CISC 322/326 Assignment 1 Conceptual Architecture of Bitcoin Core

February 19th, 2022

Group #3: IKUN - FAMILY
Jinyang Chen 19jc66@queensu.ca
Chiyu Wang 19cw33@queensu.ca
Yuxuan Cai 18yc33@queensu.ca
Gaoyuan Bao 19gb20@queensu.ca
Rundong Yu 18ry16@queensu.ca
Zehan Wang 19zw37@queensu.ca

Table of Contents

1. Abstract:

Bitcoin is a decentralized virtual currency that has grown in popularity in contemporary society. At the core of the Bitcoin network is a software system known as Bitcoin Core, which serves as the Bitcoin protocol's reference implementation. This report examines the architecture of Bitcoin Core in depth, including its architecture analysis, design concepts, essential components, and functioning. We demonstrate the Bitcoin Core wallet, which gives users a dependable and secure way to store and manage their bitcoins. We look at how public and private keys are used to create and manage bitcoin transactions, as well as how digital signatures are used to authenticate the network's transactions. We also focus on the Bitcoin Core consensus rules, which verify that all nodes on the network agree on the current state of the blockchain. Finally, we cover the continued development of Bitcoin Core, as well as the difficulties and opportunities that lie ahead for the Bitcoin network's future, as well as collaboration among Bitcoin community stakeholders.

In short, this report presents a thorough overview of the architecture of Bitcoin Core, emphasizing its essential features and significance in the operation of the Bitcoin network. This analysis' findings are significant for Bitcoin developers, academics, and users, along with anyone interested in the technology and possibilities of decentralized cryptos.

2. Introduction:

In 2008, the global financial crisis erupted, and on November 1 of that year, a man calling himself Satoshi Nakamoto published a white paper on the P2P foundation, "Bitcoin: A Peer-to-Peer Electronic Cash System," stating his new vision for electronic money. -On January 3, 2009, the Bitcoin Genesis block was born.

In contrast to fiat currency, Bitcoin does not have a centralized issuer, but is generated by the calculations of network nodes, and anyone can participate in the creation of Bitcoin, and can be circulated worldwide, bought and sold on any computer with Internet access, and can be mined, bought, sold, or received by anyone, regardless of location, and no one can identify the user during the transaction. On January 5, 2009, Bitcoin, which is not controlled by central banks or any financial institutions, was born. Bitcoin is a digital currency consisting of a complex string of computer-generated code, and new bitcoins are manufactured through a pre-determined program.

Bitcoin Core is the original Bitcoin software client created by Satoshi Nakamoto in 2009. It is an open-source software that allows users to send and receive Bitcoin transactions, store their private keys, and generate new addresses. Bitcoin Core is the most widely used Bitcoin client and is the reference implementation for the Bitcoin protocol.

This report outlines the transparent derivation approach our team used to choose the Bitcoin Core architecture style based on the information we learned during the course. Bitcoin Core is designed using a distributed system architecture style. It is a decentralized peer-to-peer network consisting of nodes that communicate with each other to maintain a shared ledger, or blockchain. This style of architecture allows for the creation of a decentralized system that does not require a central authority or intermediary to verify transactions.

Bitcoin Core also uses a client-server architecture, where the Bitcoin Core software serves as the client that communicates with other nodes on the network, and also provides a user interface for managing bitcoins. This architecture allows for the decentralized network to be accessible to users via a user-friendly interface, while also ensuring the security and reliability of the network.

The three subsections of the architecture analysis are the bitcoin wallet, the consensus rules, and the use case. Each of the aforementioned subsections will examine this conclusion several times. Finally, the project's lessons will be explored, and a conclusion is added at the end to provide a general summary of our findings.

3. Architecture analysis:

3.0.1 Functionality and interacting parts

A full-node implementation of the Bitcoin protocol is Bitcoin Core. Users may join the Bitcoin network as complete nodes thanks to this software, which implements the network's regulations. Its functioning and how it is divided into interacting pieces are described below. A full-node implementation of the Bitcoin protocol is Bitcoin Core. Users may join the Bitcoin network as complete nodes thanks to this software, which implements the network's regulations.

Functionality:

1. Maintains a full copy of the Bitcoin blockchain
2. Validates transactions and blocks according to the rules of the Bitcoin protocol
3. Broadcasts and receives new transactions and blocks to and from the network
4. Participates in the consensus process to determine the valid chain
5. Generates and manages private keys and digital signatures
6. Provides a user interface for interacting with the network

Interacting Parts:

Network: controls the connections to the network and transfers data. Besides, it can send and receive data from and to other Bitcoin nodes.

