Video:

CISC 322 - Group 19 - Assignment 1 - Video.mp4

Roles

Seb Deluca - Subsystems, Use Cases

Robbie Huang - System Derivation, Use Cases

Ethan Kim - Abstract, Introduction, Conclusion, Presenter

Aidan Leyne - Lessons Learned, Limitations, Glossary, Review and formatting

Sean Liang - Subsystems, Use Cases, Group Leader

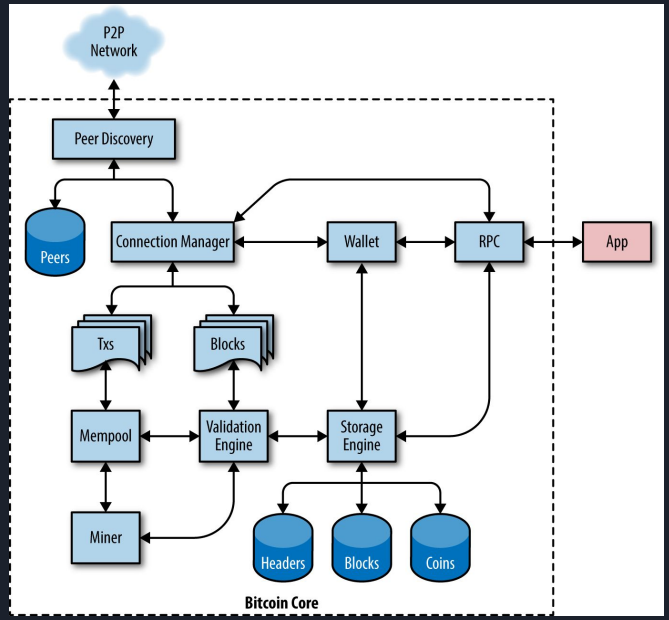
Artie Lomonaco - Abstract, Introduction, Conclusion, Presenter

Bitcoin Core

Bitcoin Core: High -Level Architecture Description

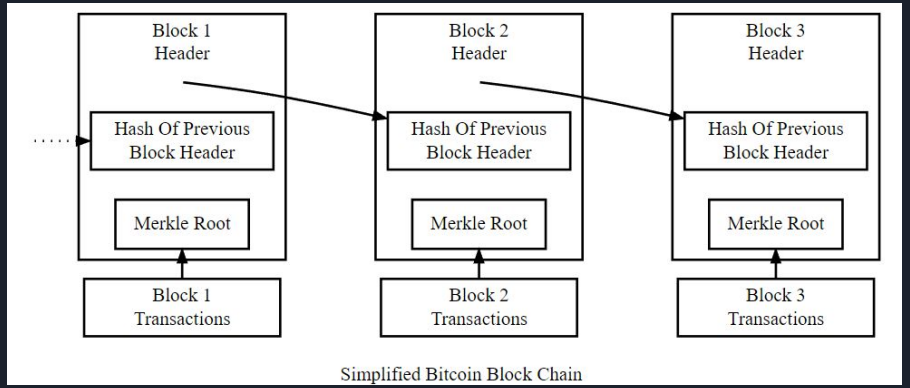
Components of the Architecture:

- Blockchain
- Transactions
- Contracts
- Wallets
- Payment Processing
- Operating modes
- P2P Networks
- Mining



Blockchain

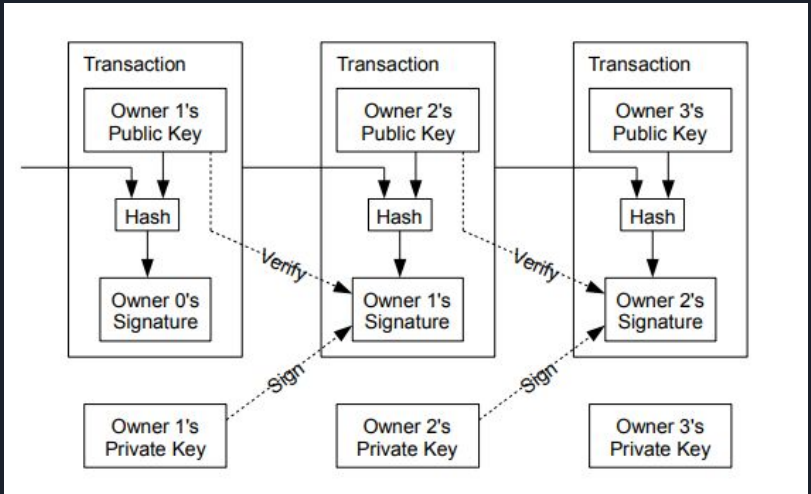
- Distributed peer-to-peer ledger technology
- Anonymous, time-stamped, secure, and programmable
- Foundation for crypto-tech; currencies, NFT’s, smart contracts, etc.
- Designed on the premise of blocks, a block being a uniquely hashed network node
- Made famous to the public by Bitcoin

