Blockchain

Network Security - Lecture

Ruxandra F. Olimid

Faculty of Mathematics and Computer Science

Agenda

- What is a blockchain?
- Motivation/utility
- Classifications
- General concepts (transactions, consensus mechanisms, forks, etc.)
- Smart Contracts
- Security aspects
- In more detail: Bitcoin

Necessity/Motivation

Read more:

Wüst, K., Gervais, A. “Do You Need a Blockchain?” IACR ePrint Archive, 2017, p. 375., https://eprint.iacr.org/2017/375.pdf

“Do You Need a Blockchain?” Do You Need a Blockchain?, http://doyouneedablockchain.com/

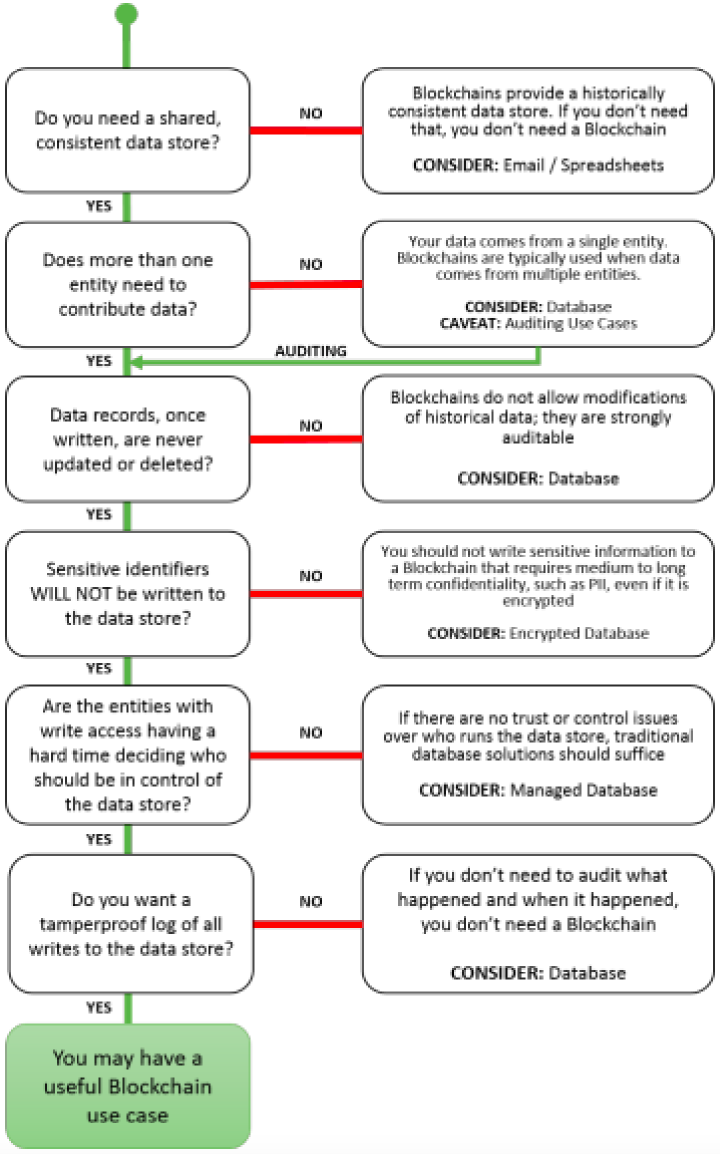


Figure 6 - DHS Science & Technology Directorate Flowchart

[Source: NISTIR 8202 –Yaga, D., Mell, P., Roby, N. and Scarfone, K., 2019. Blockchain Technology Overview]

Blockchain (I)

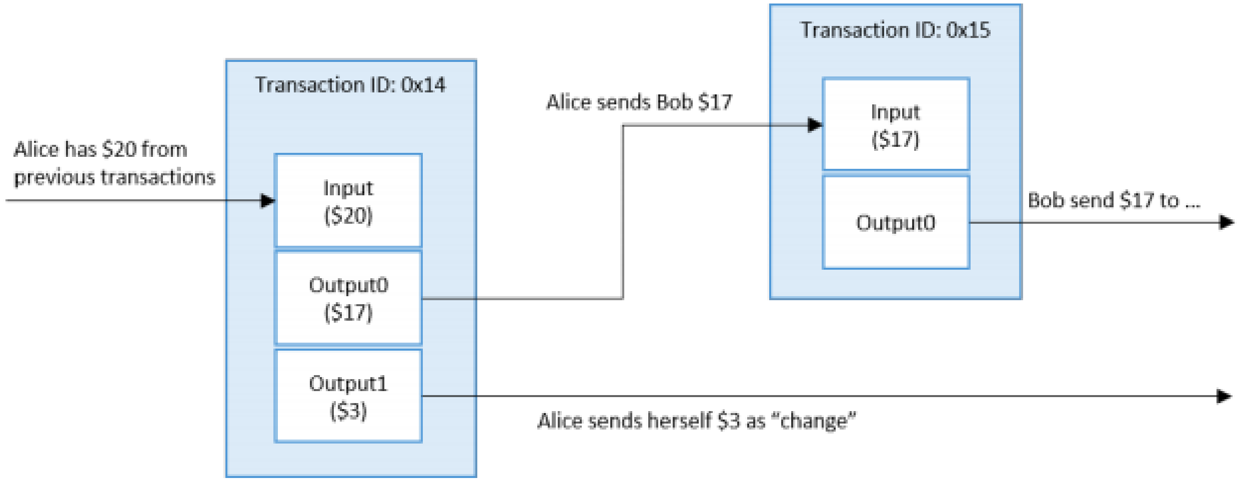


Figure 1 - Example Cryptocurrency Transaction

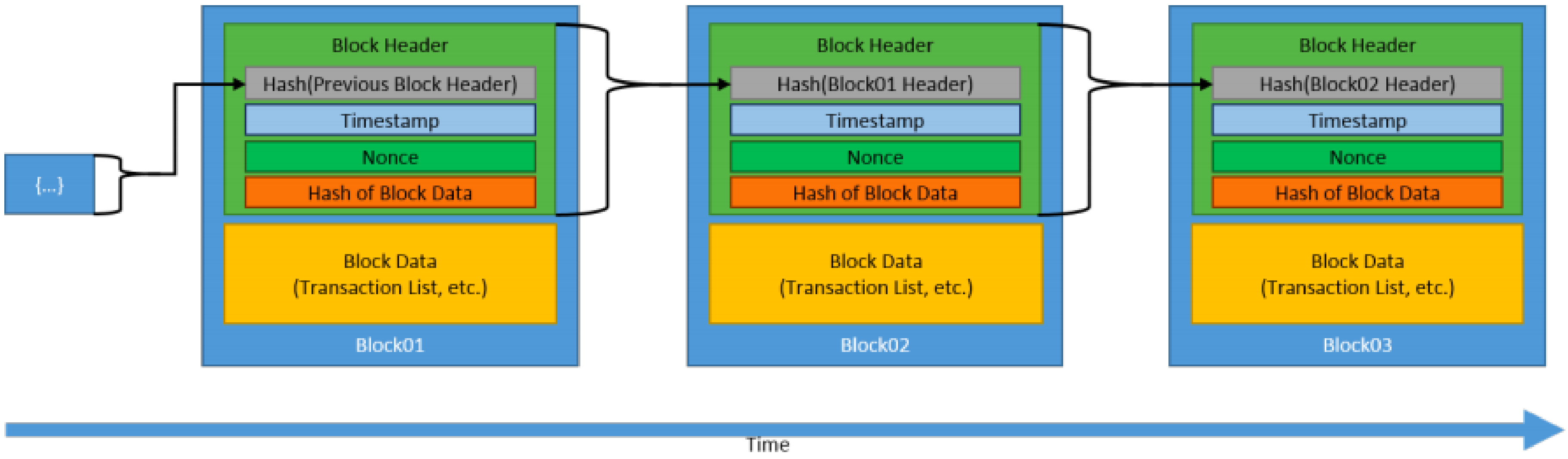


Figure 3: Generic Chain of Blocks

[Source: NISTIR 8202 –Yaga, D., Mell, P., Roby, N. and Scarfone, K., 2019. Blockchain Technology Overview]

Classification

- ***Permissionless***
  - Anyone can publish blocks (i.e., “open access” to the consensus protocol)
  - No need of an authority
  - Are **public** for writing (adding blocks) and reading (the data stored in the blockchain is public)
- ***Permissioned***
  - Only authorized nodes can add blocks
  - Needs an authority (not necessarily centralized)
  - Can be **private** for reading (only authorized nodes can read the data stored in the blockchain)

Classification

Table 1. Blockchain classification

	Permissionless	Permissioned
Type of nodes	Public (i.e., open to any node)	Private (i.e., open to nodes that are authorized by the authority that manages the blockchain)
Publish transactions / blocks	Public	Private
Read transactions / blocks	Public	Public **or** Private
Data visibility / availability	Public	Public **or** Private
No. of accepted nodes	Large and easily scalable	Low and usually not scalable for many nodes
Time to join the network	Faster to join the network (no authorization / registration)	Slower to join the network (authorization / registration required)
Governance	Publishing nodes, software developers	The owner / consortium of the blockchain
Consensus protocol	Usually slower and more expensive (in computational power and resources in general)	Usually faster and less expensive (in computational power and resources in general)
Software	Open-source, freely available for download	Open-source **or** Closed-source
Malicious nodes and majority domination	More predisposed to malicious nodes and 51% attack (e.g. Sybil attack)	Less predisposed to malicious nodes and 51% attack (legal measures can be taken against malicious nodes) but directly vulnerable to the owner of the blockchain, which has power to replace / change the blockchain blocks
Conflicts / Forks (resolved by consensus protocols)	More predisposed to conflicts / forks	Less predisposed to conflicts / forks
End of life	Difficult (nodes might continue to run)	Easy (legal measures might be taken against nodes still running)

[Source: Panait, A.E., Olimid, R.F. and Stefanescu, A., 2020. Identity Management on Blockchain--Privacy and Security Aspects. *arXiv preprint arXiv:2004.13107*. Extended version of a paper published at RCD'19]

Consensus mechanisms (I)

[Source: NISTIR 8202 – Yaga, D., Mell, P., Roby, N. and Scarfone, K., 2019. Blockchain Technology Overview]

Name	Goals	Advantages	Disadvantages	Domains	Implementations
Proof of work (PoW)	To provide a barrier to publishing blocks in the form of a computationally difficult puzzle to solve to enable transactions between untrusted participants.	Difficult to perform denial of service by flooding network with bad blocks. Open to anyone with hardware to solve the puzzle.	Computationally intensive (by design), power consumption, hardware arms race. Potential for 51 % attack by obtaining enough computational power.	Permissionless cryptocurrencies	Bitcoin, Ethereum, many more
Proof of stake (PoS)	To enable a less computationally intensive barrier to publishing blocks, but still enable transactions between untrusted participants.	Less computationally intensive than PoW. Open to anyone who wishes to stake cryptocurrencies. Stakeholders control the system.	Stakeholders control the system. Nothing to prevent formation of a pool of stakeholders to create a centralized power. Potential for 51 % attack by obtaining enough financial power.	Permissionless cryptocurrencies	Ethereum Casper, Krypton
Delegated PoS	To enable a more efficient consensus model through a 'liquid democracy' where participants vote (using cryptographically signed messages) to elect and revoke the rights of delegates to validate and secure the blockchain.	Elected delegates are economically incentivized to remain honest More computationally efficient than PoW	Less node diversity than PoW or pure PoS consensus implementations Greater security risk for node compromise due to constrained set of operating nodes As all delegates are 'known' there may an incentive for block producers to collude and accept bribes, compromising the security of the system	Permissionless cryptocurrencies Permissioned Systems	Bitshares, Steem, Cardano, EOS

Consensus mechanisms (II)

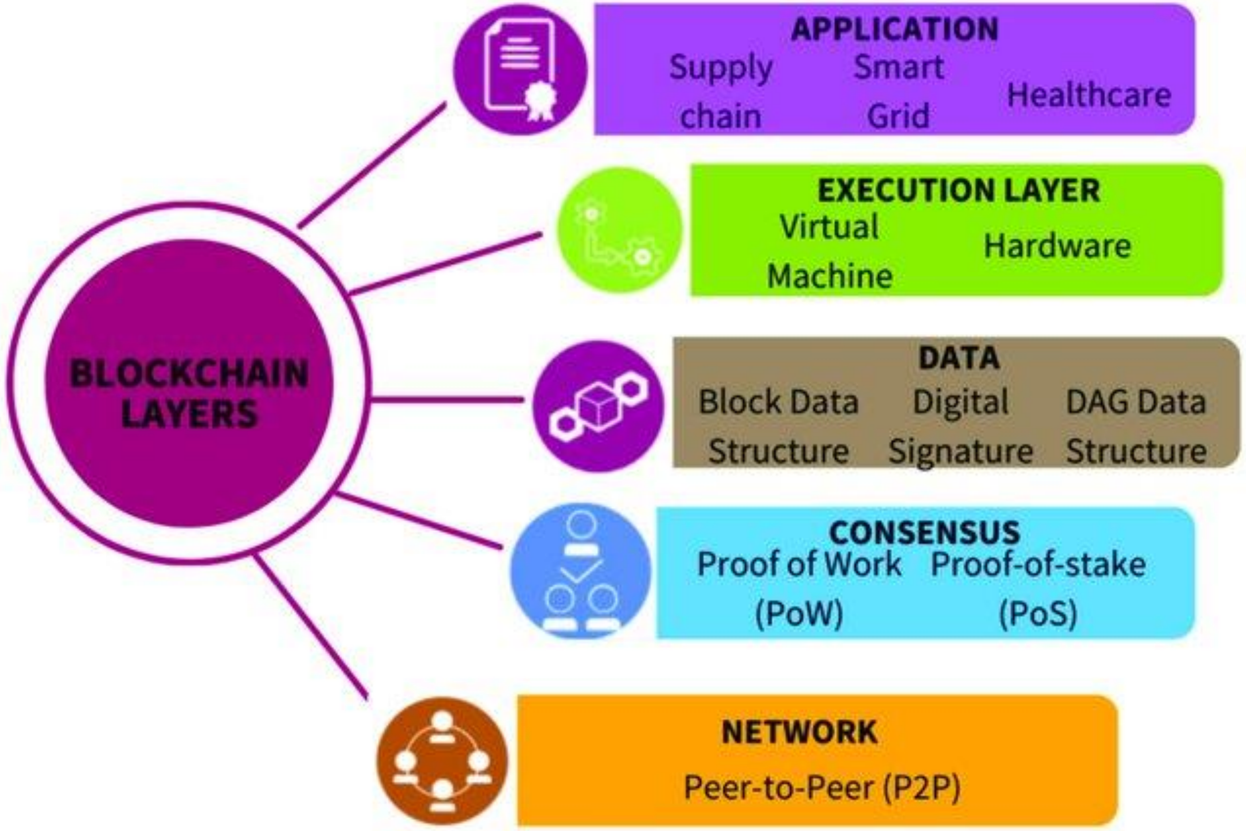
[Source: NISTIR 8202 – Yaga, D., Mell, P., Roby, N. and Scarfone, K., 2019. Blockchain Technology Overview]

Name	Goals	Advantages	Disadvantages	Domains	Implementations
Round Robin	Provide a system for publishing blocks amongst approved/trusted publishing nodes	Low computational power. Straightforward to understand.	Requires large amount of trust amongst publishing nodes.	Permissioned Systems	MultiChain
Proof of Authority/Identity	To create a centralized consensus process to minimize block creation and confirmation rate	Fast confirmation time Allows for dynamic block production rates Can be used in sidechains to blockchain networks which utilize another consensus model	Relies on the assumption that the current validating node has not been compromised Leads to centralized points of failure The reputation of a given node is subject to potential for high tail-risk as it could be compromised at any time.	Permissioned Systems, Hybrid (sidechain) Systems	Ethereum Kovan testnet, POA Chain, various permissioned systems using Parity
Proof of Elapsed Time (PoET)	To enable a more economic consensus model for blockchain networks, at the expense of deeper security guarantees associated with PoW.	Less computationally expensive than PoW	Hardware requirement to obtain time. Assumes the hardware clock used to derive time is not compromised Given speed-of-late latency limits, true time synchronicity is essentially impossible in distributed systems [13]	Permissioned Networks	Hyperledger Sawtooth

Forks

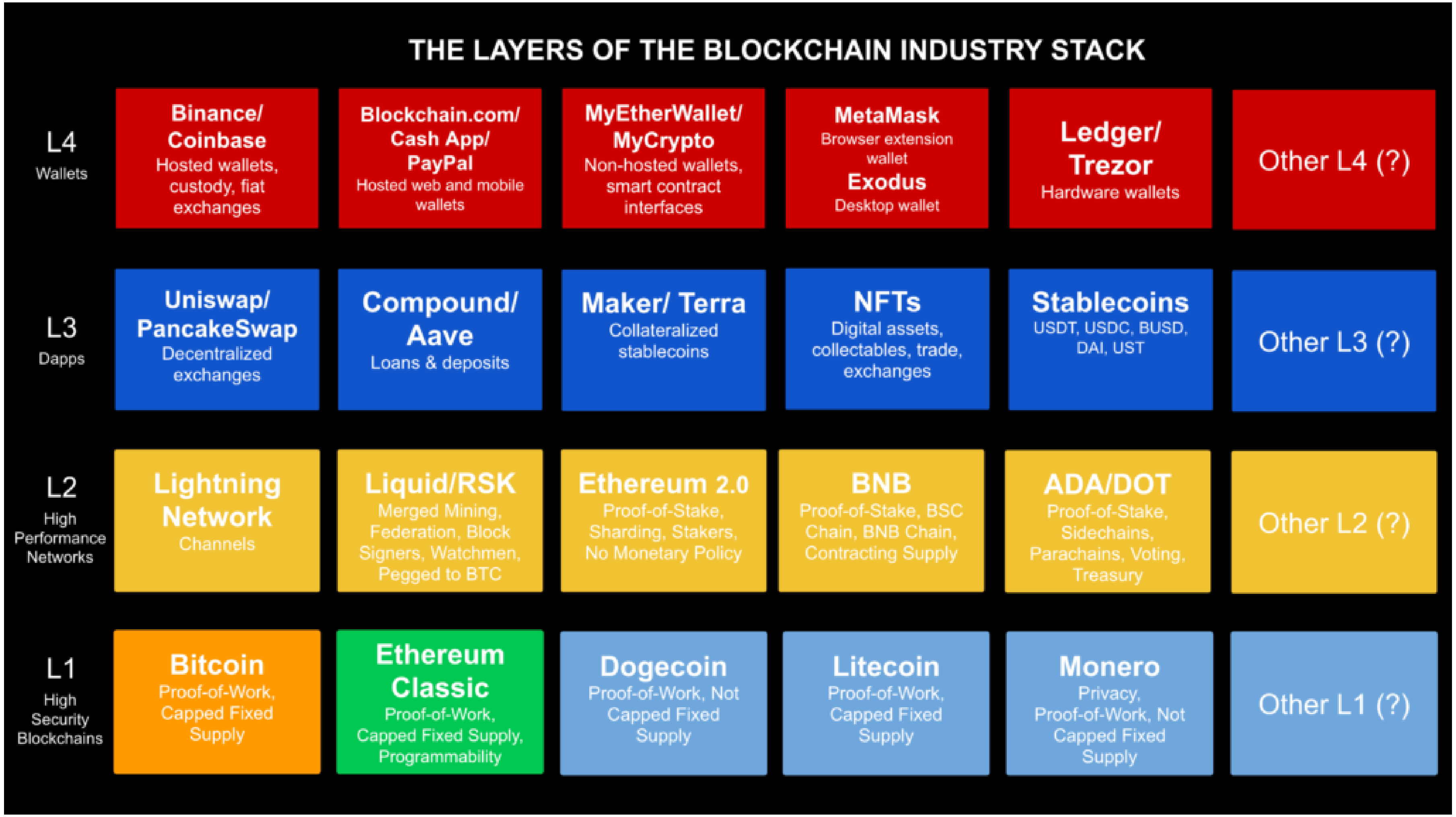
- ***Soft fork***
  - Accepts backwards compatibility
  - If there are not enough nodes to accept the new rules, the new rules will not come in place
- ***Hard fork***
  - Does not accept backwards compatibility
  - All the nodes need to accept, if not the blockchain will split in two (the old/initial version and the new version)

Blockchain Layers



[Source: Zheng, J., Dike, C., Pancari, S., Wang, Y., Giakos, G. C., Elmannai, W., & Wei, B. (2022). An in-depth review on blockchain simulators for iot environments. *Future Internet*, *14*(6), 182.]

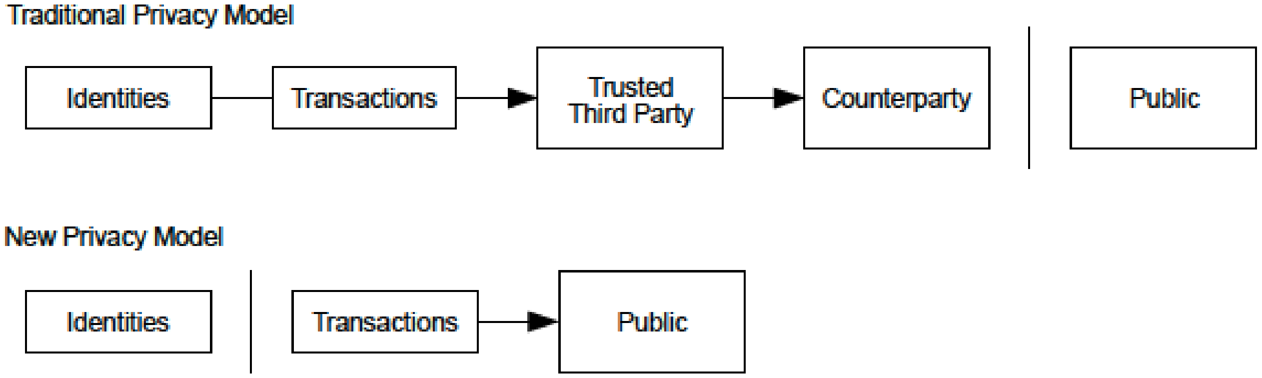
Blockchain Layers



[Source: https://etherplan.com/2021/05/12/ethereum-classic-price-predictions-for-the-current-and-coming-crypto-cycles/15792/the-layers-of-the-blockchain-indsutry-stack/]

Bitcoin

- Digital money
- Who is Satoshi Nakamoto?
- **Double-spending**?! Privacy / anonymity?! Decentralization ?!

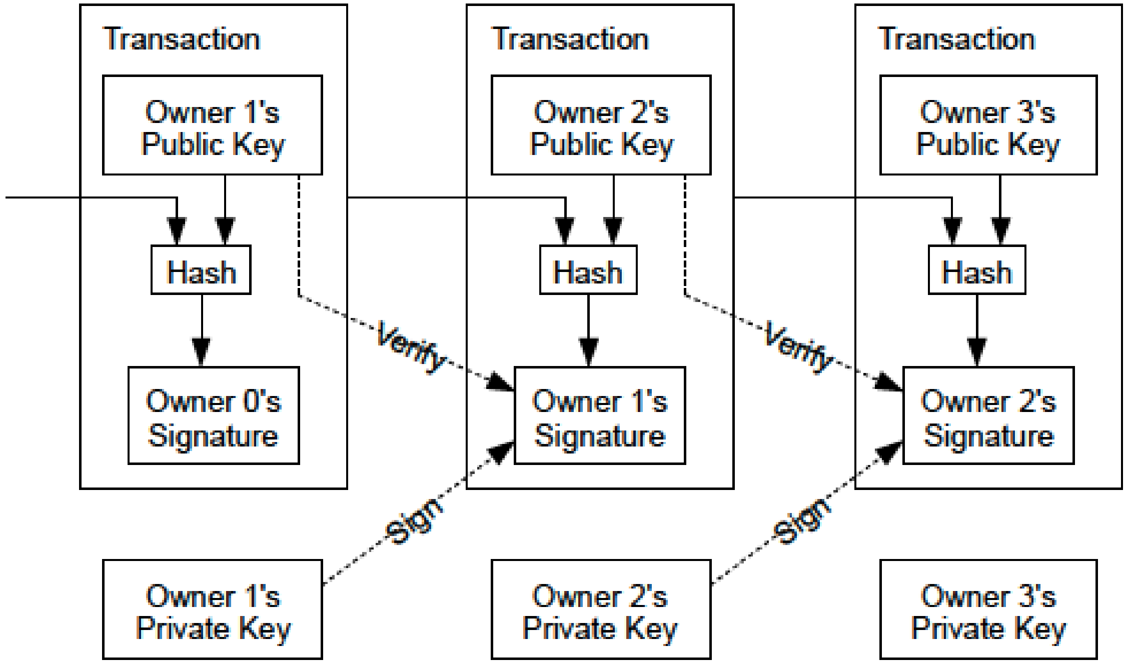


[Source: Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system.]

Transactions

[Source: Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system]

*“We define an **electronic coin** as a **chain of digital signatures**. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin.”*



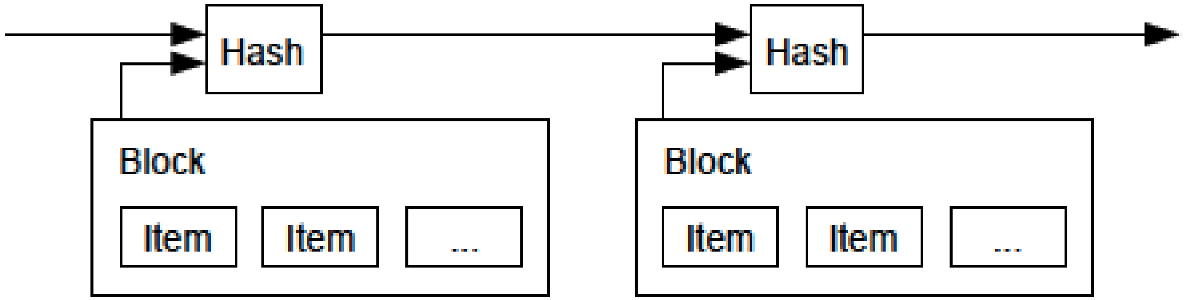
[Source: Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system.]

Timestamp server & Proof-of-Work (PoW)

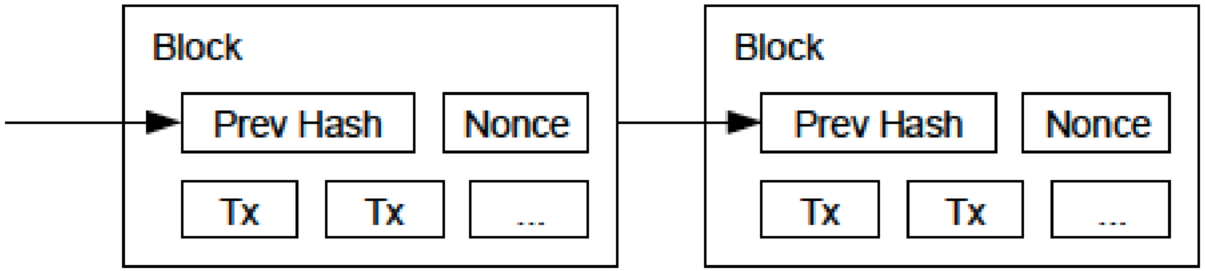
Consensus mechanism

Proof-of-Work (PoW): a problem difficult to solve (time/resource consuming)

Which is the difficult problem in case of Bitcoin?



Timestamp server



Proof of work

[Source: Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system.]

Proof-of-Work

Main idea: The longest chain wins

Direct vulnerability: the majority decides (51% attack)

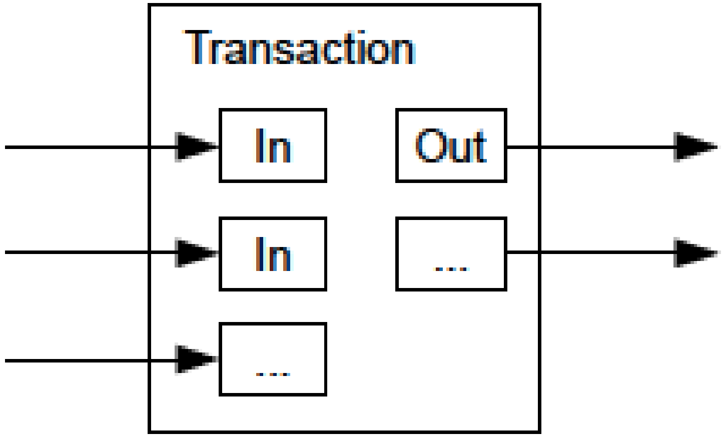
The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

[Source: Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system.]

Bitcoin mining

- *Initial block* – block 0, created by the initiator of the blockchain
- The difficulty of the hard problem is increasing in time (i.e., the required numbers of 0s in the hash value)
- Why mining? Advantages vs. disadvantages
- **Incentive**: the difference between the entrance and the exit “money” remain to the block miner



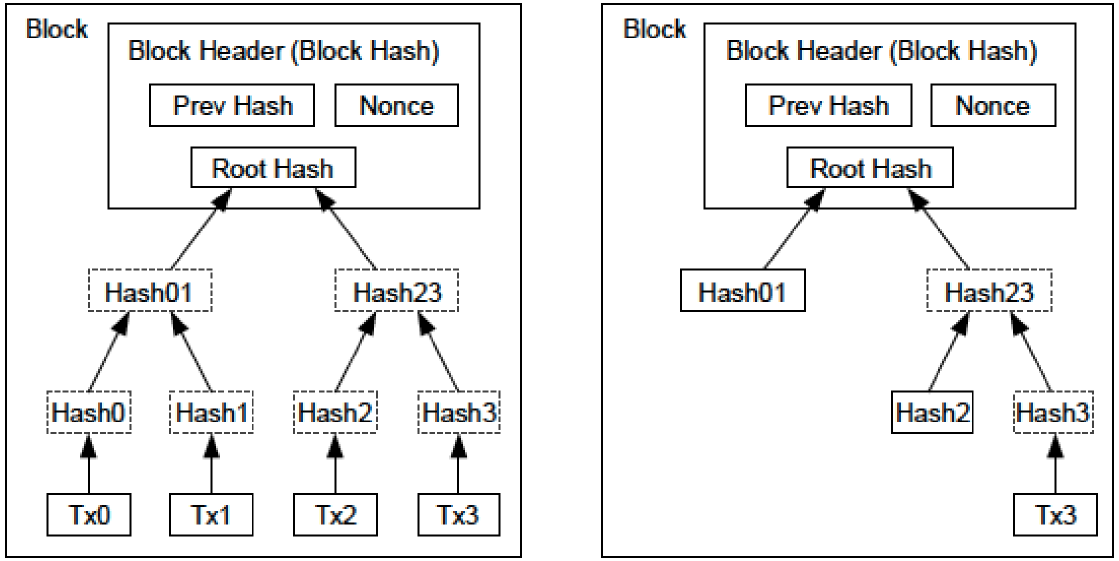
[Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system]

Why there are/might be more inputs/outputs in a transactions?

Merkle Trees

Save memory space: transactions of old blocks are stored as **Merkle Root.**

What is a **Merkle Tree / Merkle Root**?

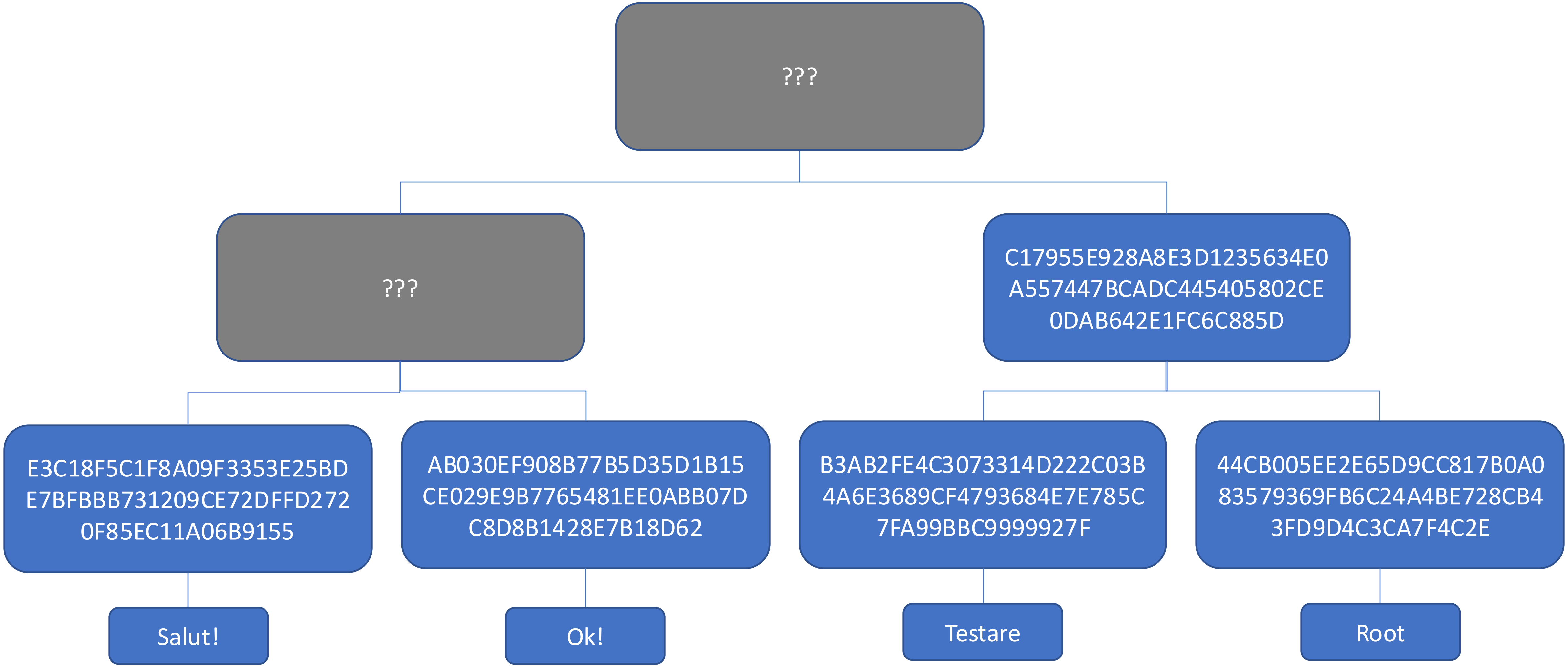


Transactions Hashed in a Merkle Tree

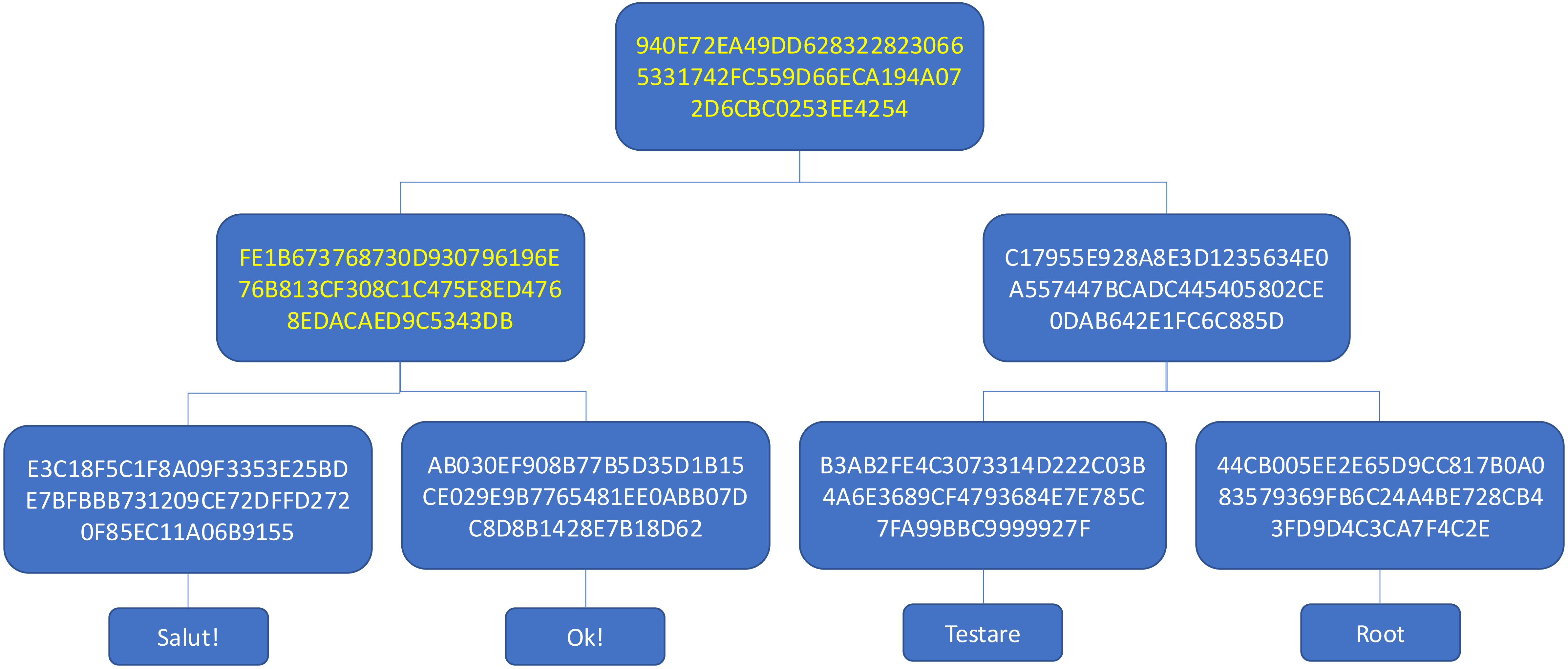
After Pruning Tx0-2 from the Block

[Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system]

Exercise – Toy Merkle Tree (SHA-256)



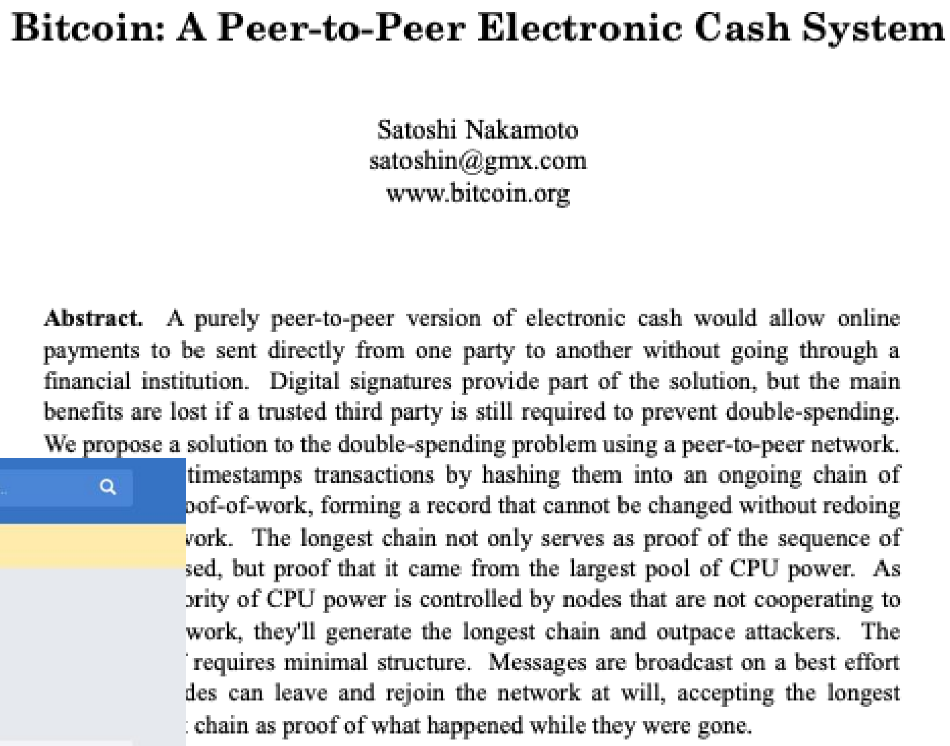
Exercise – Toy Merkle Tree (SHA-256)



Bitcoin Difficulty/Discussions

- Chart: https://bitinfocharts.com/comparison/bitcoin-difficulty.html
- Increasing difficulty: more nonces (even timestamps!) need to be checked
- Max.21 millions bitcoins (~ in 2140 *block reward* will stop; it is getting half every 4 years) – implementation constraints
- Double-spending?! Privacy / anonymity?! descentralization ?!

More about blockchain



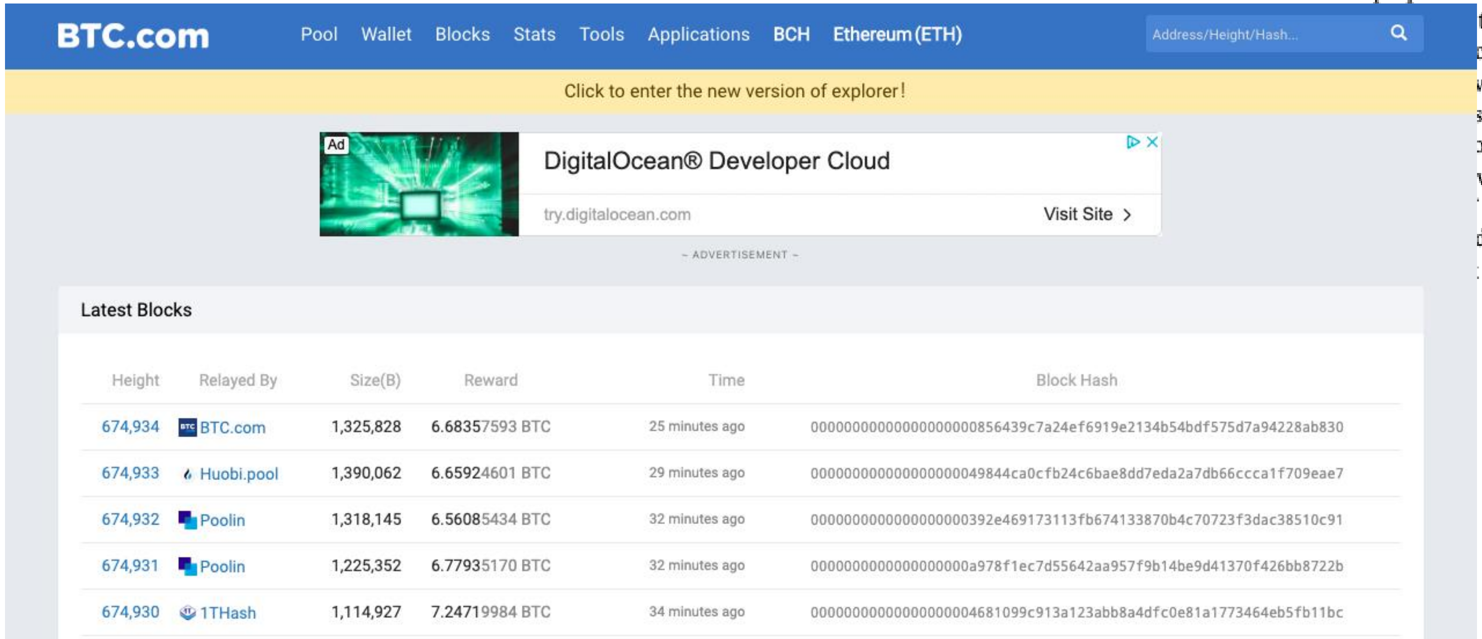
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. timestamps transactions by hashing them into an ongoing chain of oof-of-work, forming a record that cannot be changed without redoing vork. The longest chain not only serves as proof of the sequence of sed, but proof that it came from the largest pool of CPU power. As ority of CPU power is controlled by nodes that are not cooperating to work, they'll generate the longest chain and outpace attackers. The requires minimal structure. Messages are broadcast on a best effort des can leave and rejoin the network at will, accepting the longest chain as proof of what happened while they were gone.

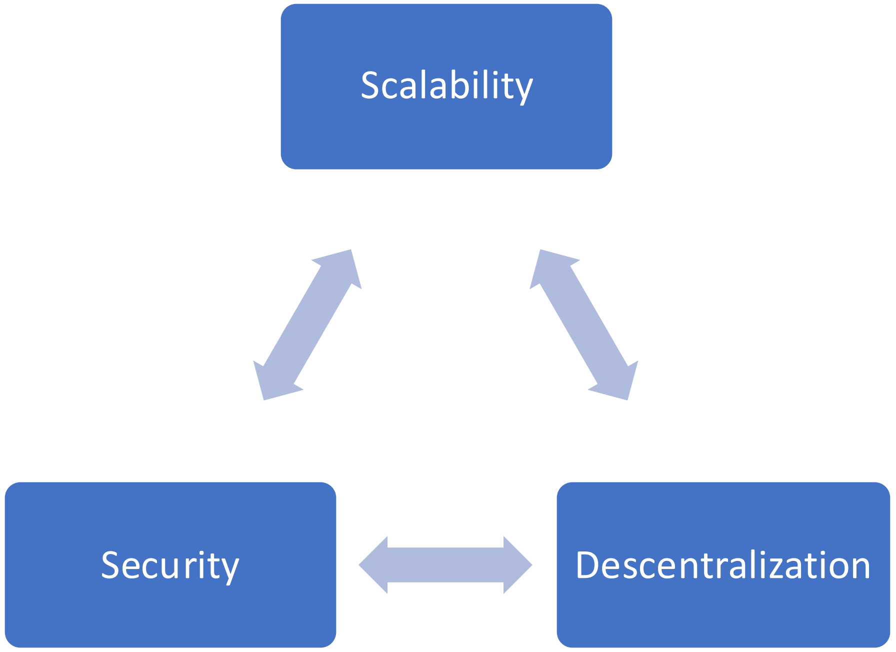
[Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system]

https://btc.com/



Height	Relayed By	Size(B)	Reward	Time	Block Hash
674,934	BTC.com	1,325,828	6.68357593 BTC	25 minutes ago	00000000000000000000856439c7a24ef6919e2134b54bdf575d7a94228ab830
674,933	Huobi.pool	1,390,062	6.65924601 BTC	29 minutes ago	000000000000000000049844ca0cfb24c6bae8dd7eda2a7db66ccca1f709eae7
674,932	Poolin	1,318,145	6.56085434 BTC	32 minutes ago	0000000000000000000392e469173113fb674133870b4c70723f3dac38510c91
674,931	Poolin	1,225,352	6.77935170 BTC	32 minutes ago	0000000000000000000a978f1ec7d55642aa957f9b14be9d41370f426bb8722b
674,930	1THash	1,114,927	7.24719984 BTC	34 minutes ago	00000000000000000004681099c913a123abb8a4dfc0e81a1773464eb5fb11bc

Blockchain Trilemma



Algorand – the first blockchain implementation that claims to satisfy all three properties

https://www.algorand.com/

[S.Micali. Algorand's Core Technology (in a nutshell)]

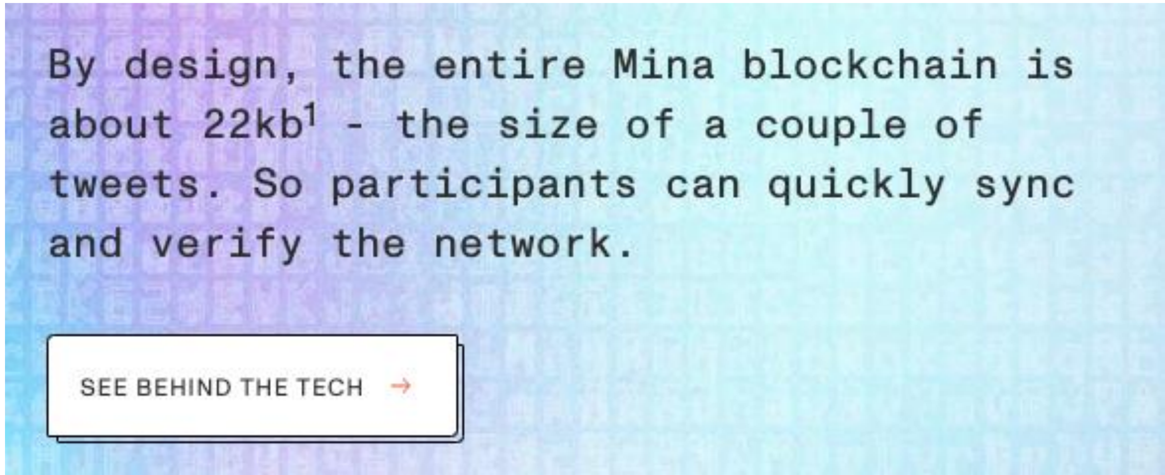
PRF verificabil pe baza unei demonstratii, folosind o cheie de verificare

Algorand – consensus protocol: *Pure Proof of Stake* + use of *Verifiable Random Function* (VRF) :

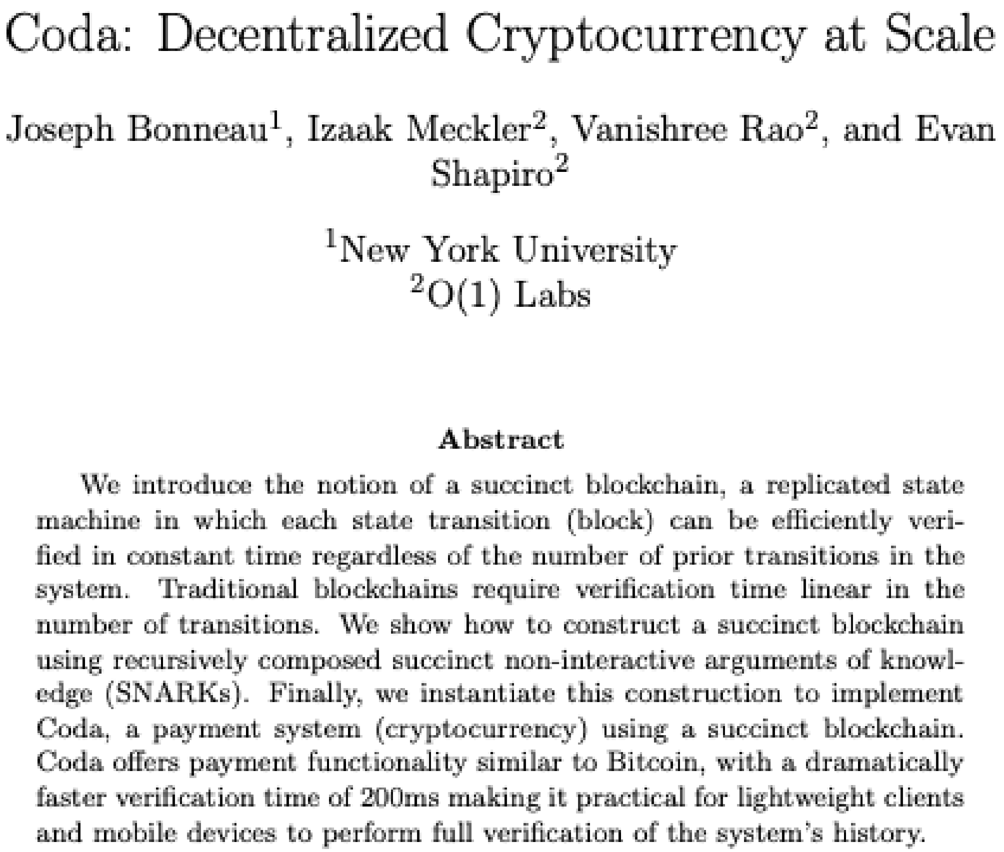
[Algorand, *Algorand Blockchain Core Protocol Overview*: https://youtu.be/gACVKaNqxPs (video)]

Mina (previous Coda)

Coda vs. Corda ☺



https://minaprotocol.com/



Coda: Decentralized Cryptocurrency at Scale

Joseph Bonneau[1], Izaak Meckler[2], Vanishree Rao[2], and Evan Shapiro[2]

[1]New York University
[2]O(1) Labs

Abstract

We introduce the notion of a succinct blockchain, a replicated state machine in which each state transition (block) can be efficiently verified in constant time regardless of the number of prior transitions in the system. Traditional blockchains require verification time linear in the number of transitions. We show how to construct a succinct blockchain using recursively composed succinct non-interactive arguments of knowledge (SNARKs). Finally, we instantiate this construction to implement Coda, a payment system (cryptocurrency) using a succinct blockchain. Coda offers payment functionality similar to Bitcoin, with a dramatically faster verification time of 200ms making it practical for lightweight clients and mobile devices to perform full verification of the system's history.

[Source: Bonneau, J., Meckler, I., Rao, V. and Shapiro, E., 2020. Coda: Decentralized Cryptocurrency at Scale. *IACR Cryptol. ePrint Arch., 2020*, p.352]

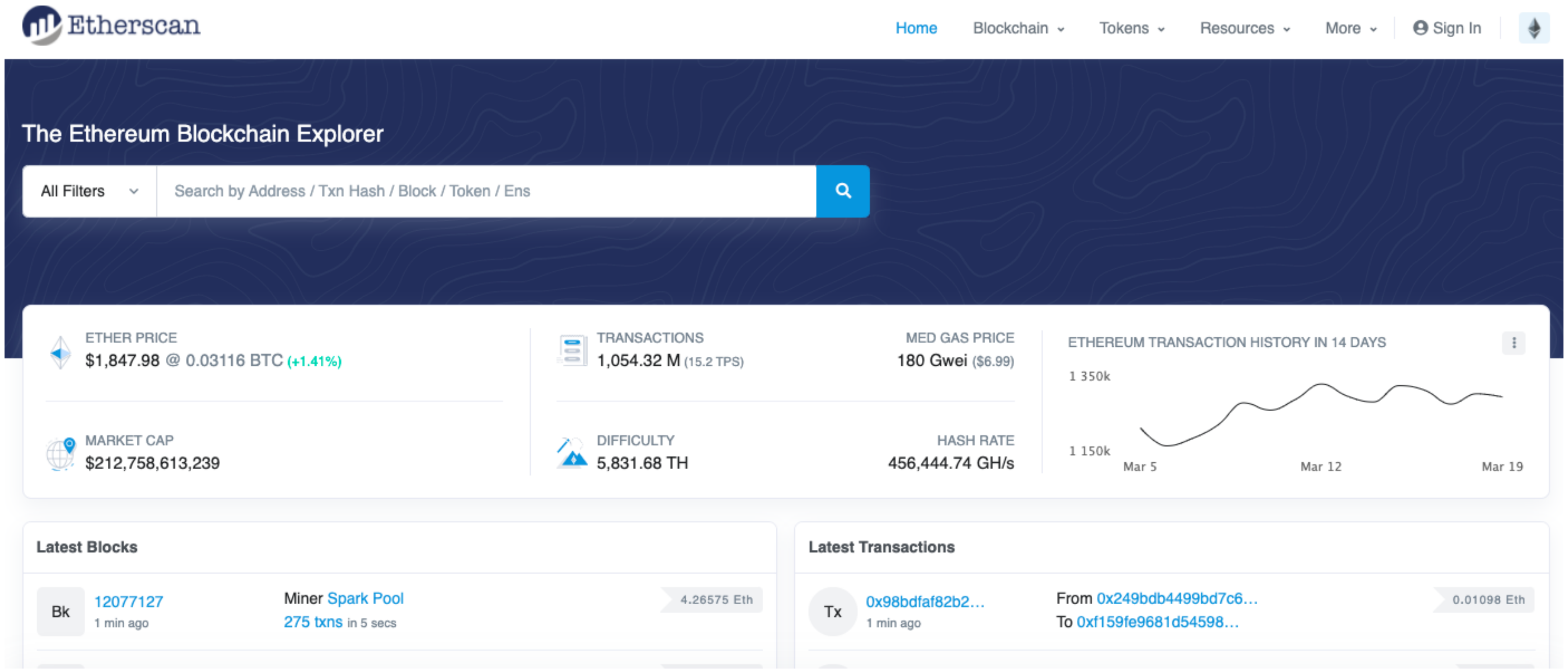
Smart Contracts

- Ethereum:
  - Programming languages: Solidity, Vyper

https://ethereum.org/en/developers/docs/smart-contracts/languages/

- Explorer:
  - Etherscan

https://etherscan.io/



Security problems

- Post-quantum cryptography (a risk for the asymmetric cryptography)
- **Immutability** – 51% attack (the blockchain can change!), storing sensitive data (once in the blockchain they usually remain in the blockchain, computational security!)
- DoS on smart contracts, malicious nodes, etc.
- Trust: majority decides, trust in software (e.g., wallets), trust full nodes, etc.
- Resources – a problem in efficiency and scalability
- …