Ethereum
Module I

Agenda

Module I

Intro

Key Concepts

Module II

Solidity

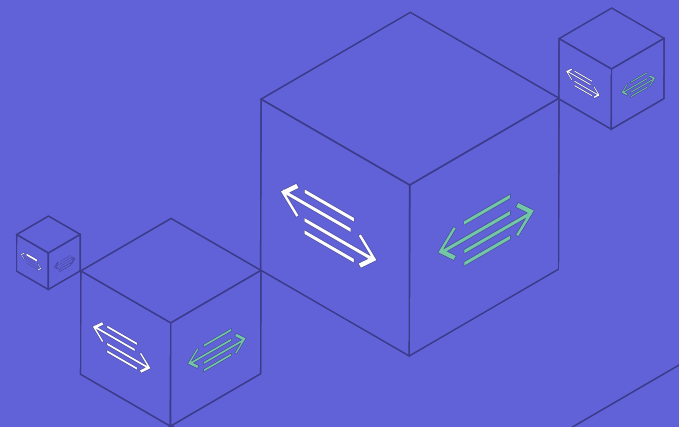
Hands-on

Module III

Web 3

Hands-on

Demo



trAse

Why Ethereum?

Open source

Broad commercial adoption

Community

Lower technical entry barrier

Smart contract development

trAse

History

- Adding Scripting language to expand Bitcoin Blockchain uses

  -> Rejected
- New platform
- 01/2014 Core Ethereum team

  Vitalik Buterin

  Mihai Alisie (Akasha)

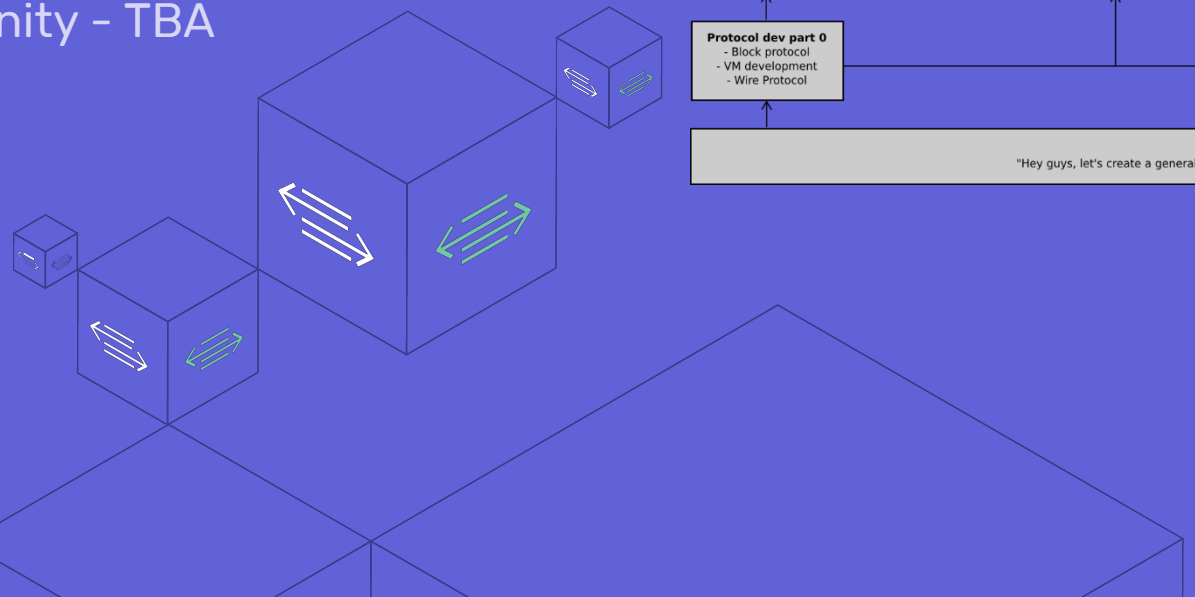
  Anthony Di Iorio (Jaxx)

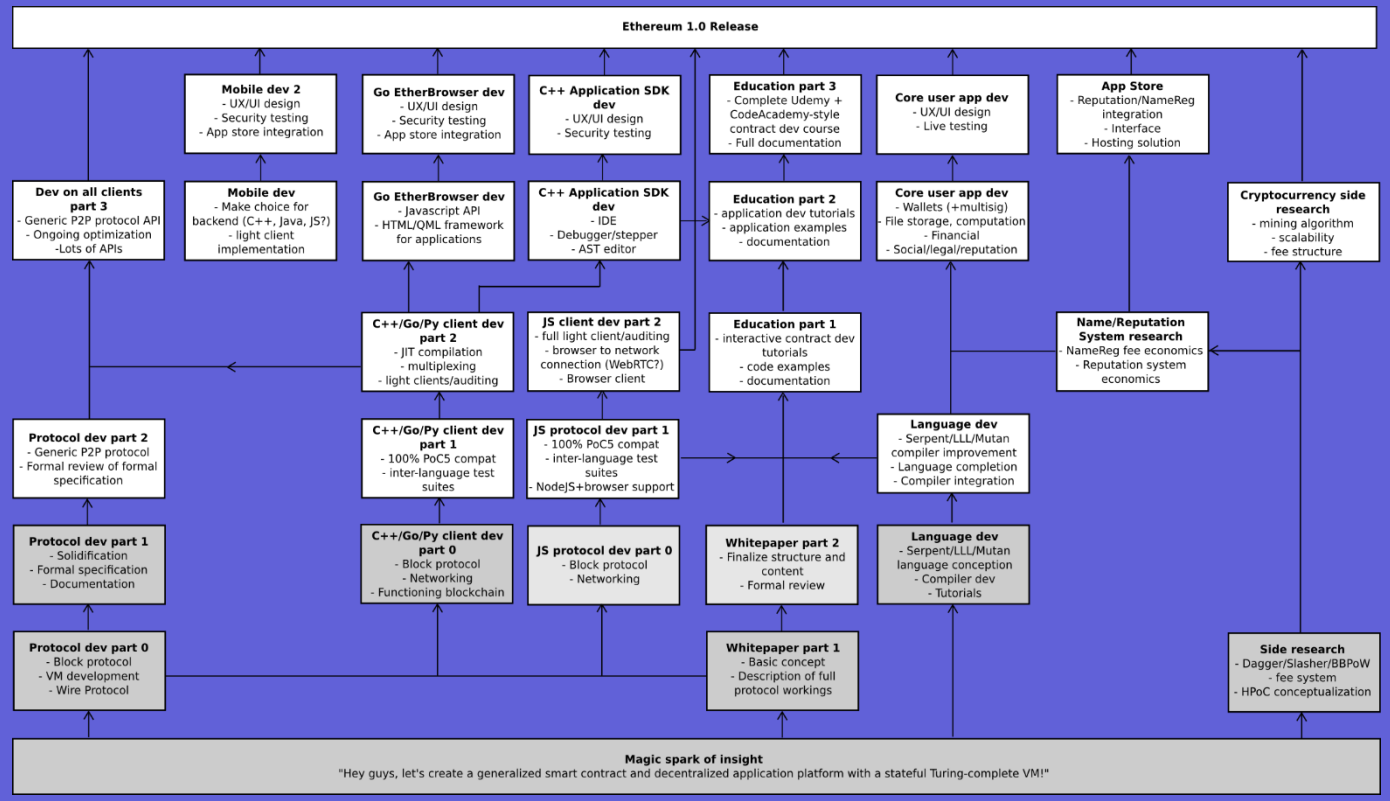
  Charles Hoskinson (Cardano)

trase

Releases

- Olympic – 05/2015
- Frontier – 06/2015
- Homestead – 03/2016
- Metropolis (vByzantium) – 10/2017
- Metropolis (vConstantinople) - TBA
- Serenity - TBA

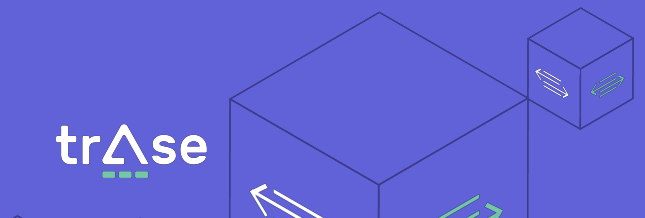




trAse

Ether

- Cryptocurrency
- Block time 14-15 seconds
- Balance model vs UTXO
- Replay attack protection in Balance model



Ether Denominations

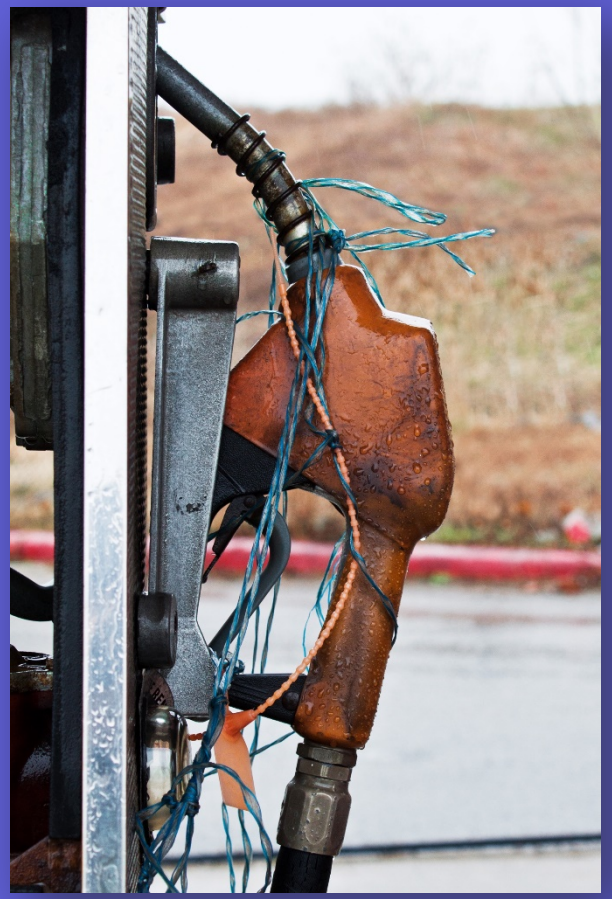
Unit	Wei Value	Wei
wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
microether (szabo)	1e12 wei	1,000,000,000,000
milliether (finney)	1e15 wei	1,000,000,000,000,000
ether	1e18 wei	1,000,000,000,000,000,000

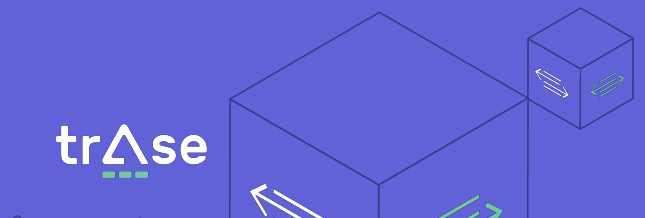
GAS – Payment model

Protect against attacks

Computation Memory Bandwidth Storage

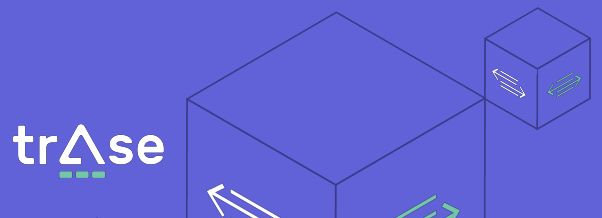
Rollback





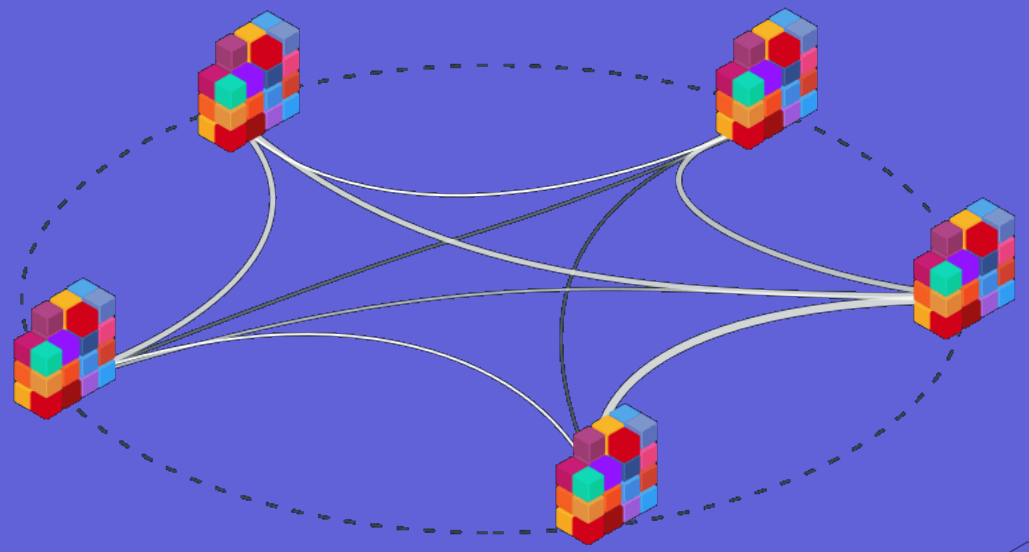
GAS – Calculate fees

Gas price	Startgas	Gasprice
Too low	Not sent to miners	No work done by miners
Low	Out-of-gas error	Mined slower
Medium	Ideal	Ideal
High	Delay in getting mined	Mined faster
Too high	Exceed block gas limit	Not sent to miners if sender is out of funds



Decentralized Applications

Decentralized applications (dApps) are applications that run on a P2P network of computers rather than a single computer.



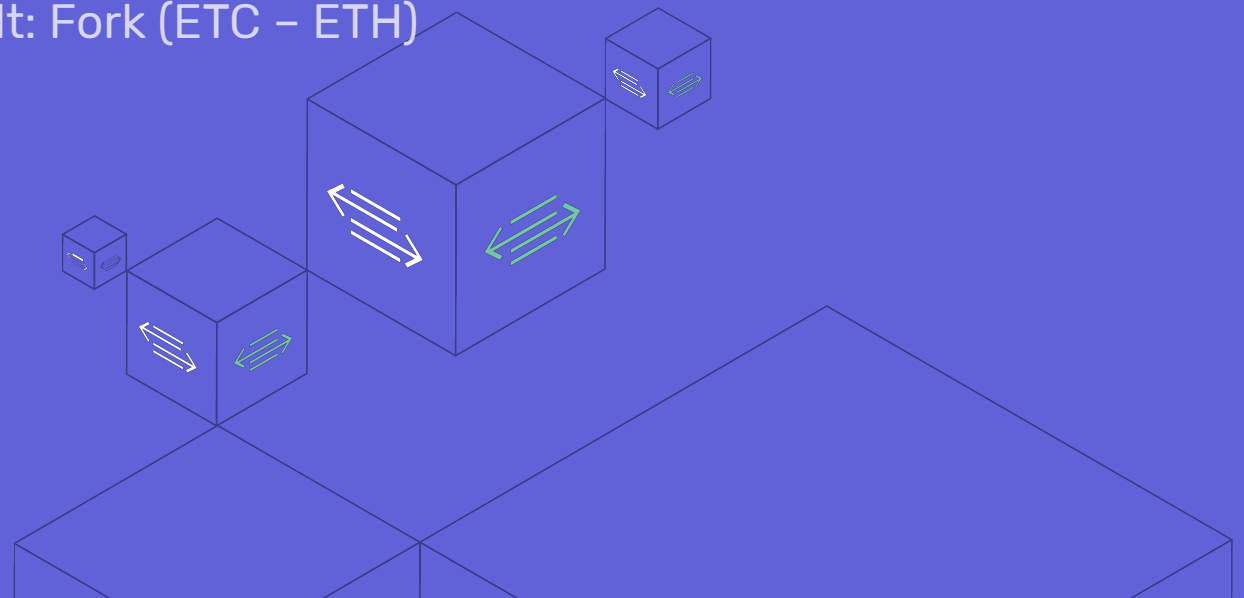
trAse

The DAO

- Decentralized Autonomous Organization
- Venture Capital Fund, stateless -> regulation?
- 28 days crowdfunding, $150 million
- Security flaws

  - Recursive Calls

Result: Fork (ETC – ETH)



trAse

Consensus - Proof Of Work

trAse

Consensus - Proof Of Work

- Why?
  - Distributed trustless consensus
  - Remove malicious/faulty transactions
  - Limited supply, monetary benefit

trAse

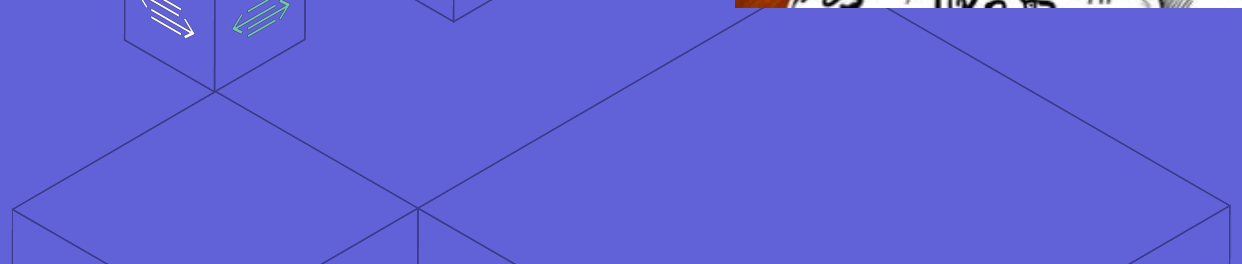
Consensus - Proof Of Work

- How?

trAse

Consensus - Proof Of Stake

- Stake
- Miner – Forger
- More stake = more chance
- Degree of luck
- Incentive: fees vs new currency



trase

Consensus - Proof Of Stake

Advantages:

- Less Energy
- Security
- Decentralization

Disadvantages:

- Nothing at Stake

trase

Casper Protocol

Helps achieve decentralization

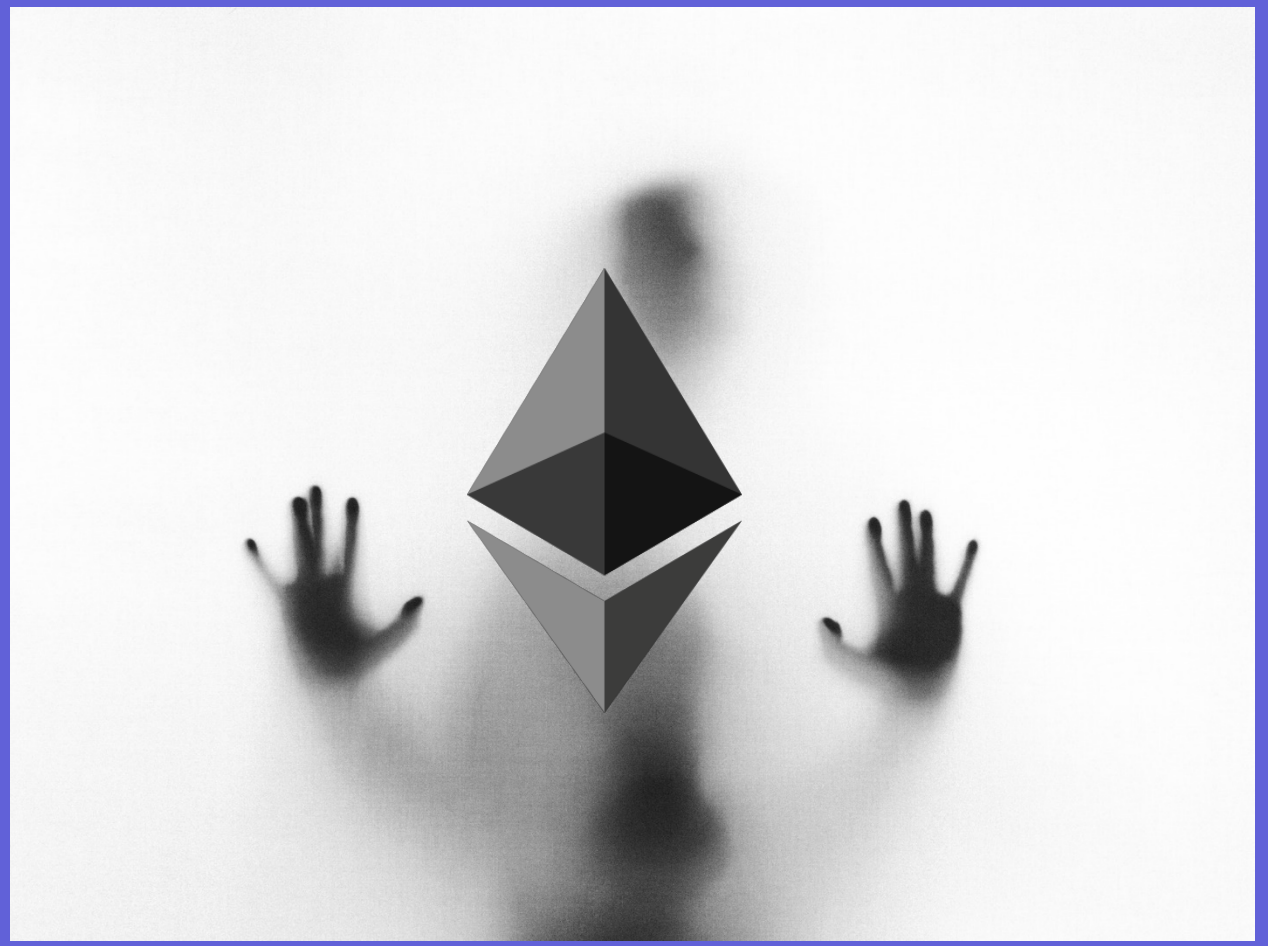
Energy efficiency

Economic security

Scaling

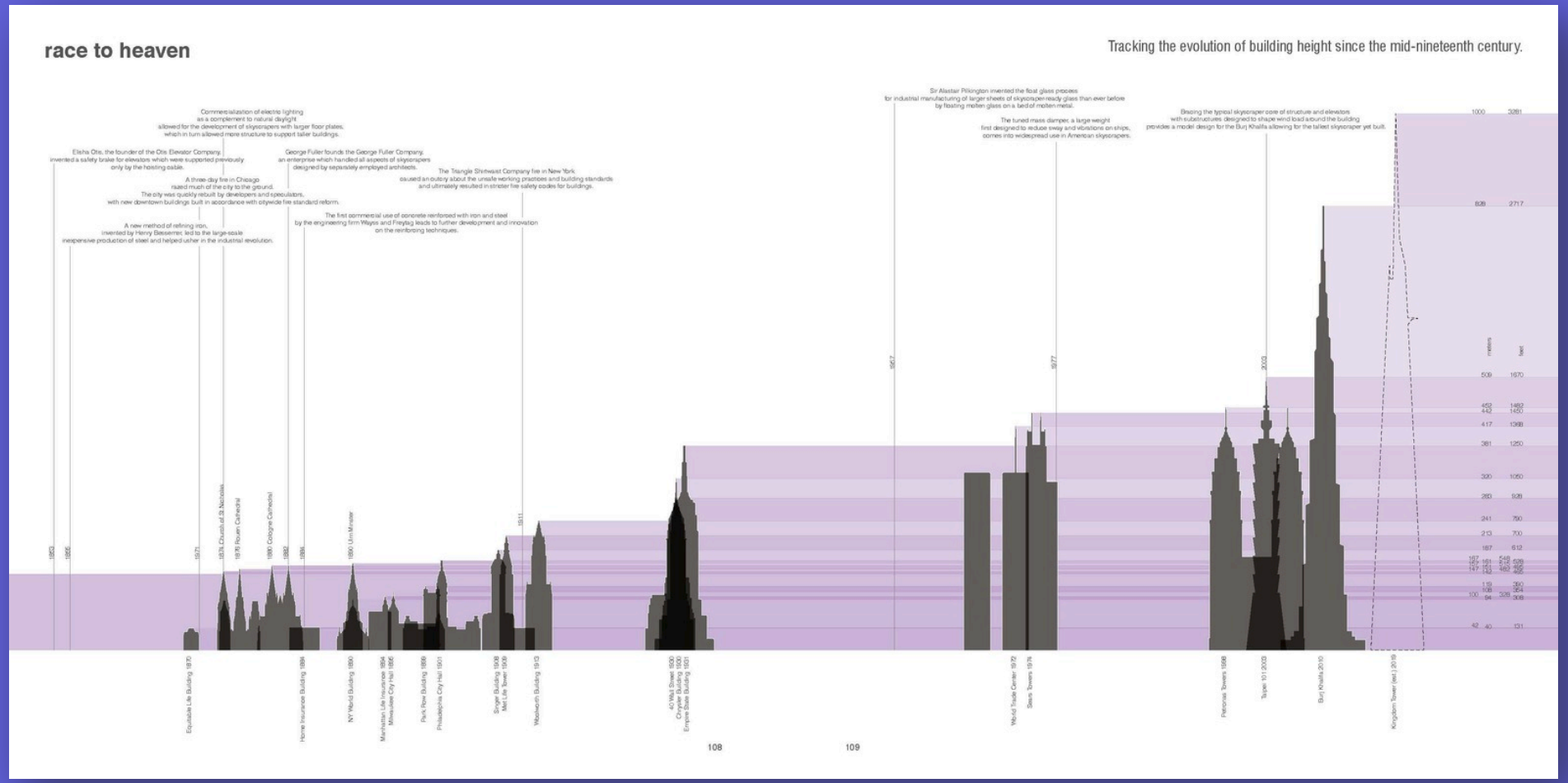
Transition to POS

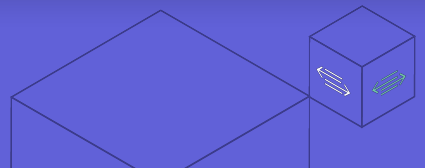
Sharding



trAse

A word on scaling





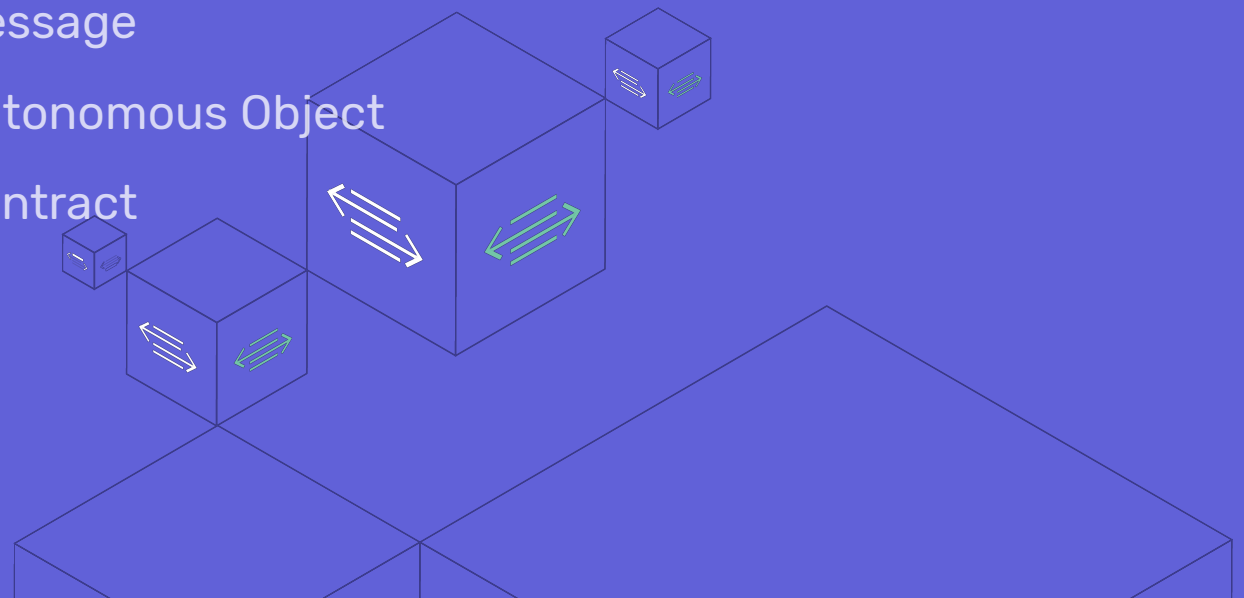
trAse

Key Concepts

trAse

Important Keywords

- Hash
- Tuple (!= C# tuple)
- Account Nonce
- Uncle
- Gas
- Message
- Autonomous Object
- Contract



trAse

Hashes

- Arbitrary input
- Output fixed length
- Small chance of collisions
- In Ethereum: Keccak-256
- 1 small change

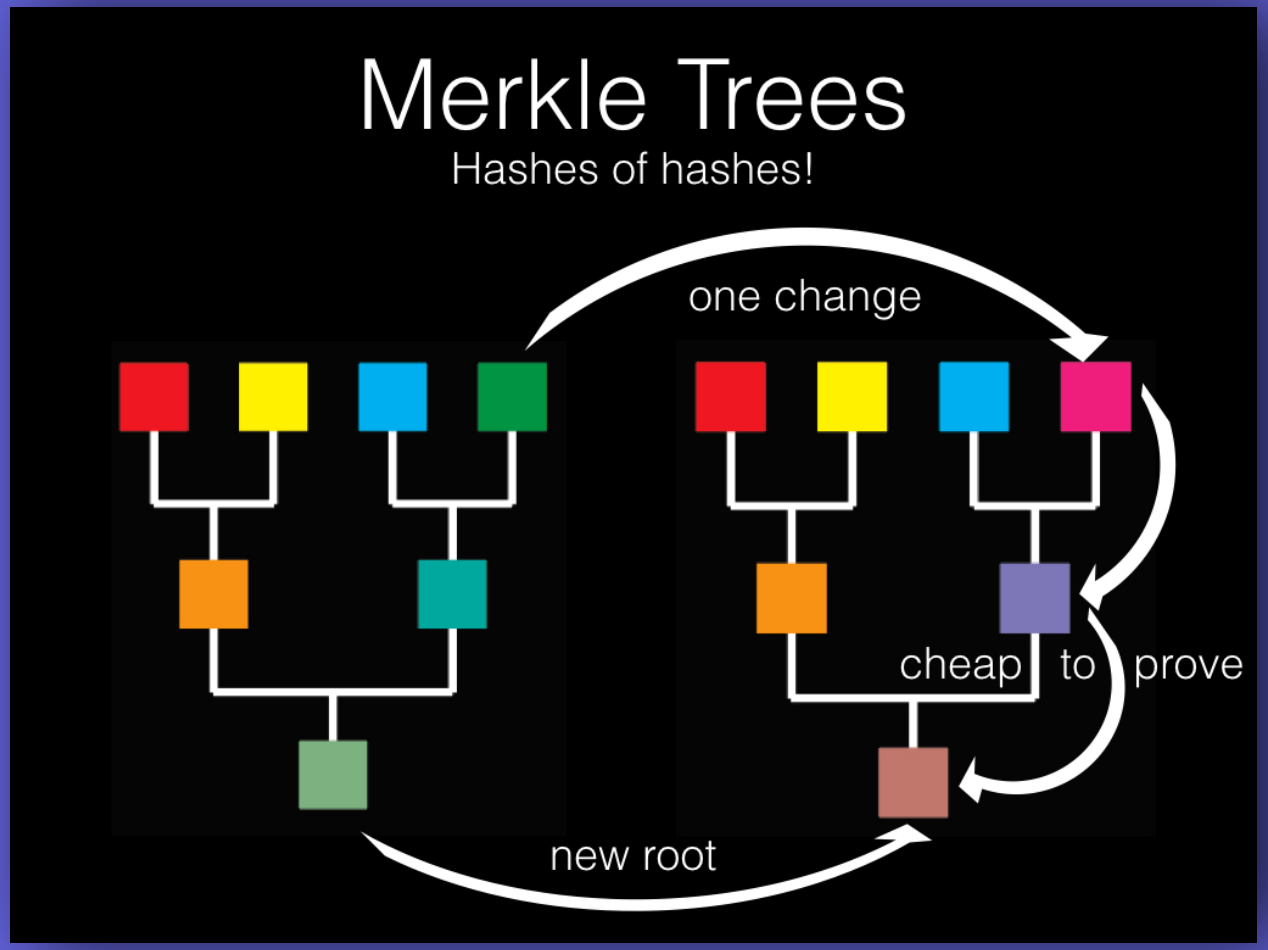
  —> Generates new hash

Input	Output
“Vitalik” —>	2b6ab720e1 69042d13b3c d63cc64db9e
“Vitaliik” —>	a323ddd0f65 285828fa774 c78eb3af84

trAse

Merkle trees

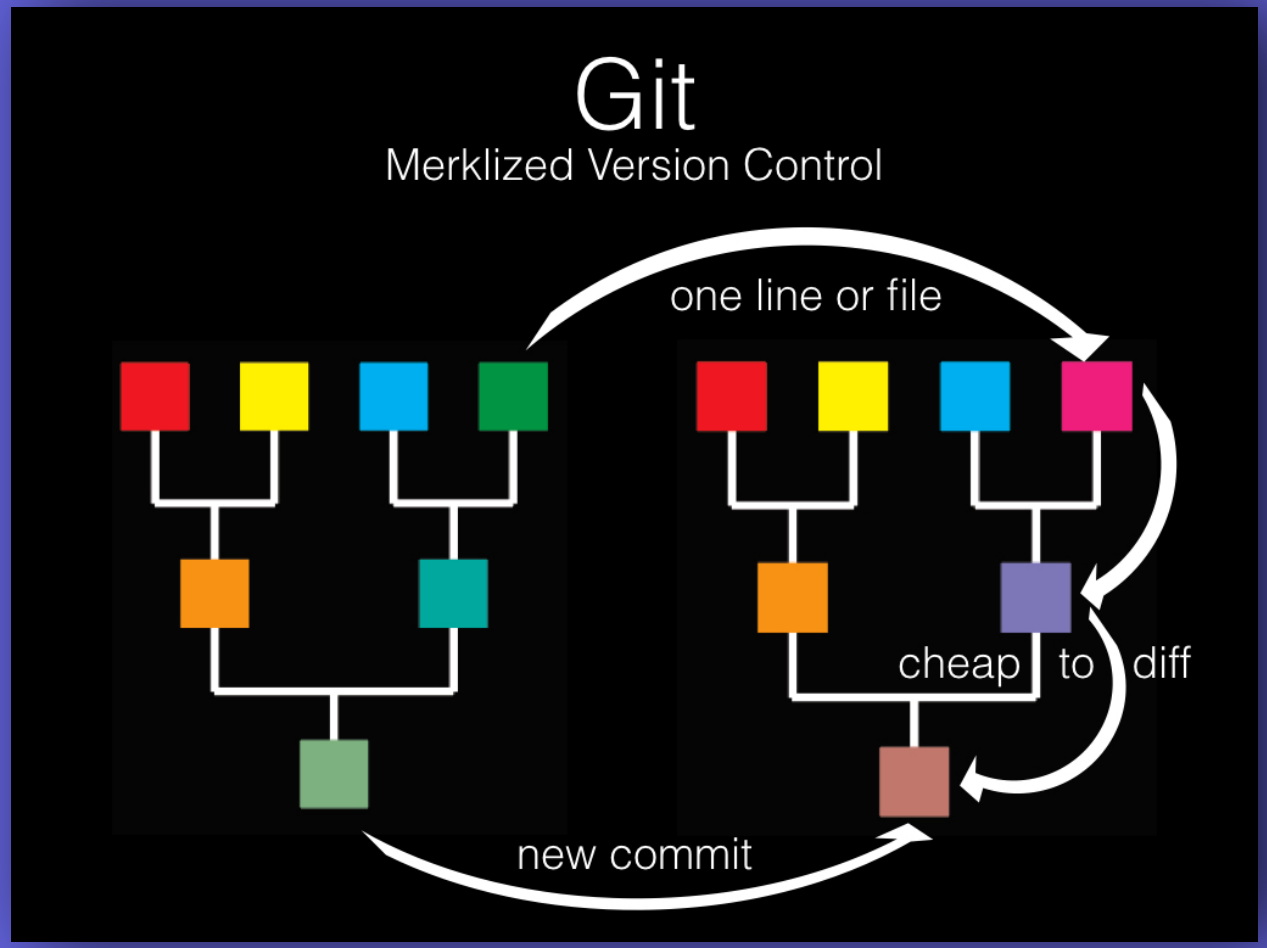
- Root hash
- Changes are reflected throughout the tree
- Only keep the new part
- Merkle proof
- Ethereum: Patricia tree



trAse

Merkle trees

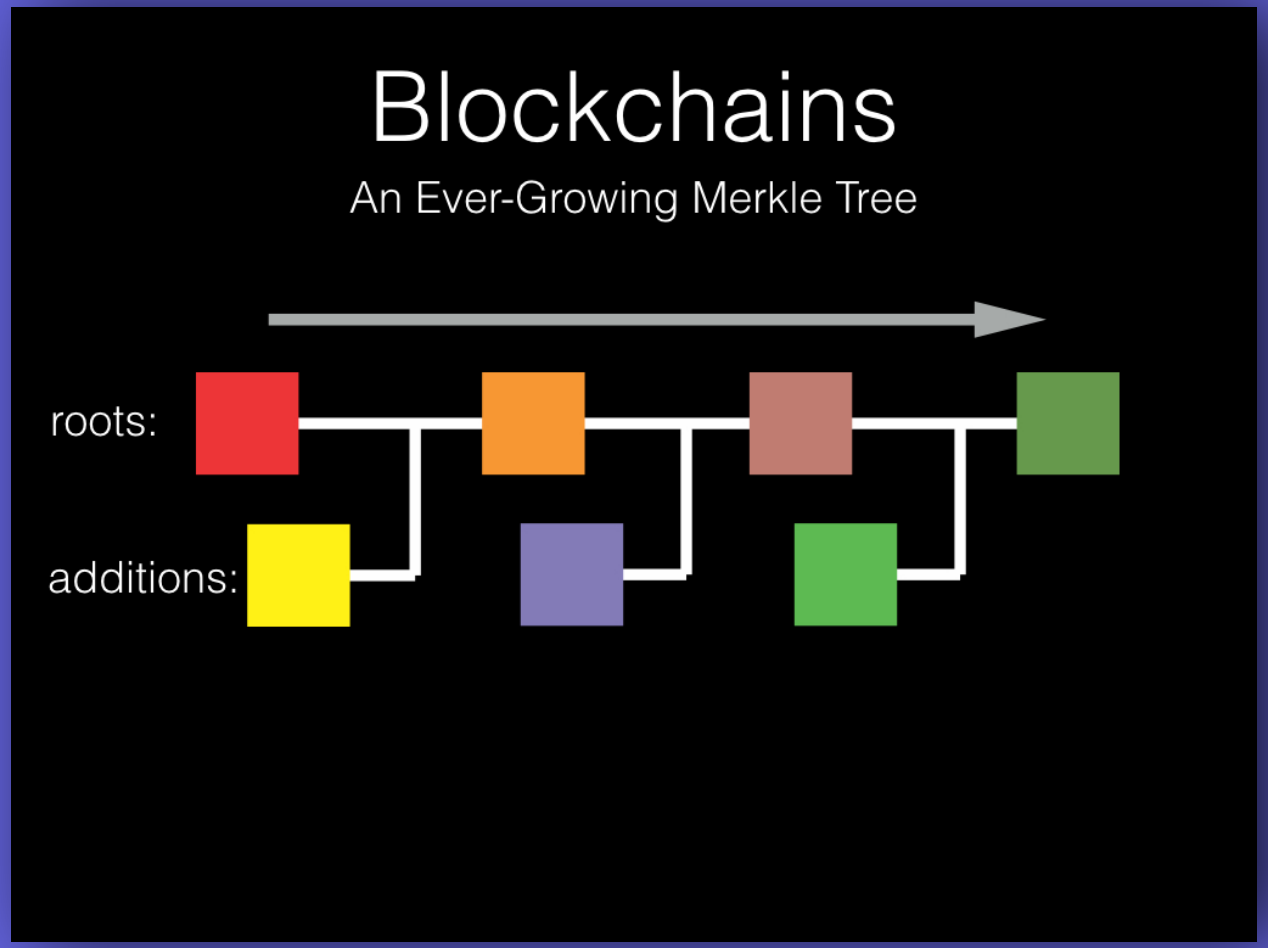
- Root hash
- Changes are reflected throughout the whole tree
- Merkle proof



trAse

Blockchains

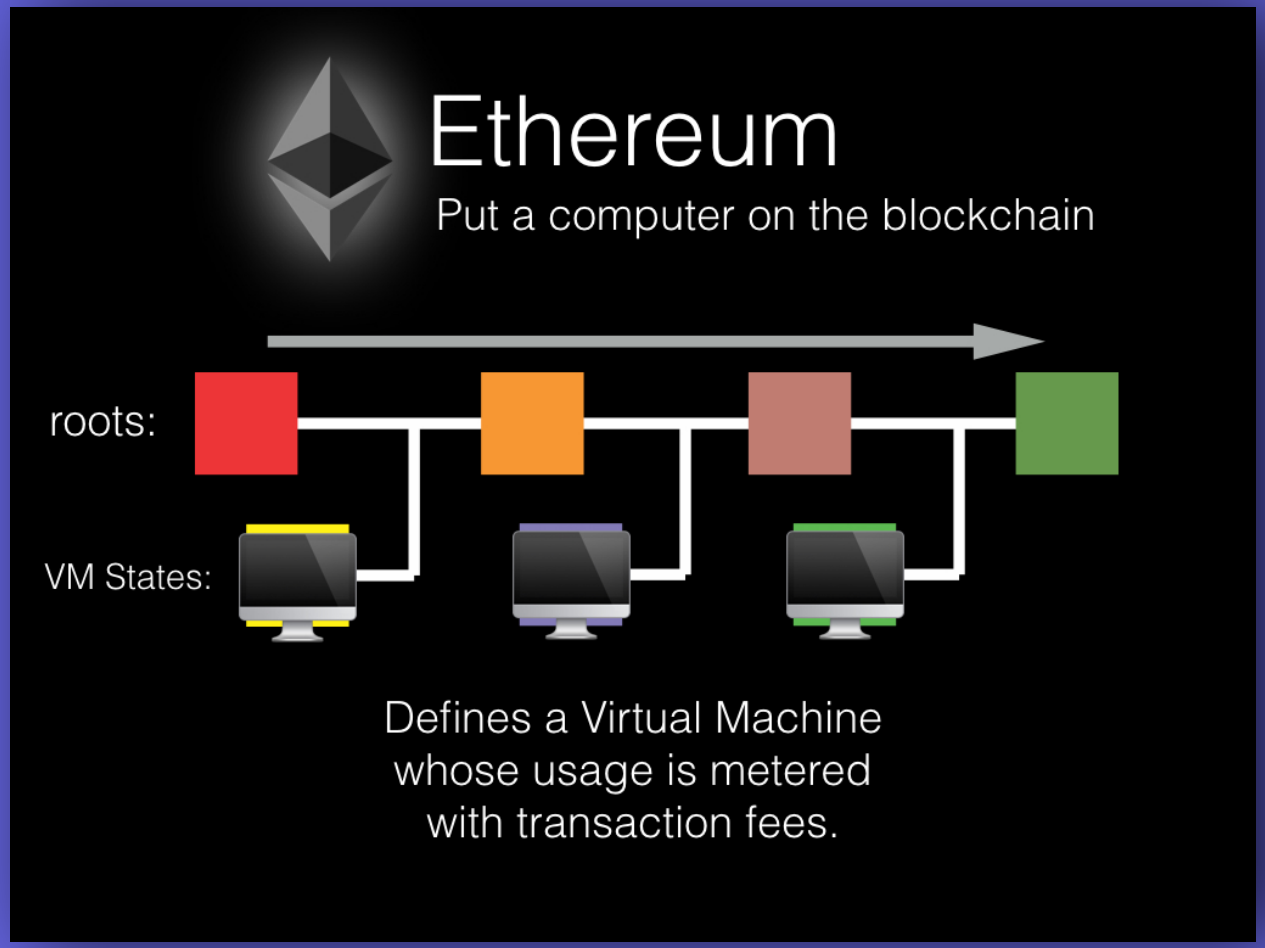
- Hash + hash = new root hash (new block)
- Full history is available
- Synchronized – specific ordering
- No “double spend”



trAse

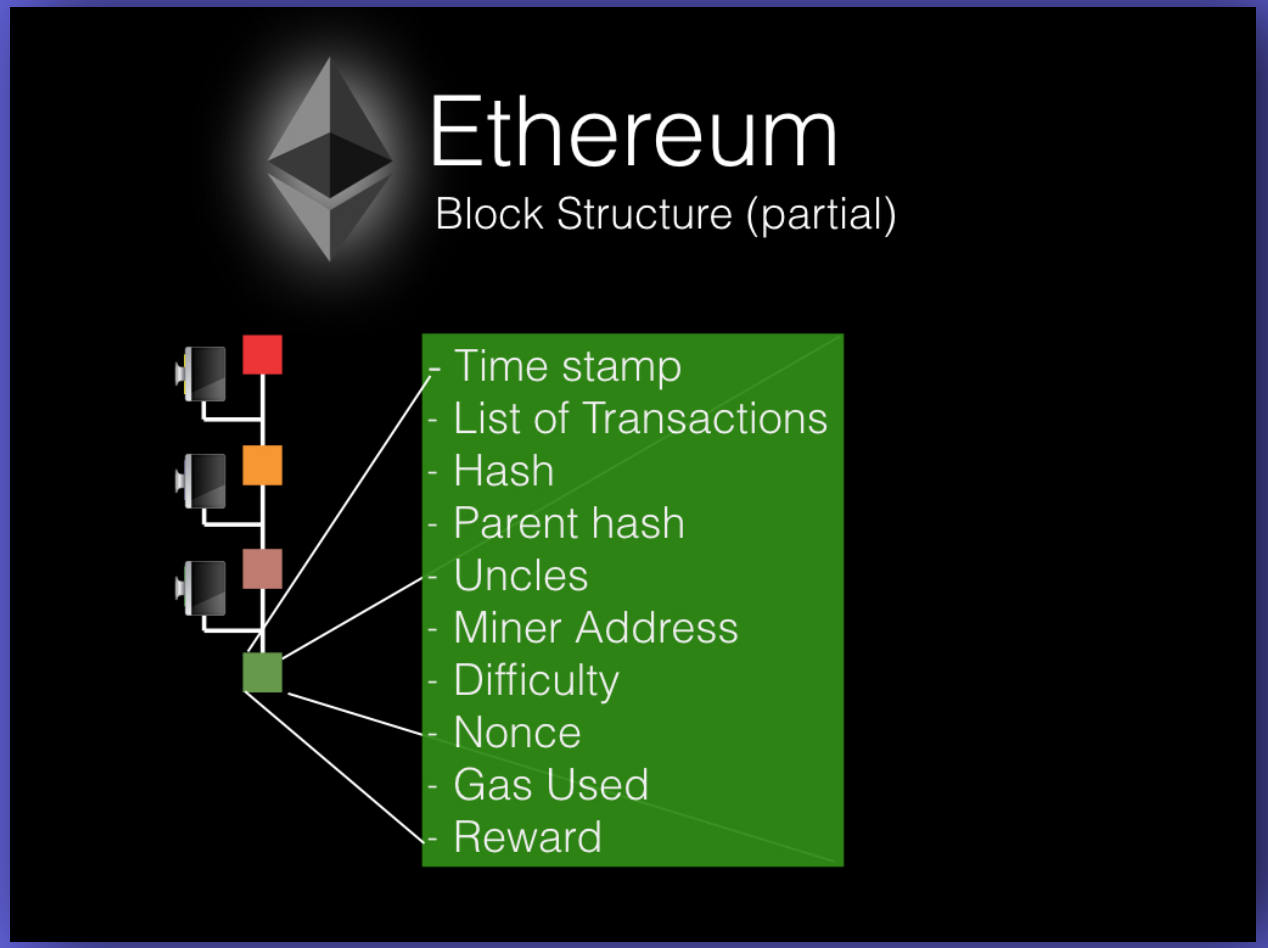
Ethereum

- Bitcoin —> Transactions
- Ethereum —> VM States
  - State updates (Computer operations)



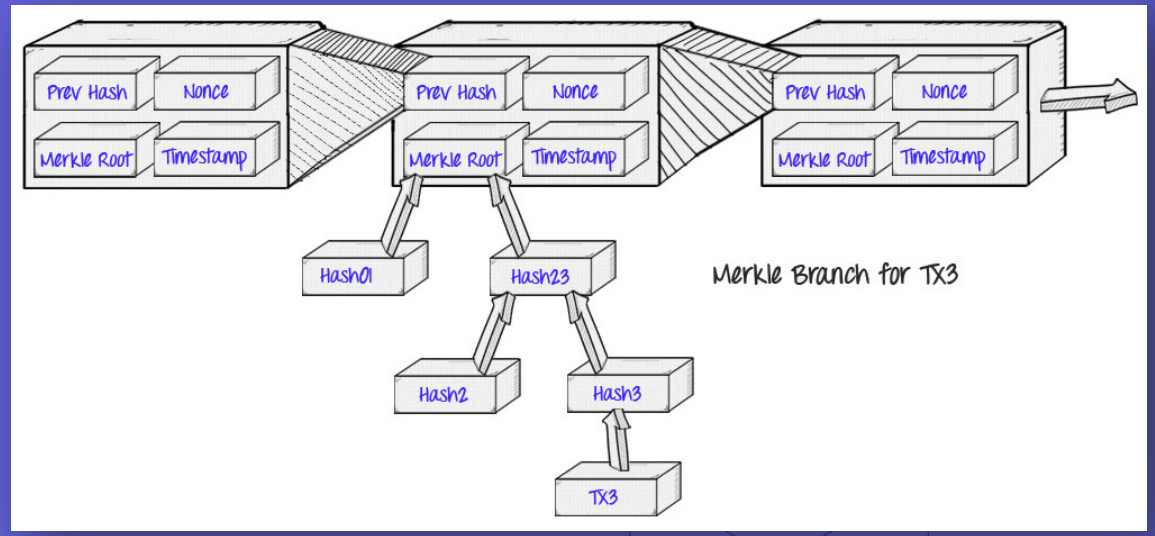
trAse

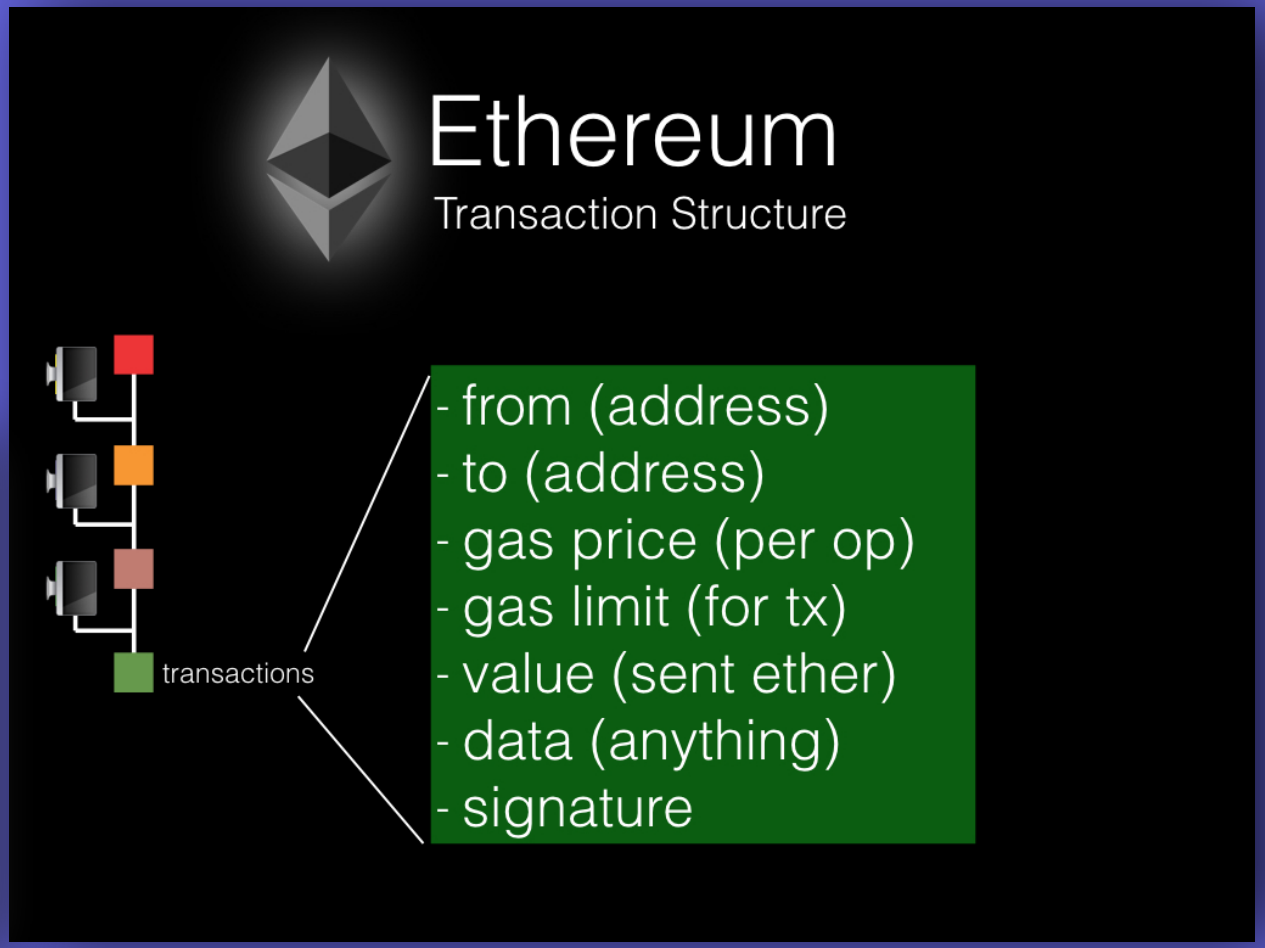
Block overview

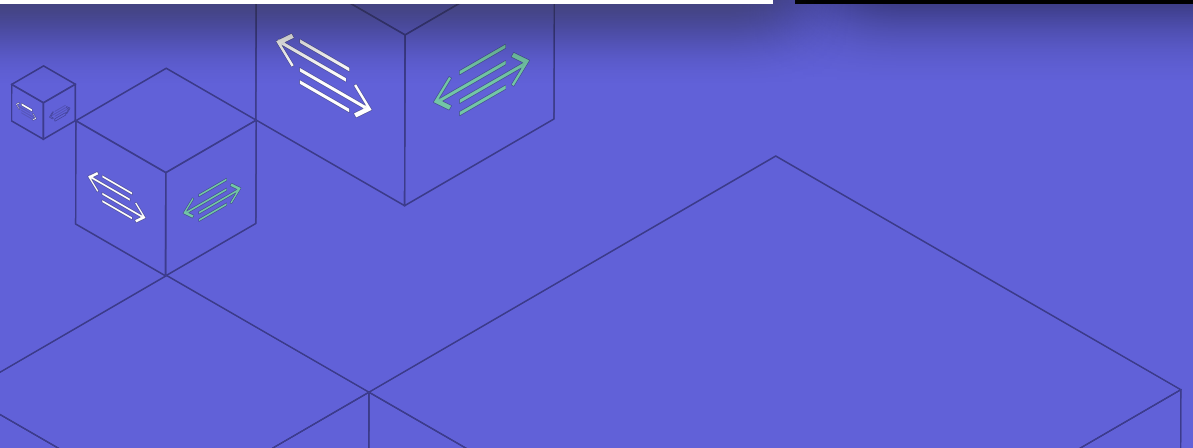


trAse

Transaction overview



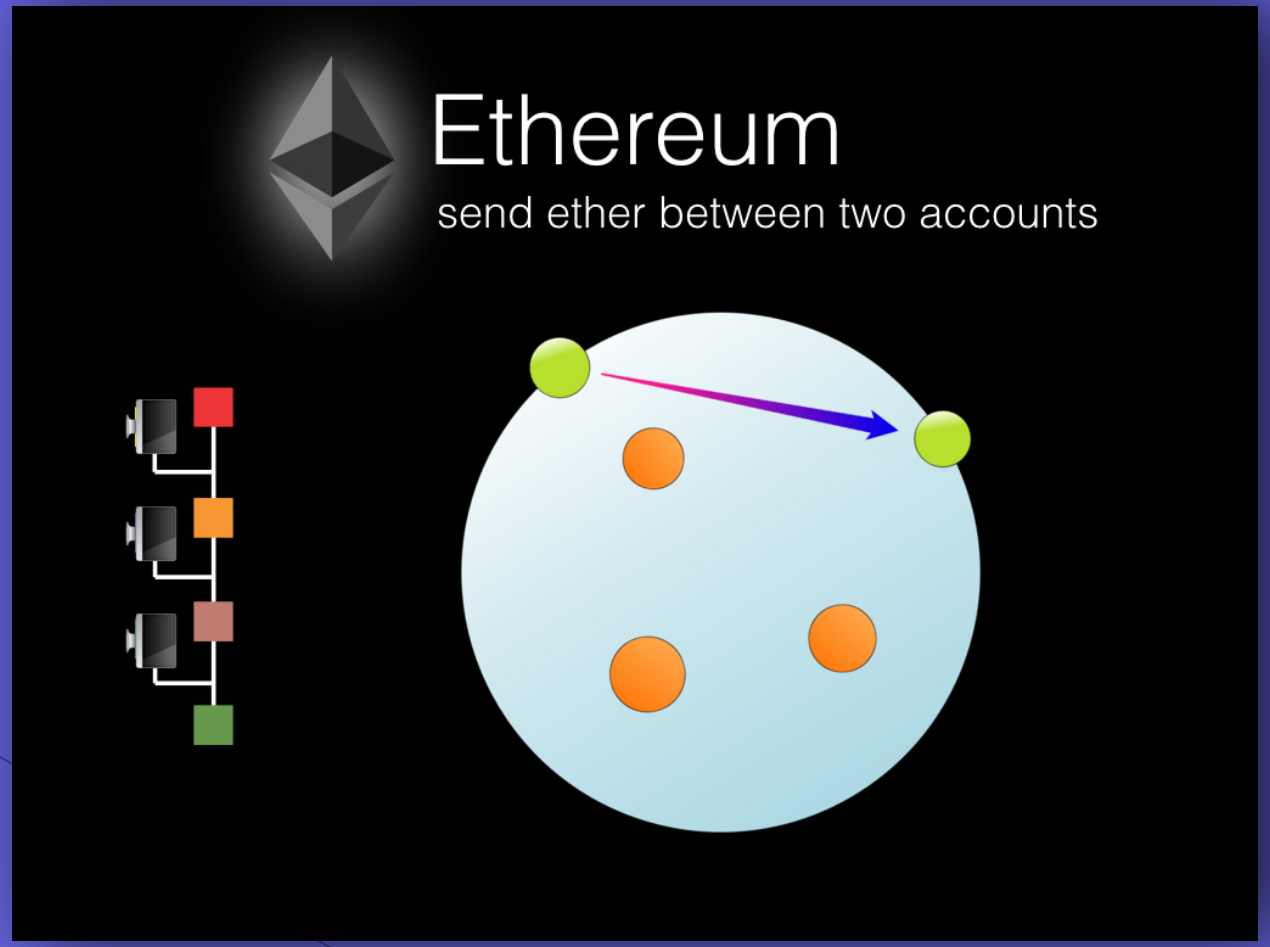




trAse

Transactions & Smart Contracts

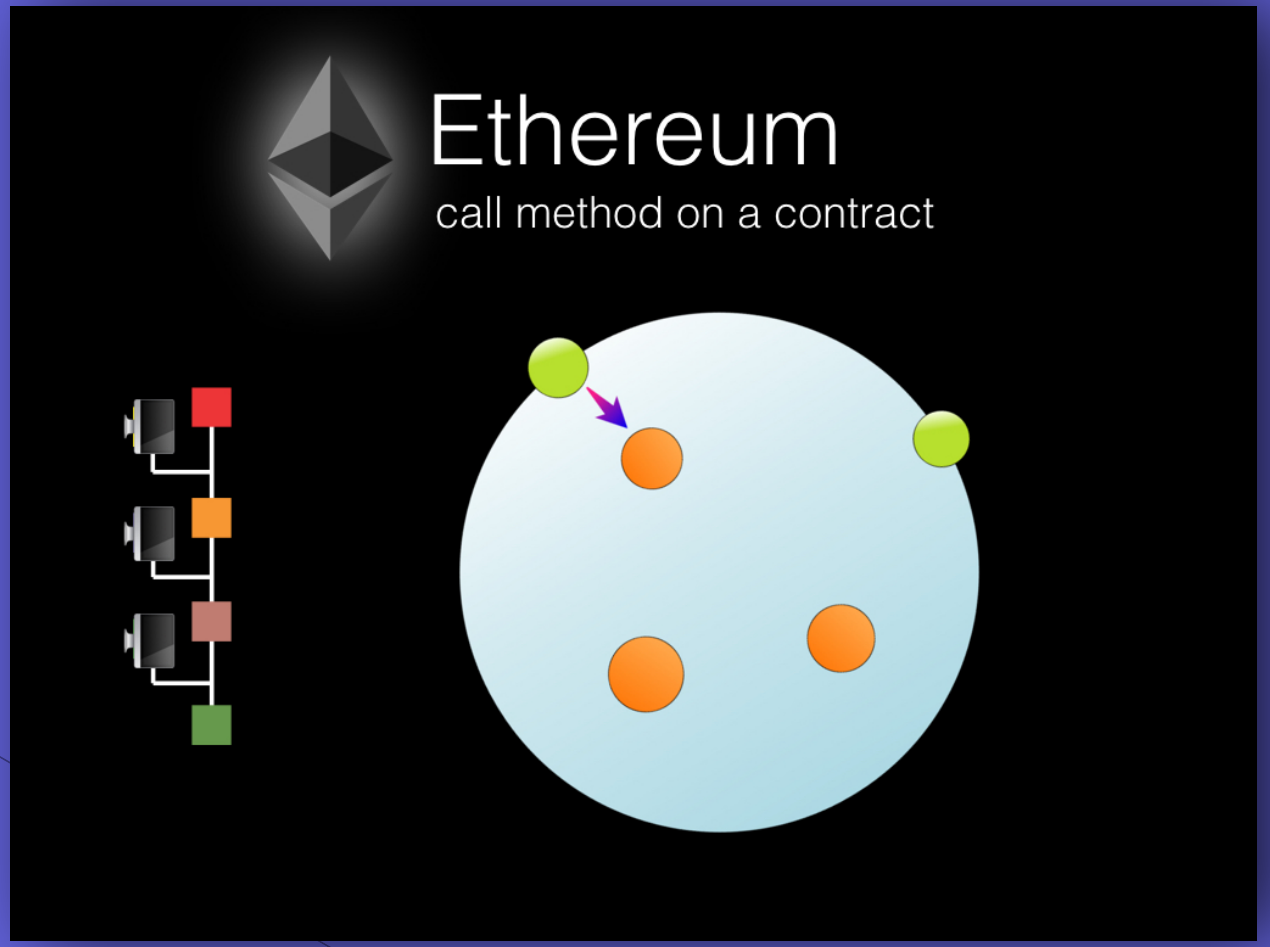
- Transactions between accounts accounts (ETH)



trAse

Transactions & Smart Contracts

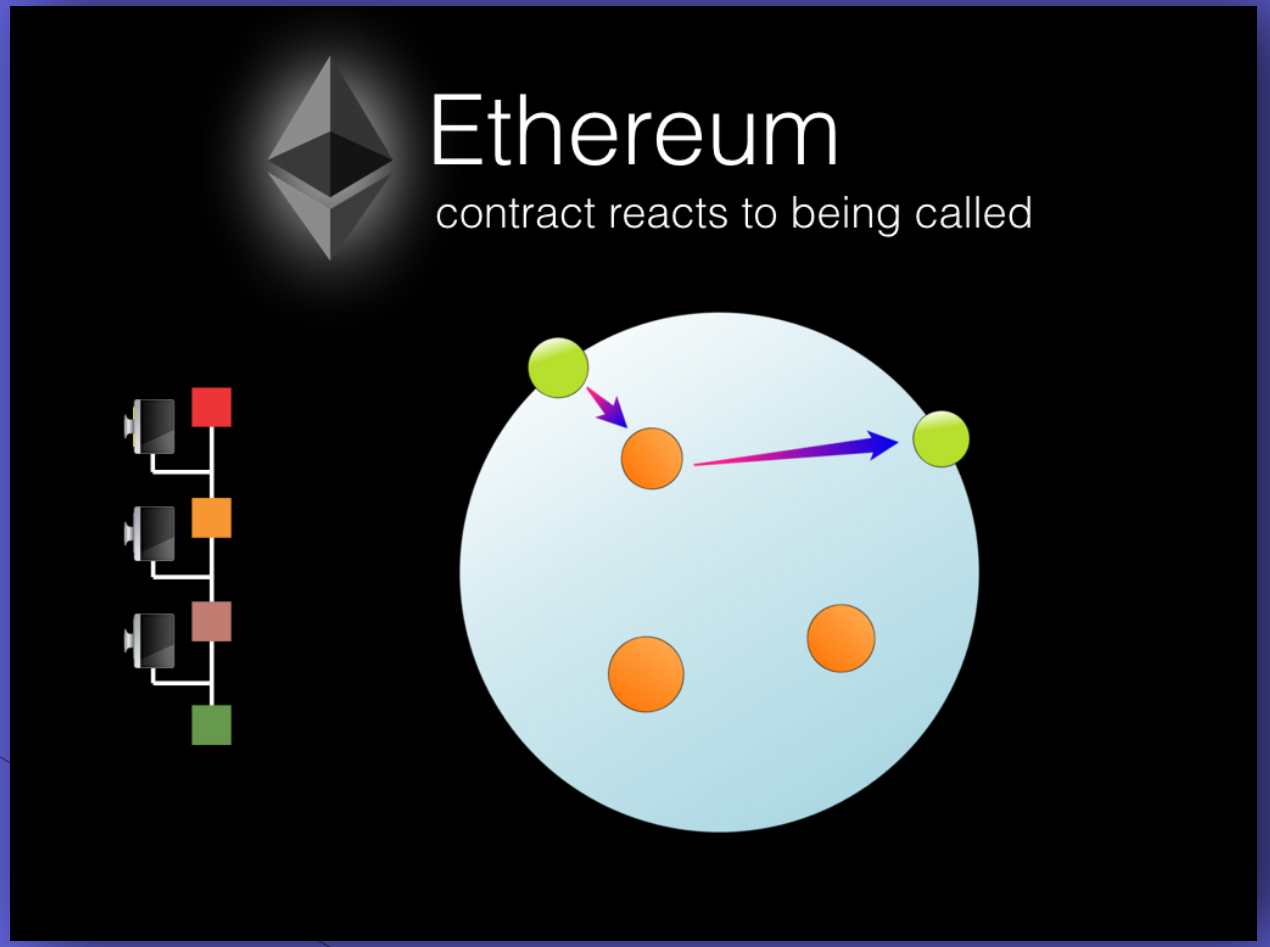
- Interactions with smart contracts



trAse

Transacties & Smart Contracts

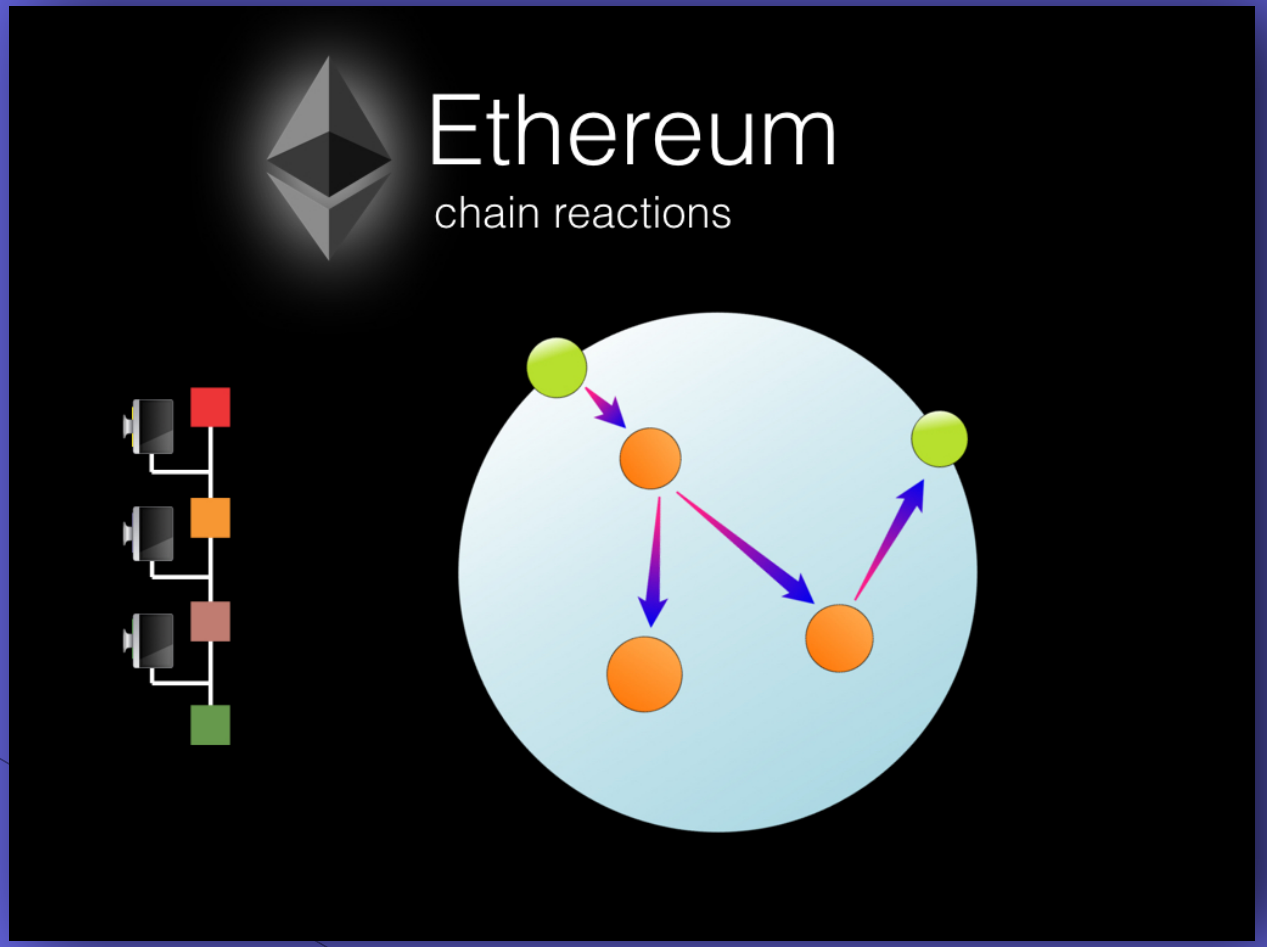
- Interactions with smart contracts that interact with users



trAse

Transactions & Smart Contracts

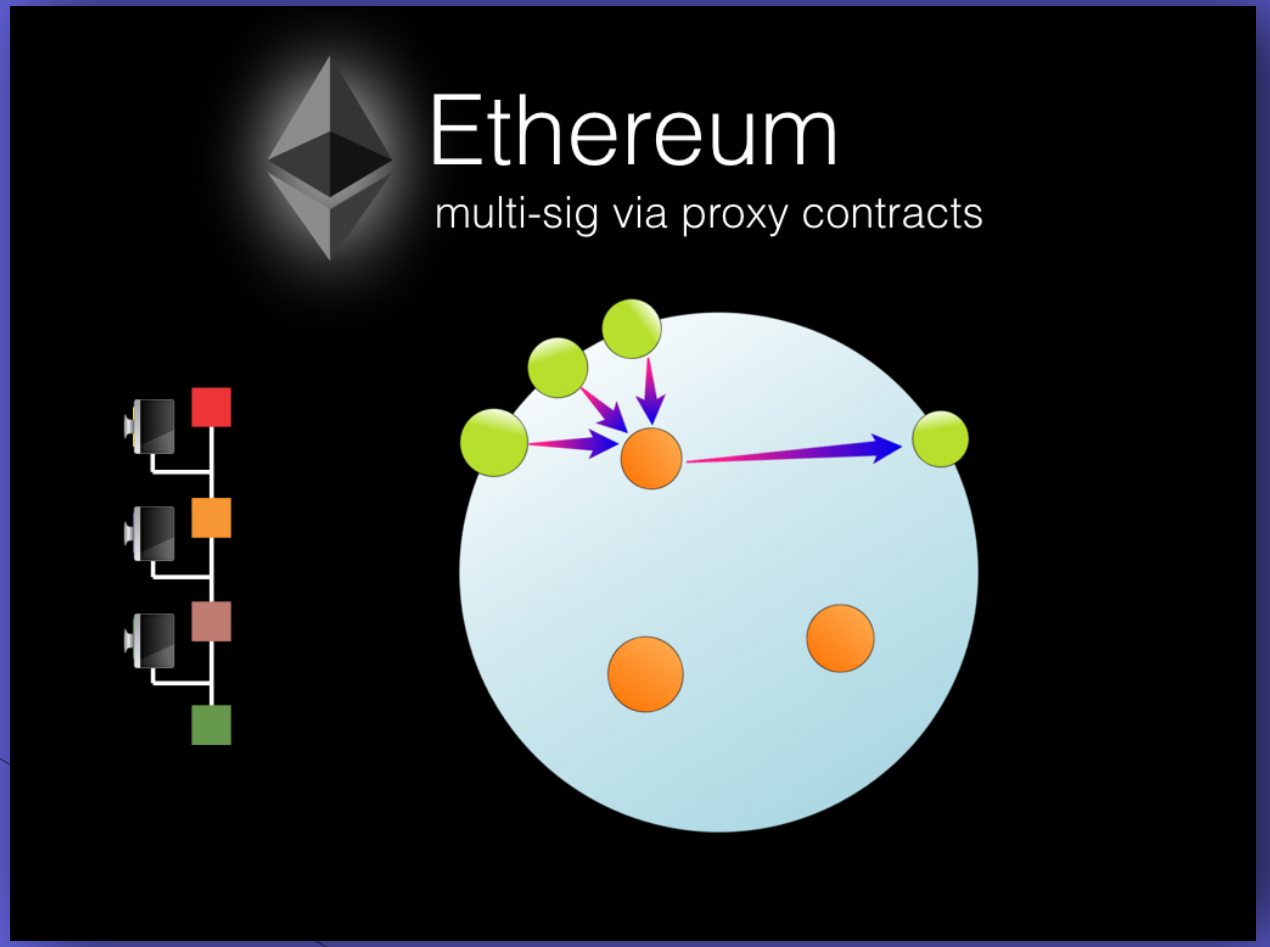
- Complex chain reactions



trAse

Transactions & Smart Contracts

- Complex chain reactions



trAse

Questions?

trAse


trAse