Introduction to Blockchains

Sushmita Ruj

Recap

- Public Key Infrastructure
- PGP
- Certificates
- Certificate Revocation
- Certificate Transparency

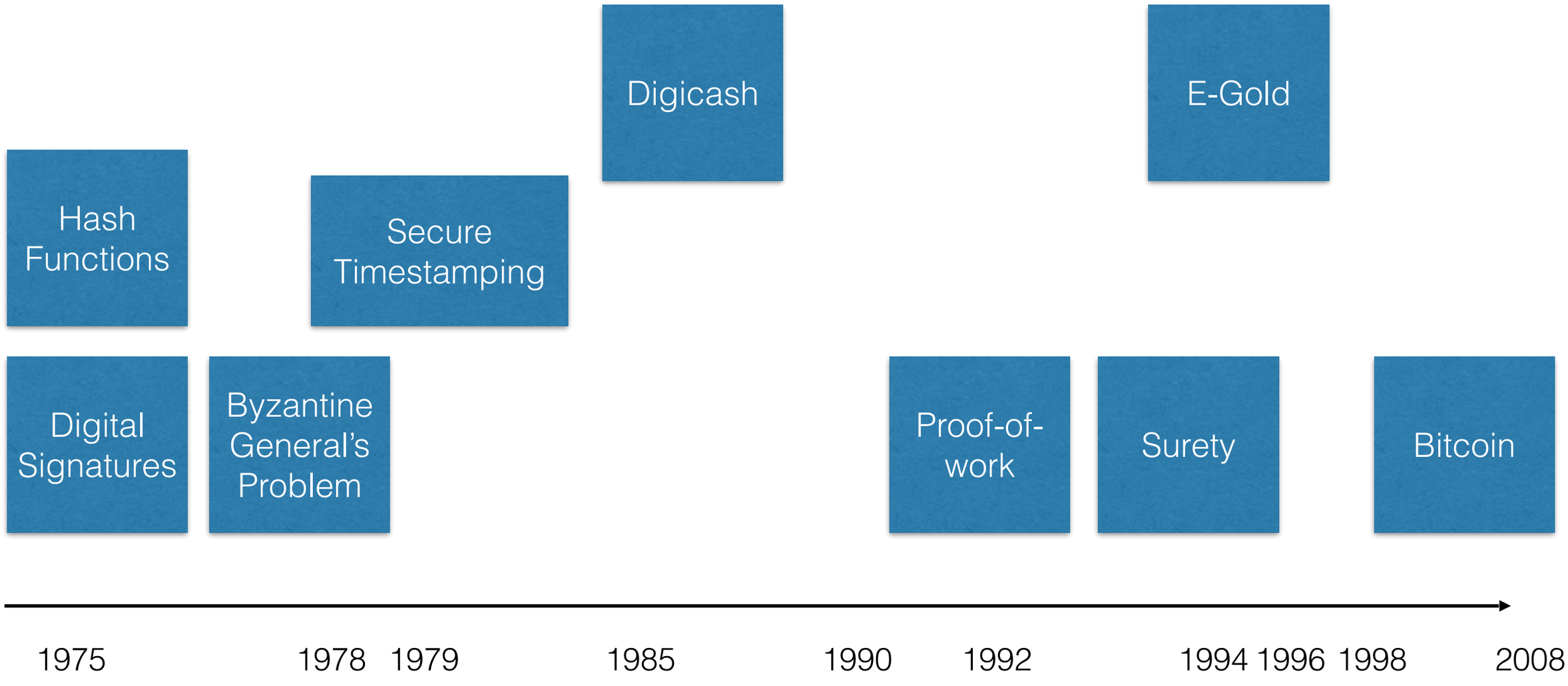
This Lecture

- History
- Blockchain Basics
- Attacks on Blockchains
- Privacy
- Open Questions

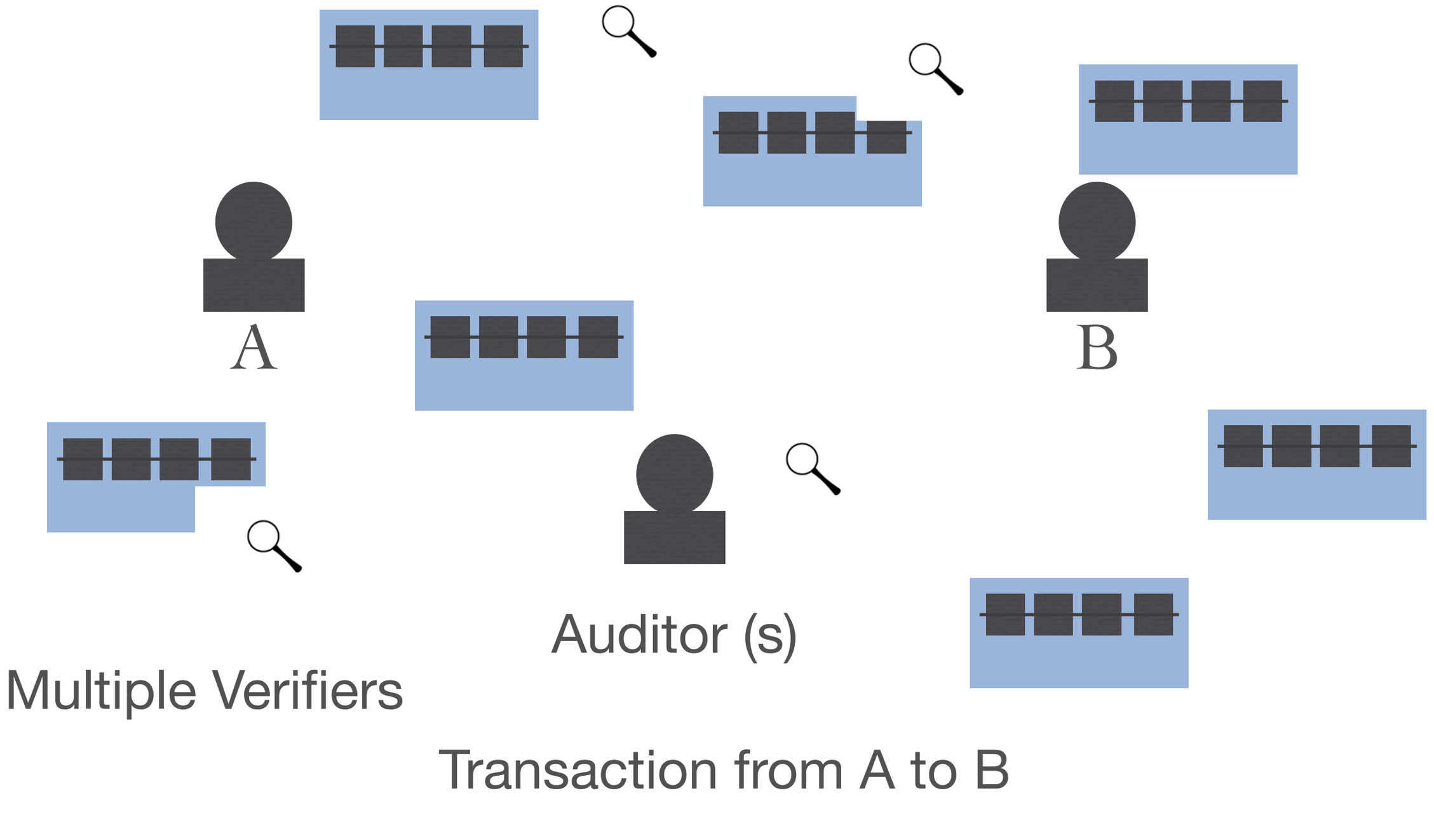
Plan

- History
- Blockchain Basics
- Consensus
- Transactions
- Cryptography questions

History


Hash Functions
Digital Signatures
Secure Timestamping
Byzantine General's Problem
Digicash
Proof-of-work
E-Gold
Surety
Bitcoin
1975
1978
1979
1985
1990
1992
1994
1996
1998
2008

BLOCKCHAIN: Shared, replicated verifiable ledger



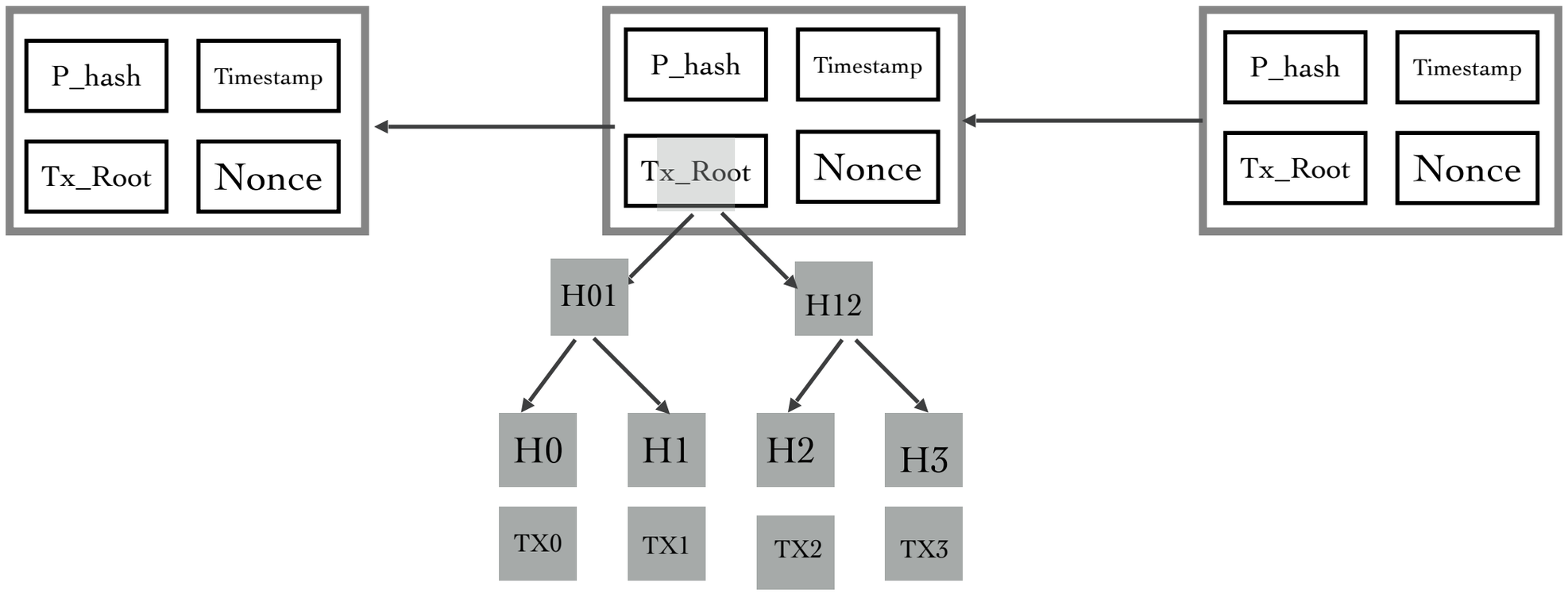
Blockchain: Integral Concepts

- Distributed Ledger
- Immutable
- Consensus

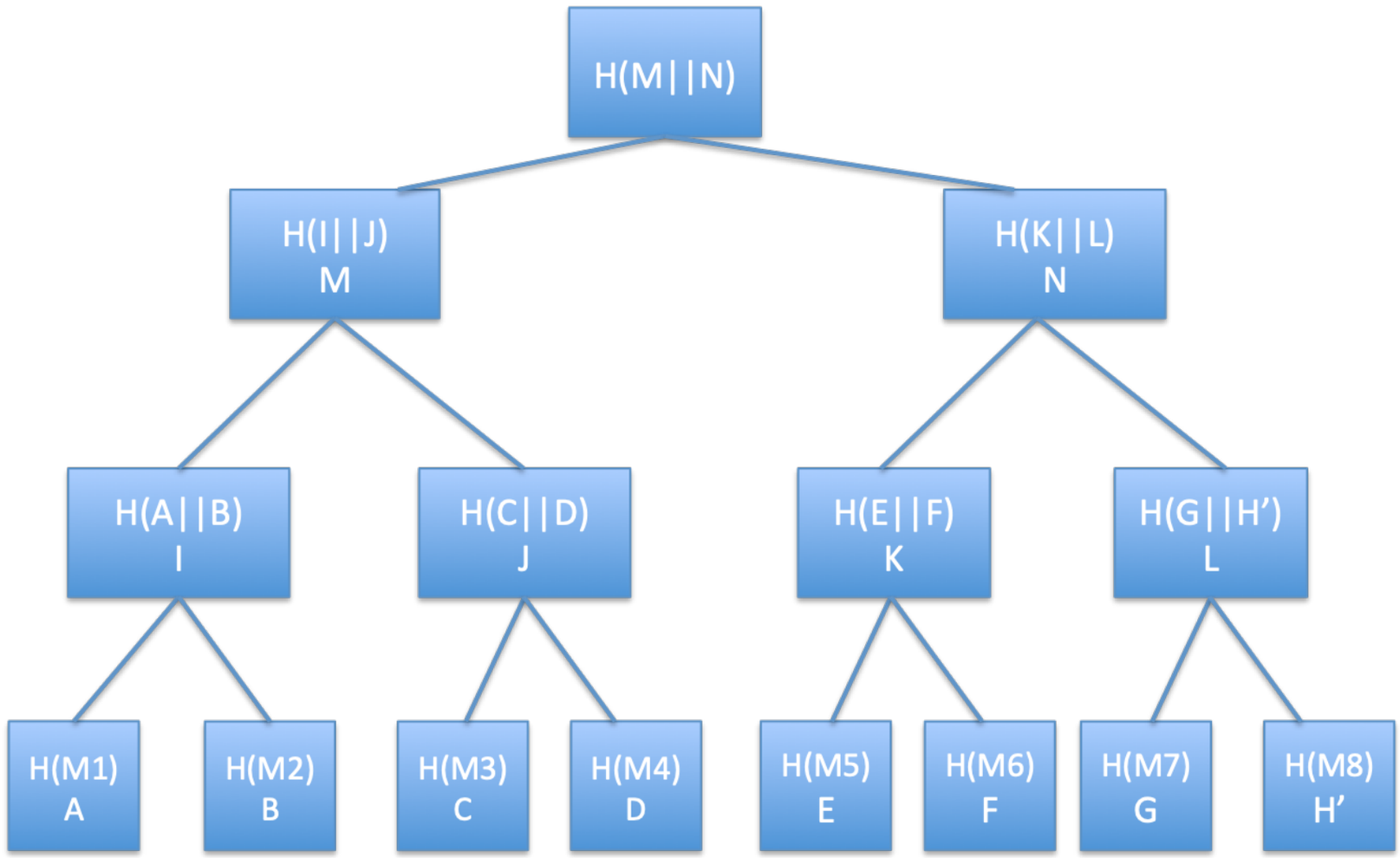
Blockchain: Requirements

- Scalability
- Performance
- Security & privacy

Blockchain

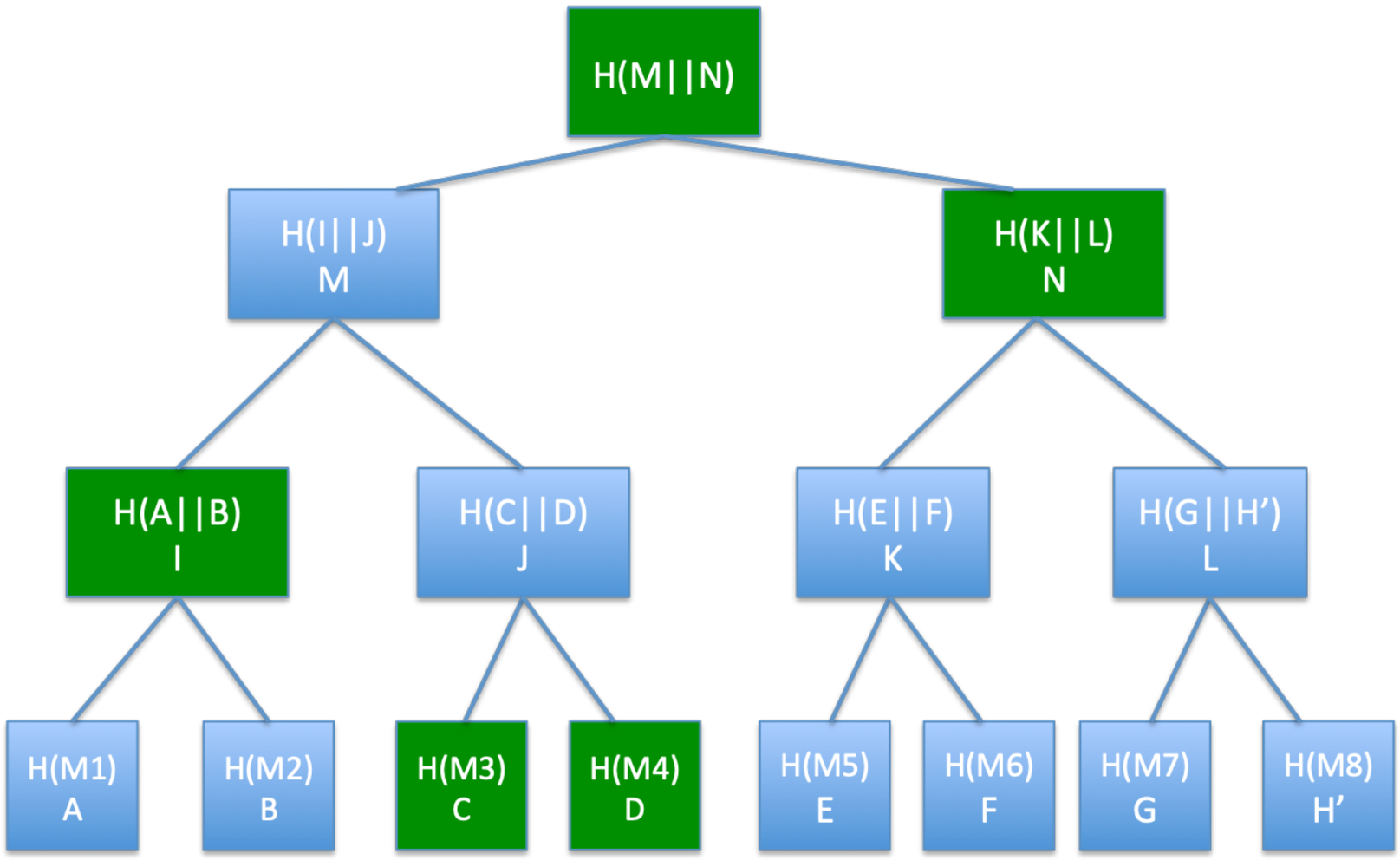

P_hash
Timestamp
Tx_Root
Nonce
P_hash
Timestamp
Tx_Root
Nonce
P_hash
Timestamp
Tx_Root
Nonce
H01
H12
H0
H1
H2
H3
TX0
TX1
TX2
TX3

Merkle Tree



To check D, Proof = <H(M4), H(M3), H(A||B), H(K||L), H(M||N)> should match with root

Merkle Tree



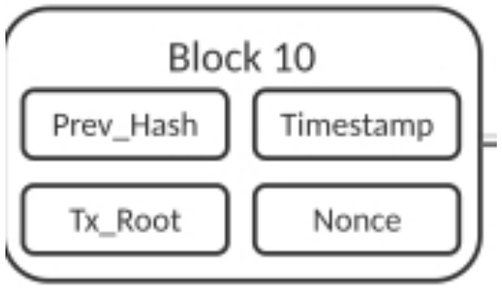
To check D, Proof = <H(M4), H(M3), H(A||B), H(K||L), H(M||N)> should match with root.

Proof size log(n), n is the number of blocks

Bitcoin Mining

- Keep changing nonce until

$$H(\quad) \leq Z$$



SHA-256

Difficulty level

Difficulty level is so set that it takes about 10 minutes to solve the puzzle

- Verification is easy
- Currently the Bitcoin network calculates more than 125,000,000 TeraHashes/sec

Every 2016 blocks (approximately 14 days), the difficulty target is adjusted to keep the average time between new blocks at ten minutes

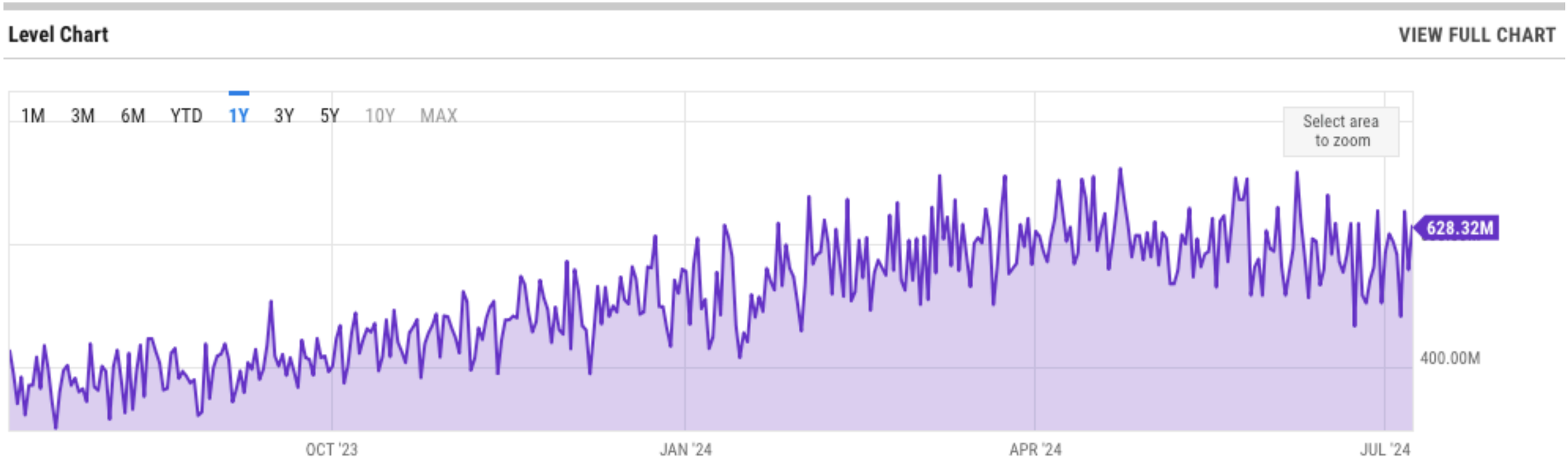
Majority consensus is considered.

Miner receives 3.125 BTC (as of April 19, 2024)

What we know?

- Proof of work
- First proposed by Dwork-Naor (1993) to combat email spam
- Hashcash: Adam back (1997) Fighting spam, finding SHA -1 hash with at least leading 20 zeros
- PoW in Bitcoin is a successor of HASHCASH

Hash Rate



https://ycharts.com/indicators/bitcoin_network_hash_rate

Bitcoin mining is insane!

Ref: Wikipedia

Double spending: Can it really be prevented?

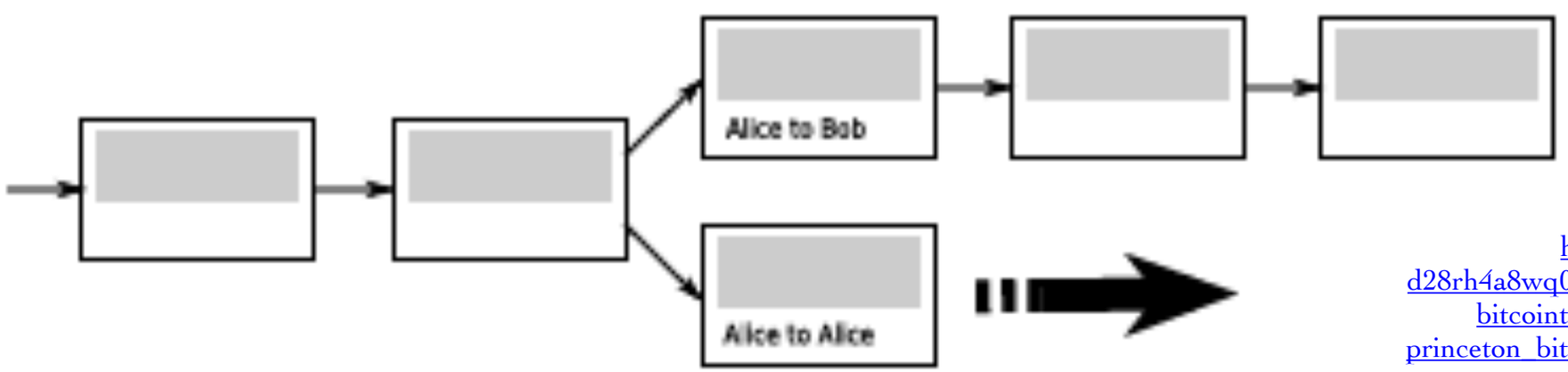
-Alice sells a car to Bob

-Receives the payment from Bob

-Alice creates her own account and makes the payment to her own account

-If she has enough computing power, she can create alternate chain and grow it longer than than the valid chain

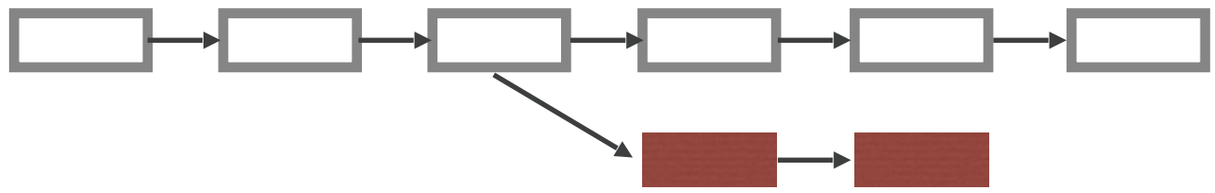
-



https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1

Nakamoto Consensus

- **Resolving Forks:**
  - Choose longest chain
  - First received (if there is tie)



- **Rewards:**
  - Blocks on main chain receive full reward
  - Orphaned blocks receive no reward
- **Weakness:**
  - A <50% attacker can modify the blockchain with high probability

Classical Consensus

- Two-phase commit protocol (Jim Jaray 1978)
- Transaction manager atomically commit a transaction, depending on different resources held by a distributed set of resource managers
- Scalable but no resilience against faulty managers; can get into a deadlock
- Three-phase commit: Recovery by releasing locks on resources
- Replicated state machine (Schneider 1990): For building reliable distributed computations: any computation is expressed as a state machine, accepting messages to mutate its state.

Types of Networks

- Synchronous networks: the delays messages may suffer can be bound by some time .

- Asynchronous networks messages may be delayed arbitrarily, and there exists no reliable bound for their delay

- Partially synchronous/ eventually synchronous: Network at some stage will eventually be synchronous despite potentially a long period of asynchrony.

- Impossibility result (Fischer et al.1985) : Deterministic protocols for consensus are impossible in the fully asynchronous case, and have known solutions in the synchronous case (also known as the “Byzantines General’s Problem”)

Failure Models

- Crash failure model: Nodes may fail at any time, but they fail by stopping to process, emit or receive messages. Failed nodes remain silent forever

- Protocols tolerating crash failure models: PAXOS, RAFT, etc

- Byzantine failures model: failed nodes may take arbitrary actions—including sending and receiving sequences of messages to defeat properties of the consensus protocol.

Properties

- Liveness: Requests from correct clients are eventually processed
  - Validity: Ensures that if a node broadcasts a message, eventually this message will be ordered within the consensus
  - Agreement: If a message is delivered to one honest node, it will eventually be delivered to all honest nodes
- Safety/consistency: If an honest node accepts (or rejects) a value then all other honest nodes make the same decision
  - Integrity: Guarantees that only broadcast messages are delivered, and they are delivered only once
  - Total order: Ensures that all honest nodes extract the same order for all delivered messages
-

Consensus for Blockchains

- Traditional distributed consensus: BFT, PBFT, Paxos, RAFT
- Lottery Based Consensus
- Verifiable mechanism to choose Committee/Leader
- To be elected, use “proof of-X”
- Proof-of-X (X=stake, authority, space, elapsed-time etc)
- Hybrid protocols: Committee instead of one leader

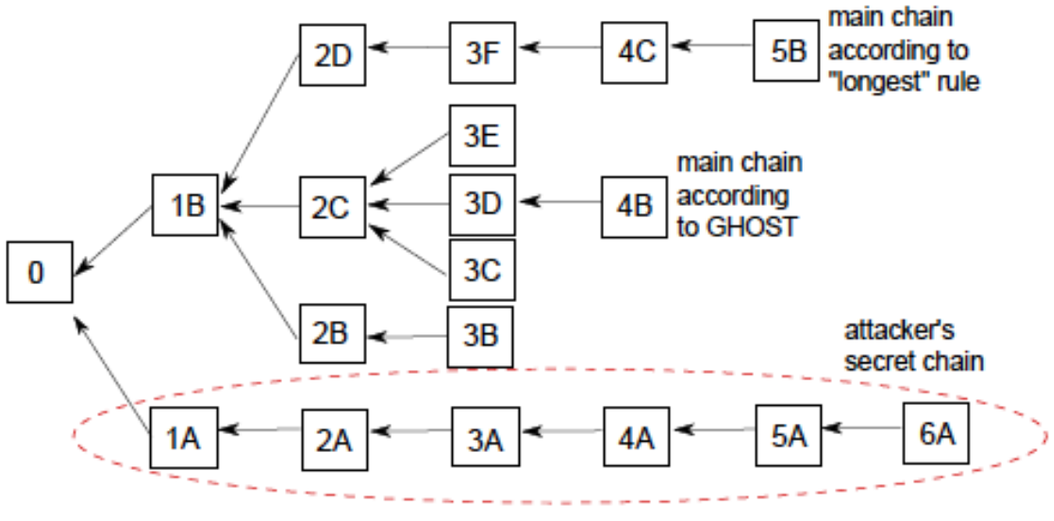
Ethereum's PoW

- Greedy Heaviest Observed Subtree (GHOST) by Yonatan Sompolinsky and Aviv Zohar in December 2013

- Purpose was to prevent stale blocks; blocks created by miners with less computing power

- Uncle blocks: Tree Structure instead of chain

- Fork resolving strategy: Choose the heaviest path as main chain, where weight depends on how dense the subtree is



Proof of Stake (PoS)

- Rationale: Users having more stake have more interest in running the system
- Participants vote on new blocks weighted by their in band investment such as the amount of currency
- Randomly elect a leader from among the stakeholders, which then appends a block to the blockchain
- Assumption: Majority of the wealth is controlled by honest nodes.
- Public Leader election: Outcome is visible to all the participants
- Private election: the participants use private information to check if they have been selected as the leader, which can be verified by all other participants using public information (DoS resilient)
- Validators are chosen based on the number of staked coins they have.
- If a validator submits bad data or fraudulent transactions, they could be punished by ‘slashing’.
- Examples: Ouroboros, Snow White, Dfinity, Ethereum
- Privacy??

Proof of Stake (PoS): Attacks

- Nothing-at-stake: Miners are incentivized to extend every potential fork. Mine on multiple chains to improve their chances

- Prevention: Introduce penalty (Snow white: take back stake, if you mine on multiple chains)

- Grinding attacks: Re-creates a block multiple times until it is likely that the miner can create a second block shortly afterwards.

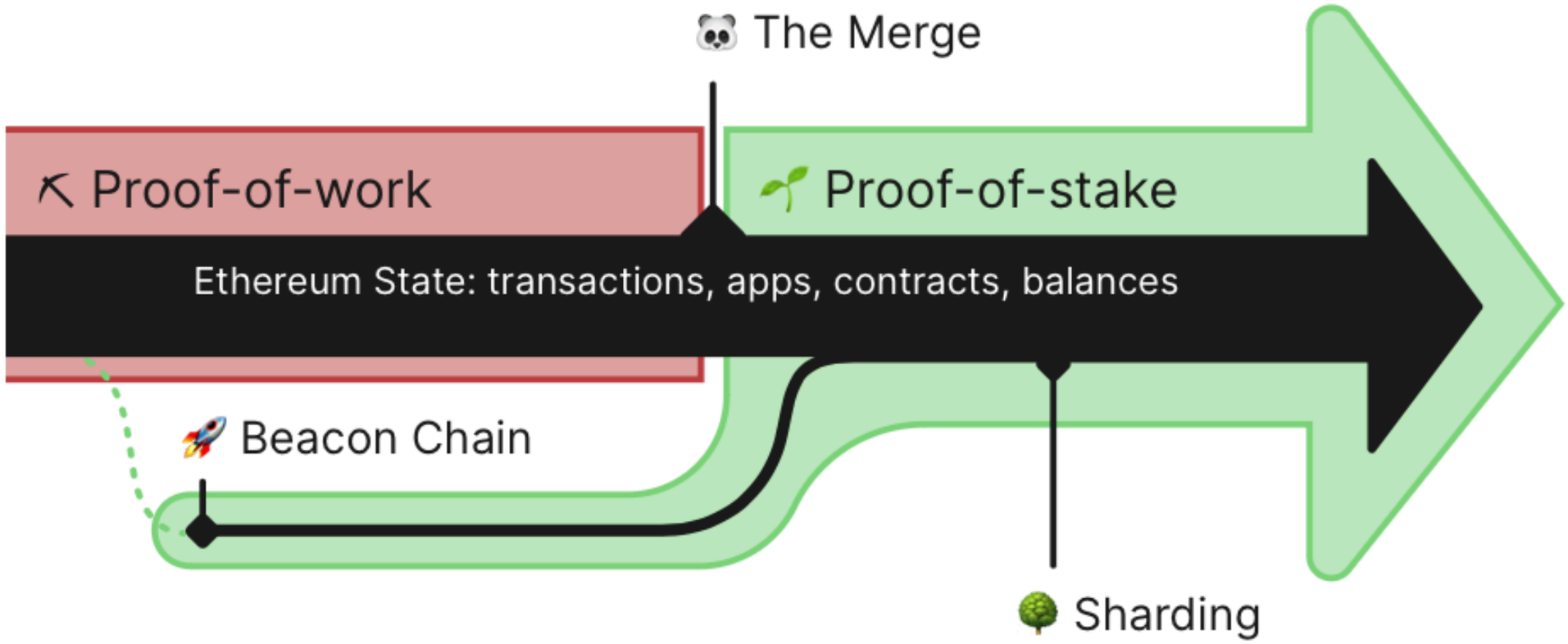
- Prevention: Miner should not be able to influence the next leader selection. Use unbiased source of randomness.

- Long range attacks: Bribe a miner who holds large stake to sell the keys. Rewrite all history

- Prevention: Checkpointing

- Bribery Attacks. Bribery attack, where the attackers financially induce some validators to approve their fork of blockchain, is enhanced in PoS,

Ethereum 2.0



https://ethereum.org/en/roadmap/merge/

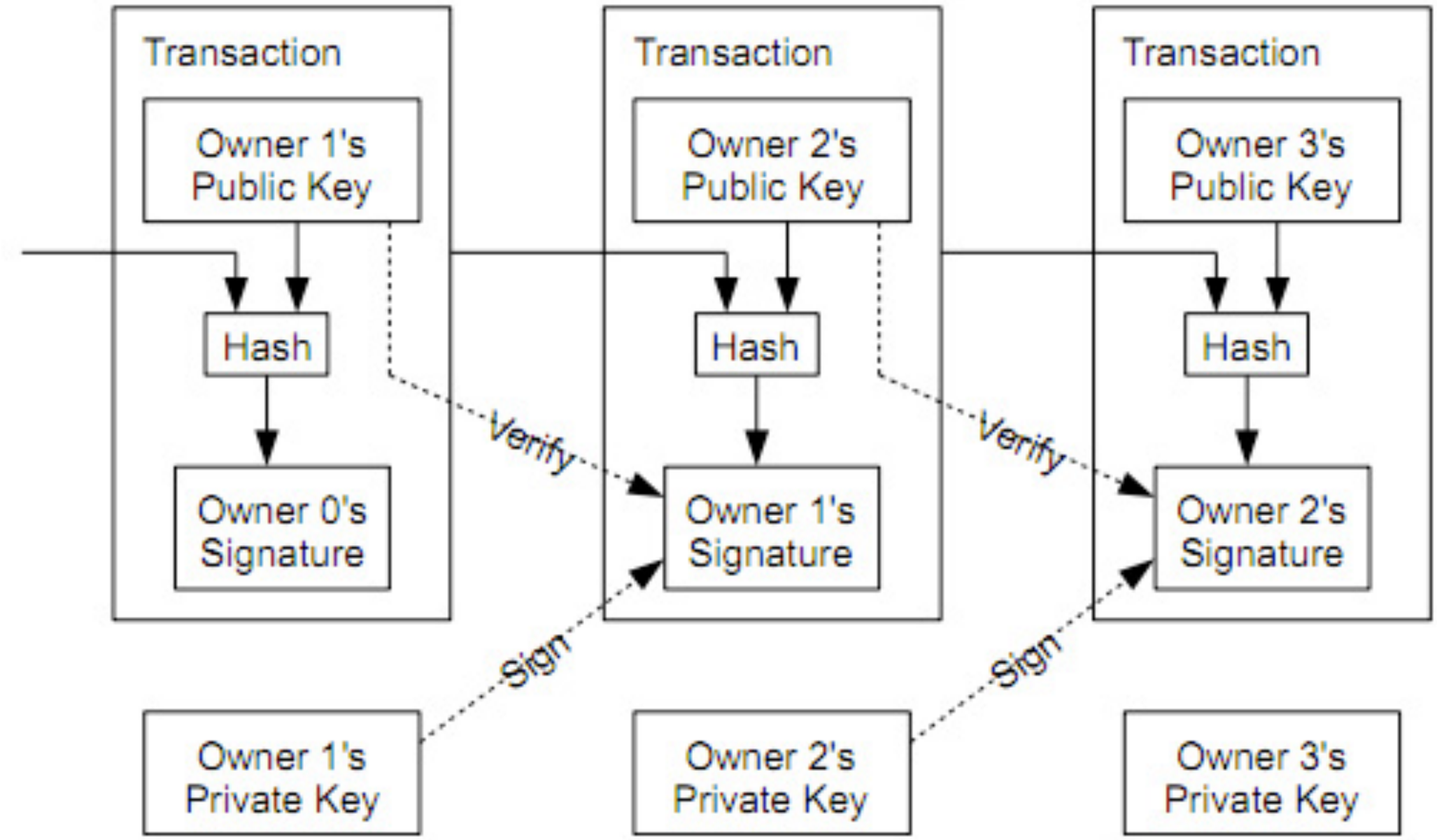
Bitcoin Wallets

- Storage for Bitcoins
- Bitcoins have to be spent on its entirety
- A global list of unspent transactions is maintained
- This like is called list of UTXO
- Various assignment algorithms are followed to choose which transaction to spent next
- Much like money in our pockets
- Except the list of all UTXO is known to everyone

Bitcoin Address

- Each entity can have multiple addresses
- Associated with each address is a public key and secret key
- Bitcoin address = version + RIPEMD-160(SHA-256(Public Key)) + checksum

Transactions



Bitcoin Paper- Satoshi Nakamoto

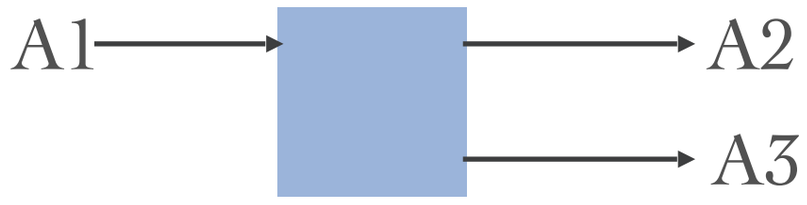
```
{
   "ver":1,
   "inputs":[
      {
         "sequence":4294967295,
         "prev_out":{
            "spent":true,
            "tx_index":198929482,
            "type":0,
            "addr":"1SurBqvoK1KK55Zs9pqHVWejY75PVeb7F",
            "value":2500935344,
            "n":1,
            "script":"76a91404e683ae268f628aeb52cea7126cd25a65fb3f5188ac"
         },
"script":"4730440220619010e602aeb92062fec403cf45259f5465a8a4fd12fd50f34d07930a1abd9f0220647f96848aa6178b101ad6c3197d83
1b6c30002a9cb416fd49866b4a122ee0fc012102e96b8d54c9493feb84d77b94a5bb40fc11e3bd058a107481c0dbda5ebd75c3f3"
      }
   ],
   "block_height":443663,
   "relayed_by":"67.205.74.206",
   "out":[
      {
         "spent":false,
         "tx_index":198929679,
         "type":0,
         "addr":"1NHwiH9hDamwgqhuRiJo6pHYTUWjgB5huy",
         "value":2873347,
         "n":0,
         "script":"76a914e98ef7c68533402e24d69d4159b9abb428f8a65288ac"
      },
      {
         "spent":true,
         "tx_index":198929679,
         "type":0,
         "addr":"1SurBqvoK1KK55Zs9pqHVWejY75PVeb7F",
         "value":2498043679,
         "n":1,
         "script":"76a91404e683ae268f628aeb52cea7126cd25a65fb3f5188ac"
      }
   ],
   "lock_time":0,
   "size":225,
   "double_spend":false,
   "time":1481852267,
   "tx_index":198929679,
   "vin_sz":1,
   "hash":"d85b954c77f5591e918e9fba58f3a79a0f9a5027019df6d5b4eba00341f04640",
   "vout_sz":2
}
```


Previous output

Value in Satoshi

scriptPubKey: Public key of previous output

scriptSig: Signature of this input + public key

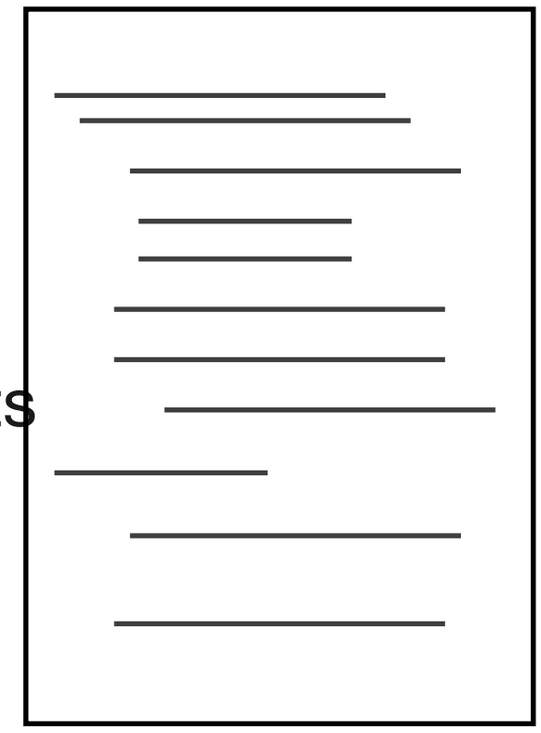


Condition 1: Sum of inputs > sum of outputs
Diff is the trans. fee
Condition 2:
Script sig should be valid signature on trans. and verified by script pub

https://www.blockchain.com/explorer

Smart Contracts

- Bitcoin is not Turing Complete
- Contract: If, then, else, loops
- Computer Programs autonomous triggered by events
- Verified automatically
- Smart Contract on Blockchains

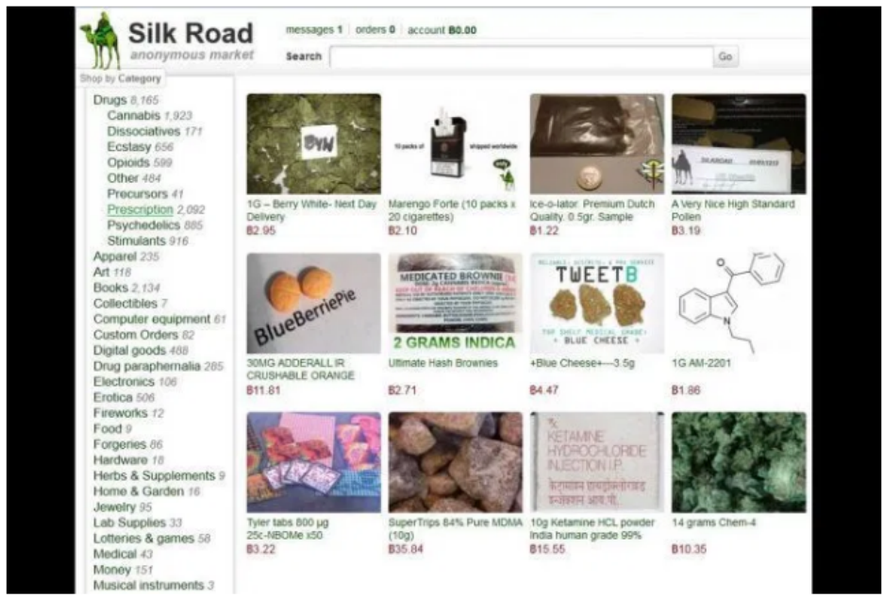


Pseudo-anonymity of Transactions

NEWS

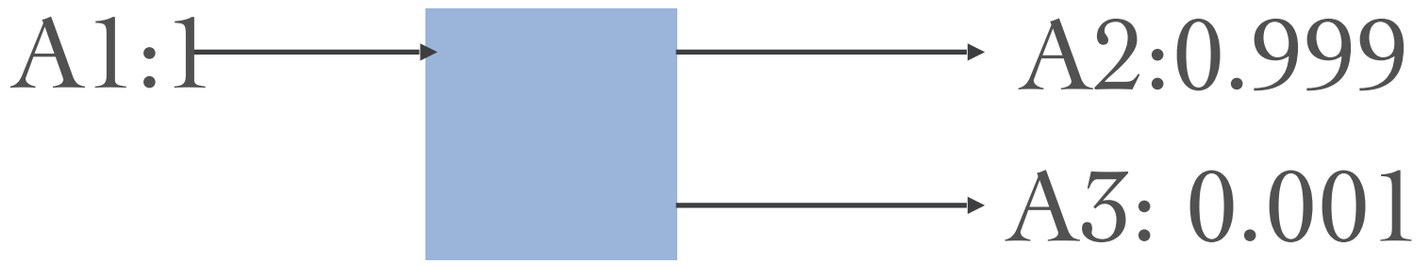
Silk Road Comes Under DDOS Attack

By **Carlos Ageng'o** - May 4, 2013 0

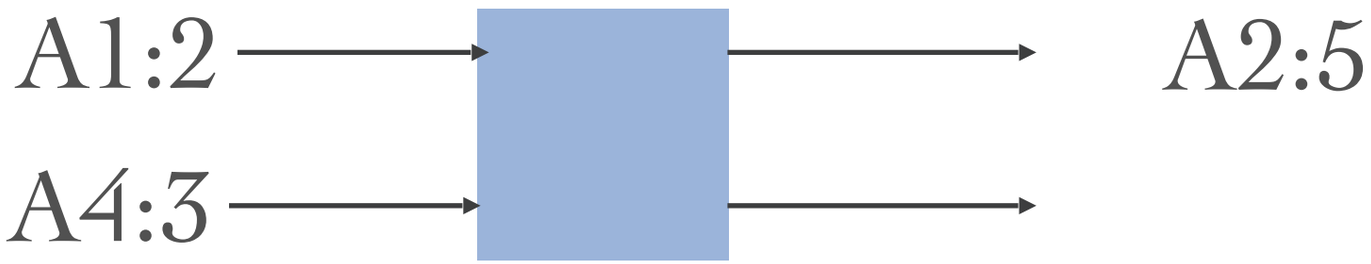


Goldfelder et al, "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies", PoPETS 2018

Likability of Pseudonyms

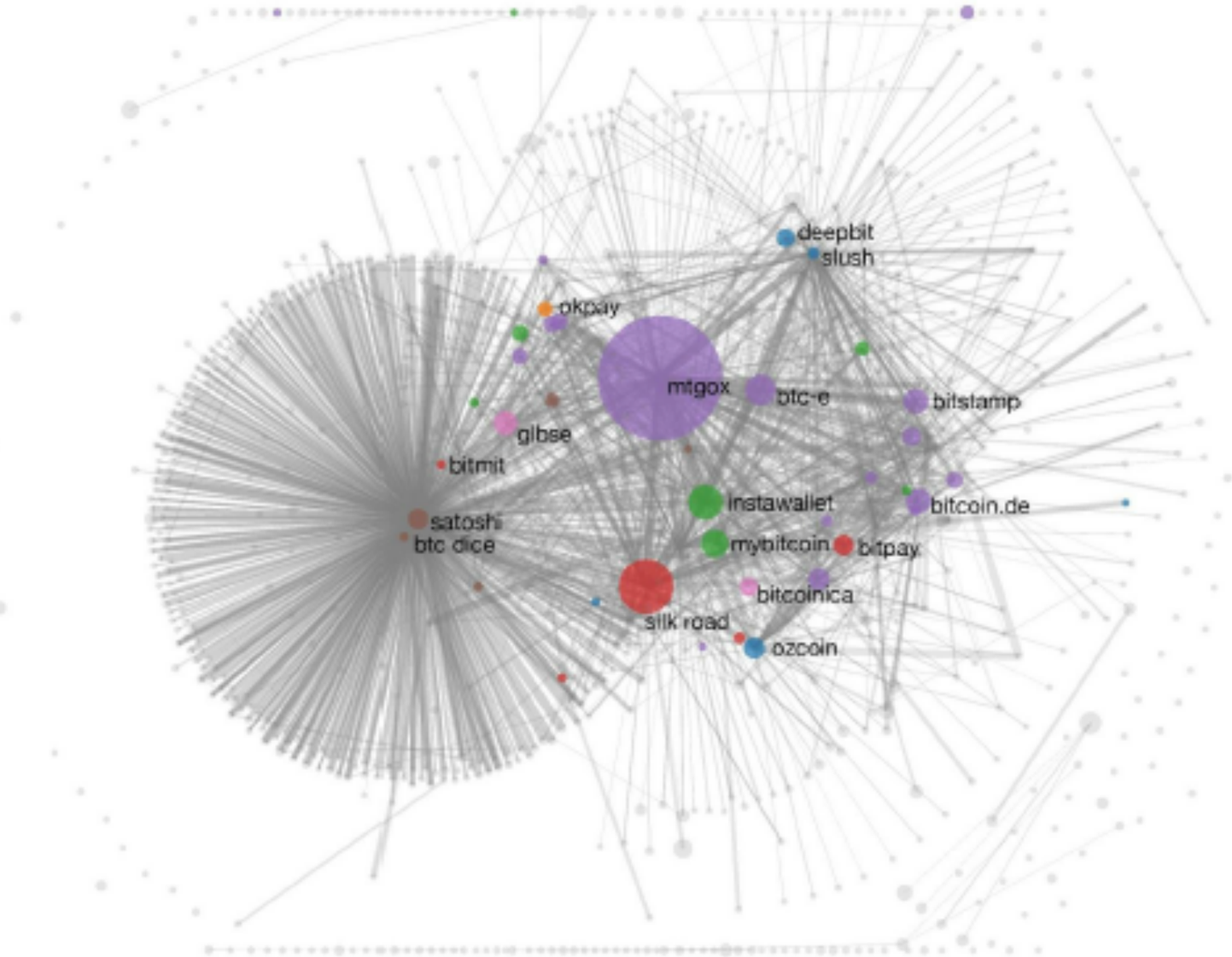


A1 and A3 might belong to same user



shared spending is evidence of joint control
Linking is transitive

Linking at Scale



Meiklejohn et al., “A Fistful of Bitcoins: Characterizing Payments Among Men with No Names”, IMC’13

Analysis of Ransomware

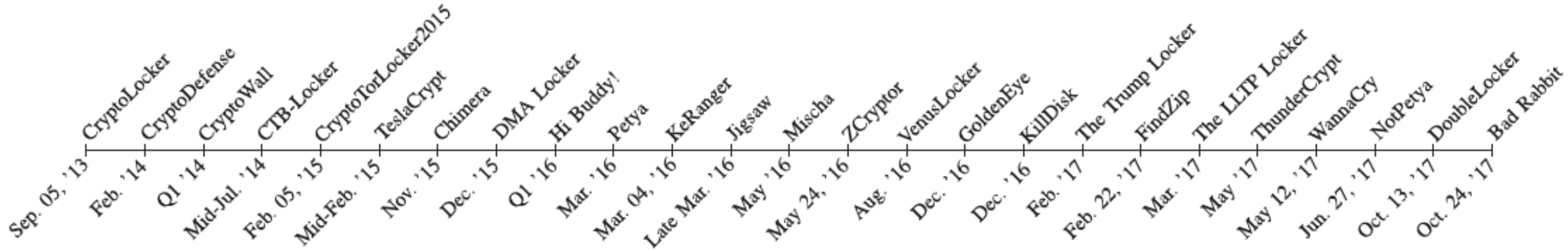


Fig. 3 – Occurrence of Bitcoin ransomware.

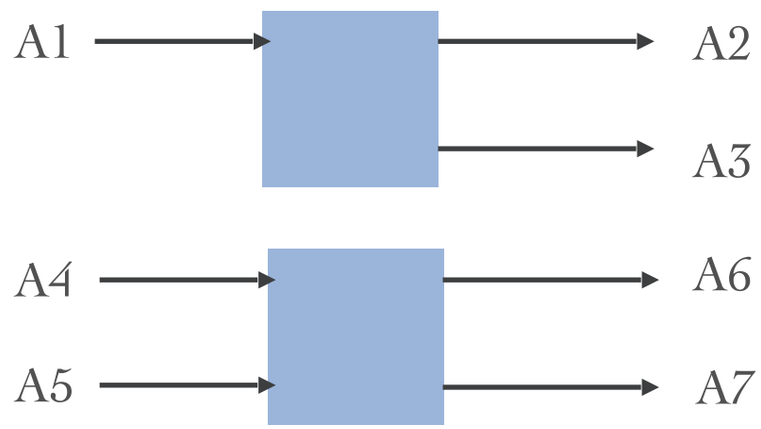
Table 1 – Summary of overall payments and ransom payments to the ransomware for which the observed payments align with their period of activity and ransom demands .

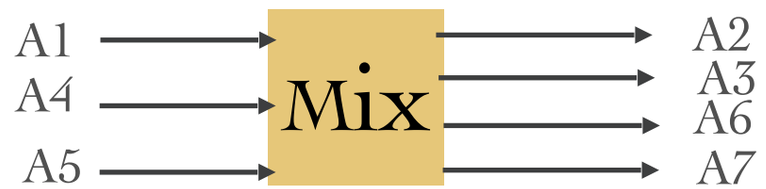
Ransomware	Overall			Ransom		
	Payments	BTC	USD Value	Payments	BTC	USD value
CryptoLocker	51,766	133,045.9961	42,292,191.17	804	1403.7548	449,274.97
CryptoDefense	128	138.3223	70,113.41	108	126.6960	63,859.49
CryptoWall	51,278	87,897.8510	45,370,589.00	3,730	5,351.2329	2,220,909.12
DMA Locker	298	1,433.3463	580,763.95	117	339.4591	178,162.77
NotPetya	70	4.1787	10,284.42	33	4.0576	9,835.86
KeRanger	13	10.0044	4,175.35	10	9.9990	4,173.12
WannaCry	341	53.2906	99,549.05	238	47.1743	86,076.76

Conti, Gangwal, Ruj "On the economic significance of ransomware campaigns: A Bitcoin transactions perspective", Computer & Security, 2018

Mixing Transactions

- Various mixing services are used
- Coinjoin, Sharedcoin, etc
- Attacks on shared coin available
- Mixing service will gain knowledge about transactions
- Privacy Preserving mixing
- Sequences of mixes





Chaum, “Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms”, CACM’81

Anonymity using Mixing

- Coinjoin (2013): Central Mixer, knows the link between senders and receivers

- MixCoin (FC'14): Mixer is accountable in case of theft, but knows the transactions

- TumbleBit (NDSS'17): Mixer is oblivious of the transactions and compatible with Bitcoins

- CoinShuffle/Coinshuffle++(NDSS'17): Users perform secure multiparty computation, without involving third party service

ZCash

- Decentralised Anonymous Payment
- Zero Knowledge Succinct Non-interactive ARguments of Knowledge (zk-SNARKs)
- Anonymous transactions of variable amounts
- Hides transaction amounts and the values of coins held by users
- **zk-SNARKs uses trusted set-up, vulnerable!**

- Ben-Sasson et al, “Zerocash: Decentralized Anonymous Payments from Bitcoin”, S&P’14

Monero

- POW cryptocurrency influenced by Cryptonote
- Privacy achieved using Ring Signatures
- Ring Confidential Transactions (RingCT) to obfuscate the amount sent in a transaction using range proofs and commitments
- Bulletproofs used for ZK-Proofs

Applications!

- Do I really need a Blockchain?
- Credential Management
- Financial
- Supply Chain
- Digital Exchange
- **Blockchain for Social Good!**

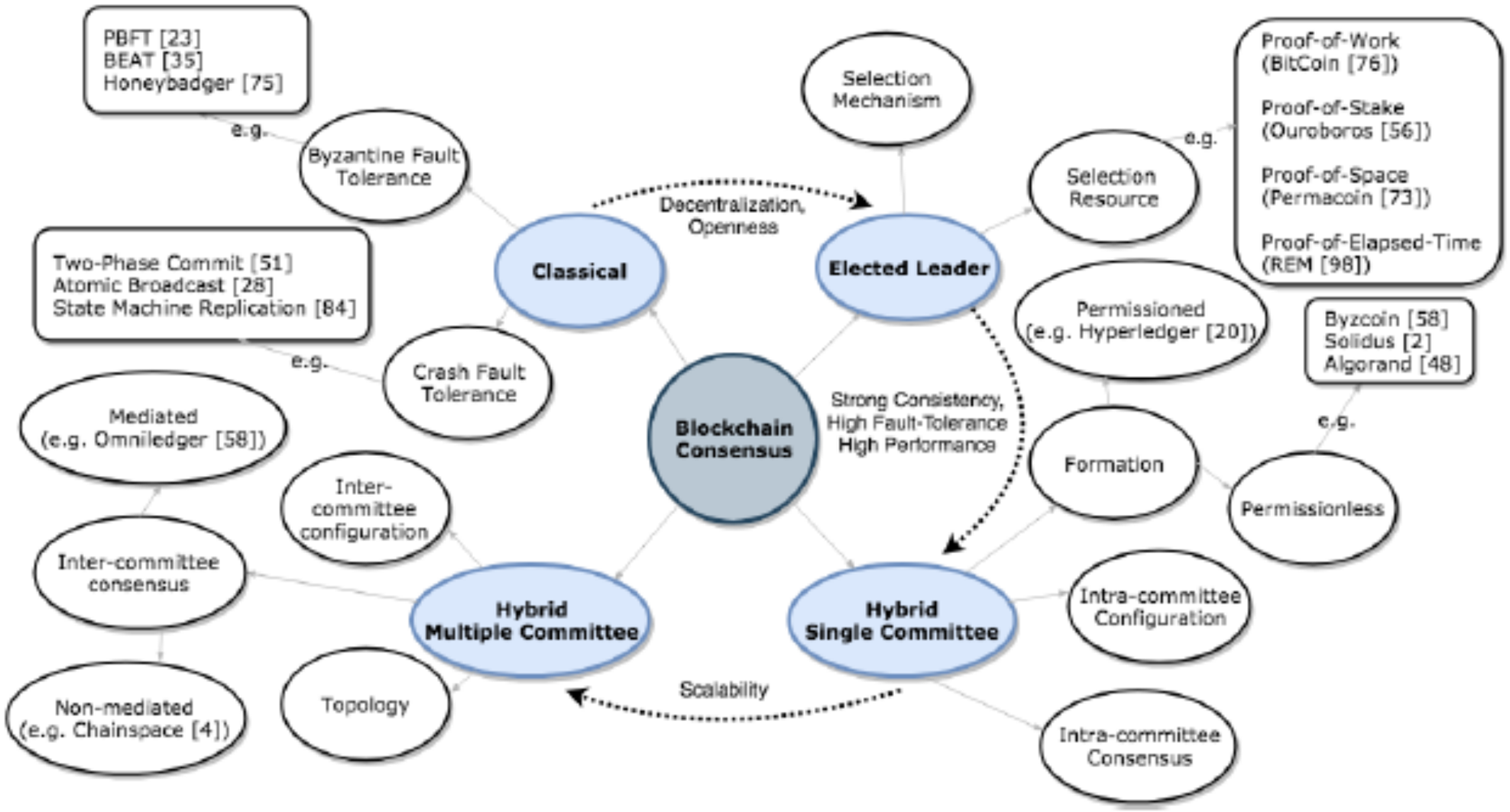
Cryptography Challenges

- Scalability and interoperability
- Signature schemes
- Privacy, Zero-Knowledge Proofs
- Verifiable randomness for Consensus algorithms
- Post Quantum Blockchains

Thank you

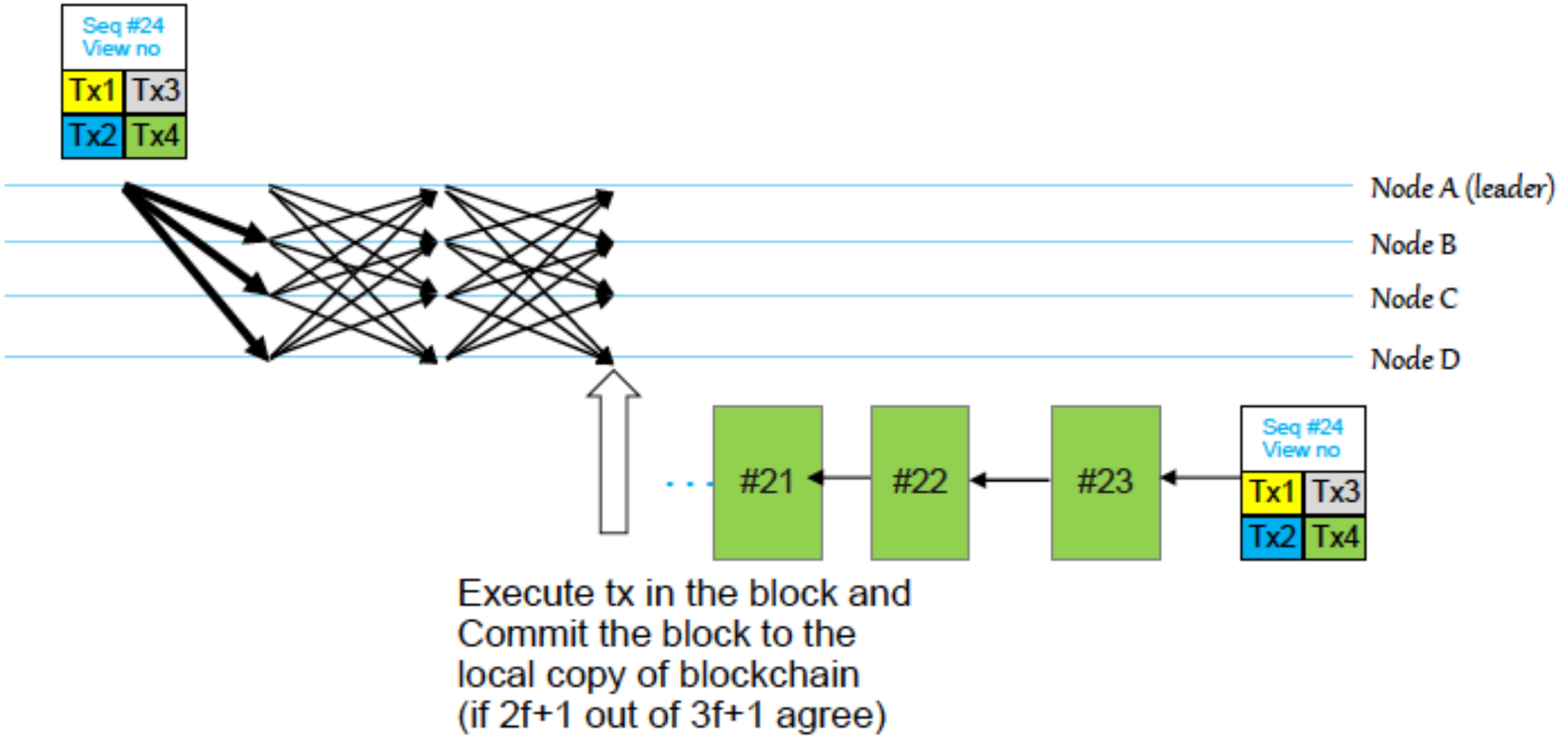
Optional: Consensus

Consensus



- Bano et al. "SoK: Consensus in the Age of Blockchains", AFT 2019.

Practical Byzantine Fault Tolerance (PBFT)



Castro-Liskov'02

Proof-of-Work Consensus

- Bitcoin’s Nakamoto consensus
- 51 % attack
- Selfish mining- Stubborn mining-rational mining attack
- Block withholding attack
- Network partitioning attack
- Increasing block size and decreasing inter block interval increases the chance of forking
- Due to propagation delayed, miners may waste effort in attempting to mine on top of blocks that are no longer the latest ones

Proof of Authority

- Stake does not say anything about the actual holding of a validator
- PoA consensus is essentially an optimized Proof of Stake model that leverages identity as the form of stake rather than actually staking tokens
- In order to create block, entity needs to authenticate itself
- Their identities need to be formally identified on-chain with the ability to cross-reference these identities through reliable data available in the public domain (such as a public notary database)
- Eligibility to becoming a validator must be difficult to obtain in order to ensure the long-term prospective position of the validator is one of clear incentive, both financially and reputation wise, to remain an honest validator.
- There must be complete uniformity in the process for establishing validators
- Kovan test net: validation using a client side POA Network Dapp as well as through the public notary system
- Not fully decentralised