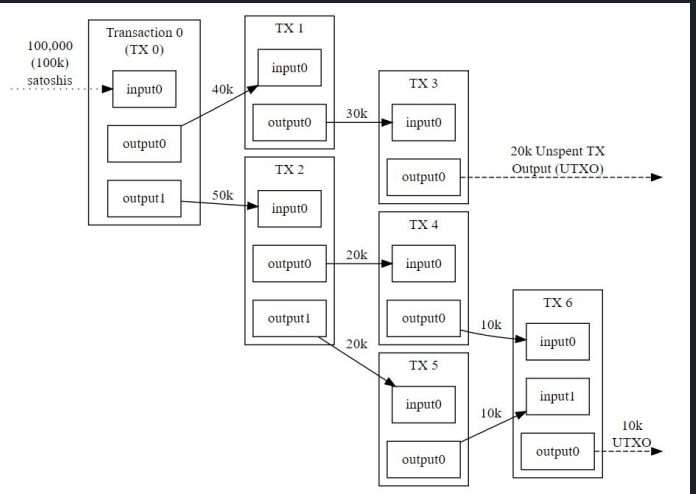


Simplified Bitcoin Block Chain

Transactions

- A transaction is the action from one owner to another with a digital signature by sending a hash of the previous transaction and public key to the new owner.
- The new owner would now sign with his private key which indicates the authorization to receive the bitcoin.
- With these aspects the networks' users can verify that the transaction passed, avoiding double spending since there was only one transaction that occurred





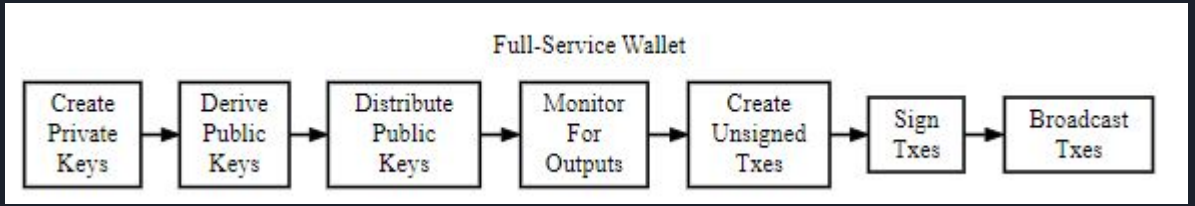
Contracts

- Method of enforcement for blockchain transactions
- Bitcoin contracts work on the premise of a public key and private key
- The private key associated with a public key acts as a signature for creating a new contract
- This new contract can be used as an actionable transaction
- Contracts can be built with multiple “signers”
- For example, a 2-of-3 multisig address would require the digital signatures of any two out of three specified public keys to spend the funds