Blockchain: maintains a complete copy of the blockchain that includes a set of transactions and is regularly added to.
Consensus: ensures that all nodes in the network concur on the blockchain's current state. It accomplishes this by upholding the Bitcoin protocol's regulations and disallowing any erroneous transactions or blocks. In addition, it does this by preserving the rules of the Bitcoin protocol and forbidding any incorrect transactions or blocks.
User Interface: offers a graphical user interface to manage their Bitcoin transactions and communicate with the program.

The interacting pieces communicating with one another provide the software's overall functioning. As an illustration, the network component receives new transactions and blocks from other nodes. It sends them to the consensus component for validation following the specifications of the Bitcoin protocol.
The blockchain component receives the verified transactions and adds them to the blockchain. The wallet component also produces and signs new transactions to transmit Bitcoin to other addresses on the network and utilizes the blockchain to calculate the amount of the user's account.
Bitcoin Core is a sophisticated software system that communicates with the Bitcoin network to uphold the confidentiality and reliability of the blockchain. Its features and interconnected components provide customers with a safe and dependable platform for connecting to the Bitcoin network.

3.0.2 Control and data flow

Bitcoin Core consists of several parts that work together to maintain the Bitcoin network's functionality.

Network Communication: Bitcoin Core communicates with other nodes on the Bitcoin network via the peer-to-peer network protocol. The node exchanges information about blocks and transactions with other nodes by sending and receiving messages.

Transaction Pool: Stores transactions that have been broadcast to the network. Unconfirmed transactions not included in a block are temporarily stored in the transaction pool.

Block Validation: Verifies blocks to ensure they adhere to the network's consensus rules. This procedure entails confirming the validity of each transaction contained in the block, and the proof-of-compliance works with the necessary difficulty level.

Chain Selection: A block is added to the local version of the blockchain once it has been verified. The longest and most reliable chain is chosen by Bitcoin Core using a chain selection algorithm, after which new blocks are added to the chain.

Wallet Management: A built-in wallet in Bitcoin Core controls a user's Bitcoin addresses and private keys. Transactions must be signed and published to the network by the wallet.

User Interface: Users can communicate with the software using the Bitcoin Core user interface. Users may change network settings, transmit and receive bitcoin, and examine transaction history.

Depending on the precise action being carried out, the control and data flow between these parts might be complicated. To ensure the network runs smoothly and safely, Bitcoin Core generally organizes the transfer of control and data between these parts.

3.1 Bitcoin wallet

In terms of the architecture analysis of bitcoin wallet. The bitcoin wallet consists of two main components, one is the user interface, which is the interface where users interact with the wallet, and users can make some operations, like registration, create transactions, and so on. The other one is the wallet management session, which is used to manage user's wallet information, which includes the public and private that used to authorize transactions, the account balances, bitcoin addresses and so on. In addition, bitcoin wallets should have a component that links with the bitcoin network to get the data of blockchain and verification of transactions.

3.2 Consensus rules

The architecture analysis of the Consensus rule of bitcoin consists of four main components. The first component is transaction verification, which is used for validating the transactions in the bitcoin network is legal, including checking the bitcoin addresses of sellers and buyers, the signatures from them, and other information about this transaction. The second one is blockchain, which is used for verifying the transactions are packaged into the correct block, and validate whether the mining process is good during the whole process. The third one is nodes, which include all the nodes of the bitcoin network, and used to check if the node is legal and secure to make sure all the operations on the bitcoin network are right. The last one is the computing algorithms for the consensus rule, which make sure the above operations and components works correctly, like bitcoin uses elliptic curve cryptographic algorithms to verify the correctness of transaction signatures.

3.3 Use case

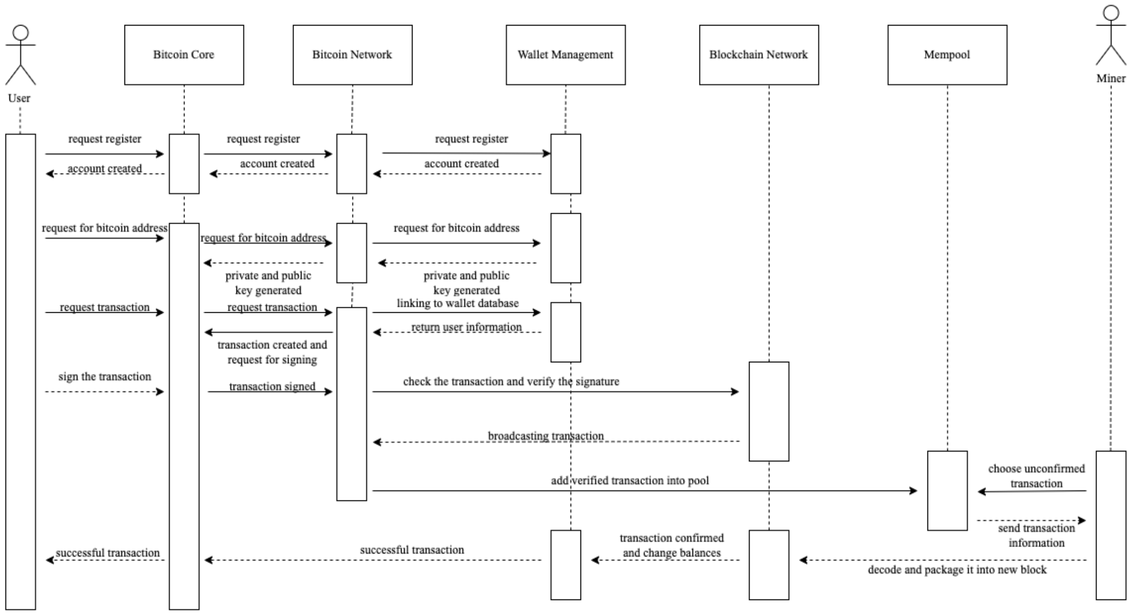

User
Bitcoin Core
Bitcoin Network
Wallet Management
Blockchain Network
Mempool
Miner
request register
account created
request register
account created
request register
account created
request for bitcoin address
request for bitcoin address
request for bitcoin address
private and public key generated
private and public key generated
request transaction
request transaction
linking to wallet database
return user information
transaction created and request for signing
sign the transaction
transaction signed
check the transaction and verify the signature
broadcasting transaction
add verified transaction into pool
choose unconfirmed transaction
send transaction information
successful transaction
successful transaction
transaction confirmed and change balances
decode and package it into new block

Figure 1. Use case transaction confirmation

This diagram shows one of the use cases of Bitcoin core: transaction confirmation. Confirmation transactions confirm a bitcoin transaction that has been added to the blockchain to ensure security and privacy. As for the transaction process, first of all, users should download one of the bitcoin software, like bitcoin core and bitcoin wallet; we used bitcoin core in this case. After downloading and installing it, the users need to register their accounts in bitcoin core. Then, their registration requests will be sent to the bitcoin network, confirming the user's registration and creating accounts. After that, users can request a bitcoin address on bitcoin core, and the bitcoin network will generate the user's public and private keys based on their bitcoin address, and both keys will be stored in the user's wallet. The public key is used to receive cryptocurrency payments, and the private key is used to decrypt the received cryptocurrency, and to sign the transaction, thus proving ownership and making transfers. Next, users can request the transaction on bitcoin core, which requires the verification of the user's wallet; the transaction is created once the proof is proved. In addition, the transaction needs the signature of the users, and then the bitcoin network will check the signature and transaction information; the verified transaction will be broadcasted to all the nodes in the bitcoin network, then the transaction will be added to the mempool, and which contains all the unconfirmed transactions. Finally, the miners will take one of the transactions in the mempool, decode the package into a new block, and then send it to the blockchain network, which is the confirmation of the transaction.

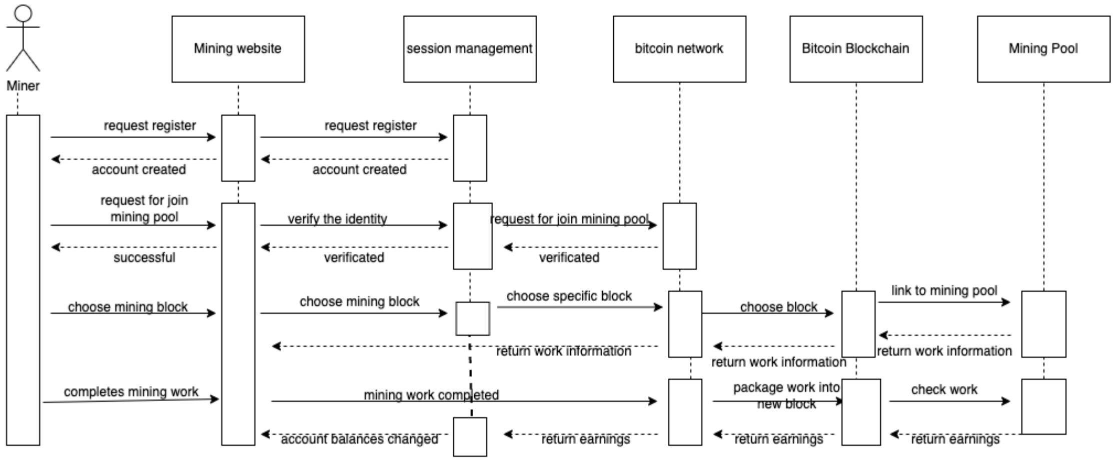
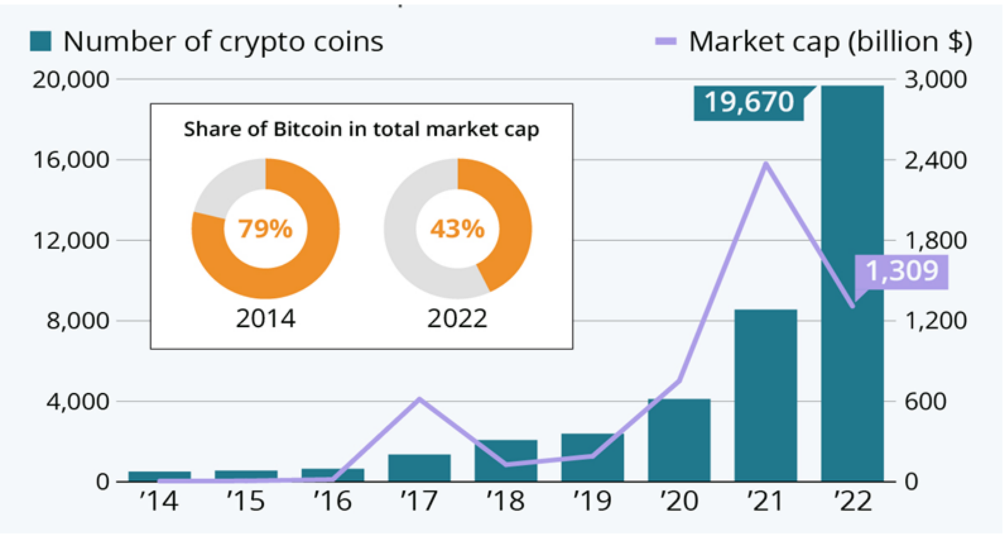


Figure 2. Use Case Bitcoin Mining

This diagram describes another one of the use cases of Bitcoin core: Bitcoin Mining. Mining refers to the process of verifying bitcoin transactions by solving cryptographic puzzles. As for the mining process, Miners should interact with bitcoin mining websites firstly and register an account. After that, Once Miner's account is created and identity verified, miners are authorized to choose a mining pool to join, which interacts with the bitcoin network. After a miner linked with the bitcoin network and its blockchain, the miner can choose a blockchain and link it with the mining pool and then he can select a mining work from the mining pool. In addition, the miners can complete his work by specific mining tools, then he returns the completed work, which is the confirmation for a bitcoin transaction, to the bitcoin network and packages it into a new block to blockchain, the work is done. Additionally, the mining pool checks the work and returns the earnings to the miner by sending the bitcoin to the bitcoin wallet address of the miner.

3.4 How does the system evolve

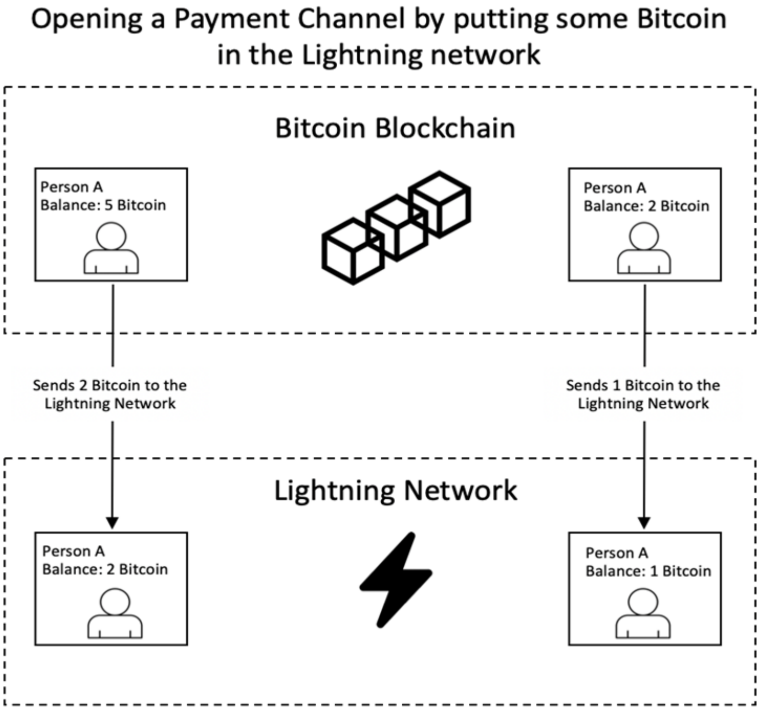
When it comes to evolve of system, after the international financial crisis in 2008, the traditional monetary payment system was greatly impacted. Driven by financial technology innovation, new digital currency technology has risen. The most famous and successful virtual currency in the world is Bitcoin. The concept of Bitcoin was first proposed by Satoshi Naka-moto in 2008. The traditional financial transaction bookkeeping system is centralized, and banks or central trading institutions are responsible for recording the transfer of funds. Nakamoto believes that the transaction cost of this recording method is very high, and it relies too heavily on centralized trading institutions. Improper operation will lead to the crisis of the financial system and great credit risk. Therefore, he designed a decentralized public transaction bookkeeping system (Jan 2017). Online payment is initiated by one party and directly paid to the other party without any financial institutions. The transaction information is sent to all participants in the transaction system, which is witnessed and recorded by everyone. In order to encourage participants to record transactions, Nakamoto designed an incentive mechanism to invite all trading participants to solve a very difficult mathematical problem through a specific algorithm. The one who successfully solves the problem first will get the final bookkeeping right of the trading block and the Bitcoin reward in the block. This method of obtaining Bitcoin is called "mining", while those involved in bookkeeping are called "miners", and the computer used to solve problems is called "mining machines". At the beginning of 2009, Nakamoto released the first version of open source Bitcoin client, announcing the birth of Bitcoin, and obtained the first 50 Bitcoins through "mining".



Compared with traditional currencies, Bitcoin has positive innovative significance. First of all, the issuance is objective and independent. It abides by objective rules and is not controlled by subjective institutions. The transaction of Bitcoin has its own established rules (Zheng, 2012). It has independence from the central bank and commercial financial institutions, and low credit risk. At the beginning of its establishment, the Bitcoin issuance mechanism set a total issuance amount of 21 million Bitcoins. At the same time, the "mining" reward is not fixed, but will be halved every four years. At the beginning of 2009, 50 Bitcoins were awarded for each block. By 2013, the number of block awards will be halved to 25. By 2017, the number of block awards will be halved again to 12.5, and so on, until all 21 million bitcoins have been distributed. The issuance rules of this process are very strict. It is determined at the beginning of the issuance that no one has the right to modify these rules and conduct additional issuance outside the rules. There is no limit to the participants. Anyone who opens the computing equipment can participate in the "mining", that is, in the process of currency issuance, with a wide range of democracy.

The transaction bookkeeping system is safe and stable, difficult to tamper with, and can effectively protect privacy. All transaction participants of Bitcoin jointly confirm the transactions in the Bitcoin system over a period of time and record them on the blockchain to form new blocks. The bookkeeping right of the Bitcoin system is decentralized, and every miner has the bookkeeping right. The miner who successfully seizes the bookkeeping right will receive the new Bitcoin reward of the system. The Bitcoin network shares a public account, which contains each transaction that has been processed and allows users to verify the validity of each transaction by computer. The authenticity of each transaction is protected by the digital signature of the corresponding sending address, so that all users can control the sending of bitcoin from their own address. At the same time, Bitcoin can achieve the privacy of transactions through the combination of public key and key (Drainvile, 2012).

The actual calculation and resource cost are in line with the labor value theory. There are real issuance costs for Bitcoin acquisition, including the purchase and operation of mining machines, payment of electricity bills, etc. With the prevalence of Bitcoin mining, the cost is rising. Due to the increasing difficulty of computing and the intensification of competition over time, the mining mode of Bitcoin has been highly concentrated, and people have begun to buy giant mining machines and build large-scale mining sites in areas rich in electricity. According to the recent market calculation of equipment cost and electricity cost, the comprehensive cost of digging out a Bitcoin has exceeded 10000 dollars.

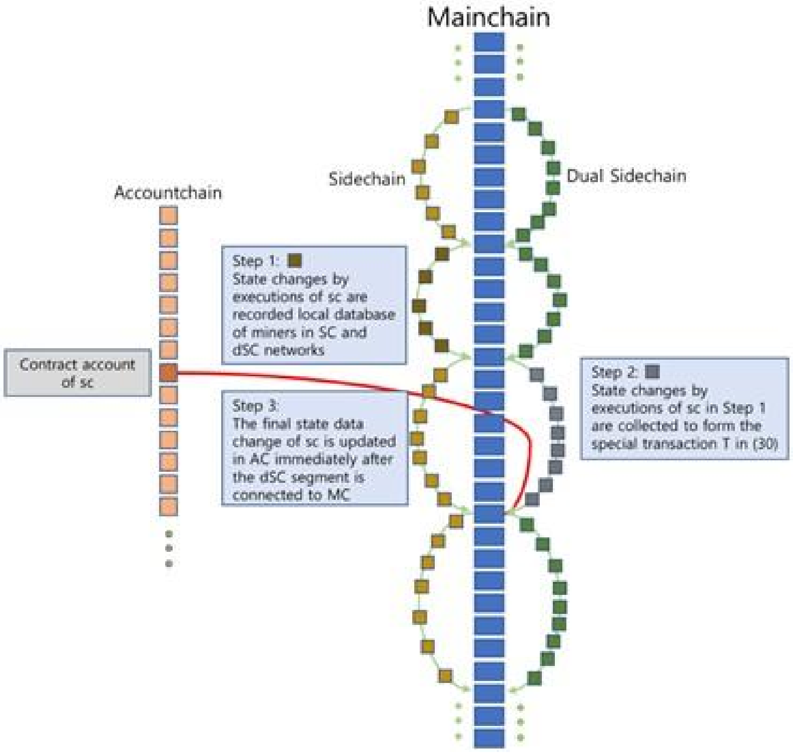

Opening a Payment Channel by putting some Bitcoin in the Lightning network
Bitcoin Blockchain
Person A
Balance: 5 Bitcoin
Person A
Balance: 2 Bitcoin
Sends 2 Bitcoin to the Lightning Network
Sends 1 Bitcoin to the Lightning Network
Lightning Network
Person A
Balance: 2 Bitcoin
Person A
Balance: 1 Bitcoin

The regulation is loose and the trading system is free and independent. After the international financial crisis in 2008, the international community has significantly strengthened the supervision of traditional financial institutions, and the anti-money laundering efforts have continued to increase. In order to prevent the transmission of international financial risks, the control of capital flows has been strengthened, and the cost of international capital flows and cross-border asset allocation has increased. In a sense, the virtual currency field is the only "free paradise" in the current international financial system (Huhtinen, 2014). Global financial investors have a huge demand for cross-border investment and wealth transfer, but the operation of traditional banking systems and international settlement systems faces strict review procedures, high cost and slow efficiency. Bitcoin has natural advantages in this respect: on the one hand, blockchain encryption technology can well protect the privacy of customers, it is difficult to trace the revenue and expenditure of transactions, and the flow of funds in the later period is not restricted; On the other hand, Bitcoin does not have a global unified regulator, and capital transactions do not require any approval process, which is highly time-efficient. Therefore, Bitcoin has become a very convenient way for international funds to flow freely across borders and avoid regulatory constraints.

