Bitcoin Core Conceptual Architecture

QCX: Queens Crytpo Exchange
CISC 322
Winter 2023
Presentation Link: https://youtu.be/MmTbKFivd54

Our Team

Andrew Liu - Group Leader

- Use Cases

Anirudh Tiku - Presenter

- Subsystems, Architectural Style, Data Dictionary

Daniel Mitchell

- Conceptual Diagram/ overview, Concurrency of Subsystems, Sequence Diagram, Lessons Learned

Zoya Zarei-Joorshari

- Abstract, Introduction, Architectural Style, System Evolution

Derek Ho

- Derivation Process, Subsystems

Ethan Butler

- Subsystems, Developer Roles

Overview

- General Information
- Derivation Process
- Conceptual Architecture Diagram
- Subsystems
- Concurrency
- Use Cases

General Information

- Bitcoin is an attempt to “remove the middleman” in payment transactions
  I.e. Banks, Paypal, Interac, etc.
- Bitcoin was first available to buy in 2010
- Bitcoin Core is the technical heart of the bitcoin cryptocurrency scheme
  - An open source Peer-2-Peer system that makes use of the blockchain
  - Handles transactions, bitcoin mining, receipt validation and other integral processes

Dictionary

Bitcoin Core: The client software for the Bitcoin network

Bitcoin: A decentralized digital currency that enables peer-to-peer transactions without the need for intermediaries

Address: A unique identifier for a Bitcoin account, consisting of a hash of a public key

Blockchain: A decentralized, digital ledger that uses cryptography to securely record and store transactions

Consensus: The agreement among Bitcoin network participants on the validity of transactions and the state of the blockchain

Mining: The process of adding new blocks to the blockchain and earning newly created Bitcoin as a reward

Node: A computer running Bitcoin Core software that participates in the Bitcoin network

P2P: Peer-to-peer, a decentralized networking architecture that enables direct communication between network nodes without intermediaries

Transaction: The transfer of Bitcoin from one address to another

Wallet: Software used to store, send, and receive Bitcoin

RPC: Remote Procedure Call, causes the program to execute a subroutine in a different address space.

Derivation Process

Our journey towards our final architecture involved:

- Individual members conducting research on separate aspects of the system
- Putting together the collective research into one cohesive architecture over the course of a few meetings
- Discussing the clear advantages of a Peer-2-Peer architecture that fits Bitcoin Core perfectly

