Bitcoin Core

Conceptual Architecture

Presenters: Ethan Davis, Victor Ghosh

Video: https://youtu.be/qc423K7GPB8PB8

Team Members

Ethan Davis

19ead6@queensu.ca

Presenter

Victor Ghosh

18vg5@queensu.ca

Presenter

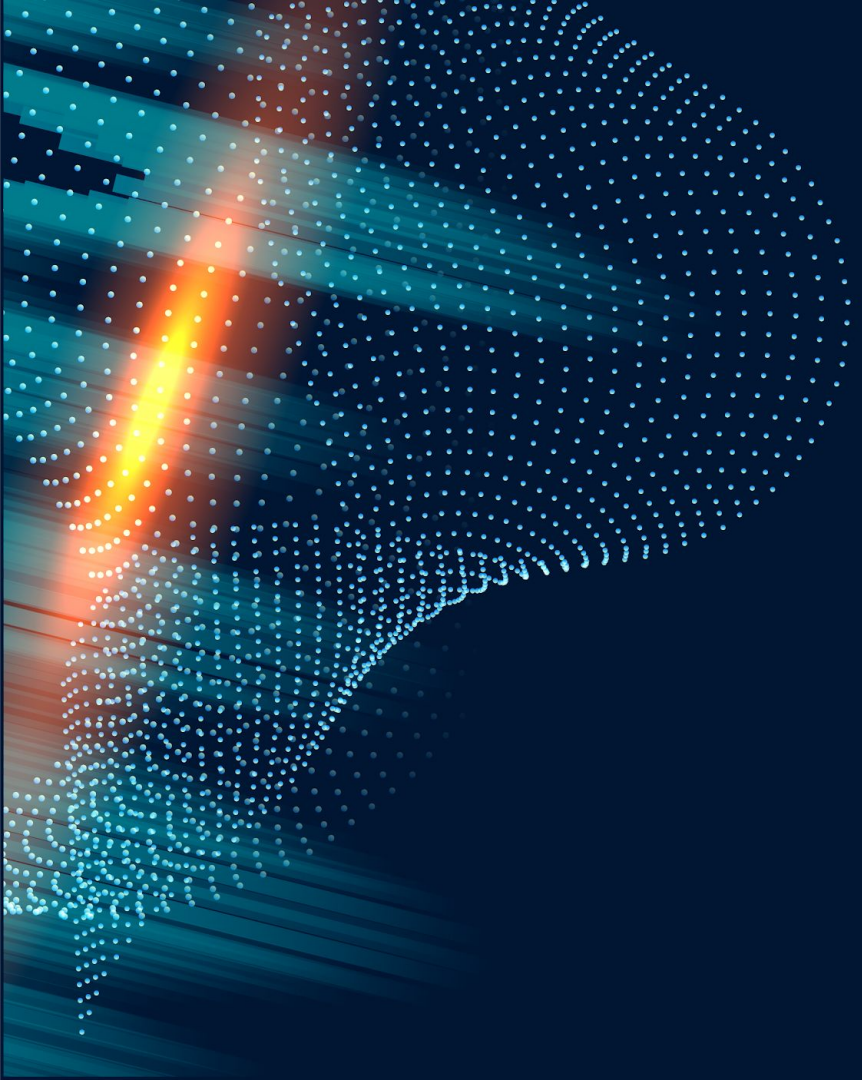
David Shen

19ds71@queensu.ca

Leader

Stefan D'Ippolito

19sadi@queensu.ca



Introduction

What is Bitcoin & Bitcoin Core?

Conceptual Architecture

01

Architecture Style

02

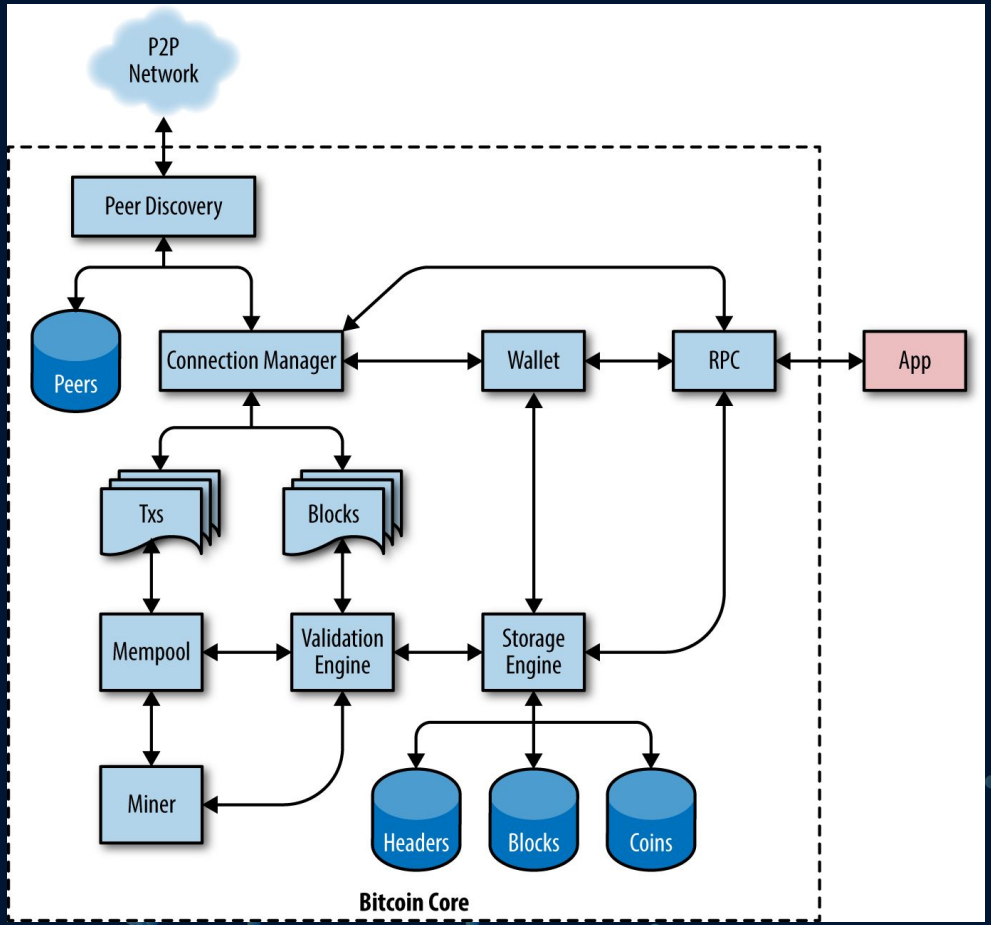
Subsystems

03

Use Cases

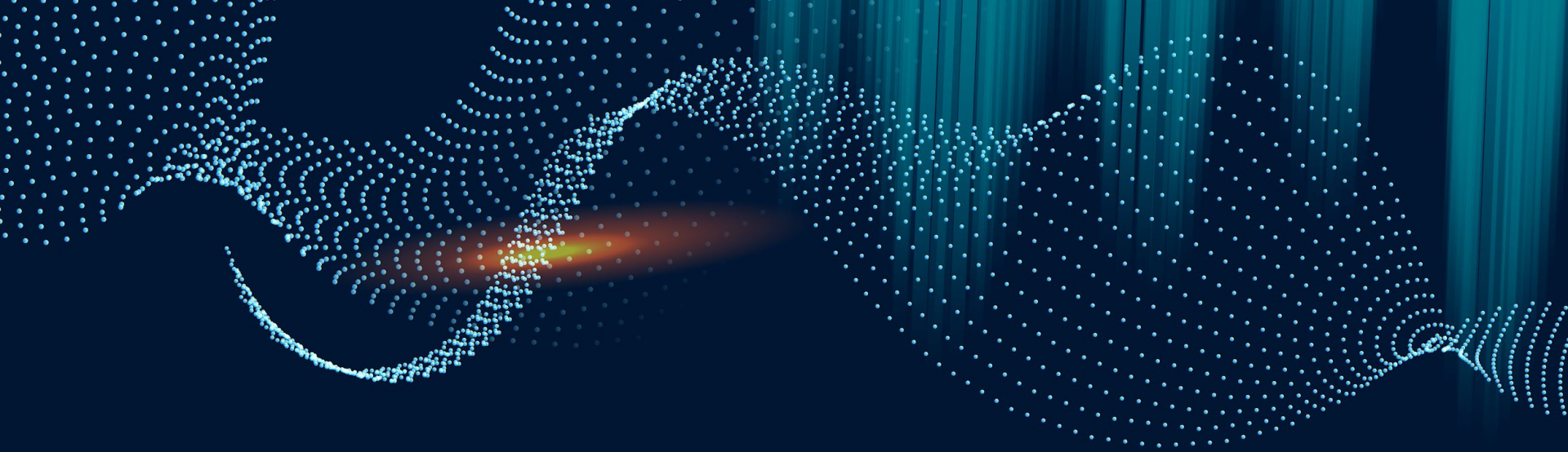
04

Version Control



01

Architecture Style



02 Subsystems