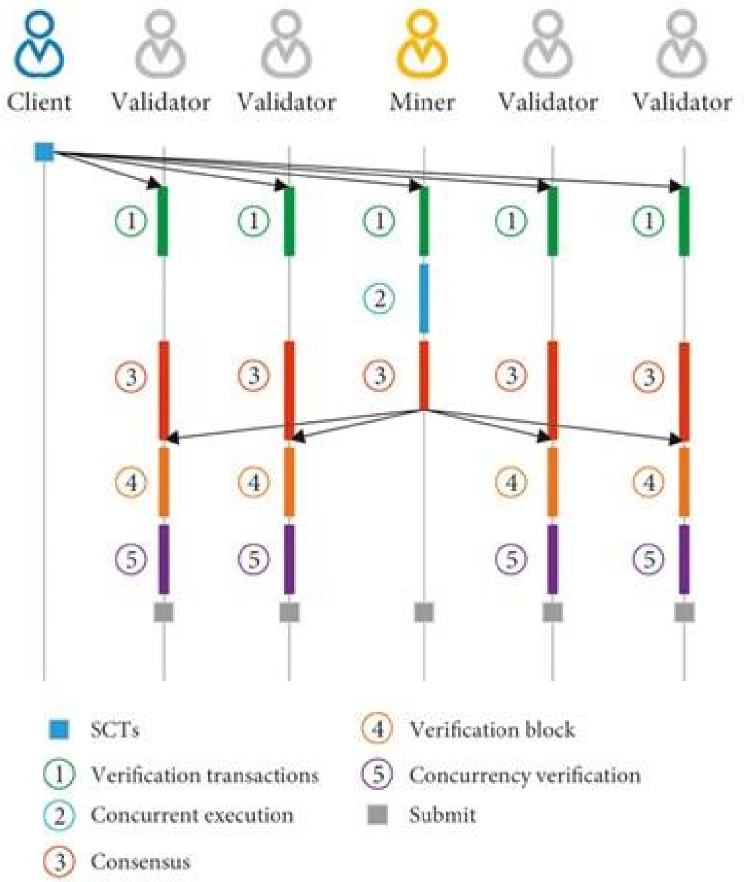
3.5 what concurrency if any is present

Also for the concurrency of Bitcoin, two years ago, our public chain had Bitcoin and Ethereum. The consensus algorithm adopted by these two public chains is called PoW. This is equivalent to solving an intelligence game together, such as guessing numbers. Who guesses first, who has the right to keep accounts. Everyone is struggling with their computing power. With the improvement of the computing powhole network, the difficulty of the problem is al.

Bitcoin has designed an algorithm to ensure an average of one block every 10 minutes. With the improvement of network computing power, it will also continuously adjust the difficulty of the game to ensure that a block is produced every 10 minutes. Through the calculation of security, it believes that there is one block every 10 minutes, and when there are six blocks, there is no other large mine that has dug up seven blocks in the time window of nearly one hour, and it can roll back all six blocks at once (Bistarelli, 2017).


Mainchain
Sidechain
Dual Sidechain
Accountchain
Step 1: ■
State changes by executions of sc are recorded local database of miners in SC and dSC networks
Contract account of sc
Step 2: ■
State changes by executions of sc in Step 1 are collected to form the special transaction T in (30)
Step 3:
The final state data change of sc is updated in AC immediately after the dSC segment is connected to MC

Therefore, what we call confirmation status is not 100% confirmation, but a probability confirmation status. Although Bitcoin says that it is confirmed by 6 blocks, you may need to wait for 12 or 20 confirmations in the exchange to actually put that account into your account, because the exchange is also afraid of risks. The Ether scheme is an extension of Bitcoin. Because Bitcoin only has a transaction in 10 minutes, which is basically unavailable for all transaction scenarios, unless it is a very large transaction, and you are willing to wait for this 10 minutes. The strategy of Bitcoin is to follow the next block after the last block is completed, which is a process of competition. Ether introduces a new concept. At the same height, for example, the previous blockchain has finished, and it is time to build a block with height of 11. At this time, there may be 100 people digging out the 11th block in a very short time window in the entire network. However, only one can eventually be linked to our main chain, so 10 are invalid.



These 10 discarded blocks are of course valuable because they also consume computational power. Ether's solution is to add the computing power of these 10 blocks to the whole main chain state evaluation process, so that it can be confirmed in a shorter time. Because in that short time window, the computing power contributed by the whole network is the same as that contributed by Bitcoin on a block. In this way, it can also reach a security index equivalent to Bitcoin. The transfer speed of Ether is about 15-20 seconds per block. It needs to wait for 12 blocks. On fire coins, it will take about 28 blocks to confirm. Because Firecoin is also afraid of taking risks. It can't be said that 100% of the 12 blocks can be confirmed (Pinna, 2016). It has a probability that it will be rolled back. Once rolled back, the Firecoin platform will have to bear great liability for asset loss, so it will wait longer in this place. This is the status quo of our confirmation in the earliest generation of public chain projects. It is a probability, not 100%.

4. Sustainable development

Bitcoin is the first and most well-known cryptocurrency in the world, and it has experienced significant growth in the past few years. The total market capitalization of Bitcoin reached an all-time high of over $1 trillion in 2021, and many institutional investors, such as MicroStrategy, Tesla, and Square, have added Bitcoin to their balance sheets. In addition, major financial institutions such as PayPal, Mastercard, and Visa have announced plans to support Bitcoin transactions, further legitimizing its place in the financial world.

Bitcoin has the potential to offer several advantages as a decentralized digital currency. One key advantage is its ability to allow peer-to-peer transactions without the need for a central authority, such as a bank. This can provide greater financial freedom and security to individuals who do not have access to traditional financial services or who wish to take control of their own finances.

