends the block header data of the ready block to the miner. After the miner receives the mining task, it increases the random number in the block header. Each time it is adjusted, the hash value of the block header is calculated using the SHA256 algorithm, as defined by the Bitcoin protocol.

If none of the hashes fall below the threshold, the mining software provides the mining hardware with the modified block header, which includes a new merekle root. The bitcoin value is added to the wallet and communicated to other users.

When the miner finds a random number that can make the hash of the reserve block header smaller than the target hash, it immediately reports the mining result to the mining node. After receiving the information, the mining node returns the block header containing the success rate to the miner's software, and then reorganizes this block header with any other blocks and validates the blocks. After validation, the mining node saves the new block to the node's local database, adds it to the node's local blockchain, and informs other users.

Lessons Learned and Limitations

Bitcoin has revolutionized the financial industry by providing a new way to store value and conduct transactions. This has led to the emergence of new fintech innovations, with blockchain technology being explored to enhance the security and efficiency of financial processes. However, Bitcoin also poses risks and challenges that require careful consideration by policymakers and investors alike, such as price volatility, regulatory uncertainty, and high energy consumption.

Despite the potential benefits of Bitcoin, there are limitations to its use that need to be addressed:

1) Scalability: One of the most significant limitations is scalability, as the current design of the network restricts the number of transactions that can be processed per second. This can result in slow transaction times and high fees during periods of peak network usage.
2) Adoption: Another limitation is the limited adoption of Bitcoin and other cryptocurrencies, which can limit the network's usefulness for certain use cases. Despite growing adoption, there are still technical complexities and regulatory hurdles that hinder broader adoption.
3) Centralization: While Bitcoin Core Architecture was designed to be decentralized, there is a risk of centralization as certain nodes or mining pools may gain a disproportionately large share of the network's processing power. This could potentially allow these entities to manipulate the network for their benefit.

Upon examining the limitations of Bitcoin, it is vital to explore the critical lessons that its architecture and implementation provide:

1) Decentralization: Decentralization is one of the most significant lessons learned from Bitcoin Core Architecture, emphasizing the importance of enabling everyone to participate in the validation and processing of transactions. This ensures that no individual entity can manipulate the network for its benefit, preserving the network's integrity and security.
2) Security: Security is another essential lesson from Bitcoin Core Architecture, with the network designed with numerous security features like cryptographic protocols, private keys, and multi-signature transactions. These features

prevent unauthorized access and protect users' funds from theft and fraud, enhancing the network's security.

3) Transparency: Transparency is a fundamental principle of Bitcoin Core Architecture, with all transactions recorded on a public ledger accessible to anyone. This ensures a high degree of transparency and accountability, allowing users to verify transaction validity and monitor the behaviour of other network participants.

Conclusion

In conclusion, the Bitcoin Core Architecture is a groundbreaking technological innovation in digital finance, with features that make it a compelling alternative to traditional financial systems. Its decentralized design ensures that it is highly resilient to attacks, with no single point of failure. The use of cryptographic techniques and public-key encryption guarantees secure and transparent transactions, while the distributed ledger provides an unalterable record of all transactions. Its scalability is highly impressive, processing thousands of transactions per second, and being open-source means developers can build upon the core technology. However, the Bitcoin Core Architecture still faces challenges such as energy consumption, scalability, and centralization risks that must be addressed to ensure its continued success. As blockchain and distributed systems continue to develop, the lessons learned from Bitcoin's architecture will play a crucial role in shaping the future of the fintech industry, paving the way for a more secure, transparent, and decentralized financial ecosystem. It is exhilarating to consider how this technology will transform how we think about money and value, opening new opportunities for innovation, inclusion, and prosperity. The potential for this technology is limitless, and as we work to address its limitations, we will be able to unlock its full potential and revolutionize the way we conduct financial transactions.

Glossary

Address: The prevailing method for users to share payment details in Bitcoin involves using a 20-byte hash formatted with base58check to generate a P2PKH or P2SH address. This has become the widely accepted practice for exchanging Bitcoin payment information.

Block: Blocks in the blockchain are comprised of one or more transactions that are preceded by a block header and secured by a proof of work mechanism.

Blockchain: The best blockchain is a sequence of blocks where each block refers to the preceding block.

Block header: The proof of work mechanism used in the blockchain involves taking an 80-byte header from a specific block and repeatedly hashing it until a certain condition is met.

Child key: A child key is generated from a parent key through key derivation. The child key can be private or public and may require a chain code to be created.

Mining: To mine Bitcoin, one must demonstrate proof of work by creating valid blocks in the blockchain. This can be done using specialized devices called miners, which are either owned and operated by people or are the devices themselves.

Public key: The public key is one-half of a keypair that can be utilized to validate signatures produced by the private key.

RedeemScript: A P2SH script is a type of script that performs a similar function to a pubkey script. It is used to generate a P2SH address, and a copy of the script is included in the spending signature script to enforce certain conditions.

Wallet: Bitcoin wallet software is a program that enables users to store private keys, keep track of their cryptocurrency balance, and conduct transactions on the blockchain network.

UTXO: An Unspent Transaction Output (UTXO) refers to a specific unit of cryptocurrency that has not yet been spent and can be used as input in a new transaction.

References

Bitcoin Core version history. Version History - Bitcoin Core. (n.d.). Retrieved February 18, 2023, from https://bitcoin.org/en/version-history

Bitcoin-NG: A scalable blockchain protocol. (n.d.). Retrieved February 18, 2023, from https://www.usenix.org/system/files/conference/nsdi16/nsdi16-paper-eyal.pdf

Bitcoin. (2022, May 9). *Bitcoin/README.md at master · Bitcoin/Bitcoin*. GitHub. Retrieved February 18, 2023, from https://github.com/bitcoin/bitcoin/blob/master/README.md

Haynie, W. (2022, April 11). *What is the economic impact of cryptocurrency?* Pelicoin Bitcoin ATM. Retrieved February 18, 2023, from https://www.pelicoin.com/blog/what-is-the-economic-impact-of-cryptocurrency

Kaspersky. (2022, February 9). *What is cryptocurrency and how does it work?* www.kaspersky.com. Retrieved February 18, 2023, from https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency