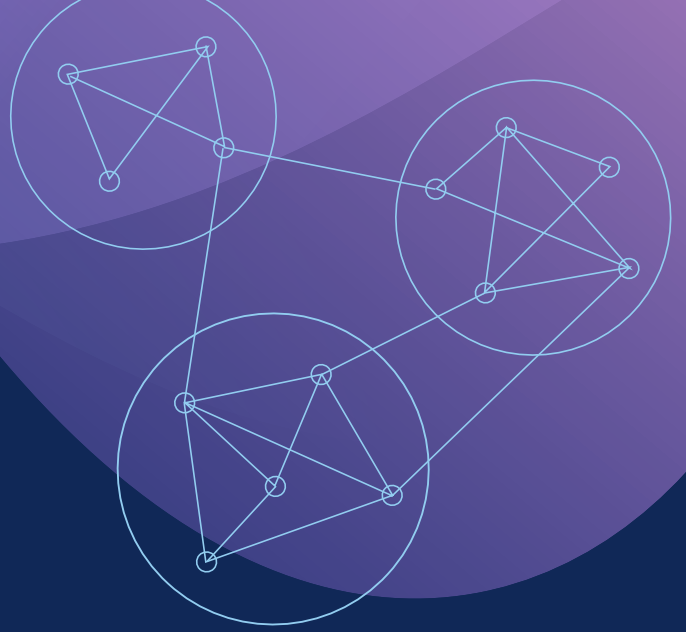
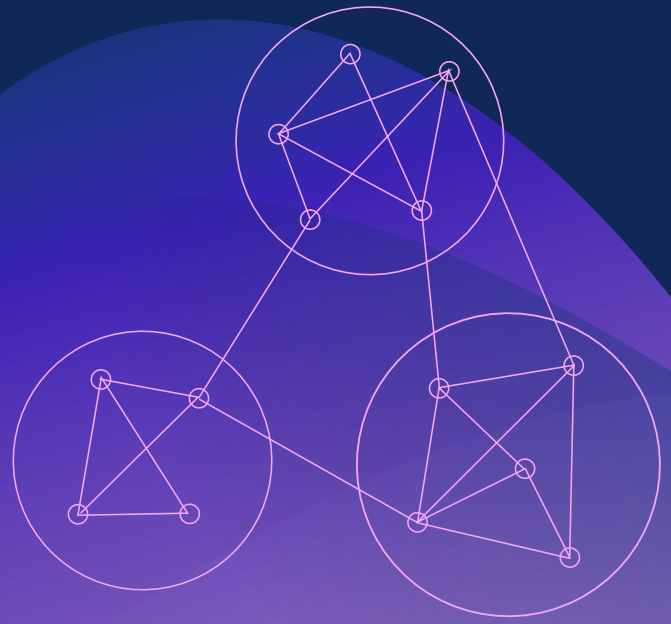


BITCOIN CORE: CONCEPTUAL ARCHITECTURE



A1 – Group 2 – Bit by Bit

https://youtu.be/Fp7sfuogN1Y

PRESENTATION BY:

- Daniella Ruisendaal - Group Leader
- Alina Padoun - Presenter
- Adam Ciszek - Presenter
- Aidan Wolfson
- Camila Izquierdo
- Tanner Big Canoe

WHAT IS BITCOIN CORE?

Bitcoin Core works with the Bitcoin peer-to-peer network, enabling users to validate blocks and transactions

