INTRODUCTION, BLOCKCHAIN TECHNLOGIES

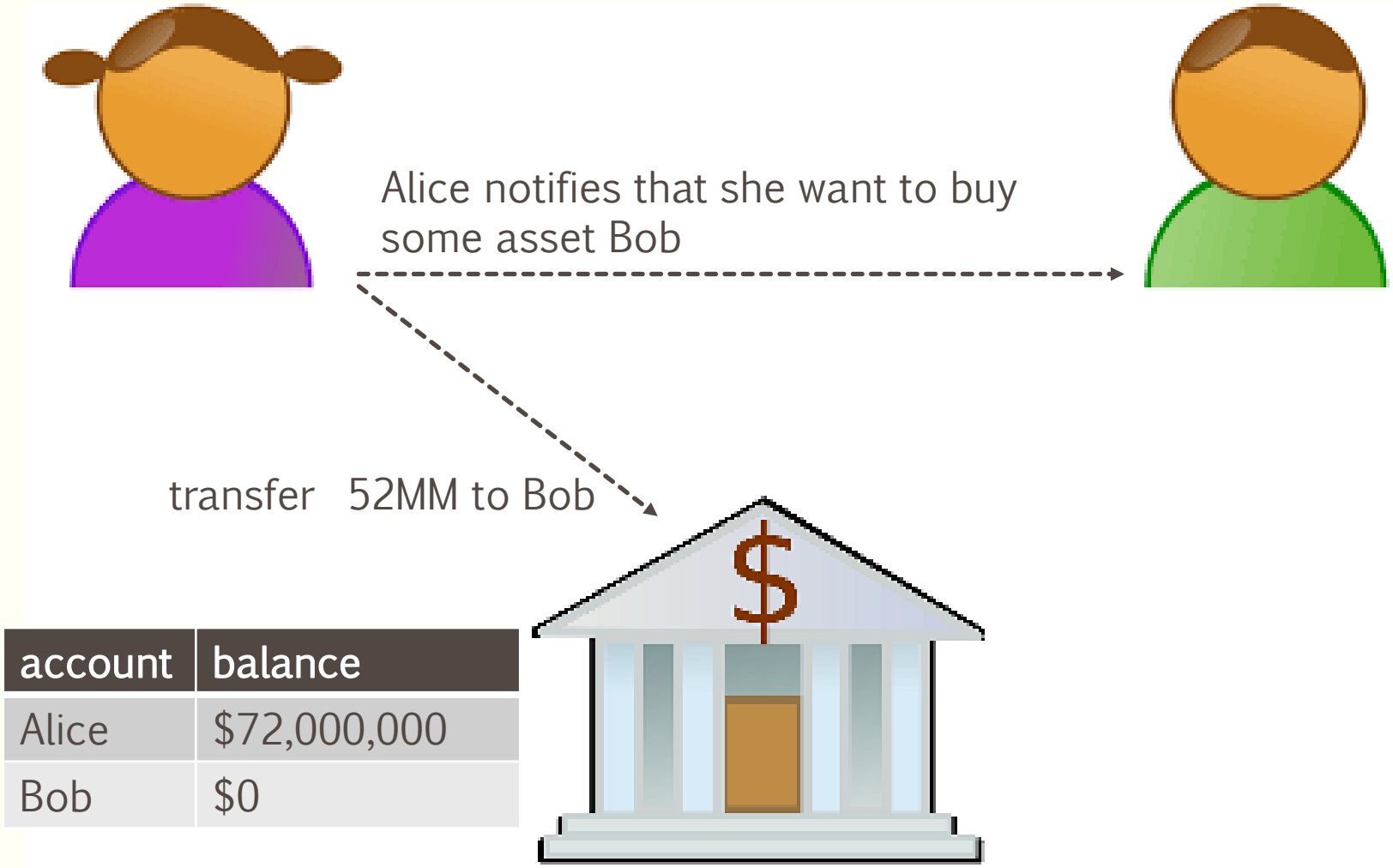
lecture 1

Course overview

- What is a blockchain and how it works
- Blockchain characteristics
- Applications of blockchain technologies *WEB3*
- Types of blockchains

BLOCKCHAIN

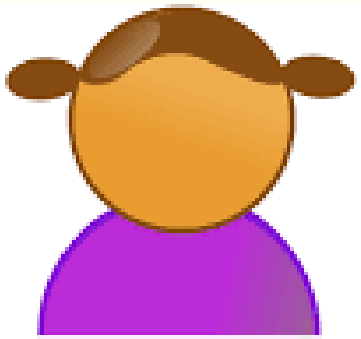
What is a blockchain/how it works



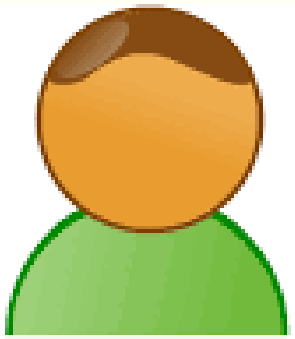
account	balance
Alice	$72,000,000
Bob	$0

traditional payments
and
cryptographic hash functions

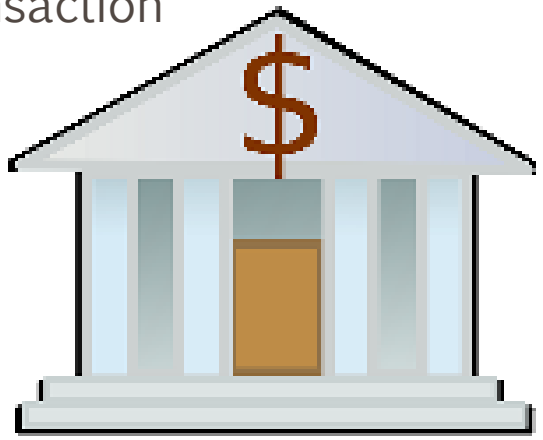
plain text is encrypted using cipher to generate a hash value of fixed length



Bob check his balance ...



Bank validates transaction



account	balance
Alice	$72,000,000
Bob	$0

traditional payments

and

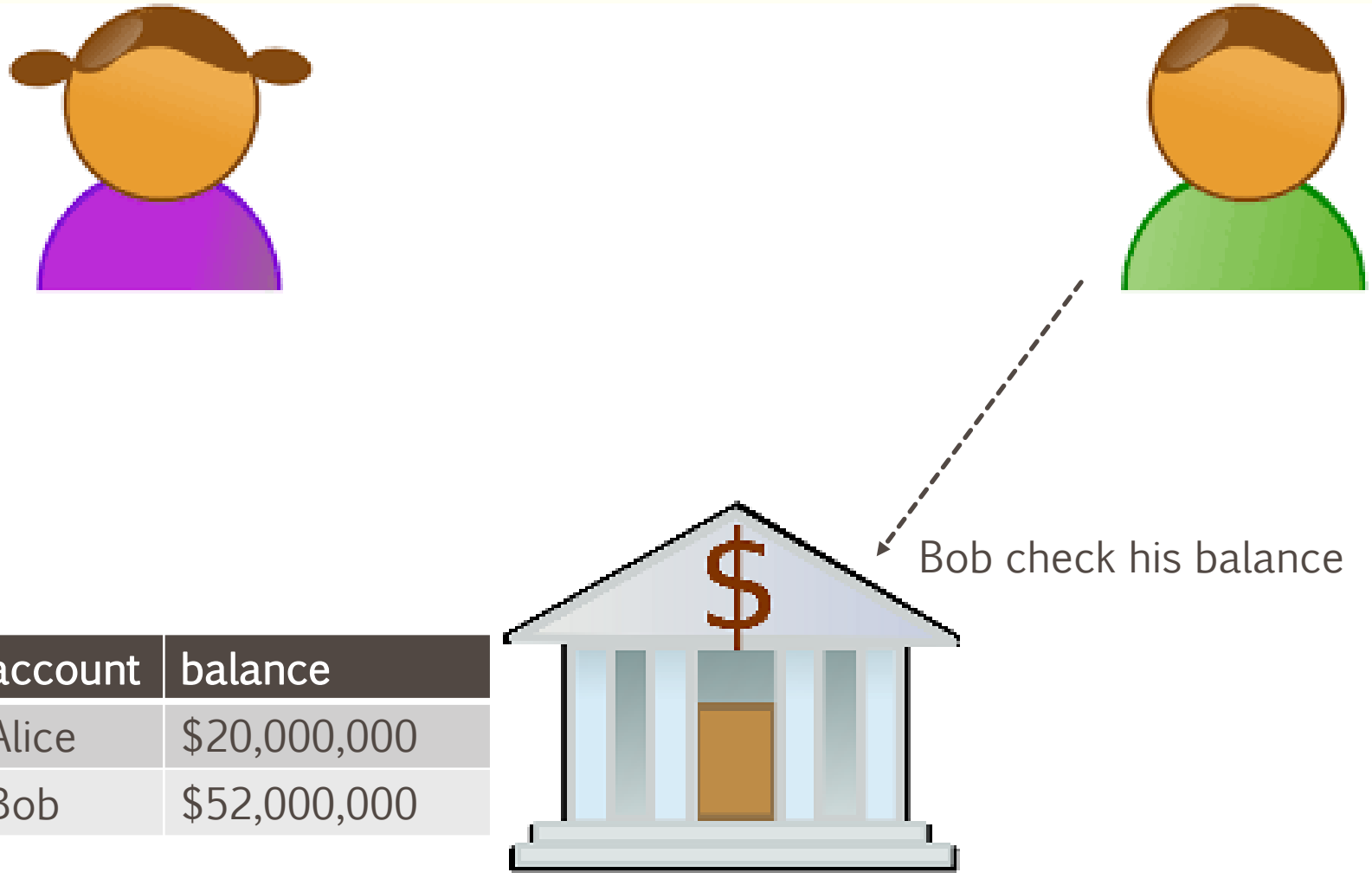
cryptographic hash functions

plain text is encrypted using

cipher to generate a hash

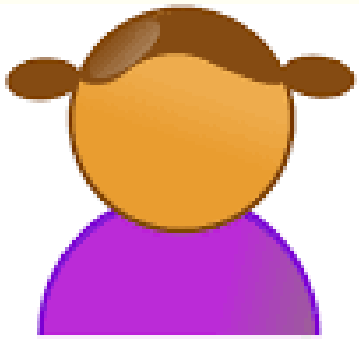
value of fixed length

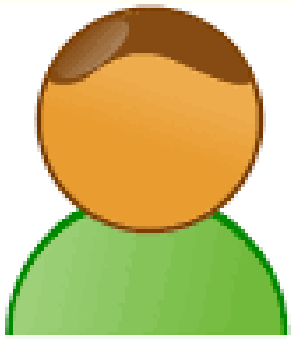
traditional payments



account	balance
Alice	$20,000,000
Bob	$52,000,000

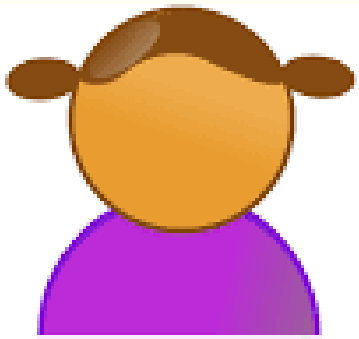
traditional payments



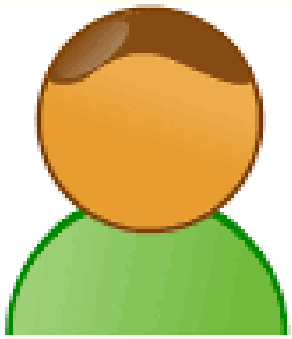


Bob sends “asset”

account	balance
Alice	$20,000,000
Bob	$52,000,000



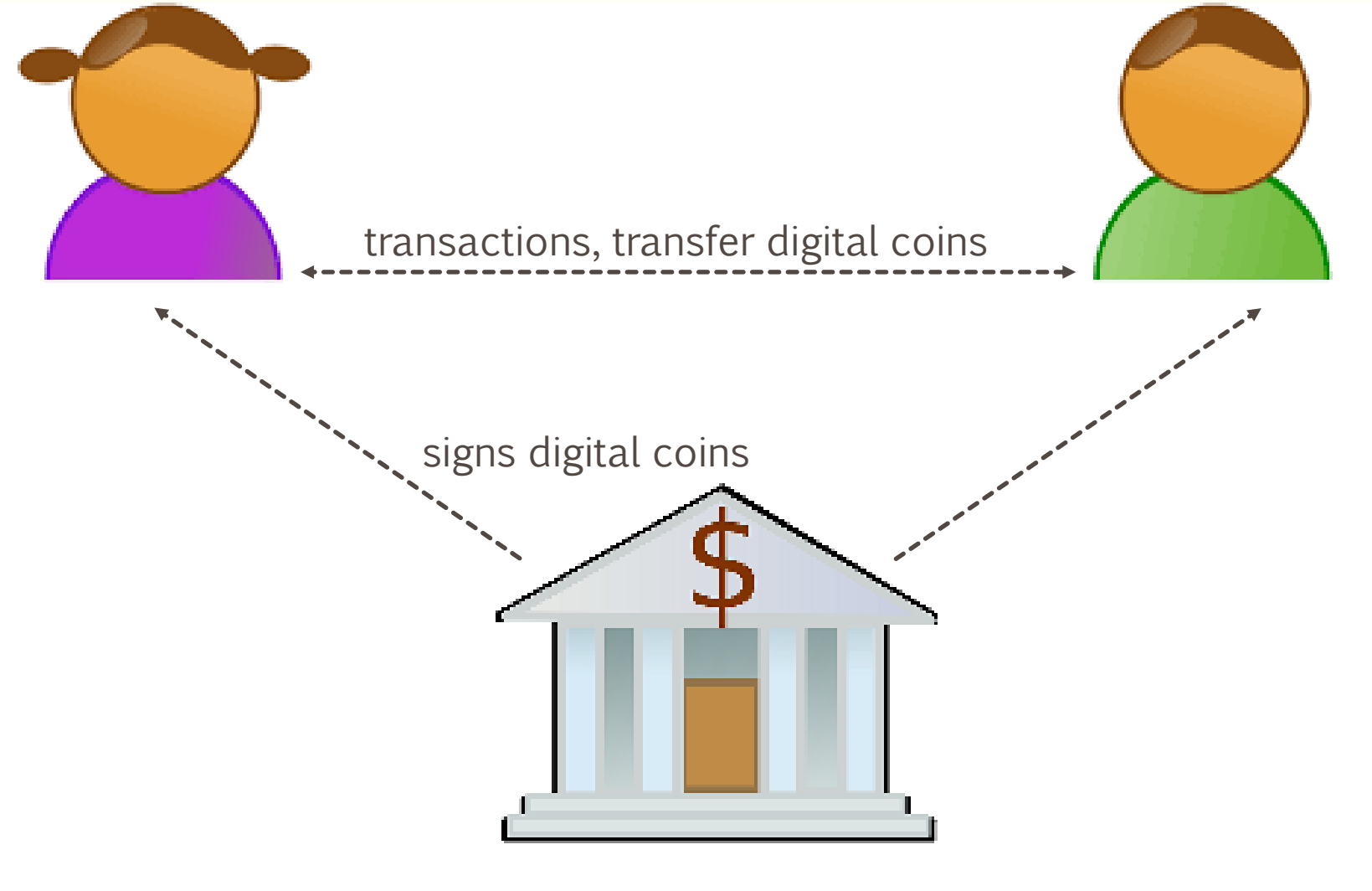
Bob sends “asset”



account	balance
Alice	$20,000,000
Bob	$52,000,000

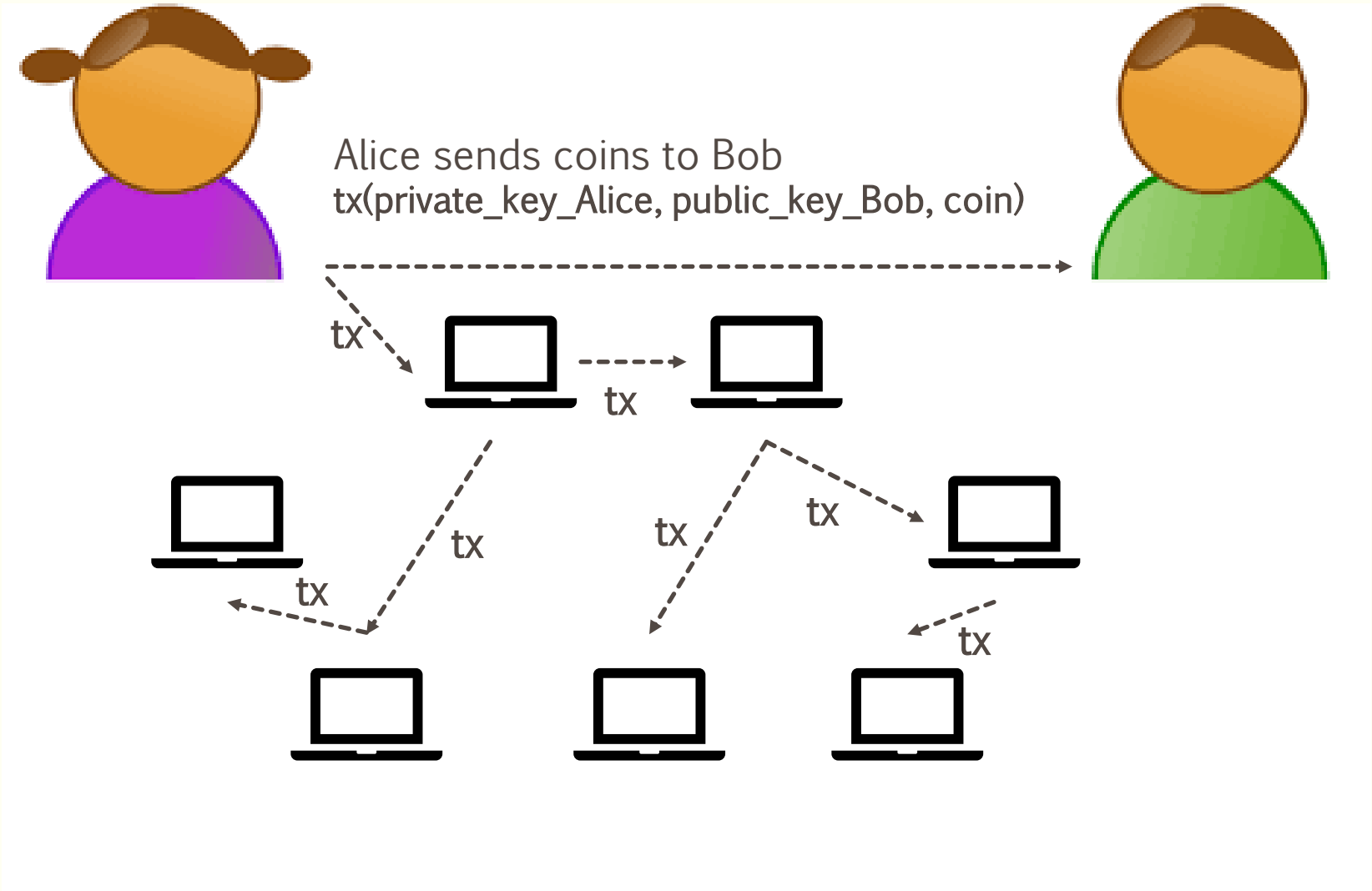
traditional payments

- Single point of failure.
- Delayed or refused transactions.
- Security
- Privacy issues.



Digital currencies

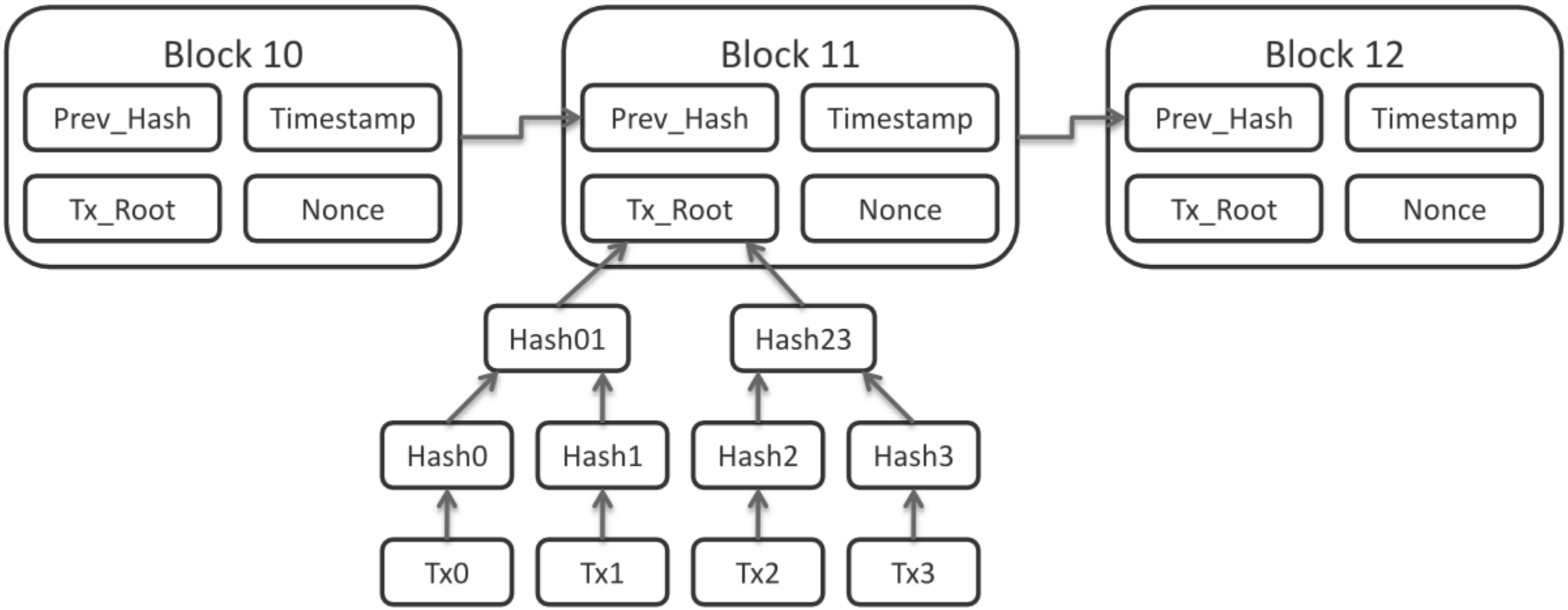
- Easy to implement
- Double spending detection.

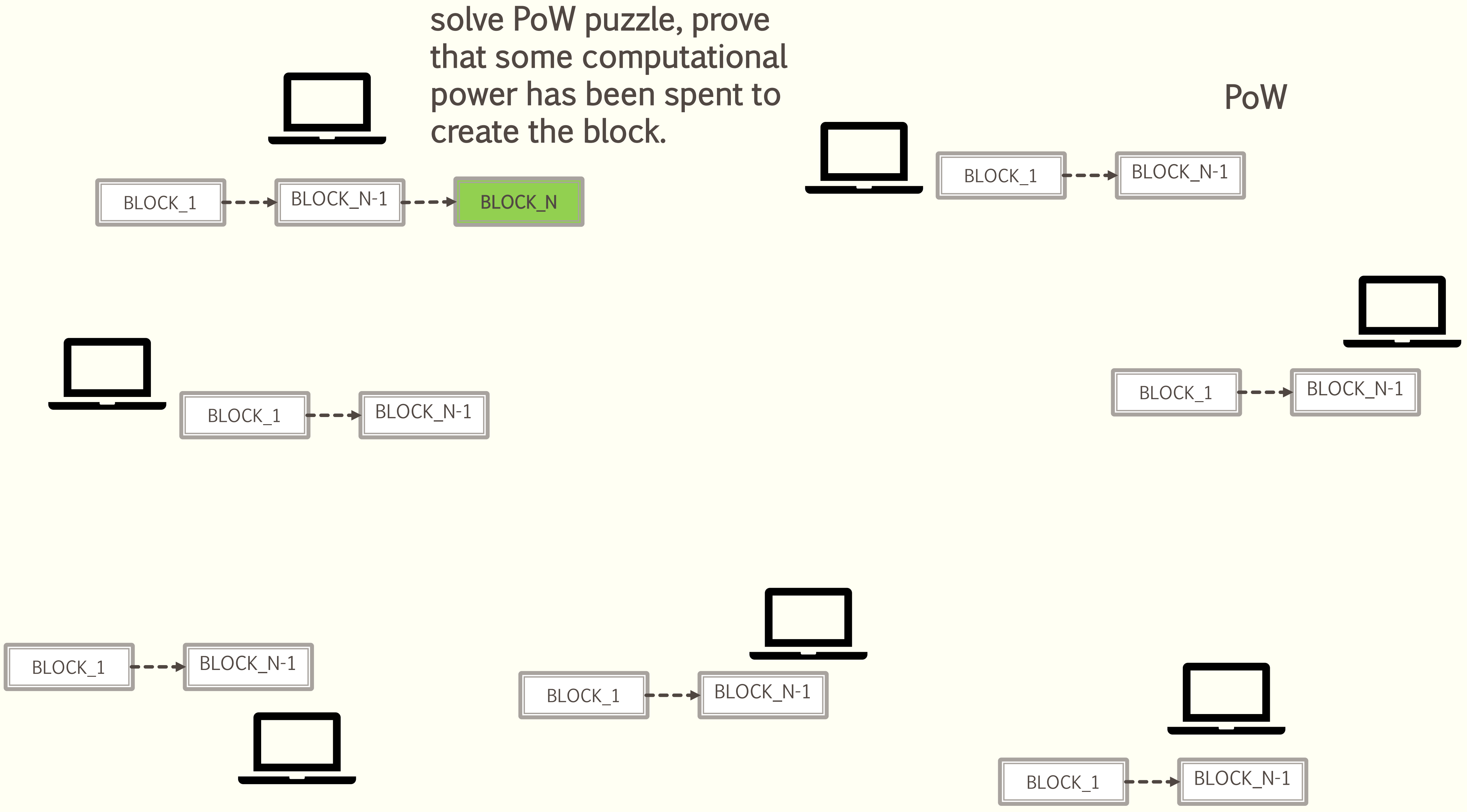


Blockchain

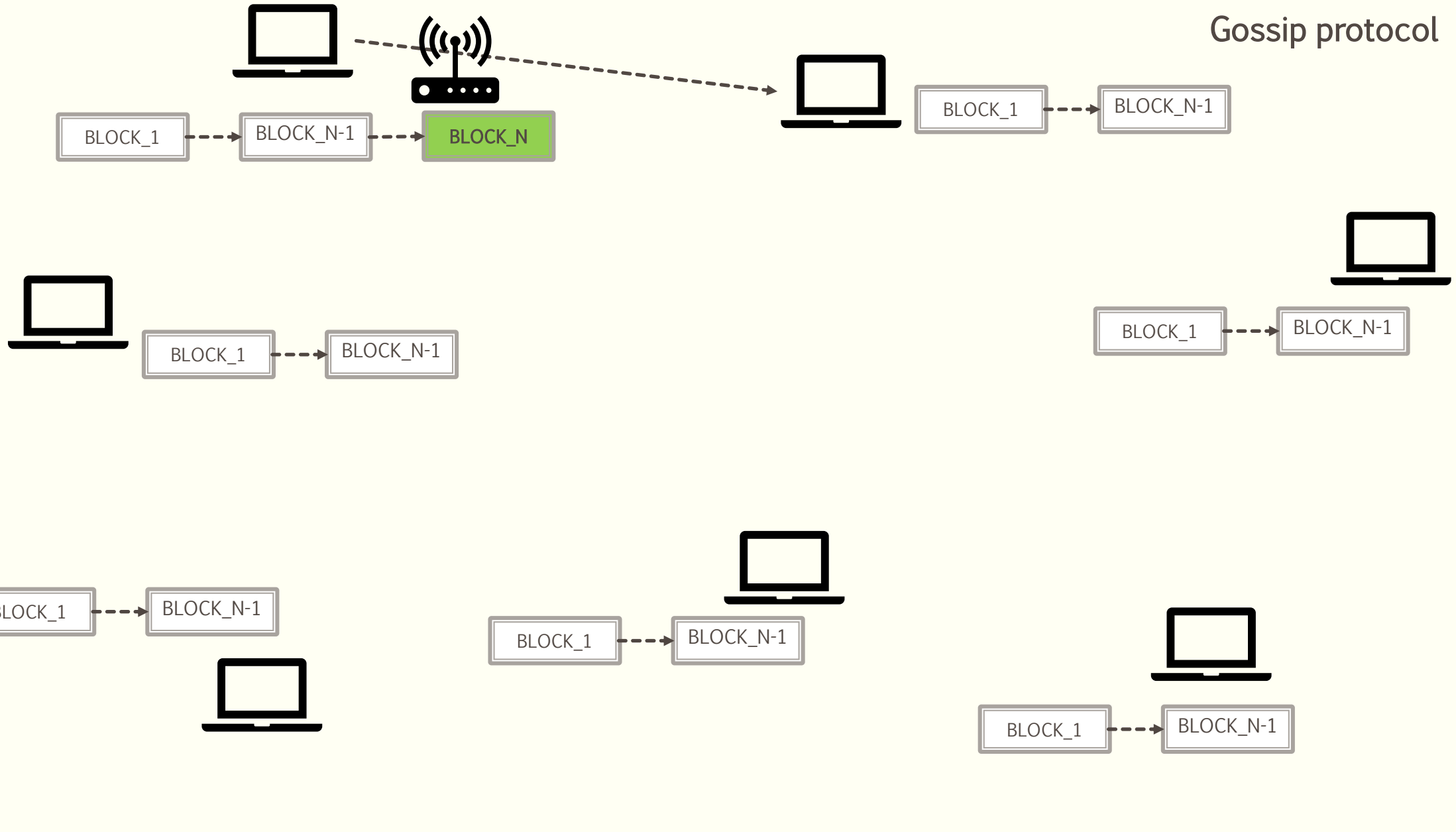
- P2P network
- Sender signs transaction
- Nodes exchange messages about transactions.
- All nodes store all transactions.

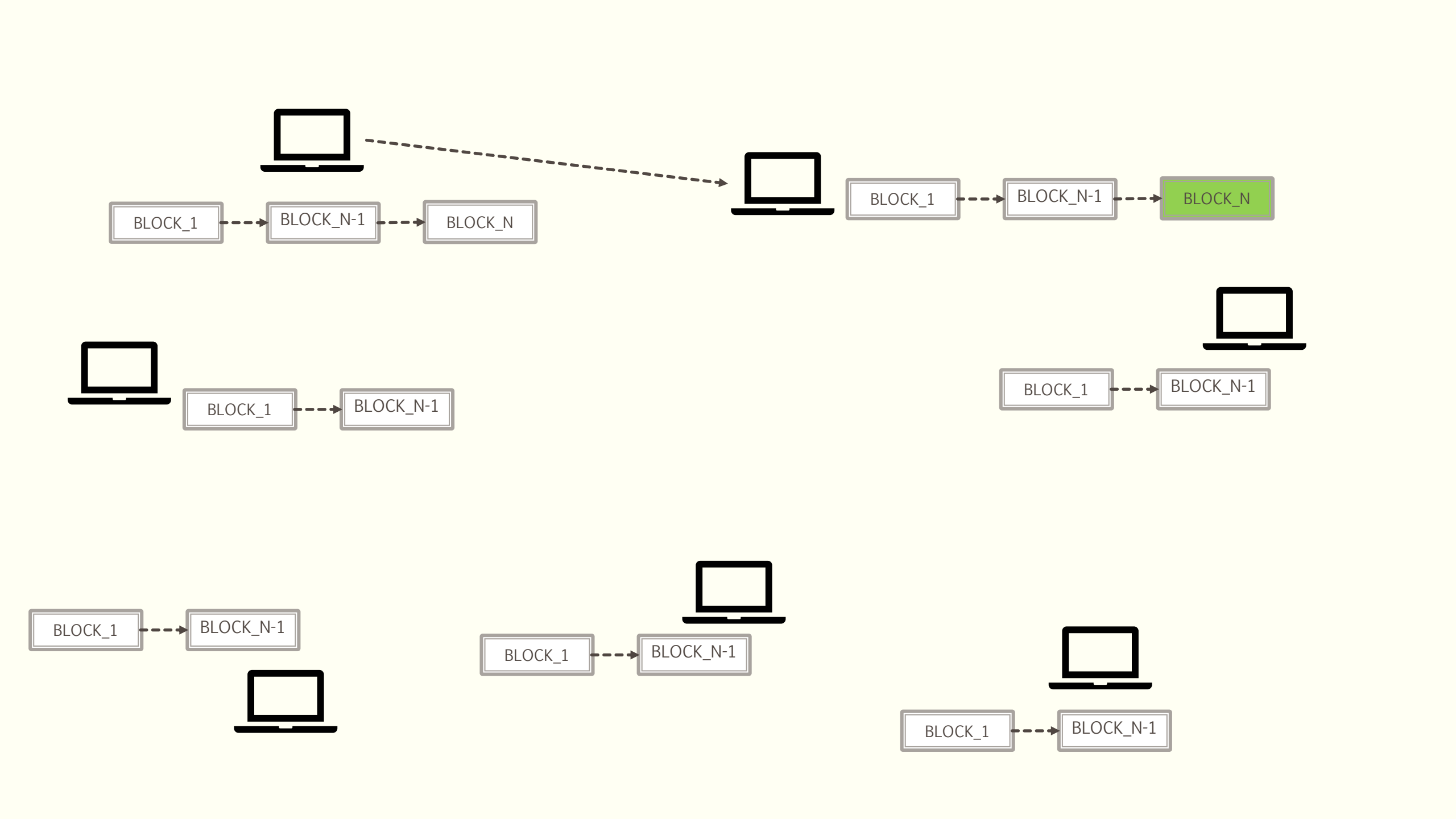
Transactions are gathered in blocks.
Each block has a header and a body.
Block is identified by its hash value.
Block header contains the hash of the previous block.
Each block has a timestamp.