Sequence Diagram: Legend

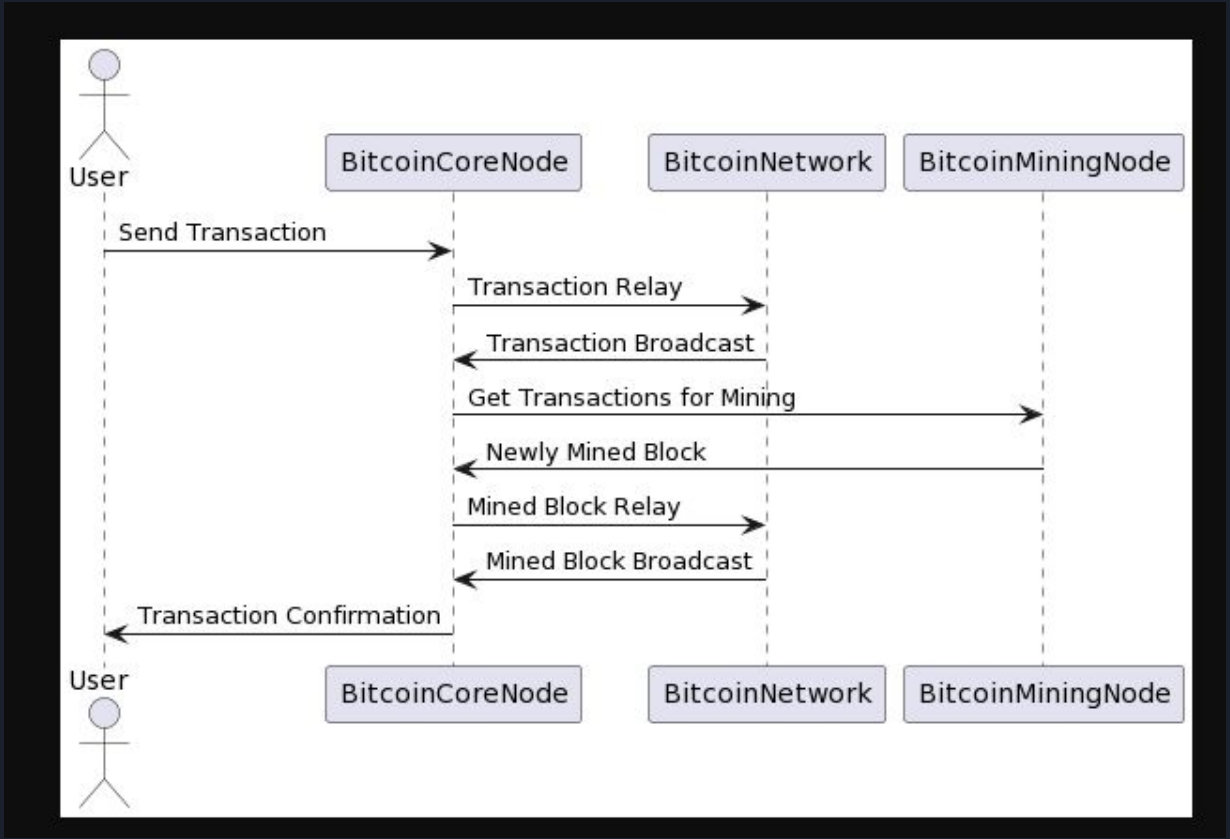
- reply message

- synchronous message

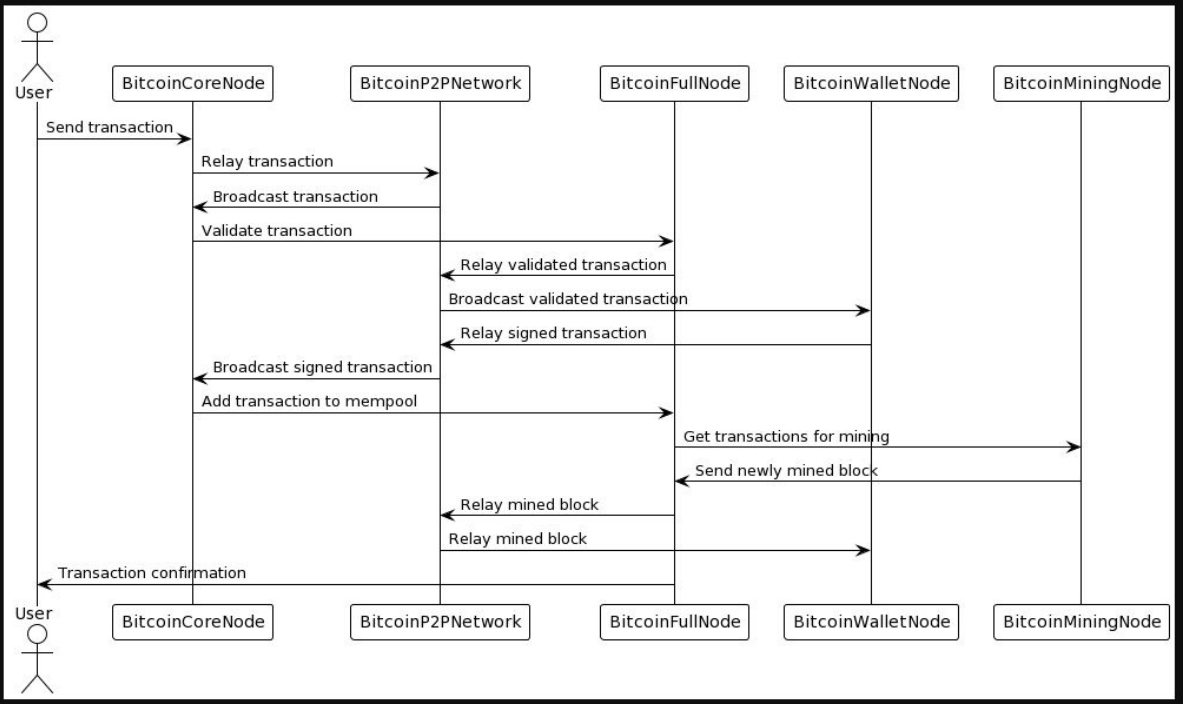
- leads to

- loops back to

Conceptual Architecture Diagram: Initial Draft



Conceptual Architecture diagram: Final Draft

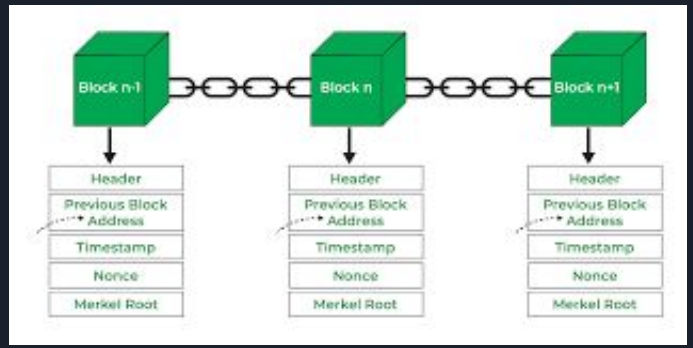


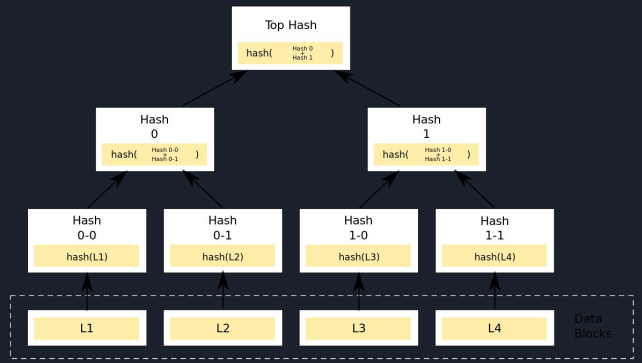
Subsystems and Dependencies

- ➔ Blocks
- ➔ Block Chains
- ➔ Wallets

Blocks

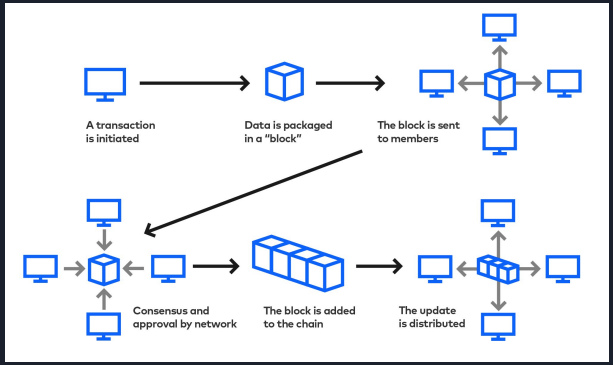
- A block holds a header, a recorded history of transactions, the previous blocks header
- Headers are used as fingerprint identifiers for each block using block header hash
- Transactions stored using Merkle trees
- The root node makes up a portion of the block header