Component Breakdown & Interactions

Peer Discovery & Connection Manager

Peer Discovery

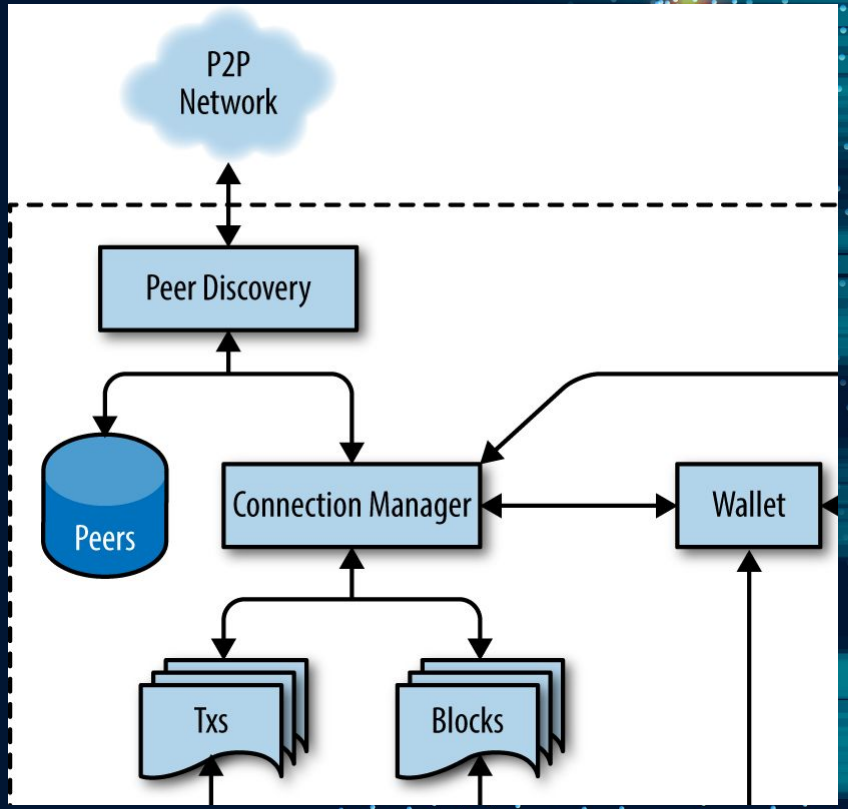
Series of DNS queries

Forward its address to its existing running neighbors rather than relying on a DNS server.

