Deep dive into Ethereum

CSE542

Agenda

- Revisiting some blockchain fundamentals
- Introduction to ethereum and differences with bitcoin
- The native currency (ETH)
- Smart contracts
- Ethereum State and State transition
- Accounts in ethereum
- Wallets
- Transaction Execution
- EVM and Gas
- Transaction execution
- Dapps and posisbilities

Problems with traditional systems

- Controlled systems, lack of transparency
- Privacy and security concerns (uncontrolled data sharing)
- Hierarchical nature and involvement of middleman
- Restrictions due to past behaviours

Decentralized Systems

- Extension of distributed systems
- More complex because of their permissionless nature
- Need to tackle intentional failures
- Goes beyond technical complexity
    - Social, Economical, etc.

Revisiting some fundamentals

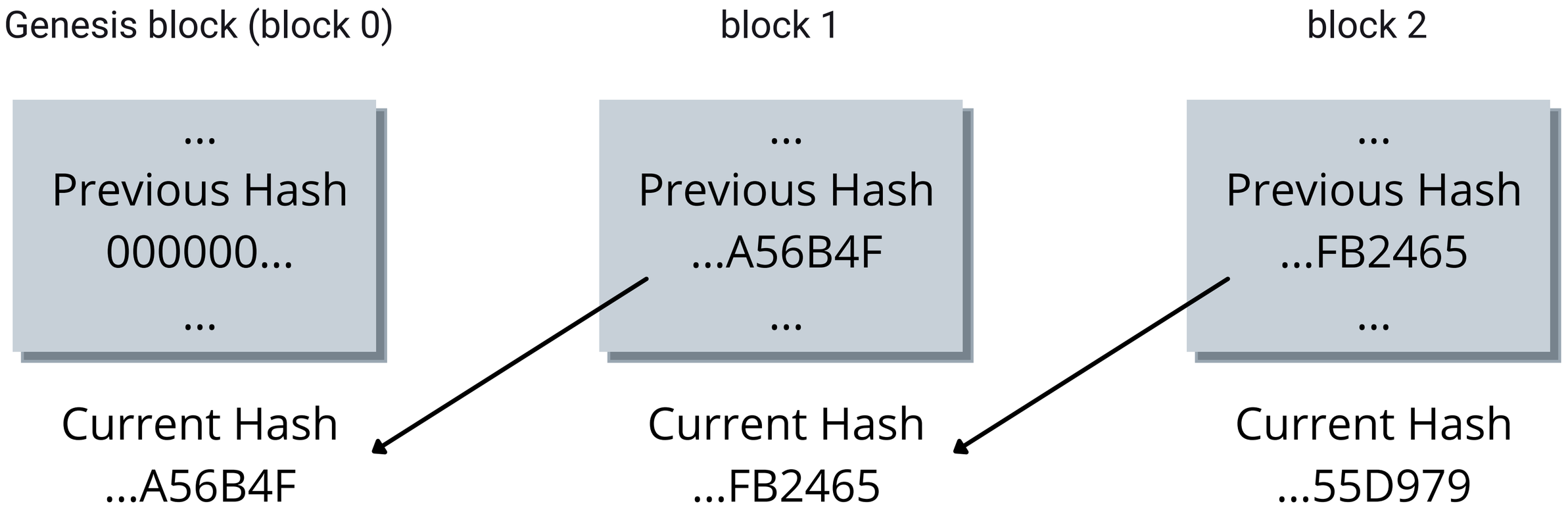
The Blockchain

Series of blocks, growing with time and are linked with each other cryptographically.

Structure of a block (quick recap)

- Block hash (primary identifier) and block number/height (secondary identifier)
- Header
  - Block number
  - Timestamp
  - Block hash (64 hex bytes) (SHA256 hashing algorithm)
  - Previous Block hash
  - Miner related details (nonce, miner, etc)
  - Metadata
- Body
  - Batch of transactions

Linking of blocks



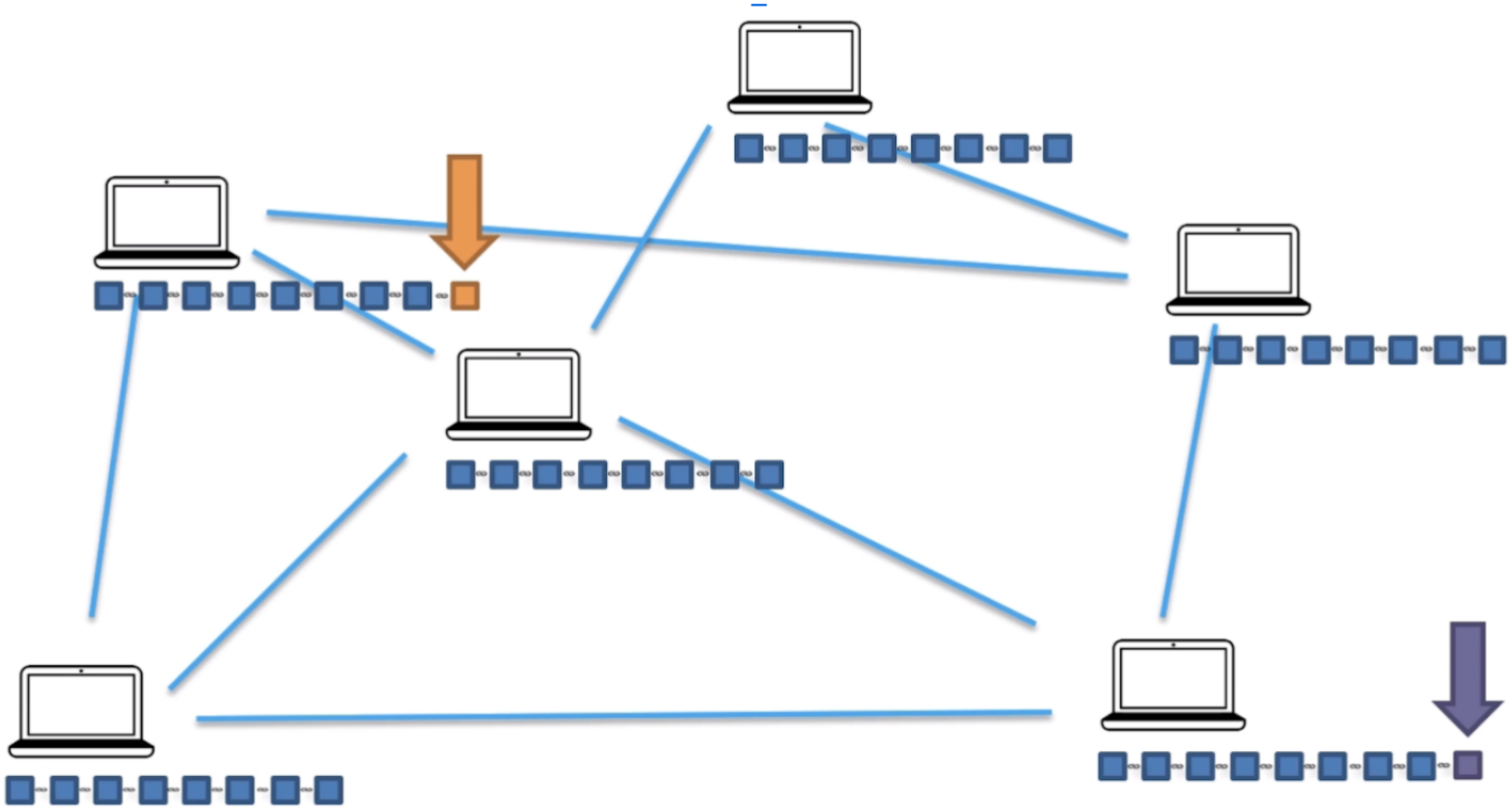
- This makes the data in blockchain immutable

The P2P Network

- A network consisting of nodes, which are free to enter and leave; equal in nature
- No server, centralized service, or hierarchy
- Ethereum, Bitcoin, etc are the protocols; blockchain is built on top of it.
- Each node/peer has a copy of whole historical data of blockchain

- Clients
  - A piece of software, one runs to become part of the network
  - E.g. geth - official implementation of ethereum in go

The P2P Network



The Consensus Mechanism

- Agreement of multiple people/entities on a particular thing (digitally)
- Set of rules, a blockchain protocol follows to mine and accept new blocks
- Makes sure that every node in the network agrees on a single chain
- Can be considered as multiple set of checks, e.g.
    - Validity of transaction
    - Validity of the block independently (aggregation of txs, hash, metadata, etc)
    - Validity of the block w.r.t. chain

PoW Consensus - Mining

- Proof of work consensus mechanism - helps in block addition i.e. Mining.
- A node picks up chunk of transactions from the pool; bundles them into block
- Try to bring the hash of the block below a specific target (0x00....0012)
- Keeps trying until achieved or received the same block at same height
- If achieved -> adds the block to the chain and propagate to peers

  Else -> accepts block from peers

PoW Consensus - Validation

- Much simpler and faster than mining
- Every node performs some validation checks before accepting a block
- If false block is propagated, it will be rejected
- This is to make sure that data inserted in blockchain is validated by majority of nodes/entities.
- Attack possible if more than 51% group together.