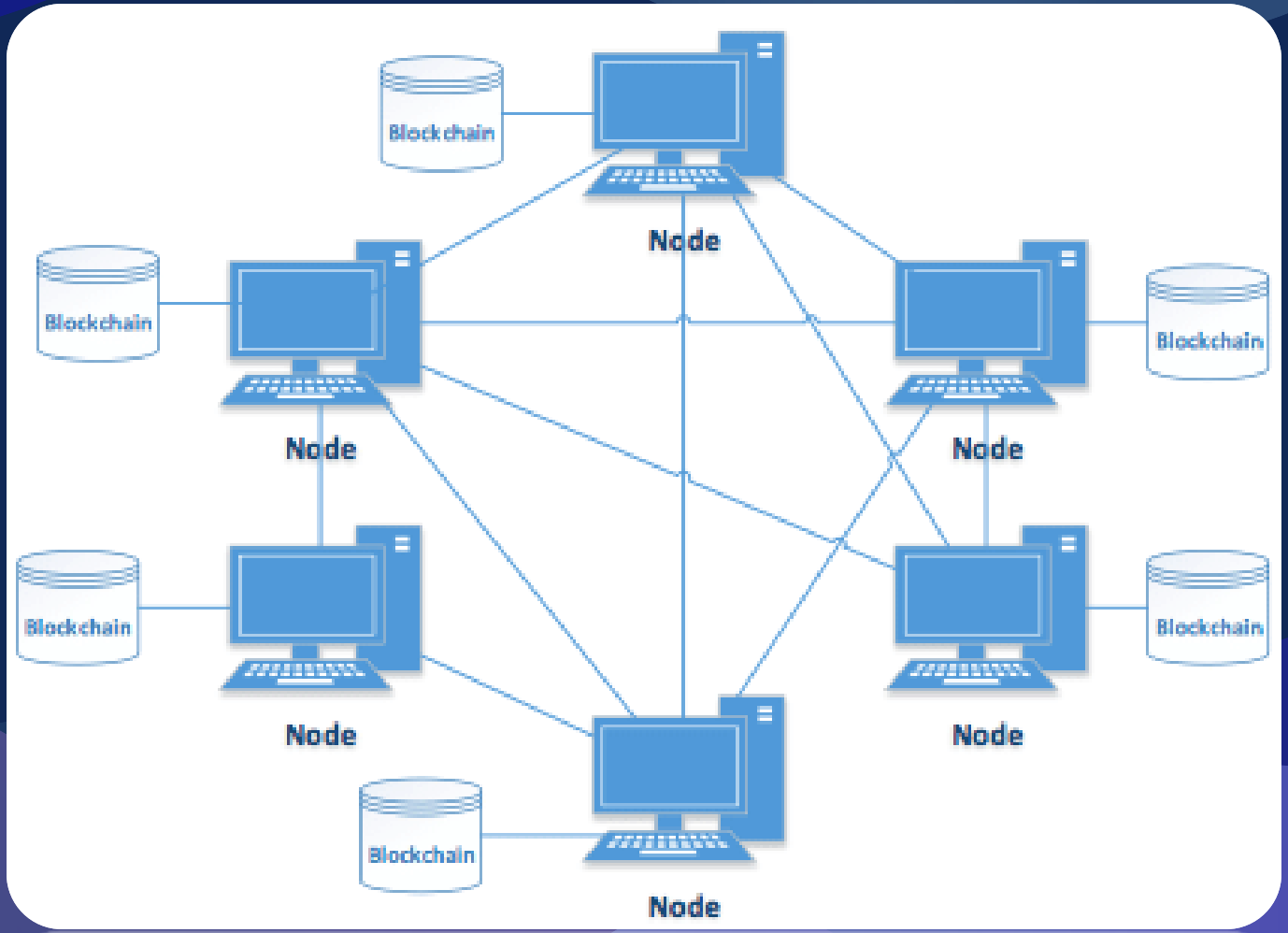
FUNCTIONALITY

- **Blockchain** is a public ledger documenting all transactions
  - Security and double spending prevention
- **Transactions** module is responsible for transferring funds
  - Public and private keys
- **Contracts** are sub-modules of transactions, enforcing financial agreements
- **Wallets** create public keys necessary to make transactions

FUNCTIONALITY(CONTINUED)

- **Payment processing** module handles the transfer of funds from payer's to payee's wallet
- **Operating modes** refer to level of security needed to verify the blockchain
- **P2P network** provides decentralized structure in which all the nodes (aka peers) support the network
  - Downloads and broadcasts the blockchain
- **Mining** is the process of solving cryptographic hash puzzles to verify new blocks and add them to the blockchain ledger