Wallets

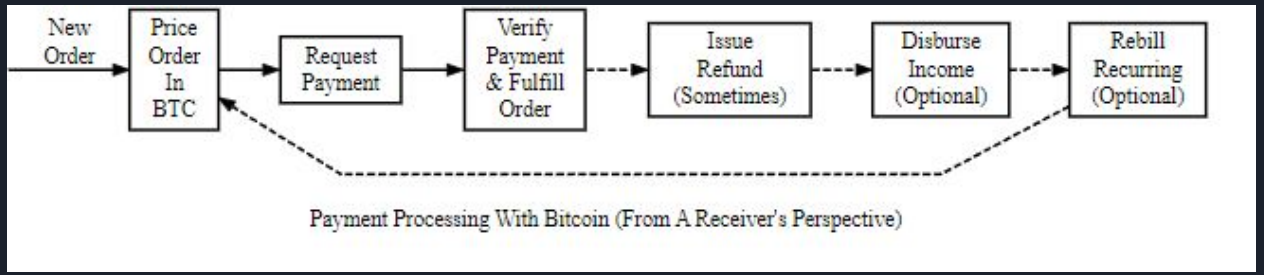
- Component/ Data Structure that:
  - controls access to a user's money
  - managing keys and addresses
  - tracking the balance
  - creating and signing transactions.
- Types of Wallets:
  - Full Service
  - Signing Only
  - Hardware
  - Distributing Only
  - Offline
  - Networked

- Interactions:
  - with the P2P Network to get information on the blockchain and announce transactions (mainly networked wallet)
  - With the RPC of Bitcoin Core, main functions of the app, allows the app to check wallet activity.



Payment Processing

- Payment processing represents the larger service allowing users to send and receive payments in exchange for products or services.
- Conventional banking systems, the payment processing is outsourced, and connected to third party APIs.
- Exchange rates between various currencies must be considered when linking two parties.. It is the responsibility of this application to collect and process the required data in order to provide fair values..
- If the values differ substantially, the system enters into a “safe mode” so a human can evaluate the situation.



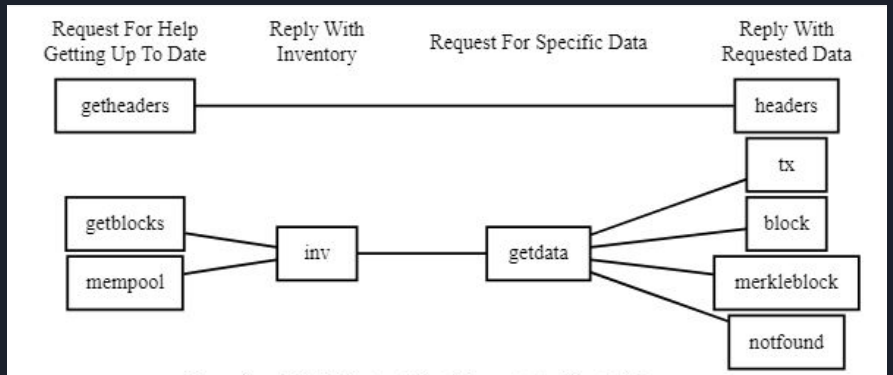
Payment Processing With Bitcoin (From A Receiver's Perspective)

Operating Modes

- There are two primary operating modes
  a. Full node
  b. SPV
- Full node validates the entire blockchain, making it a longer process
- SPV validates only the header of the chain, rendering it lighter in applications

P2P Networks

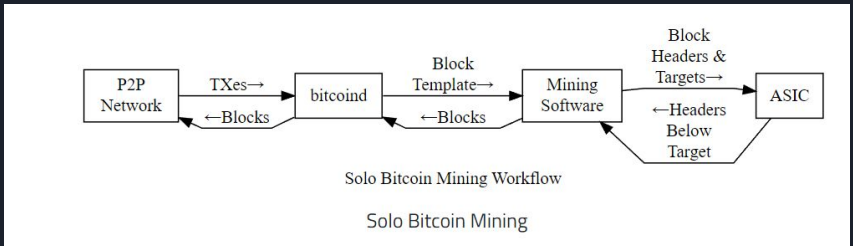
- It enables communication between nodes, facilitating the sharing of information about transactions, blocks, and the state of the blockchain.
- The network is composed of nodes - that is, every computer running the Bitcoin software. The peer-to-peer architecture allows for the removal of central servers for a protocol facilitating the communication directly to other peers.
- The network maintains the security and integrity of the blockchain through a consensus of the nodes, agreeing if new blocks are valid before appending them to the blockchain.
- Enabling the Bitcoin Network to operate as a decentralized system, without any singular entity possessing control over the blockchain; network more resilient to attacks and providing better privacy.