Connection Manager

Keeps address found and moves them to storage

Timestamp of last communication



Wallet & Remote Procedure Call

Wallet

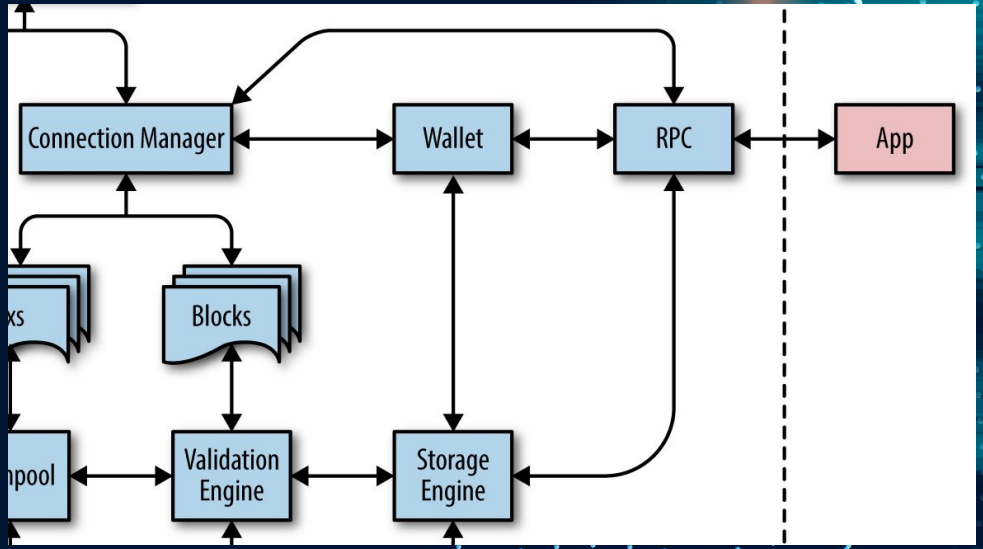
Randomly Generated Private Keys

Now uses deterministic wallet with a master key

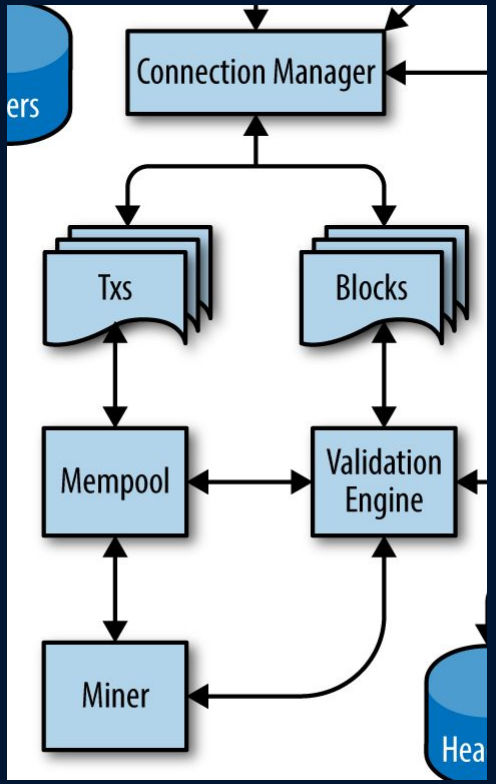
Remote Procedure Call

Interface enables programs and scripts to interact with Bitcoin Core

Varying functionalities



Transactions & Mempool & Miner



Transactions

Record of value transfer between accounts

Requires cryptographic signature

Mempool

After broadcast it is added

Await confirmation from the miner

Miner