ARCHITECTURE STYLE: PEER-TO-PEER NETWORK

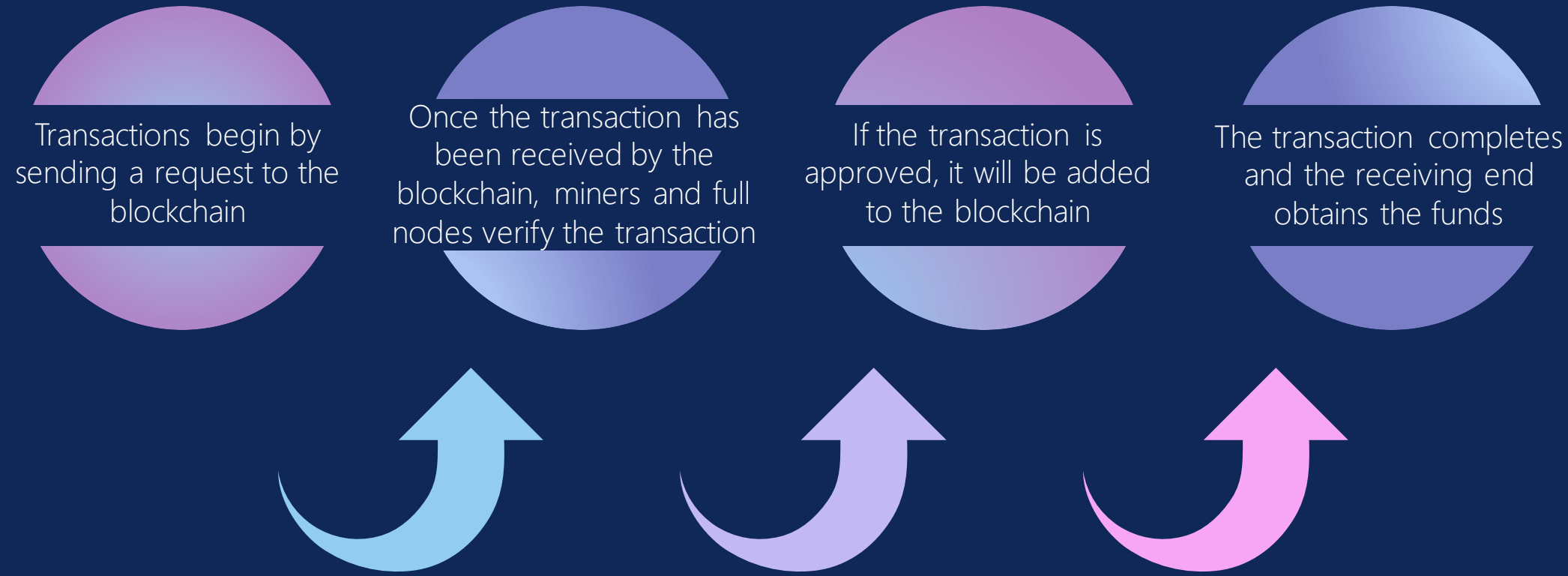


SYSTEM EVOLUTION

- P2P allows for high level of both evolvability and scalability
- Bottleneck to scalability prevents Bitcoin from ever reaching the transactions per second (tps) of businesses like Visa
  - 1700 tps vs 4.6 tps

CONTROL AND DATA FLOW

Users can request and receive funds to create transactions amongst peers:



CONCURRENCY

- Concurrency is achieved by using **multiple threads and locks** guarding shared data structures
- Many functions require grabbing the **"global lock"**, forcing other threads to wait and hindering parallelism
- Users can have separated wallets running concurrently
- **Decentralized structure** can support a large amount of concurrent connections
- Per user the default settings limit the number of concurrent connections to other peers in order to control traffic.