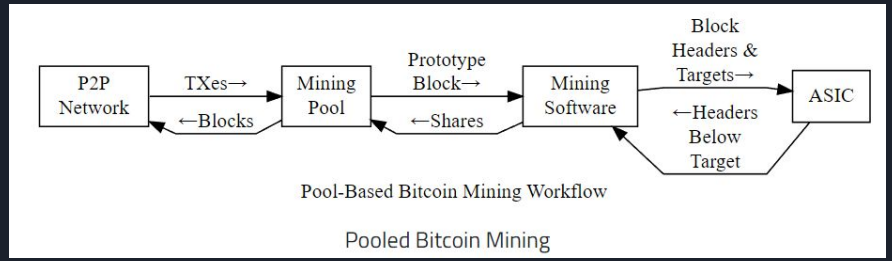


Overview Of P2P Protocol Data Request And Reply Messages

Mining

- Common application of Bitcoin Core is bitcoin mining
- Allows for peer-to-peer bitcoin mining
- Allows blocks to be distributed faster
- Allows faster block verifications





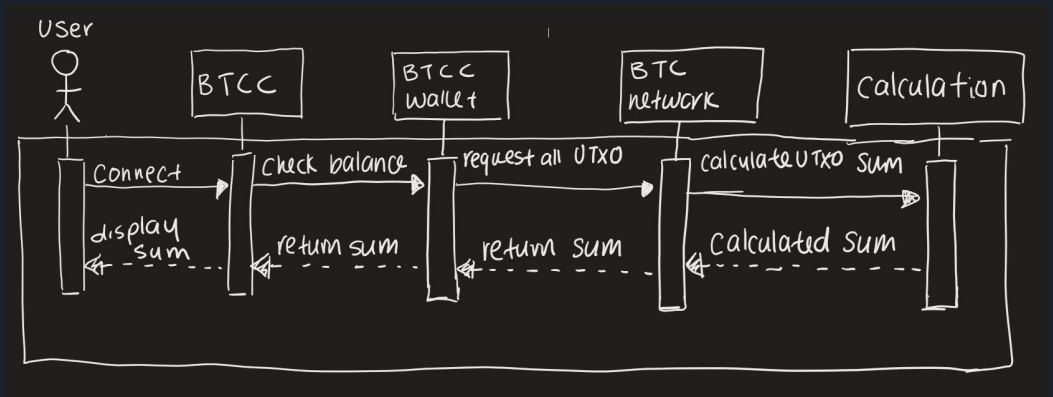
Bitcoin Core - Use Cases

Use Cases for Bitcoin Core:

- Wallet Uses
- Sending Transaction
- Receiving Transactions
- Mining Uses

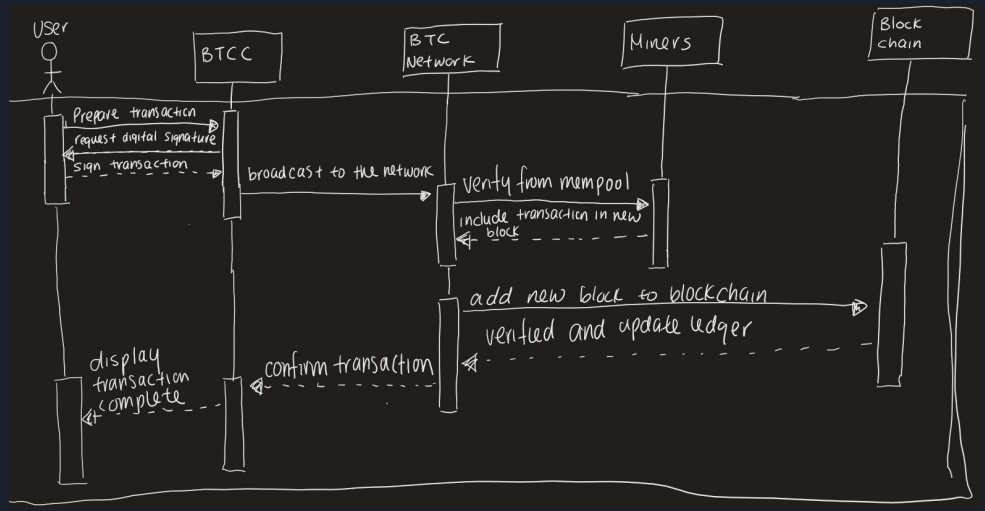
Checking Wallet Balance

- User's balance calculated by scanning the Bitcoin network for all UTXO and finding the sum to calculate the balance that belongs to the user.
- UTXO is an arbitrary value for multiple satoshi. Similar to a physical coin once a UTXO is created it is not divisible.
- During a transaction if the UTXO is larger than the desired value of a transaction, it must be consumed entirely and will give two outputs:
  - First one being the amount paid to the other user
  - Second one being the 'change' from the transaction or remaining amount after transaction which is put back into the wallet.



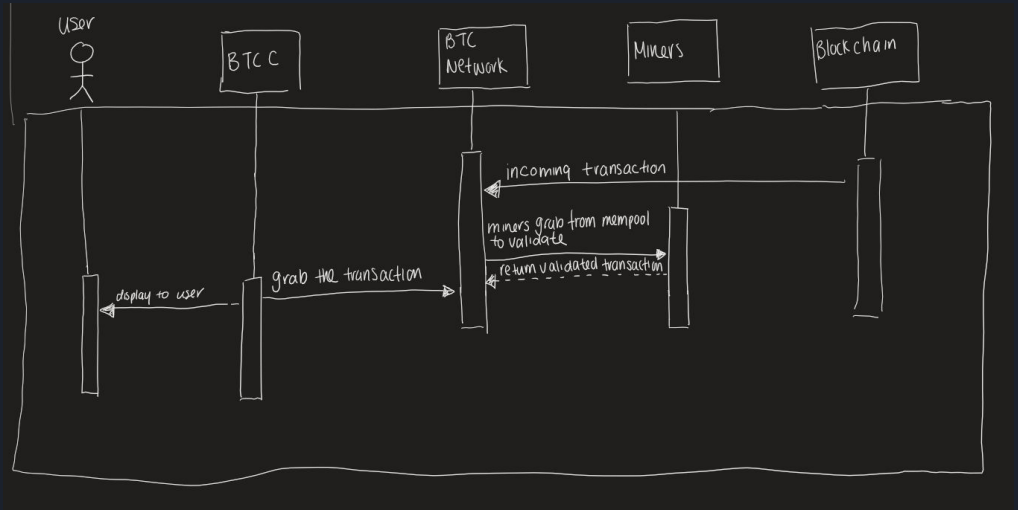
Sending Transactions

- User must specify the recipient address, the amount of bitcoin sent, and transaction fees that must be sent to the miners who process the transaction.
- Bitcoin Core will then create a digital signature with user's private key.
- Once transaction signed, broadcasted by Bitcoin Core into Bitcoin Network.
- Once validated block added to the blockchain.
- The recipient would then receive the transaction of bitcoin into their wallet
- User can view transaction status as well.