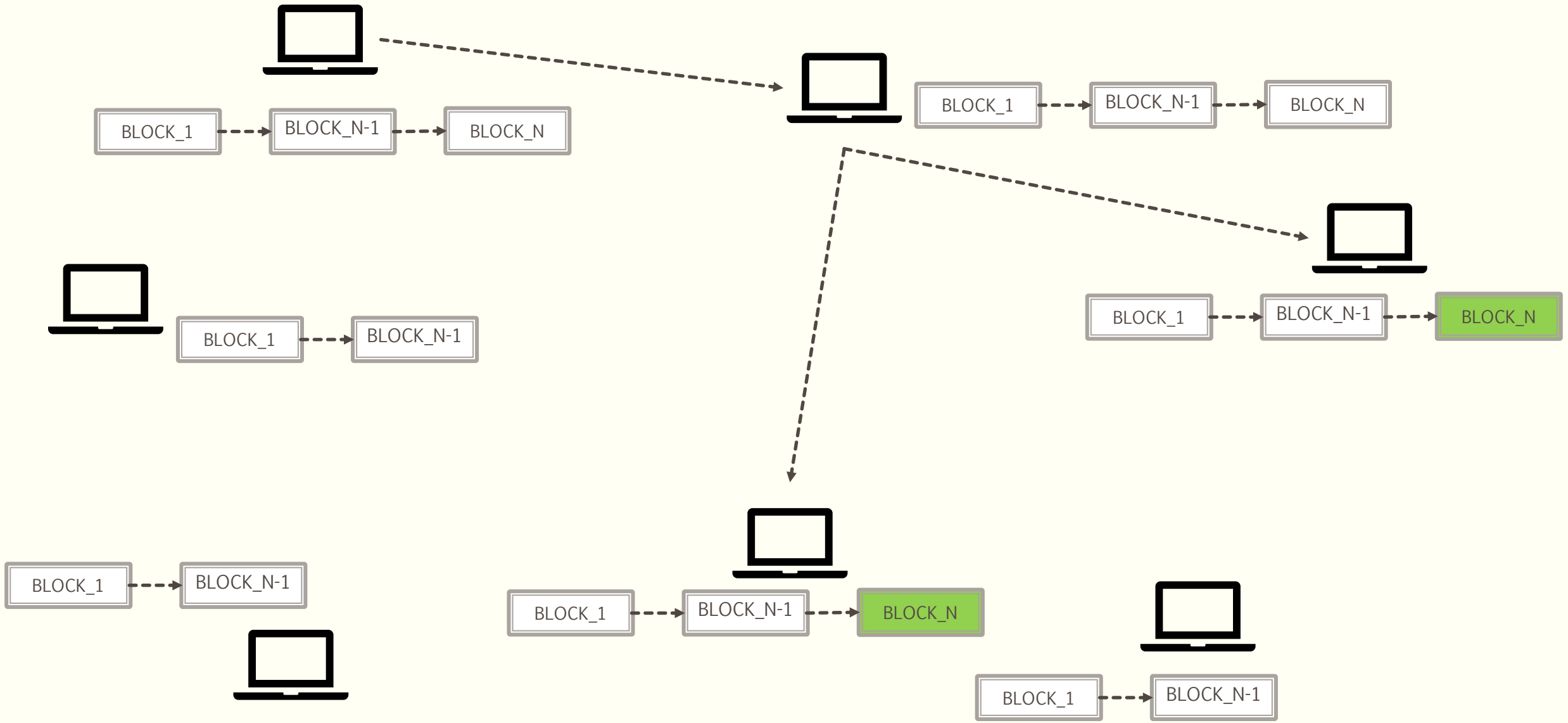


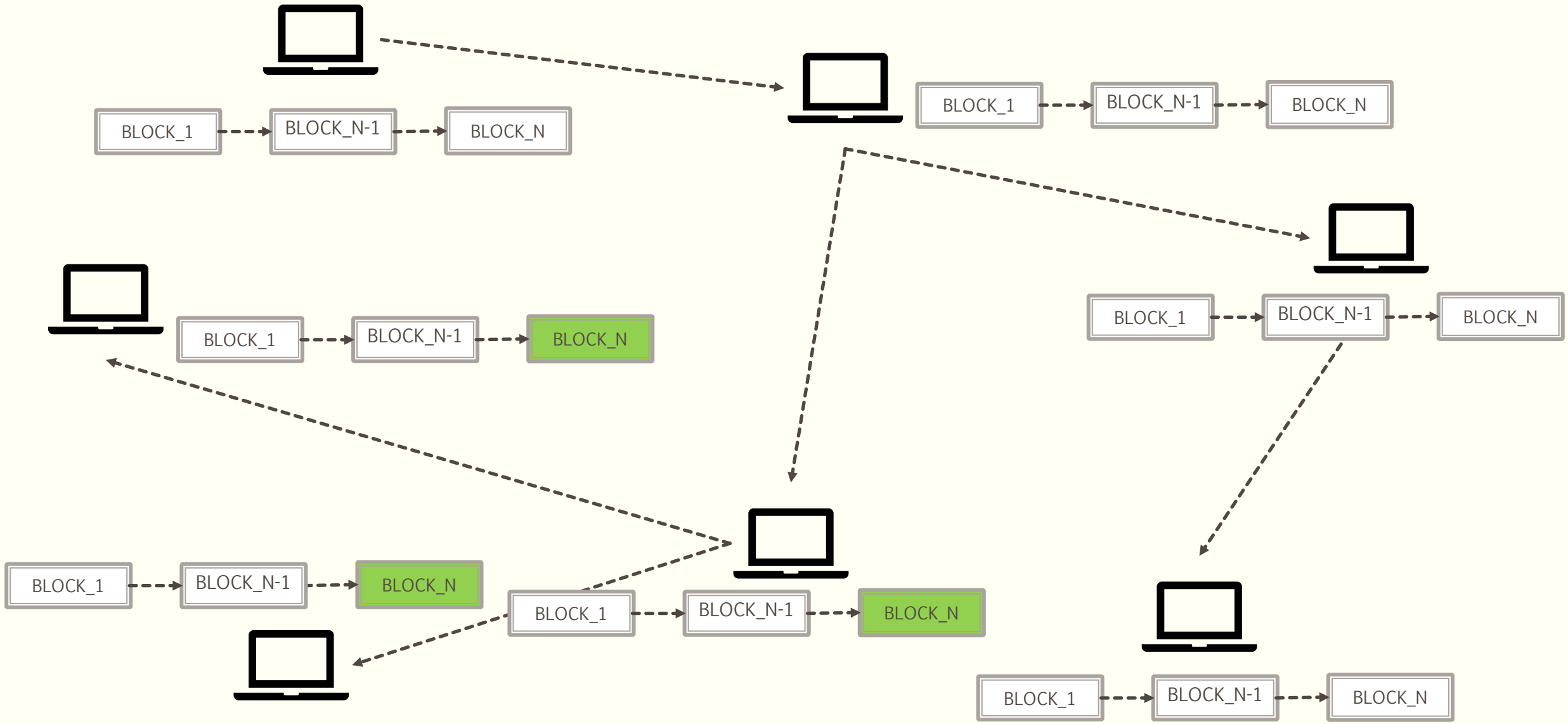

solve PoW puzzle, prove that some computational power has been spent to create the block.
PoW
BLOCK_1
BLOCK_N-1
BLOCK_N
BLOCK_1
BLOCK_N-1
BLOCK_1
BLOCK_N-1
BLOCK_1
BLOCK_N-1
BLOCK_1
BLOCK_N-1
BLOCK_1
BLOCK_N-1
BLOCK_1
BLOCK_N-1

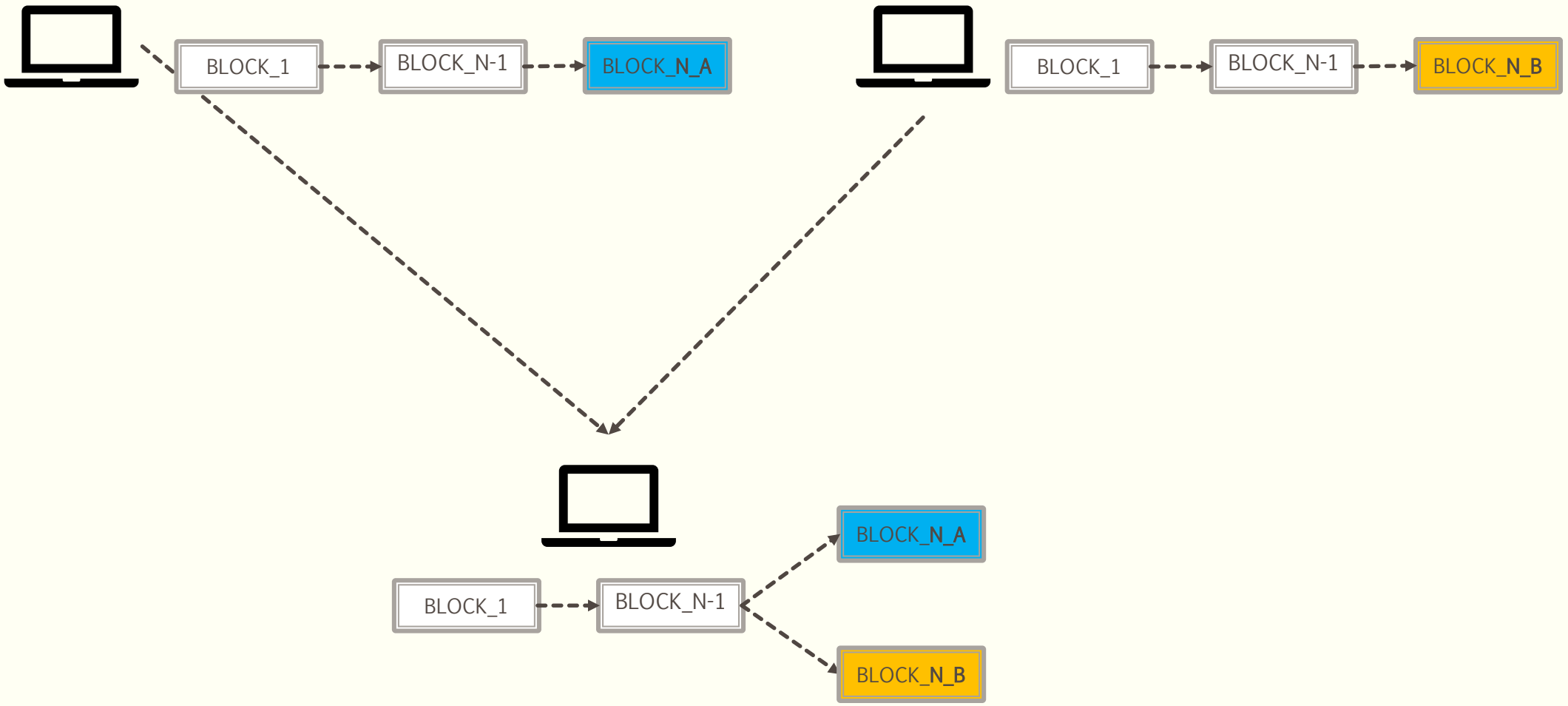
Gossip protocol



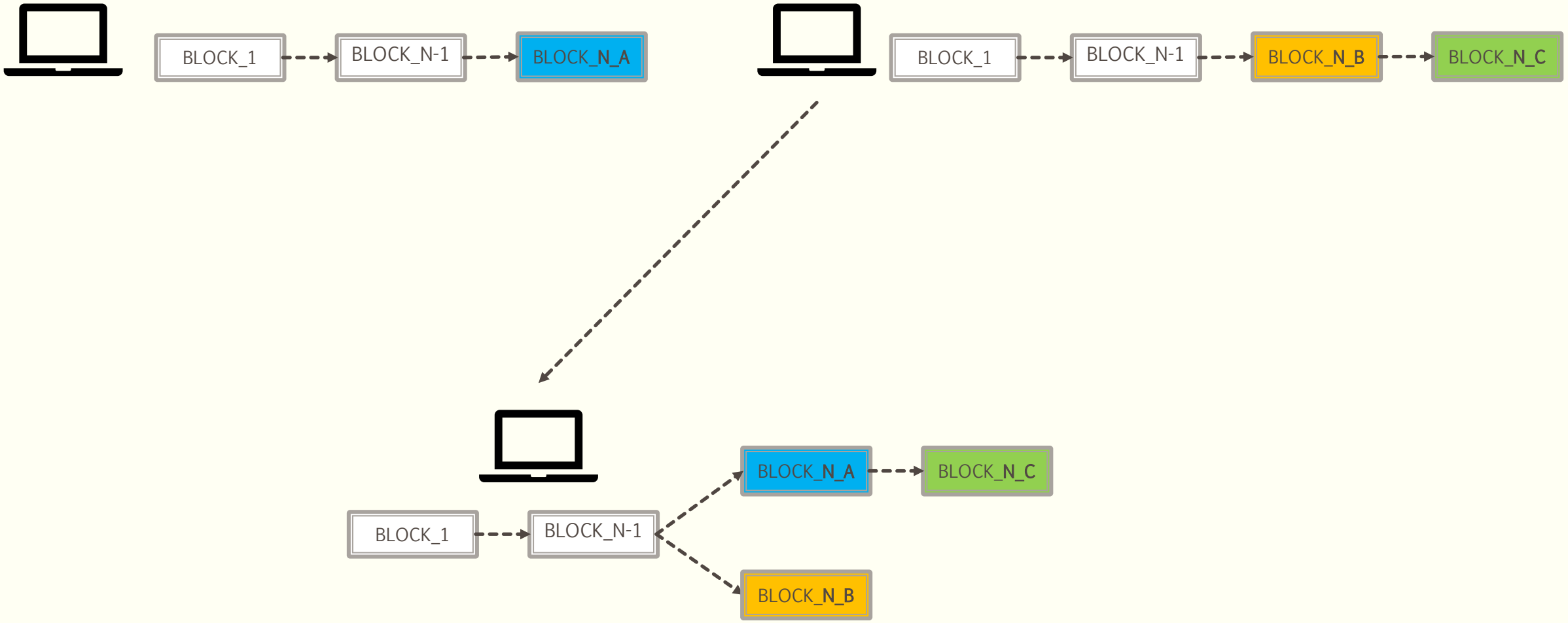

BLOCK_1
BLOCK_N-1
BLOCK_N
BLOCK_1
BLOCK_N-1
BLOCK_N
BLOCK_1
BLOCK_N-1
BLOCK_1
BLOCK_N-1
BLOCK_1
BLOCK_N-1
BLOCK_1
BLOCK_N-1
BLOCK_1
BLOCK_N-1