- The previous blocks header allows analysis of both ends of the transaction, in order to maintain a timeline
- Cultivates a ‘Block Chain’





Block Chain

- A decentralized series of blocks (ledger) that record related bitcoin transactions over time
- Blocks (list of records) made up of Parent-Child relationships
- Blockchain is distributed across a network of nodes
- Maintained via consensus mechanism (nodes validate each block)



Wallet

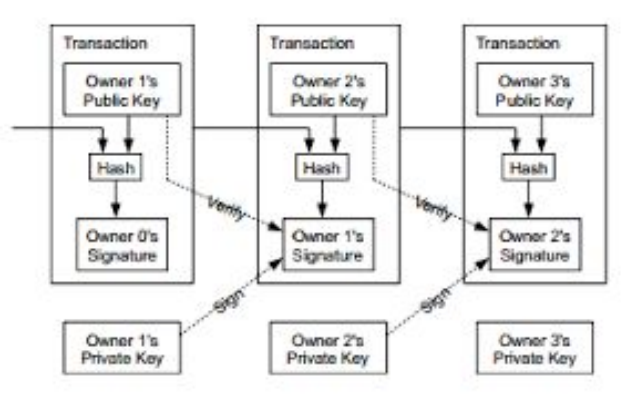
Serves as the UI for transactions, as well as the data structure that manages user key's

UI

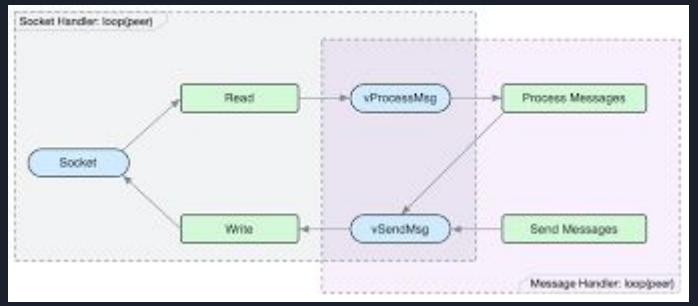
- Interacts with the P2P network via broadcasts and receipts
- Transactions are signed with a user's private key, then broadcasted
- Validated by other nodes in the network

