

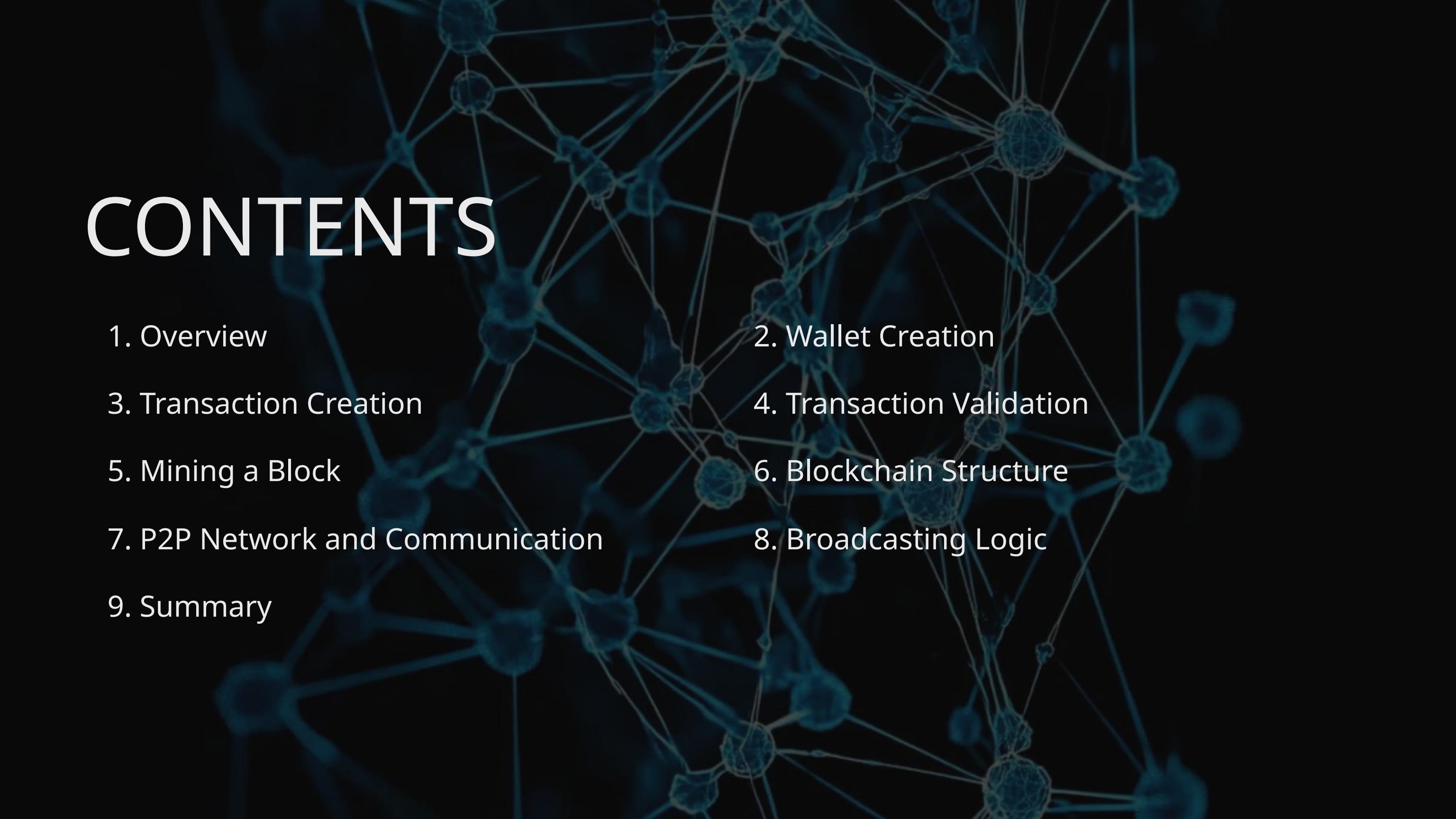
Blockchain-based Peer-to-Peer Network in Python

Author: Pi

Date: 2025.XX.XX

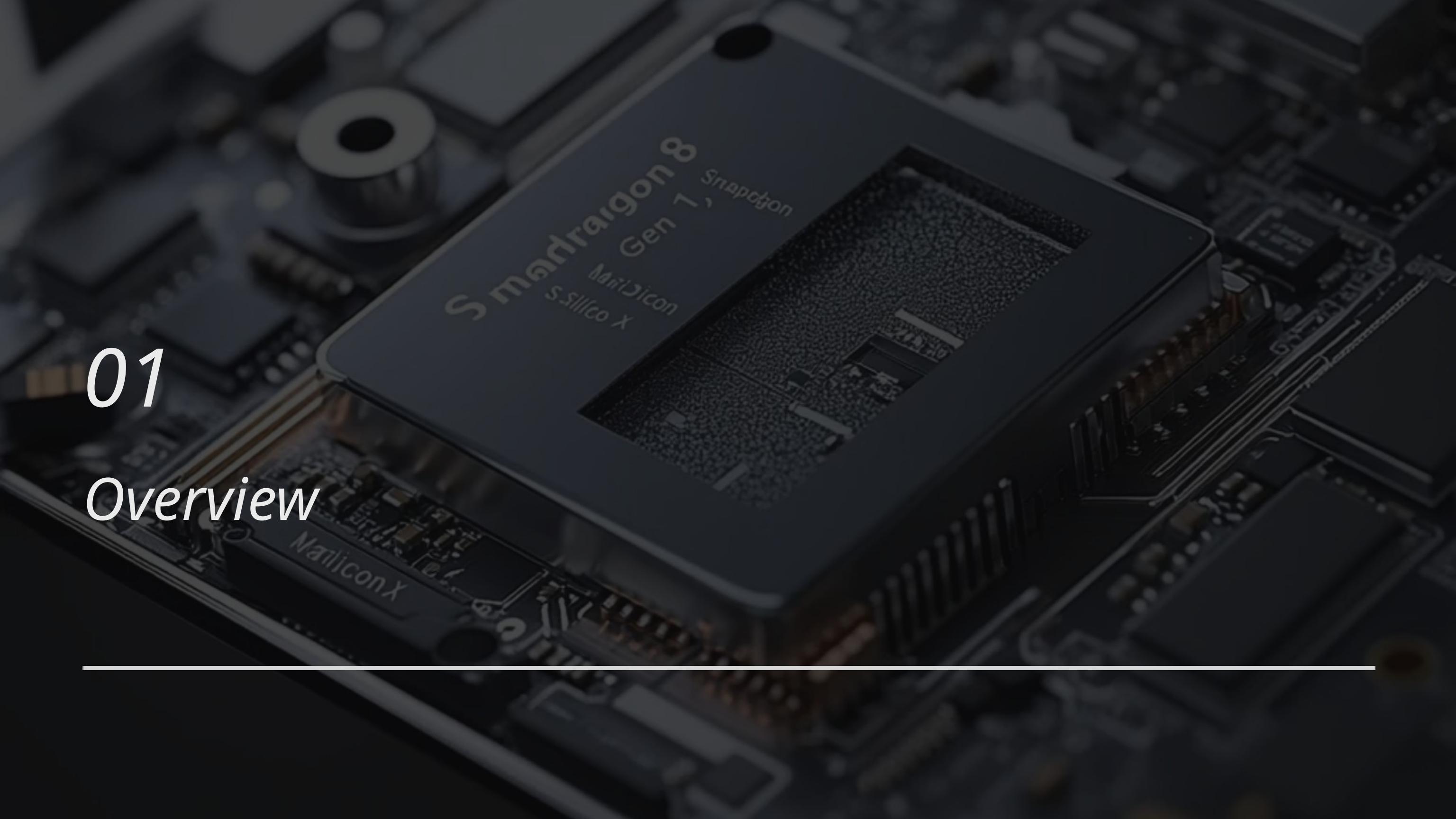


CONTENTS

- 
1. Overview
 2. Wallet Creation
 3. Transaction Creation
 4. Transaction Validation
 5. Mining a Block
 6. Blockchain Structure
 7. P2P Network and Communication
 8. Broadcasting Logic
 9. Summary

01

Overview



Goal

Implement a simplified blockchain system with:

- Wallet creation using public/private keys
- Transactions between peers
- Block creation through mining
- Peer-to-peer broadcasting of blocks



02

Wallet Creation



Purpose

Each user has a unique identity via cryptographic keys.

Logic

Generate ECDSA (Elliptic Curve Digital Signature Algorithm) key pair.

- Public key: shared for identification.
- Private key: used to sign transactions.



Data

private_key and public_key (in hex format).

03

Transaction Creation



Purpose

Represent value transfers between wallets.



Logic

A transaction includes sender, recipient, and amount.

Sender signs the transaction using their private key to prove authenticity.

Data

sender, recipient, amount, signature.



04

Transaction Validation

amaster

Transaction Validation

1 Purpose

- Ensure that only legitimate transactions are included.

2 Logic

- Verify that the signature matches the transaction content using sender's public key.

3 Flow

- Get sender's public key.
- Use it to verify the signature of the transaction.

05

Mining a Block



Purpose

Secure the network and create new blocks.

Logic

Use proof-of-work to find a nonce such that the block hash starts with certain zeros.

Include valid transactions in the block.



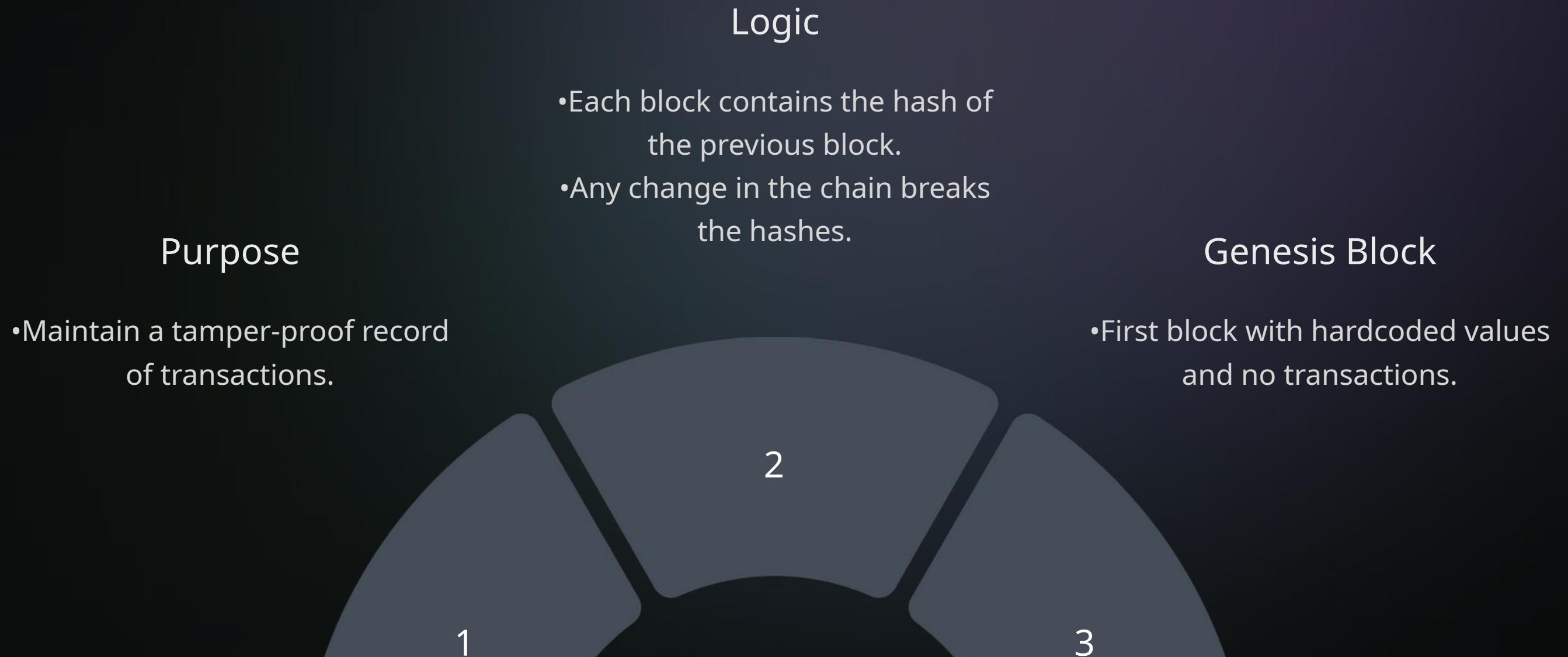
Data in a Block

index, timestamp, transactions, previous_hash, nonce, hash.