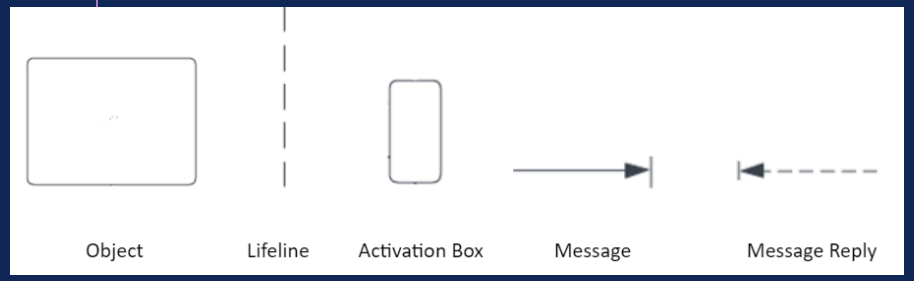
IMPLICATIONS OF DIVISION

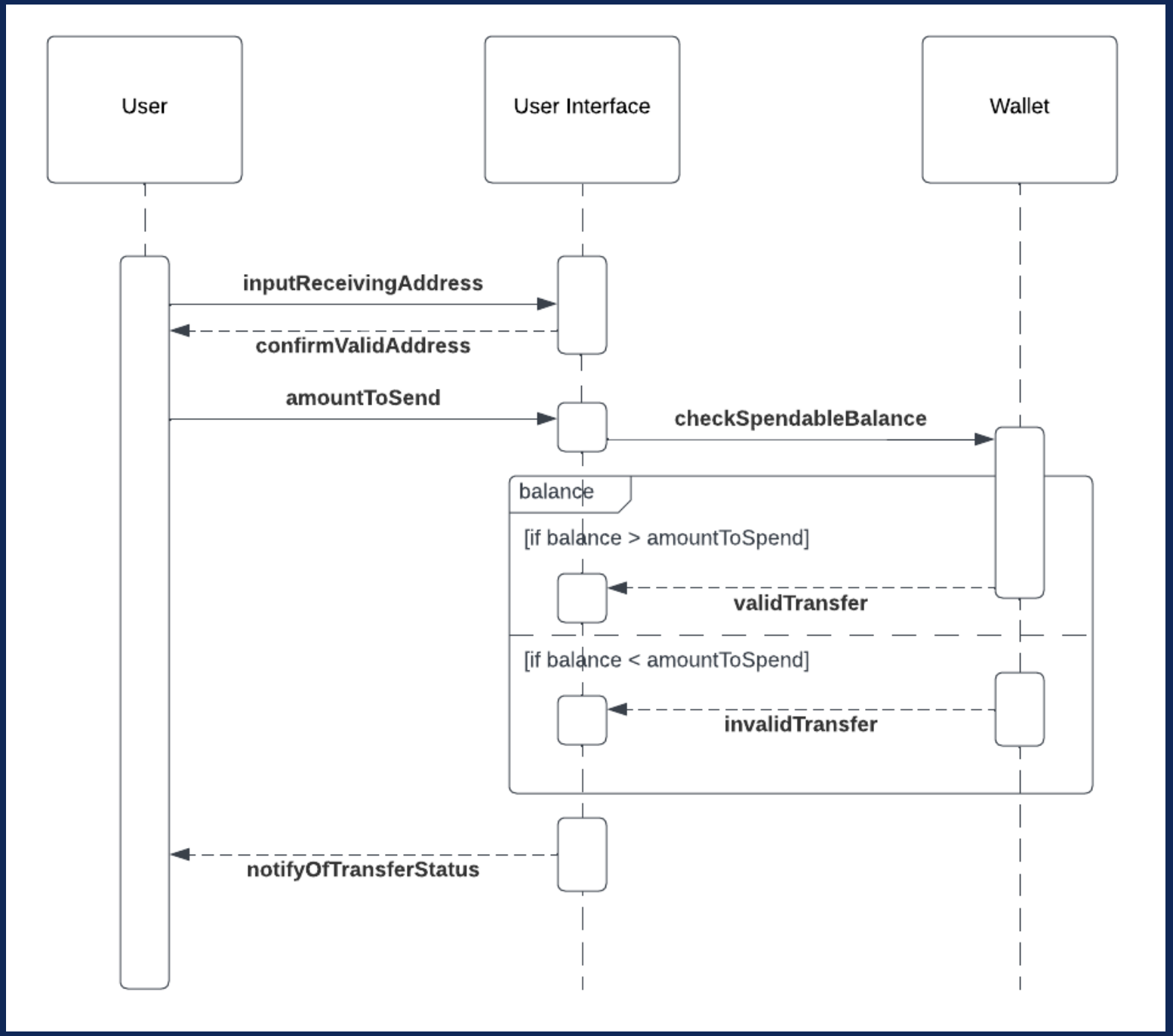
- Open-source and all about collaboration
- Small group of developers who can access the code for Bitcoin directly, limiting damage
- Fluctuation in number of developers working on Bitcoin Core
- Multiple levels of protection in place to keep the code safe:
  - Commit keys
  - Verify-commits