BLOCK_1
BLOCK_N-1
BLOCK_N
BLOCK_1
BLOCK_N-1
BLOCK_N
BLOCK_1
BLOCK_N-1
BLOCK_1
BLOCK_N-1
BLOCK_N
BLOCK_1
BLOCK_N-1
BLOCK_1
BLOCK_N-1
BLOCK_N
BLOCK_1
BLOCK_N-1


BLOCK_1
BLOCK_N-1
BLOCK_N
BLOCK_1
BLOCK_N-1
BLOCK_N
BLOCK_1
BLOCK_N-1
BLOCK_N
BLOCK_1
BLOCK_N-1
BLOCK_N
BLOCK_1
BLOCK_N-1
BLOCK_N
BLOCK_1
BLOCK_N-1
BLOCK_N
BLOCK_1
BLOCK_N-1
BLOCK_N


BLOCK_1
BLOCK_N-1
BLOCK_N_A
BLOCK_1
BLOCK_N-1
BLOCK_N_B
BLOCK_1
BLOCK_N-1
BLOCK_N_A
BLOCK_N_B

Longest chain rule

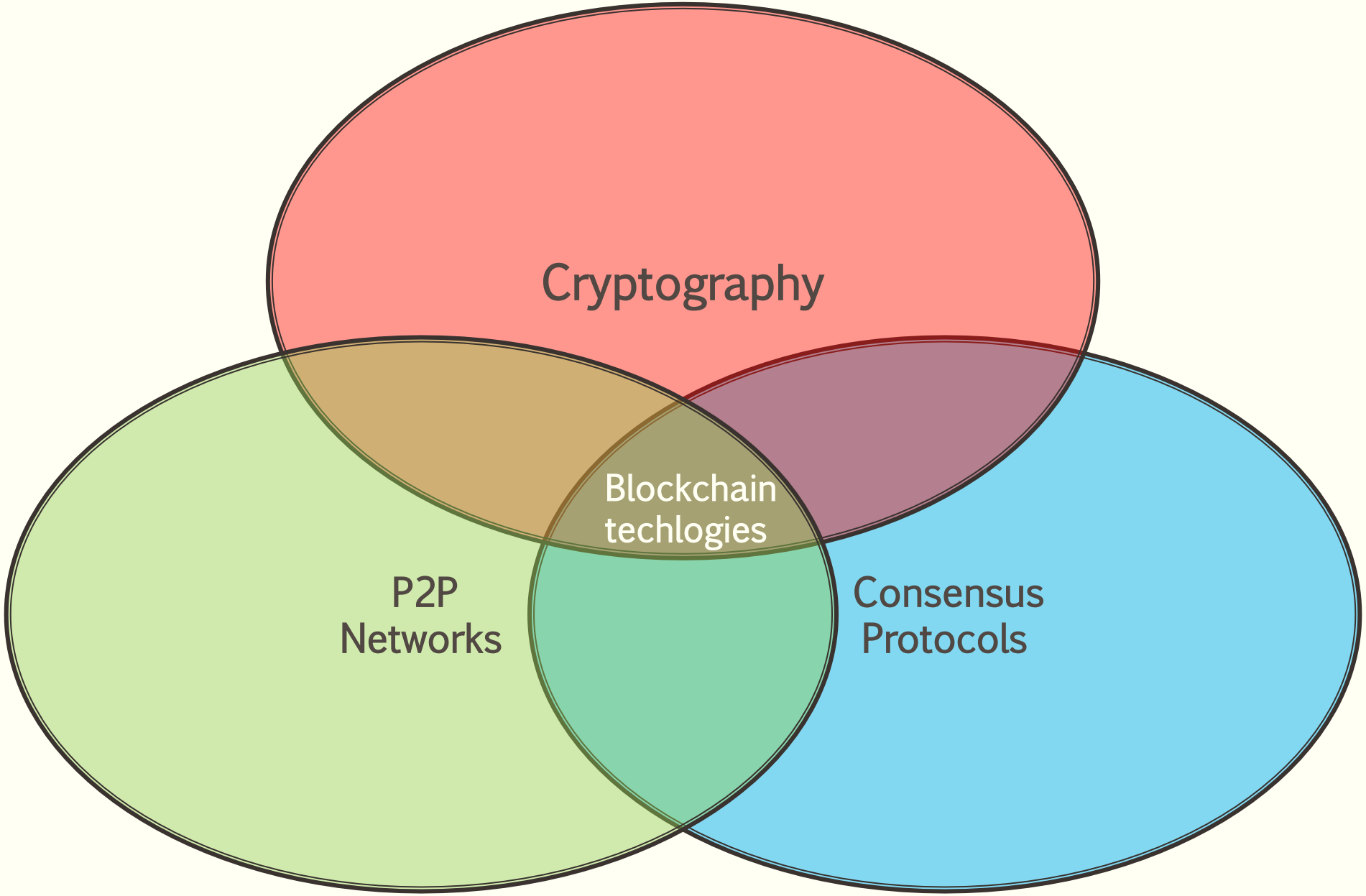


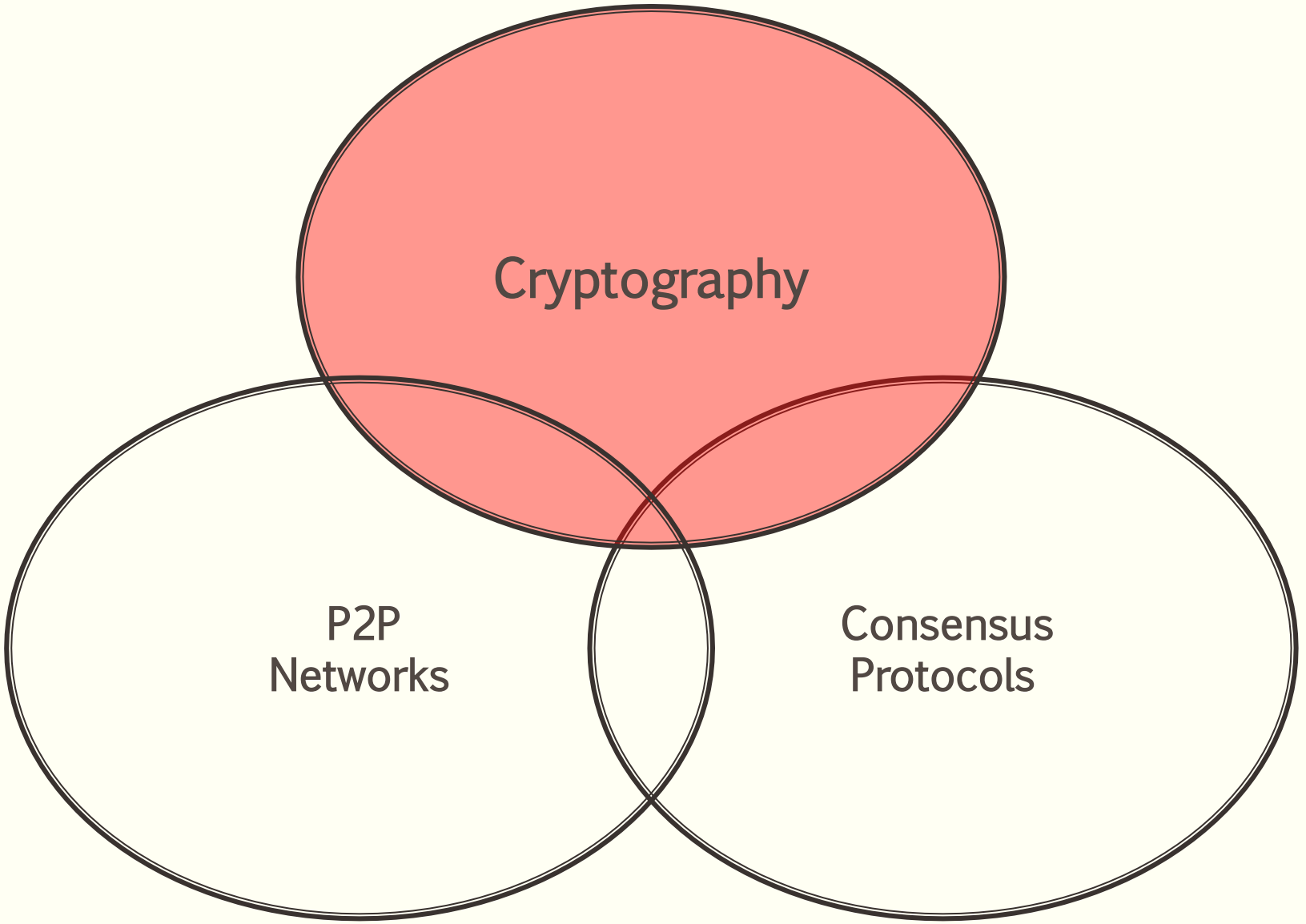
Bitcoin consensus protocol

- **Validate transactions:** Coins are not double spent; coins belong to the sender.
- **Block generation:** PoW find nonce, hash satisfies a difficulty target
- **Block propagation**: gossip all blocks (received or locally generated) should be *advertised* to peers and *broadcast*

Bitcoin consensus protocol

- **Block validation:** check block header and transactions
- **Longest-chain rule**: Blocks should always extend the longest chain.
- **Incentives/Rewards:** coinbaise transactions.


Cryptography
Blockchain
techlogies
P2P
Networks
Consensus
Protocols

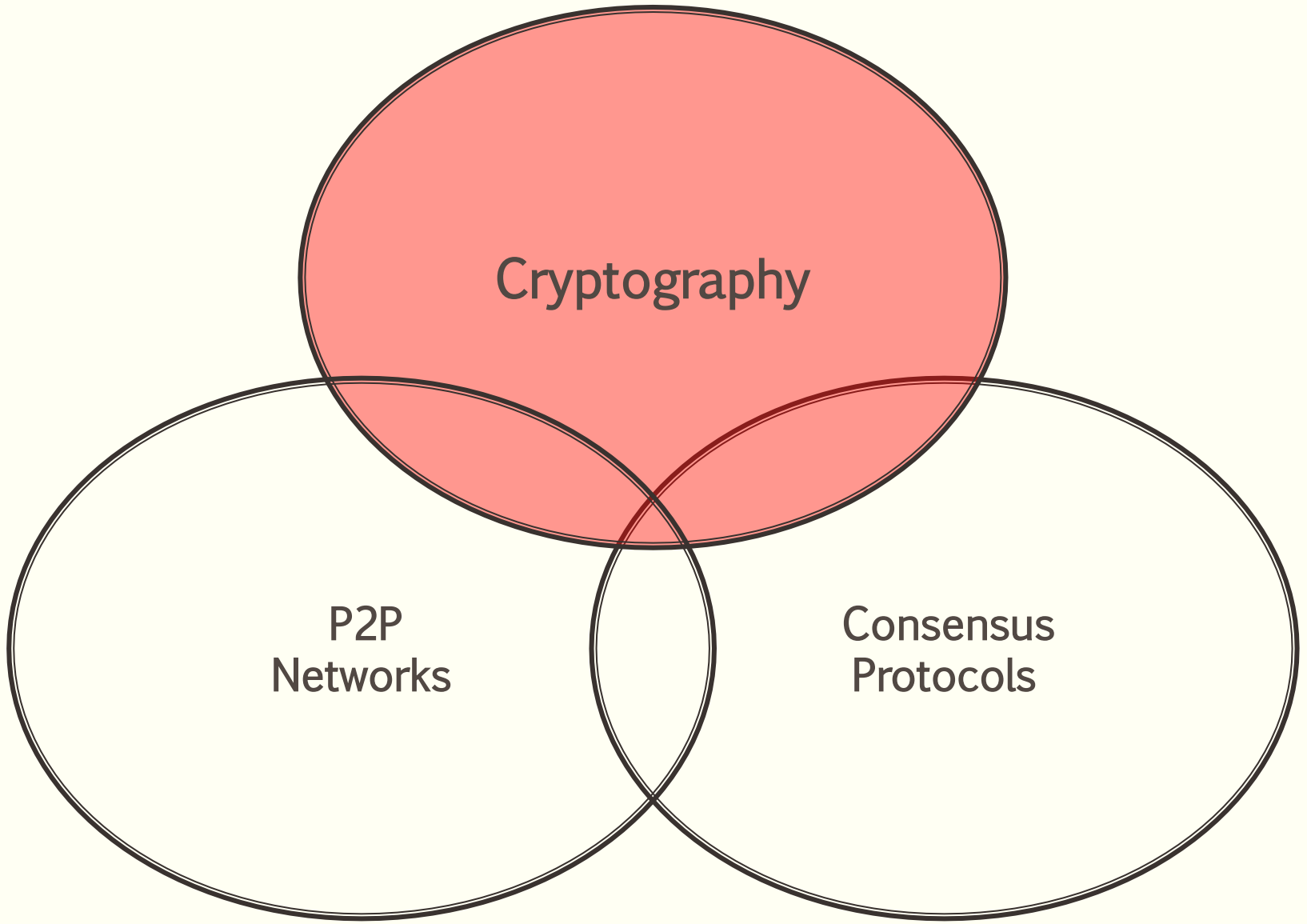


public key cryptography
and
cryptographic hash function

users encode/deocde transactions using a pair of keys: private key/public key.

signature sig=**sign**(private_key, message)

boolean ok=**verify**(public_key, signature, message)



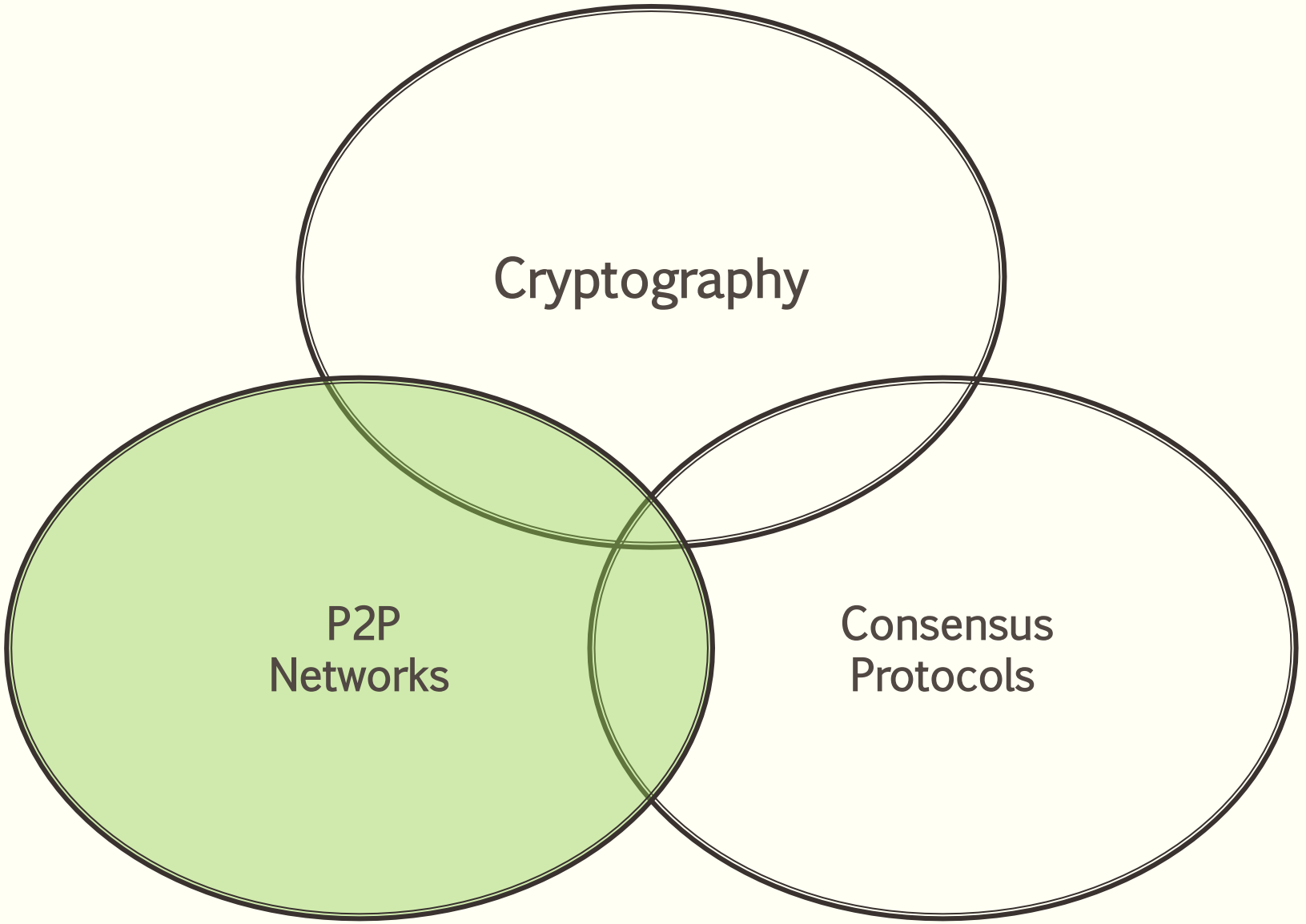
public key cryptography
and
cryptographic hash function
and
cryptographic hash function

plain text is encrypted using a cipher to generate a hash value of fixed length.

hash(message)