Validate transactions taken from Mempool

Compete to solve math problems to be the first to validate

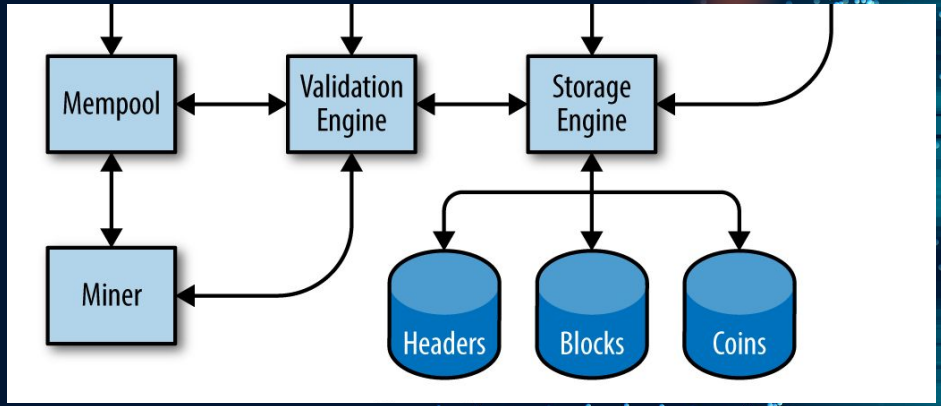
Validation Engine

Responsible for verifying transactions and blocks added to the blockchain

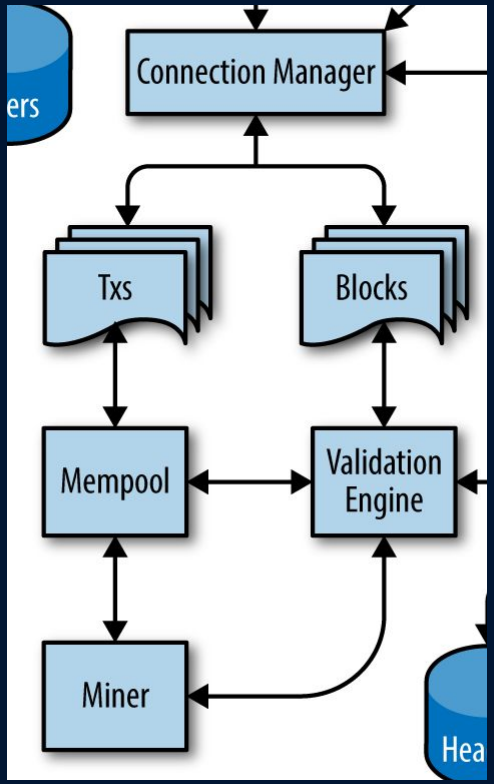
Uses combination of cryptographic techniques, consensus rules, and computational puzzles

Digital signatures and UTXOs are used to maintain security and reliability

Limits on the size of each block



Storage Engine



Responsible for storing and managing the blockchain data

Blockchain data is organized into components, including blocks, headers, and coins.