Receiving Transactions

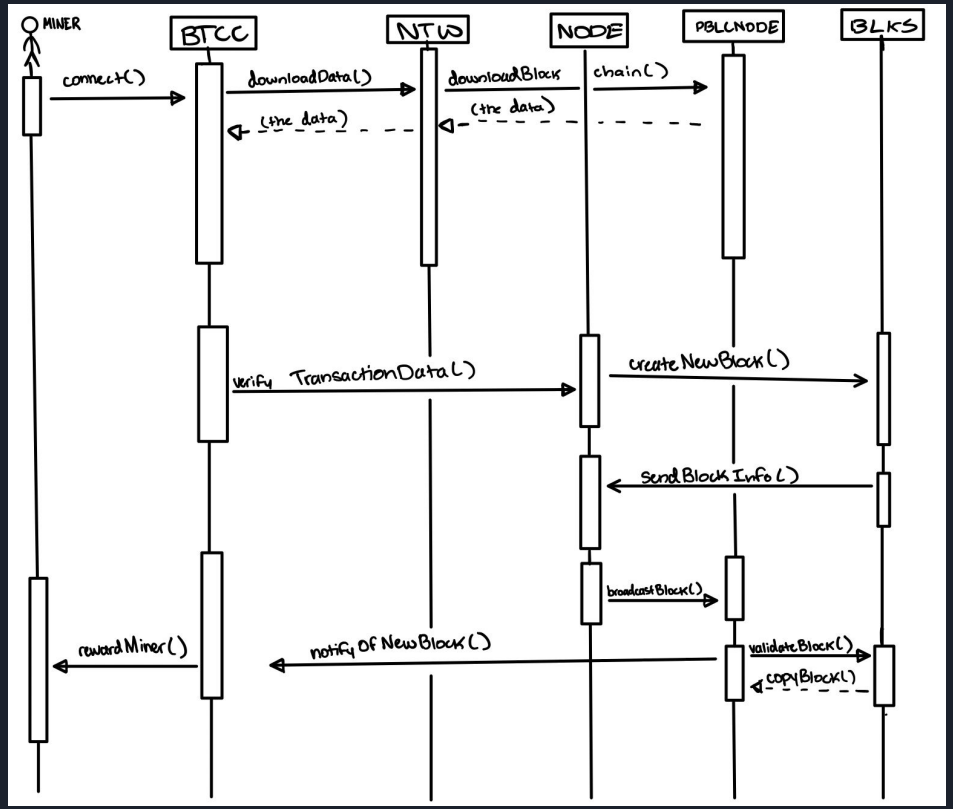
- Once sender has the wallet address they will specify the amount of bitcoin sent, as well as pay the transaction fees that must be sent to the miners.
- Bitcoin will then be broadcasted on the bitcoin network where the miners will grab it from the mempool and have it validated through mining.
- Receiver's wallet will then detect the transaction that is being sent to their wallet, it will grab it and add the transaction to the wallet.
- Afterwards the transaction is confirmed and updated on the ledger



Mining

- mining of Bitcoin is a complex process that interacts with many of Bitcoin Core's major components
- Bitcoin Core has consensus rules– rules that dictate how blocks are created and validated. Said rules are enforced by validating each block that is mined, ensuring that it follows the rules laid out in the consensus rules. ensures that the network remains secure and trustworthy.
- mining requires interaction with is the Nodes of the Bitcoin network. Bitcoin Core utilizes a peer-to-peer network that miners can use to connect to other nodes, allowing them to share information about new transactions and blocks, as well as mine them
- Verification of transactions: Miner interacts with verification component of Bitcoin Core to verify new transactions and add them to the next block that they are mining
- Interact with Blocks: creation of new blocks, as well as including transactions, adding a nonce value, and calculating a block header

Miner - Sequence Diagram



Drawbacks

- Does not have support for commercial wallets.
- UX may be clumsy first time using it
- May take days to download due to size of blockchain.
- Scalability:
  - The current design of the Bitcoin Core protocol limits the maximum number of transactions that can be processed in a given time frame. This has resulted in long wait times and high fees during periods of high network activity, which can be a significant barrier to adoption and use.
- Usability:
  - Bitcoin Core can be difficult for non-technical users to understand and use, which can be a barrier to widespread adoption and use.

Lessons Learned

- A lot has been learned about Bitcoin Core. Firstly about its main components, how they interact with each other, and how they interact with the Bitcoin network.
- It was pretty hard to find information on how the subsystems interact based off of the diagram that was in the documentation, and the terms it used were complicated.
- It would mainly focus on how the app interacts with the Bitcoin Network.
- Based off of that it was difficult to create the sequence diagrams, as well as getting and a general understanding from the documentation.
- We had to use outside sources to clarify the complicated terms.

Conclusion

- Architecture of Bitcoin Core is a fine mesh of components that deliver a streamlined Bitcoin interface.
- Open-source and innovative hybrid PoS/PoW consensus mechanism provides a quality unparalleled by competing technologies
- In summary, this report has delivered a detailed look into the high-level architecture, components, and functionality that comprise the foundation of Bitcoin Core.
- Chris Matthieu and the founding developers of Bitcoin Core have laid a path for a more equitable, open-source, blockchain future.