preimage resistance,
collision resistance

stored in hash-trees
used as commit-reveal scheme



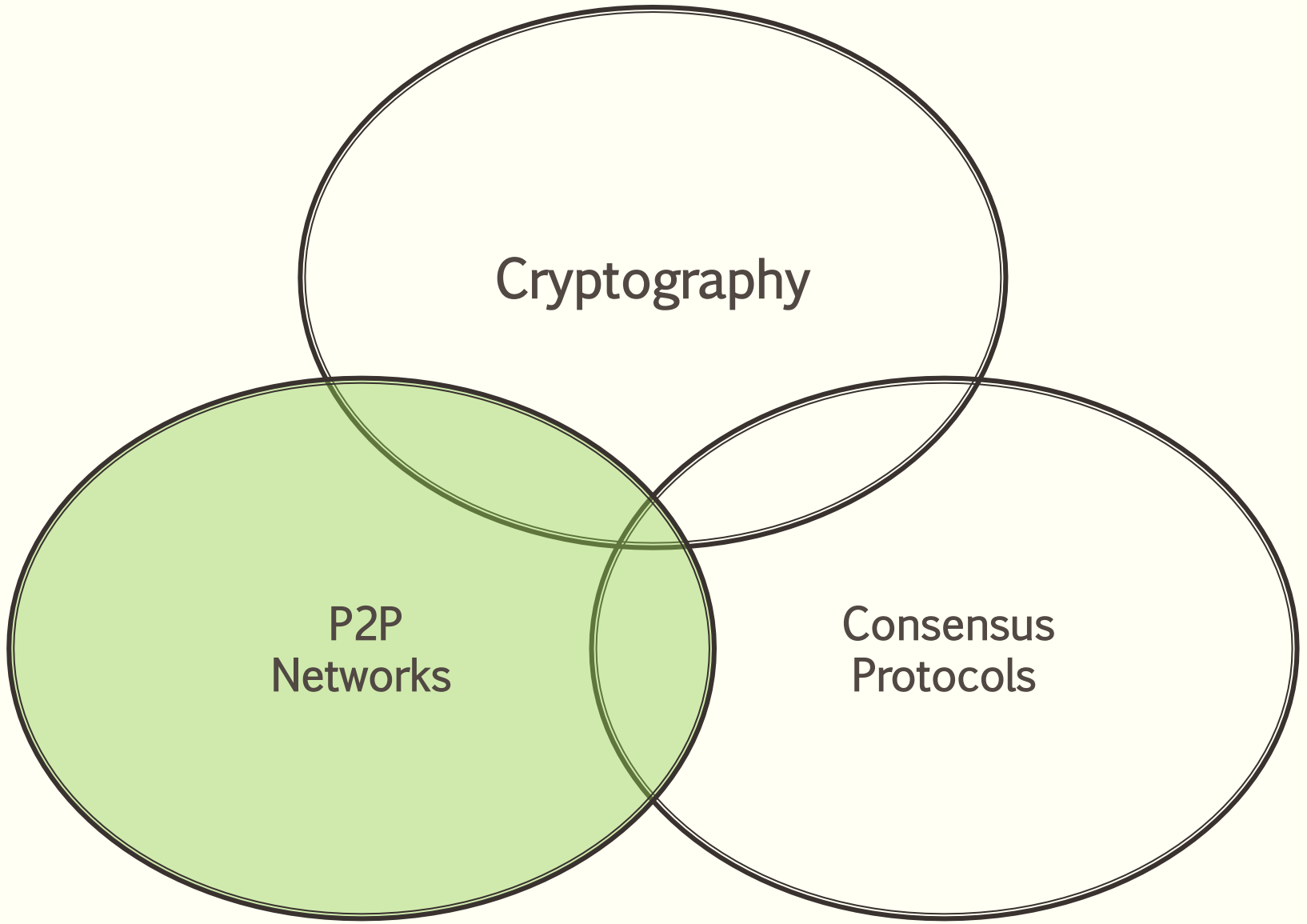
P2P architecture

and

cryptographic hash function.

Full nodes download and verify every block.

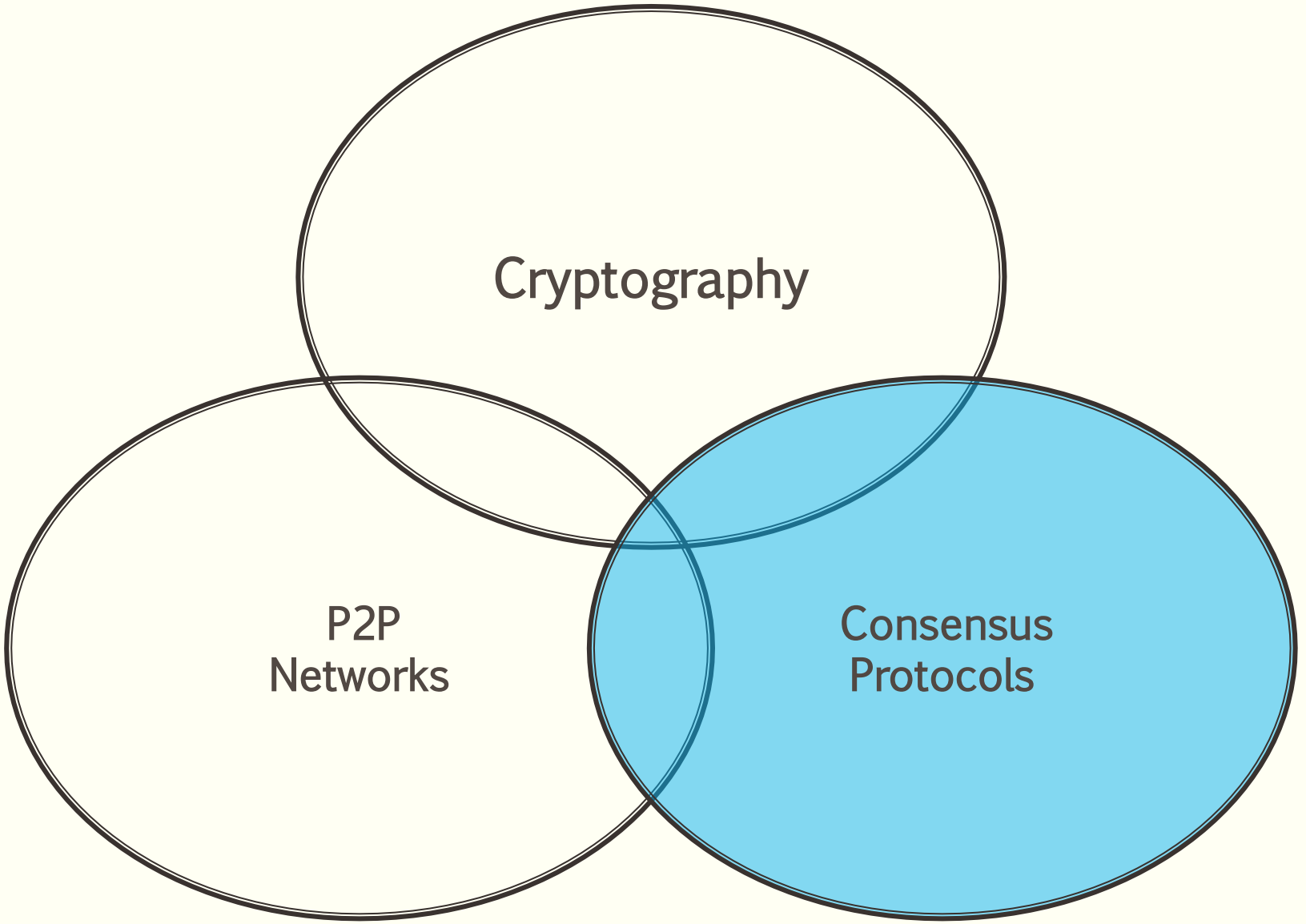
Newly joined nodes query **DNS seeds** to discover full nodes that accept connections.



P2P architecture
and
cryptographic hash function.

Initial Block Download: Before a full node can validate transactions, it must download and validate all blocks from block 1.

Block Broadcasting when a miner discovers a new block, it broadcasts the new block to its peers



Consensus protocol
and
cryptographic hash function

agree on some value,
leader election,
agree on transactions order ...

Ensures all participants agree on a unified transaction ledger without a central authority.

BLOCKCHAIN CHARACTERISTICS

Blockchain characteristics

- **Public ledger:** A public database, all nodes share the same information about transaction and accounts (UTXO model or state-machine model).
- Records added in the ledger are immutable, only new transactions are continuously appended.
- All nodes must reach consensus, deciding the validity of transactions.
- **Auditable**: Transactions are timestamp and signed.

Blockchain characteristics

- **Immutable:** A public blockchain is a series of immutable record of data. Data is time-stamped

- **Decentralized**, **peer-to-peer**: Information is stored in a cluster of computers, there is no central authority. Everyone is accountable. Everyone keeps a copy of the database.

- **Transparent**: Everyone has access to all information.

Blockchain characteristics

- **Secure**: use asymmetric cryptography, data blocks are linked via hashes (block-chain) and protected via cryptographic functions.

- **Anonymity (pseudonimity)**: each participant may store several pairs of public-private keys to sign transactions or to prove ownership of his assets (UTXOs, ETHs, NFTs etc.) Identity is not revealed.

APPLICATIONS OF BLOCKCHAIN WEB3

Blockchain 2.0 smartcontracts

- Smart contract – code on Blockchain
- Smart contract account with a public key, a private key and eth balance
- EVM – Ethereum virtual machine, Turing complete (gas limit!!!)
- Transaction
  - eth transfer
  - creation of a smart contract
  - run a function of a smart contract

Why WEB 3

- centralization
- privacy
- censorship
- security

How – Scaling Solution

- Layer 1 solutions:
  - change consensus protocol;
  - sharding

- Layer 2 solutions:
  - Sidechains
  - Rollups

Token Systems

- Company stock assets, coupons, incentives etc.
- Easy to implement, example of transaction: A sends x unit to B, provided that A has at least x unit in its balance before the transaction.
- Ethereum standards ERC-20
- Ethereum standards ERC-721 (NFTs)

Identity Systems

- DNS system, Namecoin, email authentication.
- Implement as a key(name)-value(data) database stored on blockchain network. Owner may change *data* associated with *name* or transfer ownership.
- Ethereum standard ERC-721 (NFTs)

Decentralized Autonomous Organizations

- Transparent rules, not influenced by a central authority
- Members have the right to spend funds.
- All members participate in decision making.
- Members collectively decide to add or remove members.
- Controlled by smart contracts
- DAO attack 3.6 million ETH

Supply management

- Tracking environmental conditions
- Detect unethical suppliers and counterfeit products
- Endorsement of the Forestry Certification

https://fsc.org/en/innovation/blockchain “permissioned” private blockchain ledger platform designed to verify materials trade compliance across FSC supply chains.

TYPES OF BLOCKCHAINS

Taxonomy

	Permissionless	Permissioned
anonymity	yes	no
number of nodes	large number of nodes	fewer nodes
security	high level of security	vulnerable
processing times	long	short

	PUBLIC	PRIVATE	CONSORTIUM
ownership	public	Controlled by a single organization	Group of organizations
centralization	decentralized	Partially decentralized	Partially decentralized
examples	Ethereum	Hyperledger	supply chain sector