Uses a levelDB database

Blocks

Collection of transactions that have been verified and added to the blockchain

Headers

Includes block info like: block height, timestamp, and the hash of the block

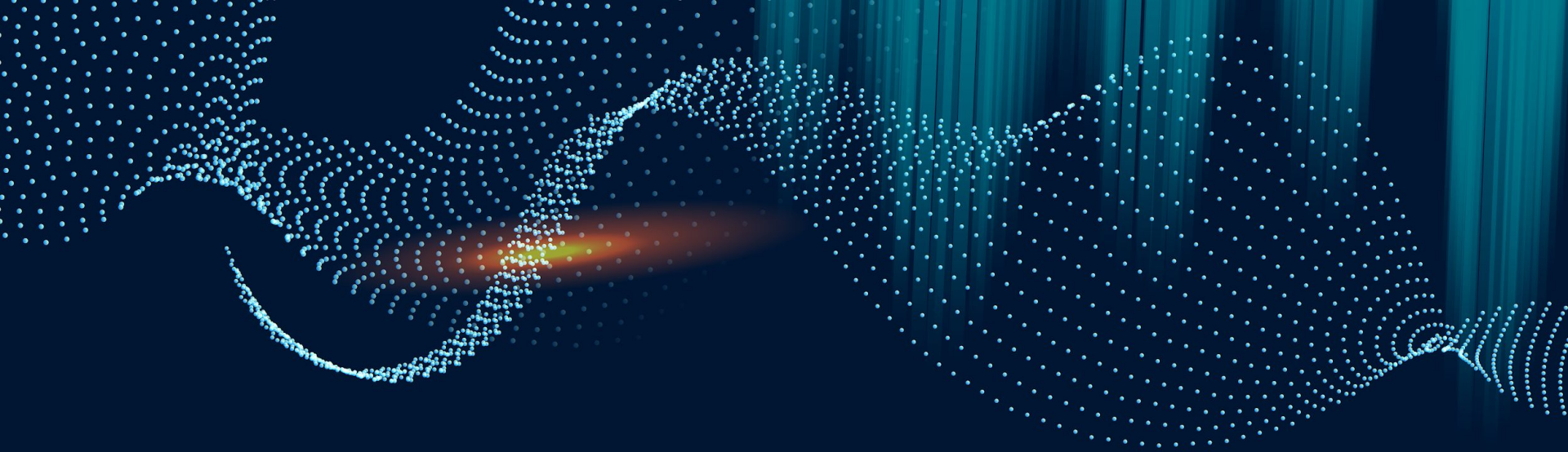
Coins

Represented as UXTO's

UTXO database has info on the transaction output

Data and Control Flow

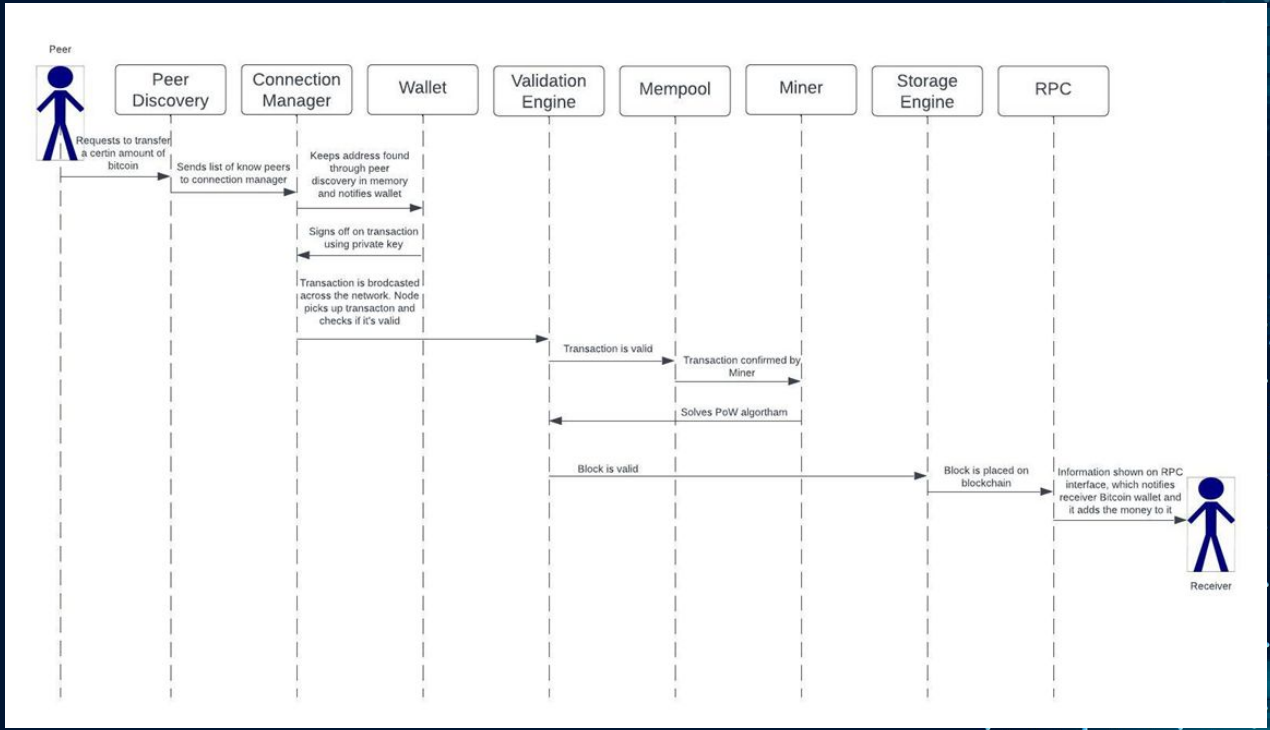
- Transaction Creation
- Transaction Propagation
- Mining
- Block Creation
- Block Propagation
- Validation