Data Structure

- Consists of private keys and information on how to use them
- Private keys associate with a public address, a unique identifier
- Keeps track of a users transaction history and balance

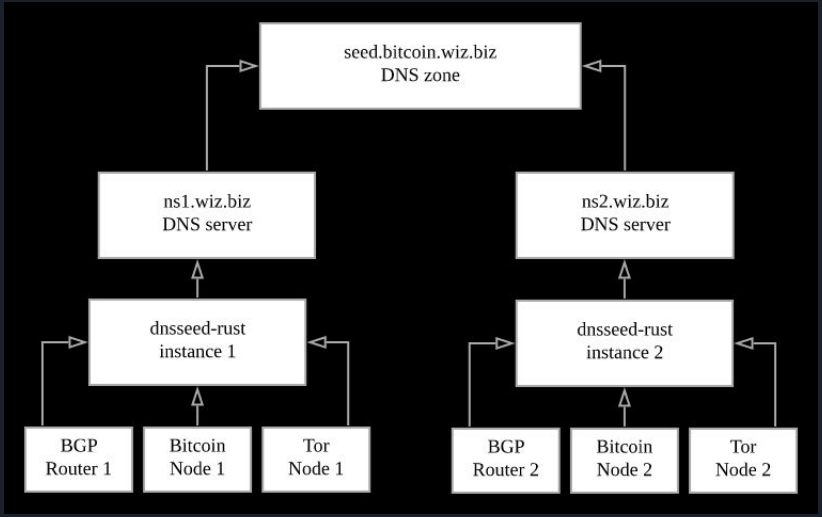


Concurrency



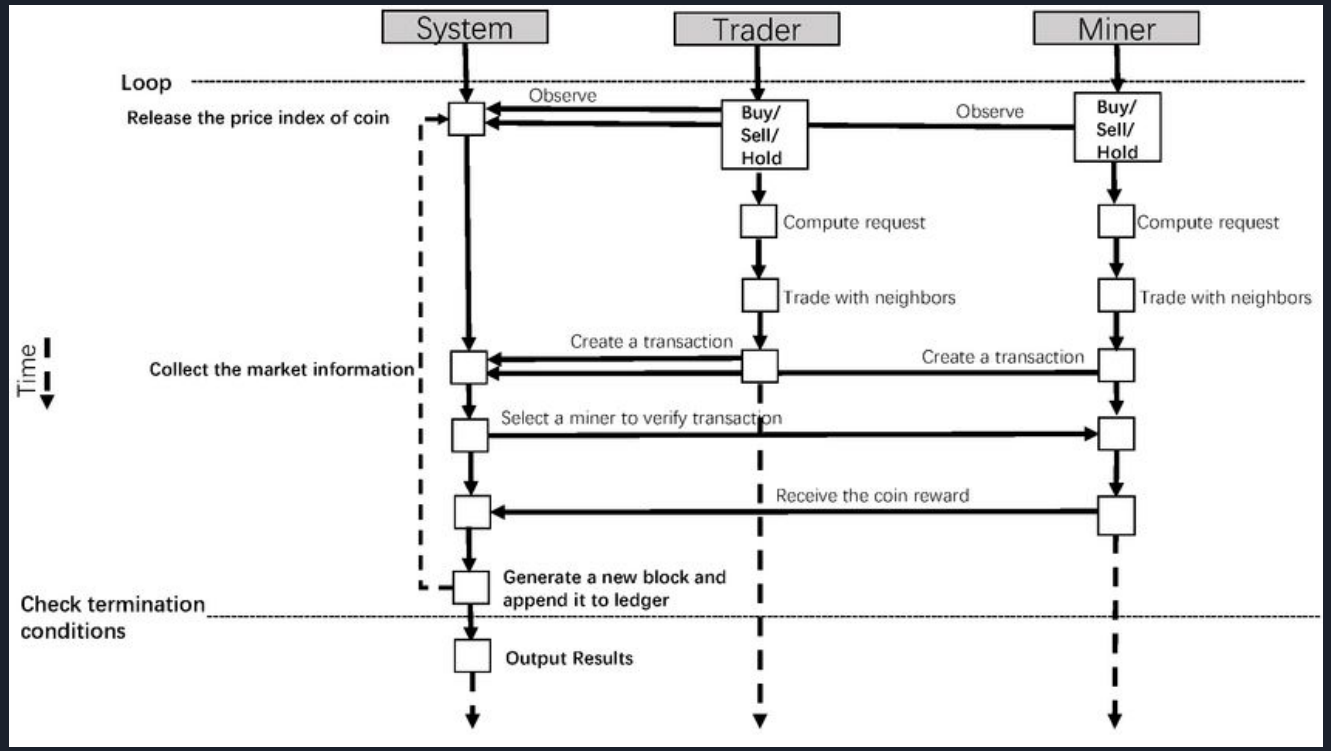
- Each task executed in a thread
- Multithreaded environment with single threaded design
- Utilizes readers writers theorem and mutex locks