SEQUENCE DIAGRAM

Use Case 1:

User A wants to send Bitcoin over to user B.

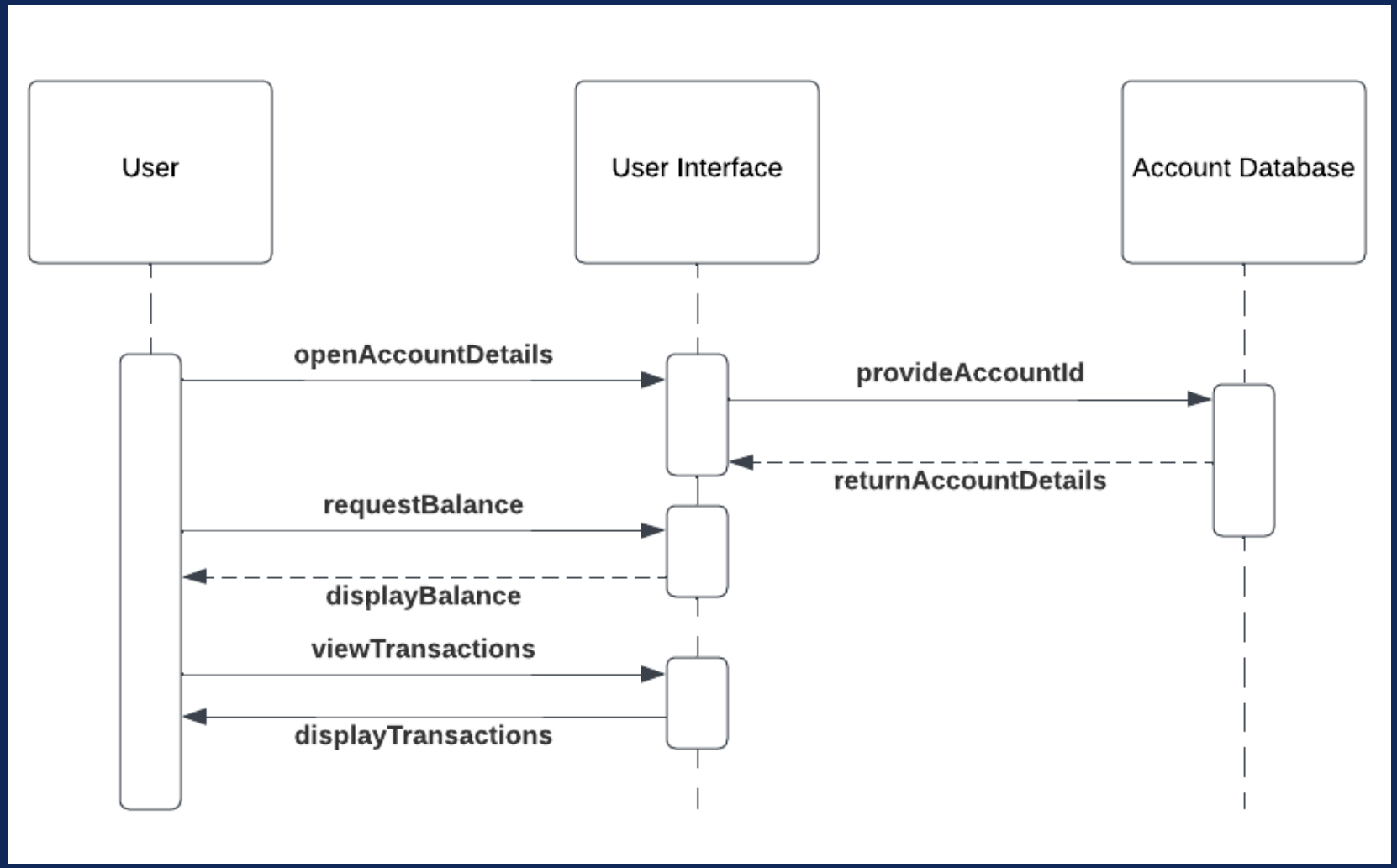


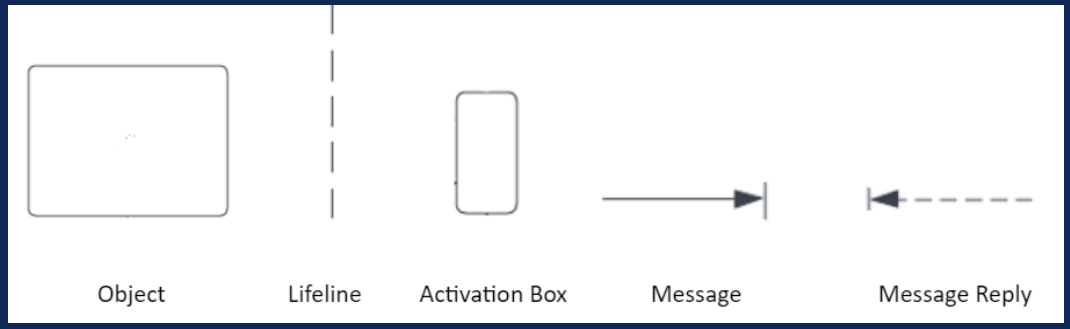


SEQUENCE DIAGRAM

Use Case 2:

User checks their balance or transactions.