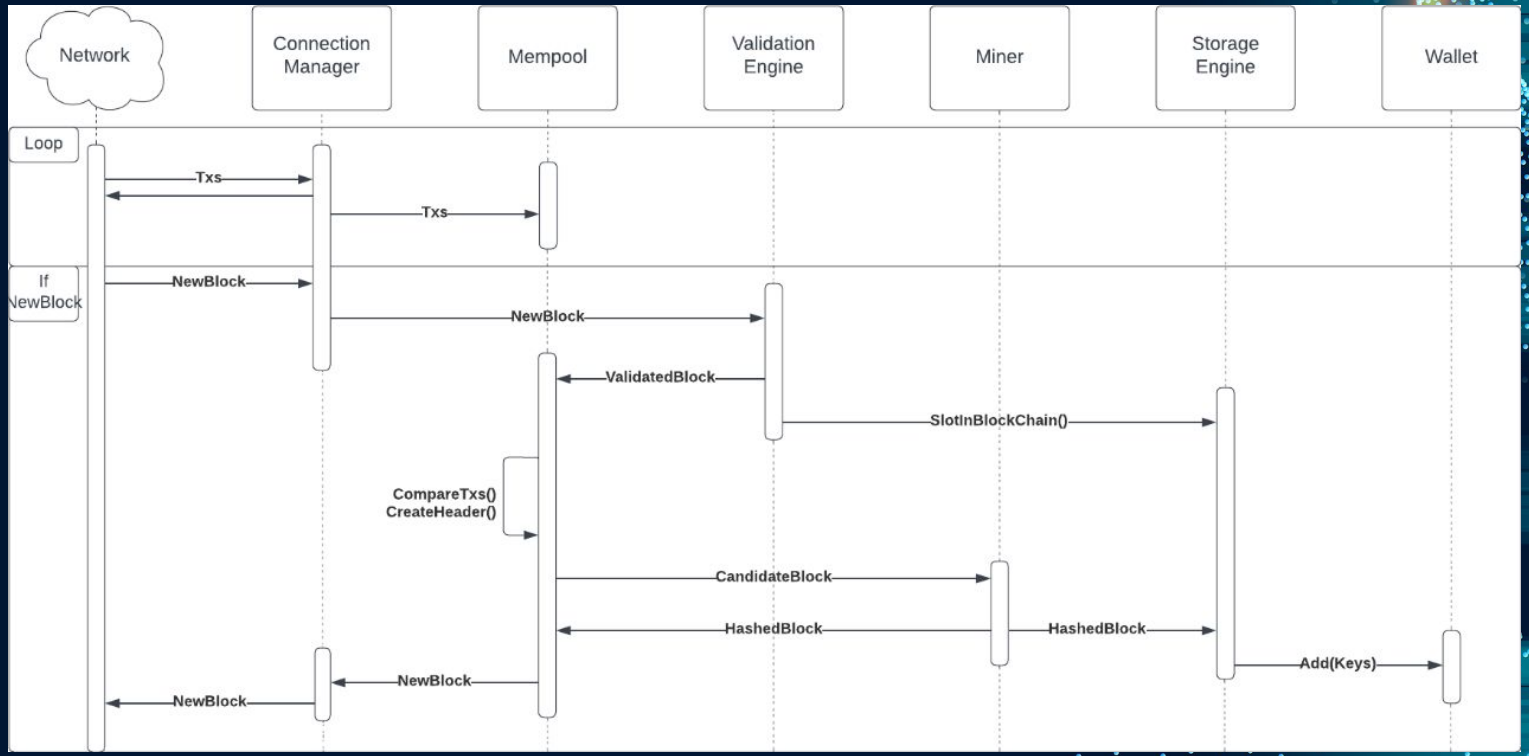
03 Use Cases

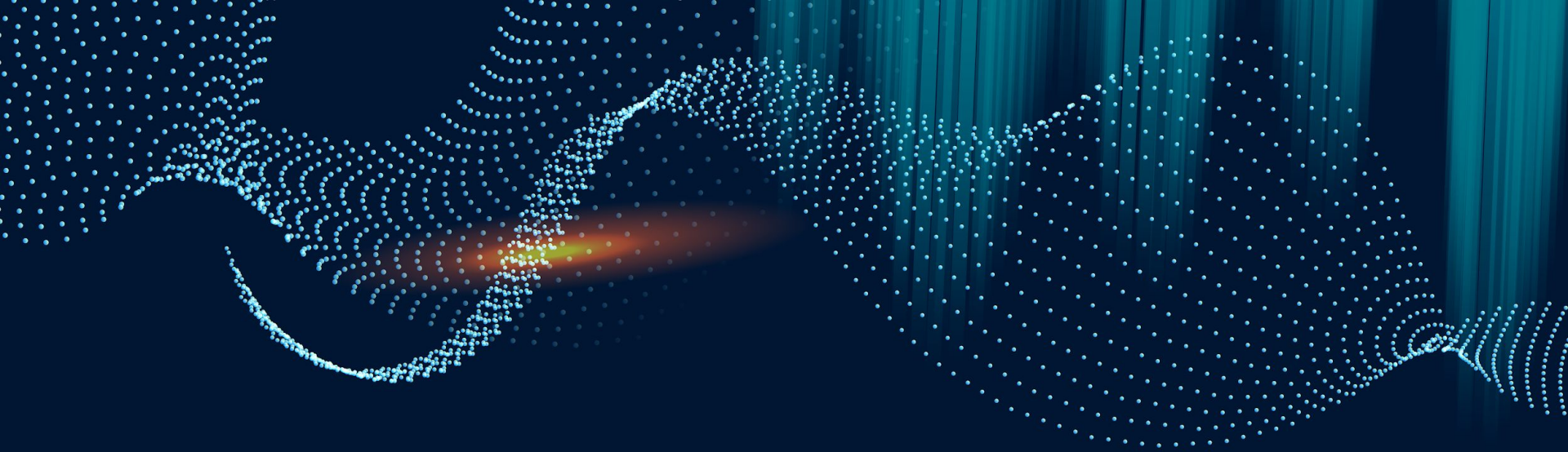
Transaction & Mining

Use Case 1: Transaction



Use Case 2: Mining





04 Version Control

Evolution of Bitcoin Core Software

Early Releases

01

Bitcoin Core 0.1.0

02

Bitcoin Core 0.3.21

03

Bitcoin Core 0.8.0

04

Bitcoin Core 0.12.0

Later Releases

05

Bitcoin Core 0.15.0

06

Bitcoin Core 0.16.0

07

Bitcoin Core 0.18.0

08

Bitcoin Core 0.21.0

Derivation Process

Responsibilities Among Developers

- Builders
- Reviewers
- Testers
- Security

Lessons Learned

Conclusion

Thanks