06

Blockchain Structure

Blockchain Structure





07

P2P Network and Communication

Purpose

Ensure decentralized communication between peers.



Logic

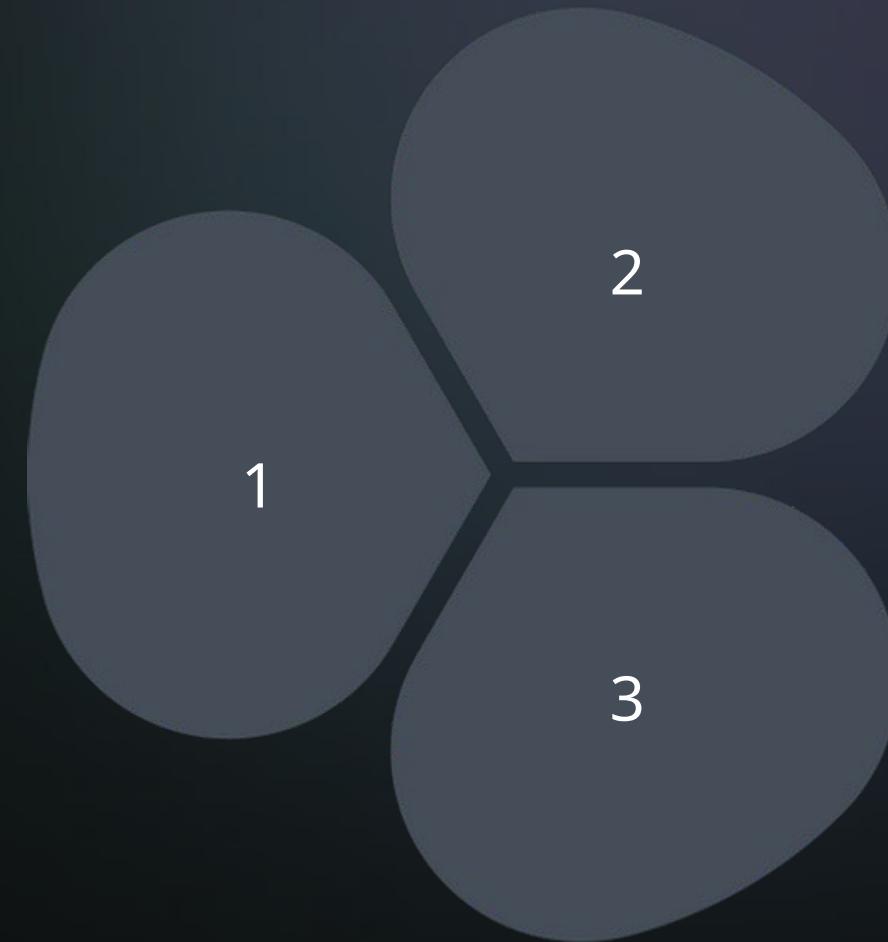
Flask server exposes endpoints to:

- Get blockchain
- Submit new transactions
- Broadcast newly mined blocks



Flow

Node mines a block.



Node sends it to other peers via
HTTP POST.

Peers validate and add to their
chain.

08

Broadcasting Logic





Purpose

Synchronize blockchain across all nodes.

Logic

After mining a block:

- Broadcast it to all peers.
- Peers validate and add it to their chain if valid.



Functions Used

`broadcast_block()`, `receive_block()`.



09

Summary

Summary

Users create wallets using cryptographic keys.



Blocks are broadcasted and validated across a decentralized network.

Transactions are signed and verified.

Blocks are mined with proof-of-work and include validated transactions.



Thank You