➢ ThreadScriptCheck()
➢ m_load_block
➢ ThreadDNSAddressSeed
➢ ThreadSocketHandler

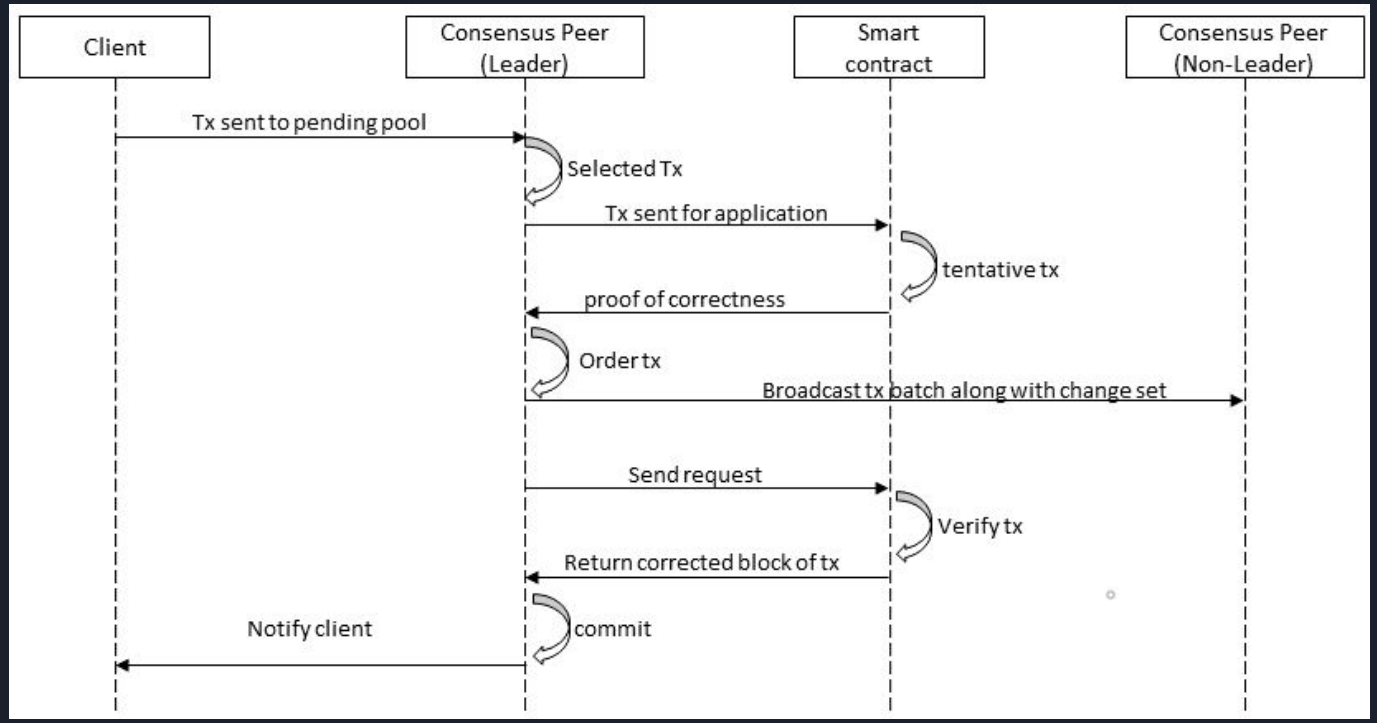


Sequence Diagrams

Use Case 1: Bitcoin mining



Use Case 2: Bitcoin transactions



Lessons Learned

- Online collaboration proved most useful and effective
- Cryptocurrency has a large malicious overhead that needs to be avoided
- Cross-checking sources is vital to accurate research

Conclusion

To Recap

- Bitcoin Core is the technical heart of the bitcoin cryptocurrency scheme
- Uses a P2P architecture to transfer and verify transactions
- Key subsystems include:
  - Blocks (contains list of transactions)
  - Blockchain (public ledger of all transactions)
  - Wallet (software application that allow users to store, manage, and send/receive bitcoins)
- Multithreaded system environment with single threaded architecture

Thank you for listening!