Introduction to Ethereum

Differences with Bitcoin

- Bitcoin's Purpose: Decentralize money and enable borderless payments
- Ethereum along with this also acts as a general purpose programming blockchain capable of running code of unbound and arbitrary complexity.
- Bitcoin's scripting language is very limited to simple evaluations, while ethereum's language is turing complete
- Blockchain model but evolved for applications beyond cryptocurrency payments

Ethereum

- Defined as a "world computer"
- Shares common elements of a blockchain: a p2p network, fault-tolerant consensus mechanism, use of cryptography primitives and a digital currency.
- Aims to decentralize computing and become a global state machine.

Ethereum (Contd.)

- Instead of the nodes only capable of transaction processing, ethereum enables people to run any piece of code in a decentralized fashion
- In ethereum, code is law.
- Same set of code is executed in each machine and everyone agrees on a final code output i.e. state change.
- Hence the code and logic becomes immutable, secure, open and most importantly same for everyone

Ether (ETH)

- Native crypto currency of the Ethereum blockchain
- Useful to meter and constraint the execution costs
- Every action requires some costs which are paid using ether

Smart contracts in ethereum

- Code written on top of ethereum blockchain is called smart contract
- As name suggests, it is a contract with some pre-defined logic before put to blockchain
- Anyone can execute the functions of contract and output is visible publicly which creates transparency among the users (of contract and blockchain itself)

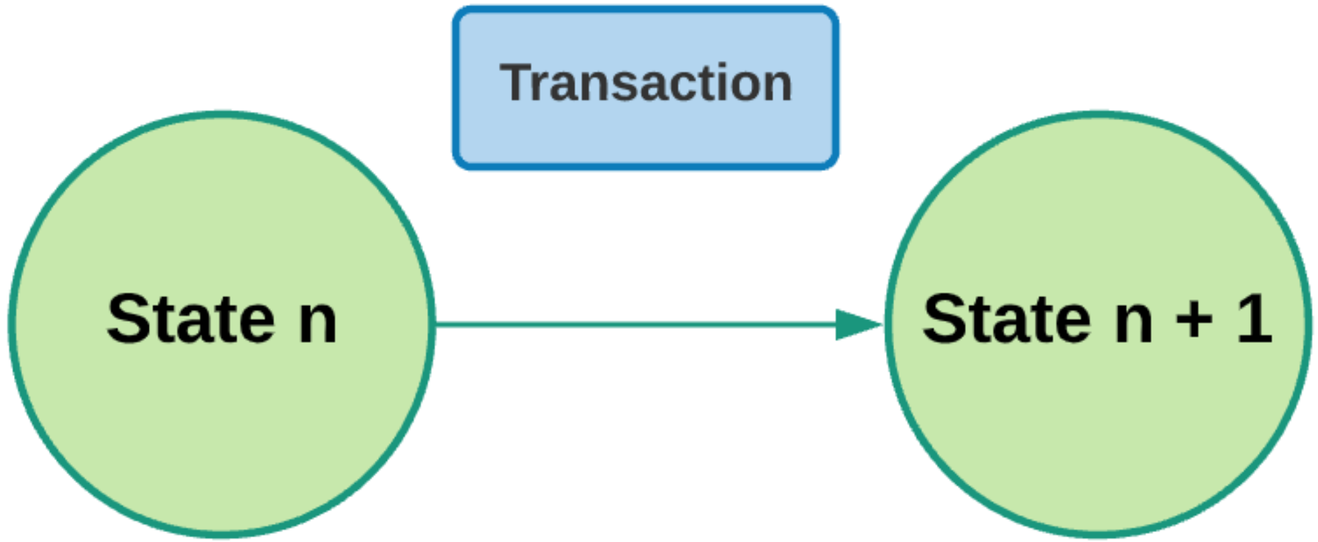
Smart contracts in ethereum (contd.)

- Every node has a copy of contract
- On function call, each of them runs the same thing
- Execution happens on Ethereum Virtual Machine (EVM)
- EVM works on OPCODES
- Majorly written in solidity (a turing complete language)

The Ethereum State

- Ethereum maintains a state of all the transactions and storage elements in a trie
- Each node has a copy of this state along with the blockchain (this is because we also have other data to maintain apart from the blockchain itself)
- The world/global state (where changes are applied by the EVM)
- So, everyone agrees on a particular state of ethereum in the consensus rounds

State transition



$$\sigma_{t+1} \equiv \Upsilon(\sigma_t, T)$$

Thank you!