USE CASE 3: MINING

Step 1

Open up the wallet in Bitcoin Core

Step 2

Navigate to the Console tab

Step 3

Start mining by entering console command

Step 4

Stop mining by entering console command

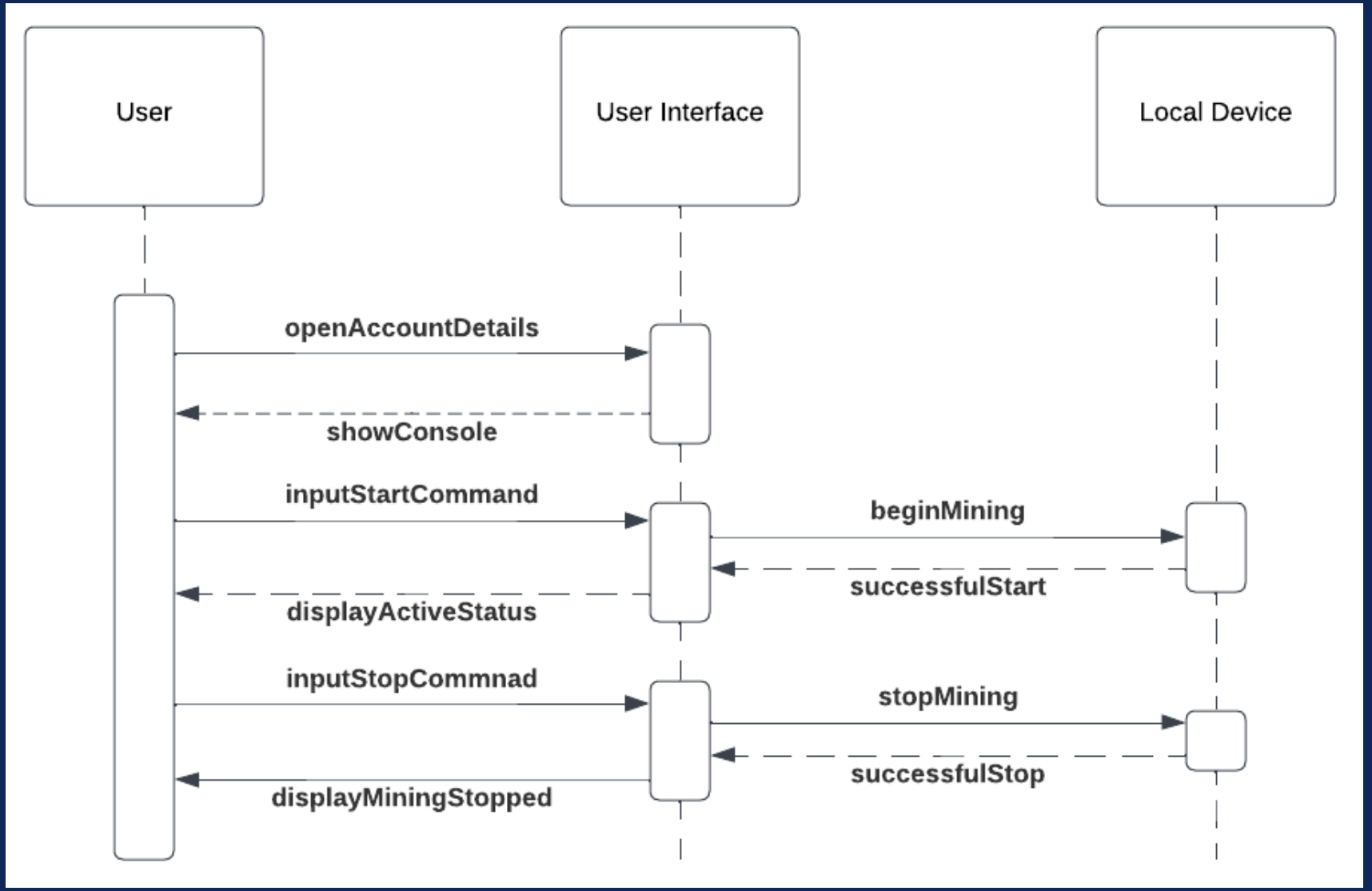
Step 5

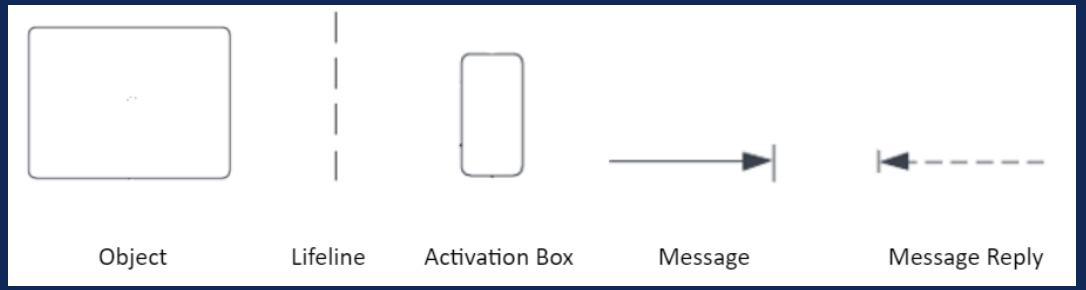
Repeat as necessary

SEQUENCE DIAGRAM

Use Case 3:

User mines Bitcoin on their device.





CONCLUSION