Another advantage of Bitcoin is its limited supply, with only 21 million bitcoins set to ever exist. This creates a sense of scarcity and could help to support its value, similar to how gold is valued for its limited supply. Additionally, Bitcoin's transaction fees can be lower than traditional financial transactions, making it a potentially more cost-effective method for transferring value.

Despite its potential advantages, Bitcoin is not without its challenges. One of the most significant is its extreme volatility. The price of Bitcoin can fluctuate rapidly, with sudden price drops of 10% or more being relatively common. This makes it a high-risk investment and limits its use as a medium of exchange, as people may be hesitant to spend their bitcoins if they think the value may drop in the near future.

Another challenge for Bitcoin is its potential impact on the environment, with the energy（electric power）consumption required for Bitcoin mining being a point of criticism, to get one cion requires a huge amount of server group, and it can cost considerable electricity. The majority of this energy comes from non-renewable sources（like petroleum or coal）, which could make Bitcoin an unsustainable technology that contributes to climate change.

In conclusion, Bitcoin offers potential advantages as a decentralized digital currency, such as allowing for peer-to-peer transactions and offering lower transaction fees. However, its extreme volatility and potential impact on the environment present significant challenges that could limit its adoption and growth. As with any investment, it is important for individuals to carefully consider the risks and benefits of Bitcoin and make informed decisions based on their own individual circumstances.

5. Conclusion

According to system evolve and concurrency we can conclude that the Bitcoin system is divided into 6 layers, from bottom to top are storage layer, data layer, network layer, consensus layer, RPC layer, and application layer. Among them, the storage layer is mainly used to store the log data and blockchain metadata during the operation of the Bitcoin system, and the storage technology mainly uses the file system and LevelDB. The data layer is mainly used to process various types of data in Bitcoin transactions, such as packaging data into blocks, maintaining blocks into a chain structure, encryption and hash calculation of content in blocks, and digital signature of block content and add timestamps, build transaction data into a Merkle tree, and calculate the hash value of the root node of the Merkle tree, etc. The chain composed of blocks may fork. In the Bitcoin system, nodes always regard the longest chain as the correct chain and continue to add new blocks thereafter. The network layer is used to build the underlying P2P network of Bitcoin, supports dynamic joining and leaving of multiple nodes, effectively manages network connections, and provides basic network support services for Bitcoin data transmission and consensus. The consensus layer mainly adopts the PoW (Proof Of Work) consensus algorithm. In the Bitcoin system, each node continuously calculates a random number (Nonce) until it finds a random number that meets the requirements. Within a certain period of time, the first random number that meets the conditions will be awarded the right to package the block, which builds a proof-of-work mechanism. The RPC layer implements RPC services and provides JSON APIs for clients to access blockchain underlying services. The application layer mainly carries various bitcoin applications, such as the bitcoin client provided in the bitcoin open source code. This layer is mainly used as an RPC client to interact with the bitcoin underlying layer through the JSON API. In addition, Bitcoin wallets and derivative applications are set up on the application layer.

For the architecture analysis, the architecture analysis of bitcoin wallet and the consensus rule of bitcoin. The bitcoin wallet is made up of two main components, a user interface and a wallet management session. The user interface allows users to interact with the wallet, while the wallet management session manages the user's wallet information, including public and private keys, account balances, and bitcoin addresses. Additionally, bitcoin wallets need a component to link with the bitcoin network to get blockchain data and verify transactions. The consensus rule of bitcoin has four main components, including transaction verification, blockchain verification, nodes, and computing algorithms. These components work together to ensure that transactions on the bitcoin network are legal, packaged into the correct blocks, and secure. Bitcoin uses elliptic curve cryptographic algorithms to verify the correctness of transaction signatures.

6 Reference:

Jan Lánsk. (2017). Bitcoin system. *Acta Informatica Pragensia, 2017*(1), 20-31.

Zheng, S. W. , & Fan, L. . (2012). Credit model based on p2p electronic cash system bitcoin. *Information Security & Communications Privacy.*

Drainvile, D. . (2012). An analysis of the bitcoin electronic cash system.

Huhtinen, T. P. . (2014). Bitcoin as a monetary system: Examining attention and attendance.

Bistarelli, S. , Mantilacci, M. , Santancini, P. , & Santini, F. . (2017). An end-to-end voting-system based on bitcoin. *Symposium*.

Pinna, A. . (2016). A Petri net-based model for investigating disposable addresses in Bitcoin system.

Satoshi Nakamoto.(n.d). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf