Distributed Ledger Technologies, a.k.a. Blockchain(s)

SSD 22/23

João Soares

Blockchains

https://www.computerworld.com/article/3481633/how-blockchain-will-kill-fake-news-and-four-other-predictions-for-2020.html

Blockchain(s)

- Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.

- A digital ledger of transactions that is **replicated** and **distributed** across the entire network of computer systems on the blockchain.

- A decentralised database managed by multiple participants, also known as Distributed Ledger Technology (DLT).

Blockchain(s)

- Enables the secure sharing of information.
- Data is stored in a database.
- Transactions are recorded in an account book called a ledger.

- Nodes are incentivized with digital tokens or currency to maintain and make updates to the blockchains.
- Blockchain allows permanent, immutable, and transparent recording of data and transactions.

Blockchain(s)

- A blockchain has three central attributes.
  - A blockchain must be cryptographically secure.
  - A blockchain is a digital log or database of transactions, meaning it happens fully online.
  - A blockchain is a database that is shared across a public or private network.

Blockchain(s)

- Stored transactions are encrypted via unique, unchangeable hashes, such as those created with the SHA-256 algorithm.
- Since all transactions are encrypted, records are immutable
  - Attempts to change the ledger can be recognized by the network and rejected.
- Blocks of encrypted data are permanently “chained” to one another, and transactions are recorded sequentially and indefinitely
  - Creating an auditable history, i.e., allows visibility into past versions of the blockchain.

Blockchain(s)

- When new data is added to the network, the majority of nodes must verify and confirm the legitimacy of the new data
  - Based on consensus mechanisms.
- When a consensus is reached, a new block is created and attached to the chain.
  - All nodes are then updated to reflect the blockchain ledger.
- In a public blockchain network, the first node to credibly prove the legitimacy of a transaction receives an economic incentive.
  - This process is called “mining.”

The Properties of Distributed Ledger Technology (DLT)

Programmable
A blockchain is programmable (i.e. Smart Contracts)

Secure
All records are individually encrypted

Anonymous
The identity of participants is either anonymous or pseudonymous

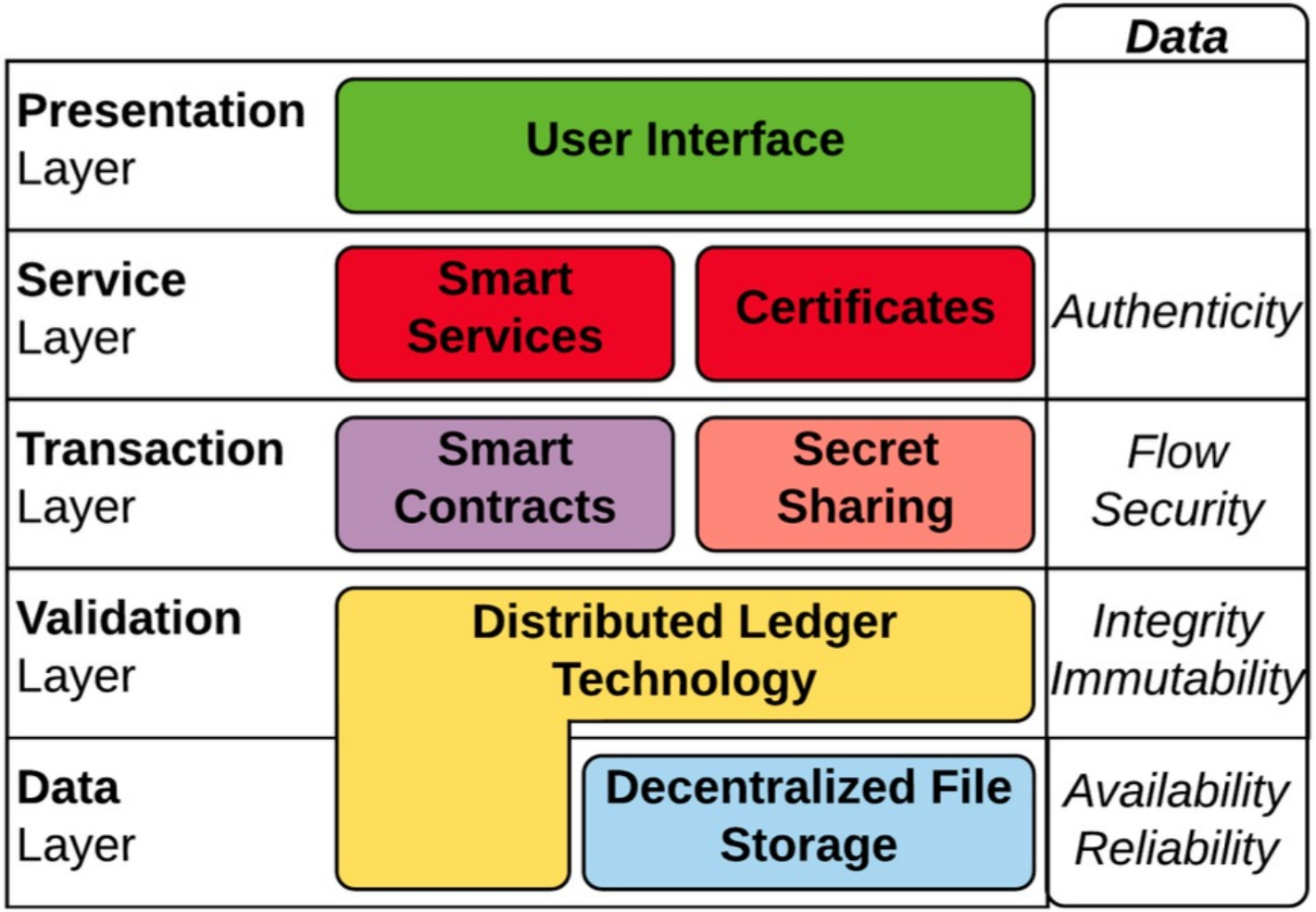
Unanimous
All network participants agree to the validity of each of the records

Distributed
All network participants have a copy of the ledger for complete transparency

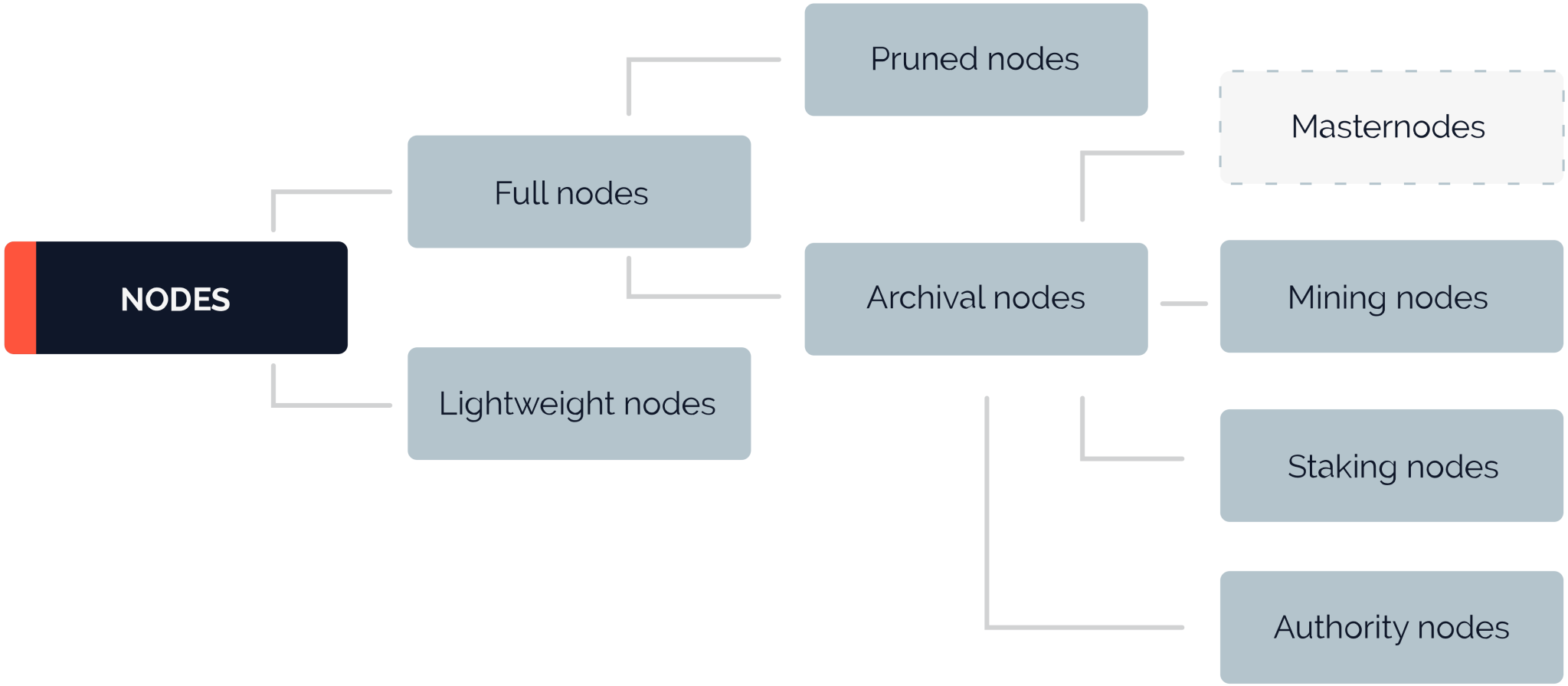
Immutable
Any validated records are irreversible and cannot be changed

Time-stamped
A transaction timestamp is recorded on a block

Layered Architecture



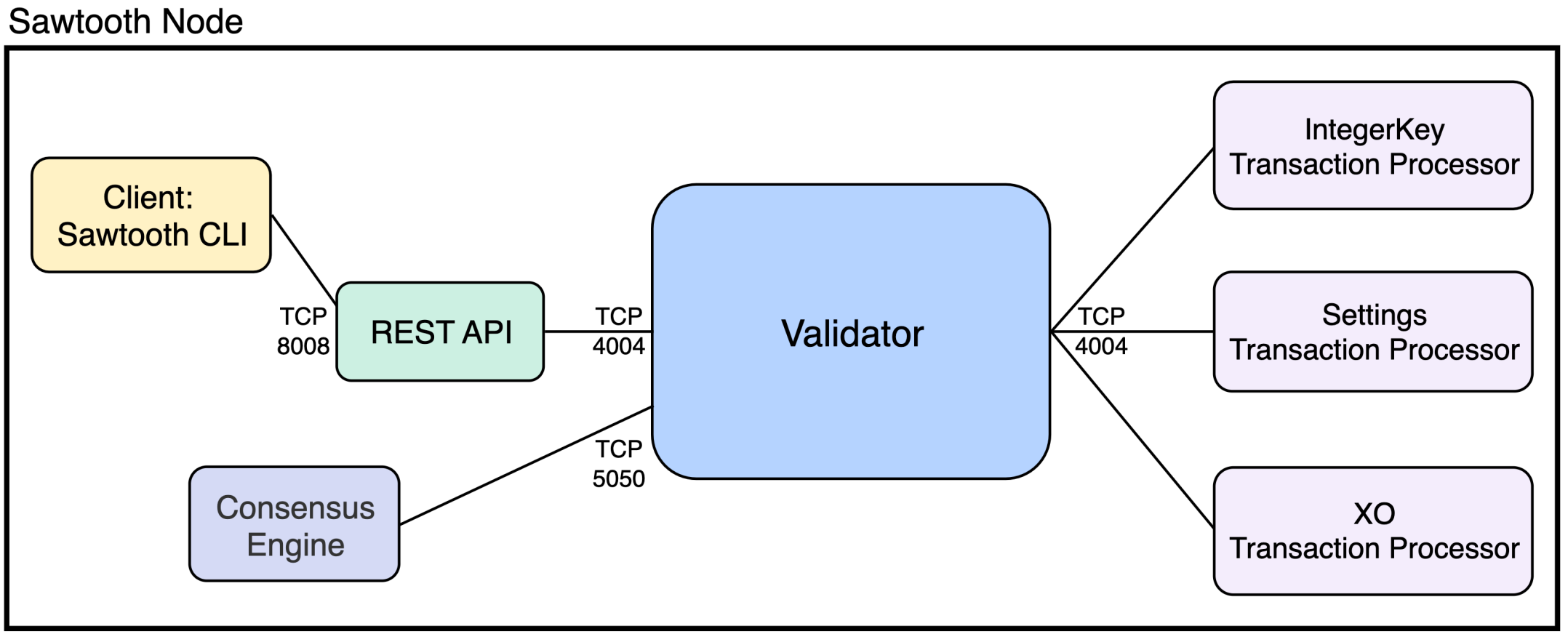
Nodes


NODES
Full nodes
Pruned nodes
Lightweight nodes
Archival nodes
Masternodes
Mining nodes
Staking nodes
Authority nodes

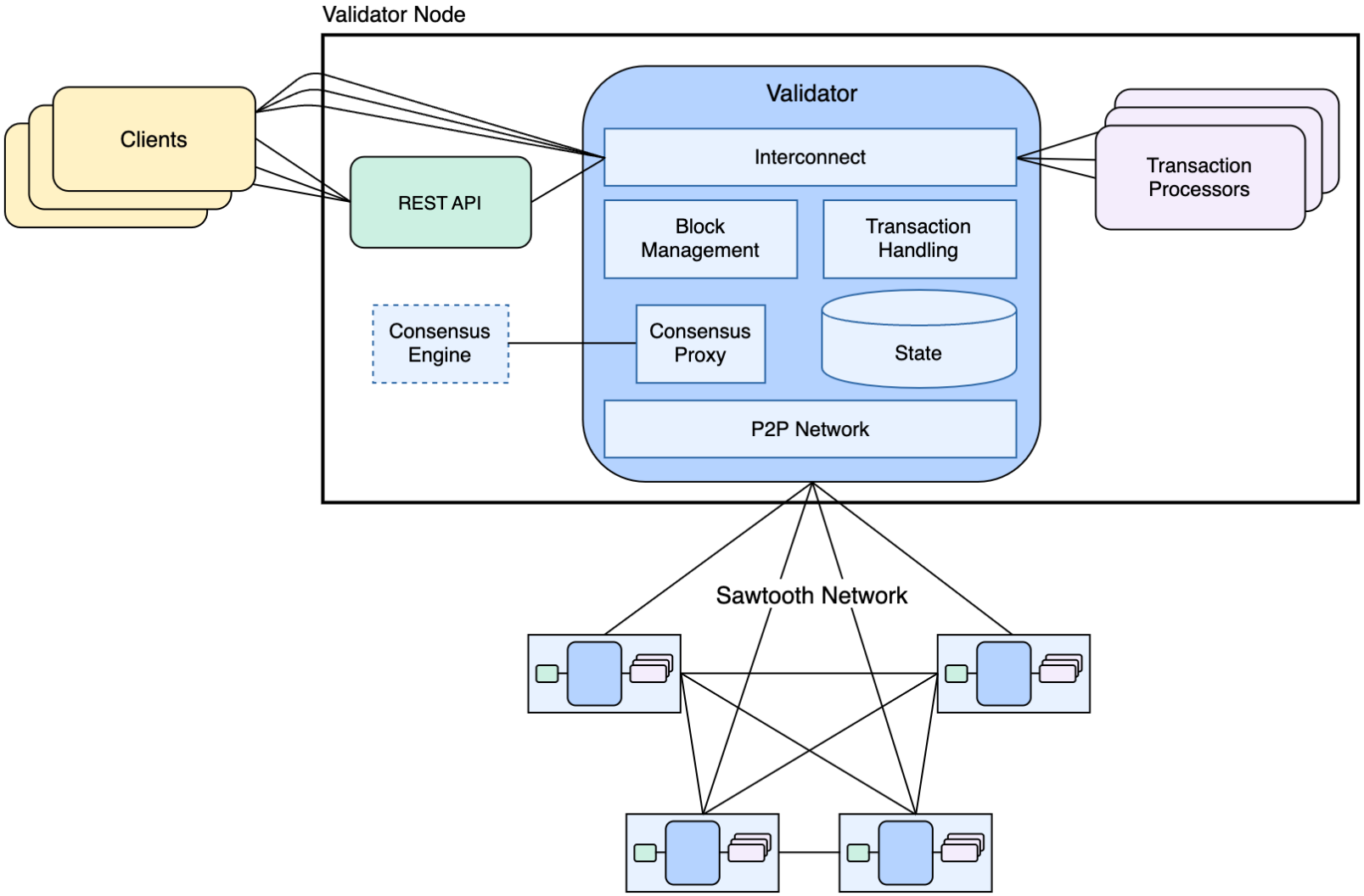
Nodes

	Pros	Cons
Full nodes	Full nodes maintain consensus, validate the blockchain, and transmit blocks in a more secure way.	They need plenty of resources, are challenging to keep up, and are less user-friendly.
Light nodes	Light nodes are resource-saving, portable, and user-friendly.	They don't validate the blockchain, they don't transmit blocks as well, and they are less secure.
Pruned nodes	Their storage is flexible.	Old blocks need to be revalidated.
Mining nodes	Light nodes are resource-saving, portable, and user-friendly.	They don't validate the blockchain, they don't transmit blocks as well, and they are less secure.
Archive nodes	They have a complete history.	storage and resource-intensive.
Masternodes	They are inexpensive to maintain and provide a mix of benefits and rewards.	They have a challenging setup process and a significant upfront cost.
Staking nodes	They have low energy consumption and a low barrier to entry.	Low transparency and a luck-based reward scheme in staking pools.

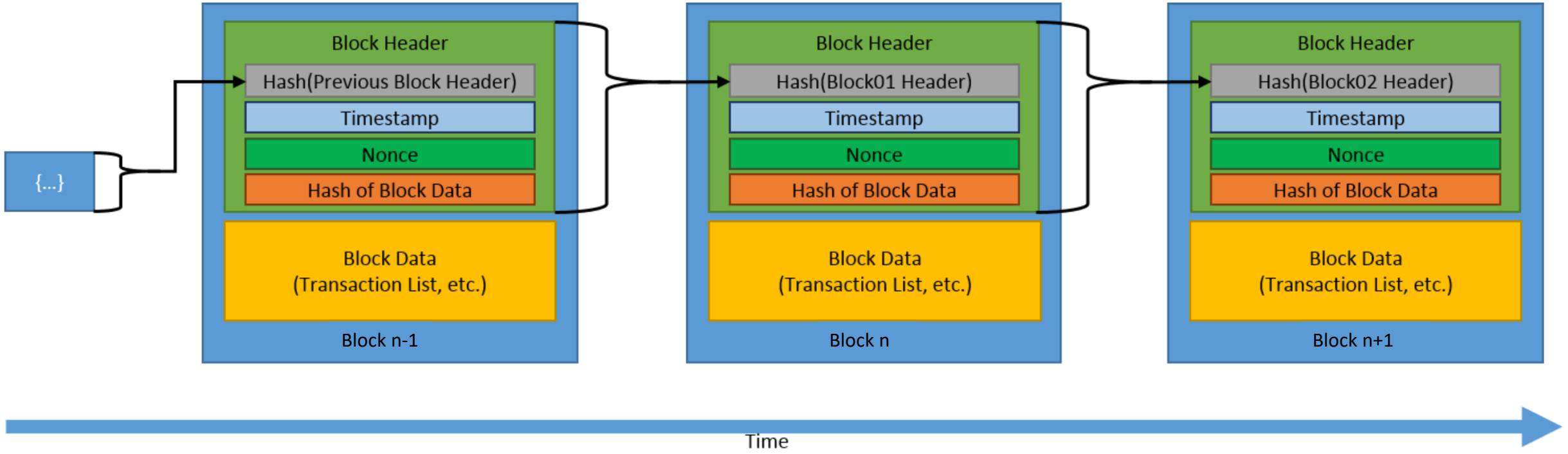
Nodes (Sawtooth Hyperledger)



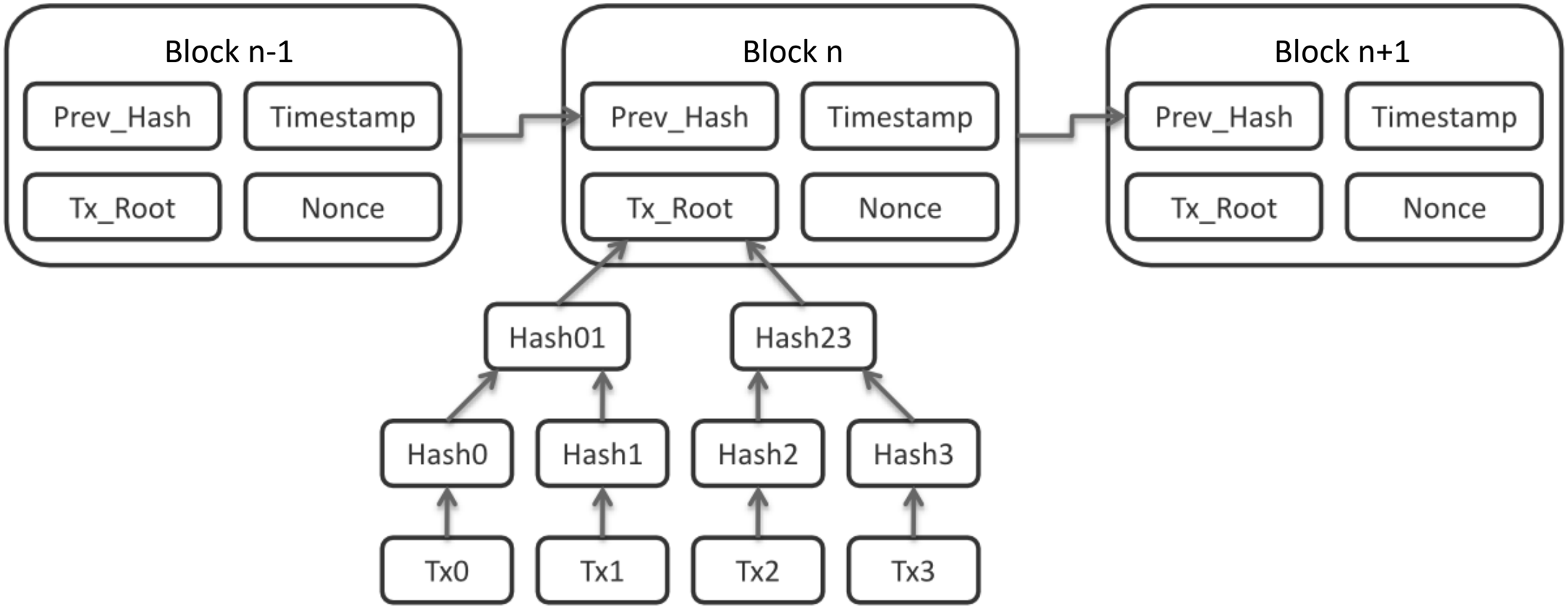
Architecture (Sawtooth Hyperledger)



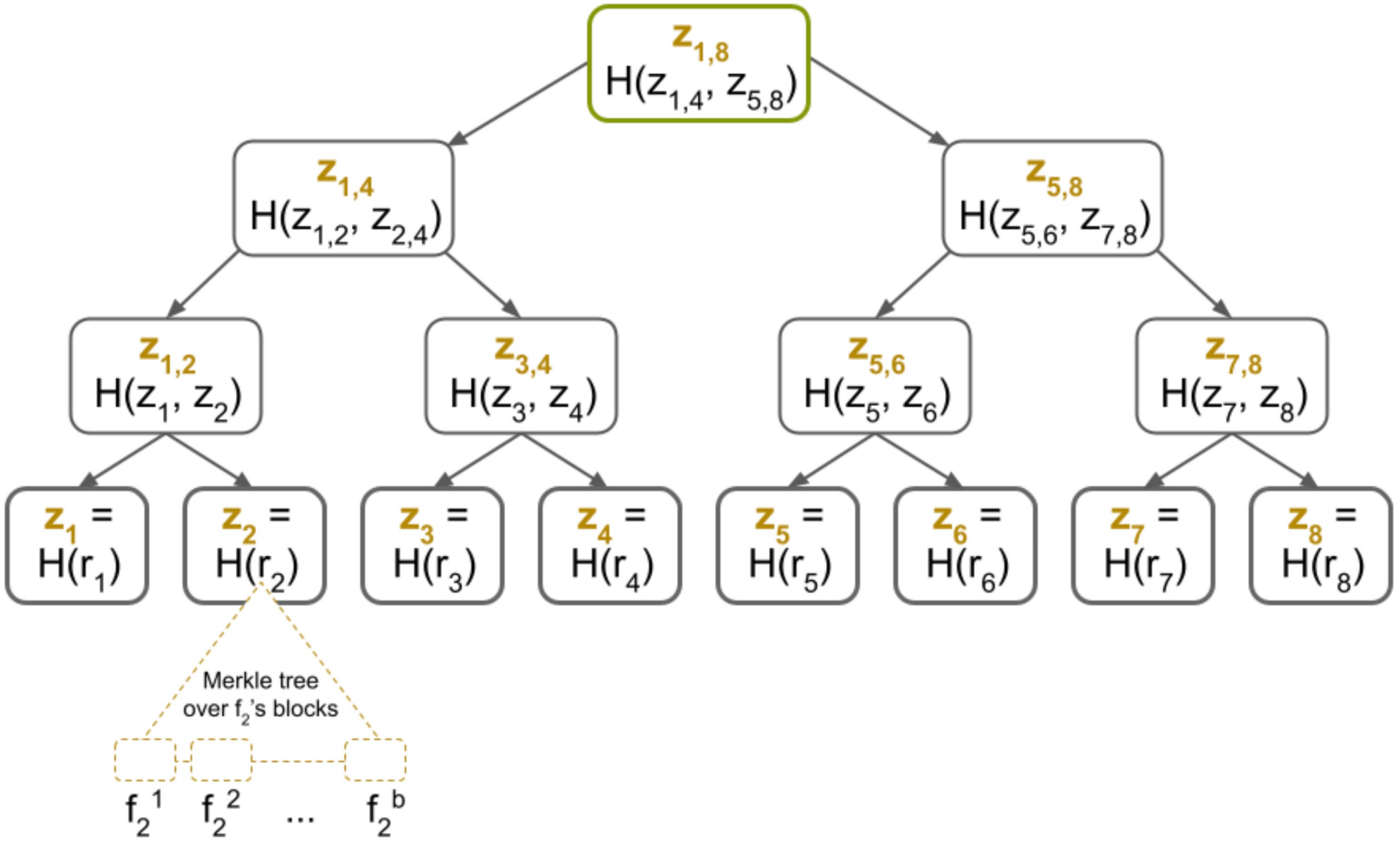
Blockchain


{...}
Block Header
Hash(Previous Block Header)
Timestamp
Nonce
Hash of Block Data
Block Data
(Transaction List, etc.)
Block n-1
Block Header
Hash(Block01 Header)
Timestamp
Nonce
Hash of Block Data
Block Data
(Transaction List, etc.)
Block n
Block Header
Hash(Block02 Header)
Timestamp
Nonce
Hash of Block Data
Block Data
(Transaction List, etc.)
Block n+1
Time

Block


Block n-1
Prev_Hash
Timestamp
Tx_Root
Nonce
Block n
Prev_Hash
Timestamp
Tx_Root
Nonce
Block n+1
Prev_Hash
Timestamp
Tx_Root
Nonce
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

Merkle Trees



Joining the Blockchain

- Peer discovery (Bitcoin)
  - New nodes must query some of the DNS servers available on the network to find the IP addresses of full nodes
    - Bootstrapping nodes
  - Asking neighbours or listening to advertisement messages broadcasted over the network
    - *Addr messages* messages contain up to 1000 addresses and can be unsolicited or solicited
  - “DNS seed results are not authenticated and a malicious operator, network, or man-in-the-middle attacker can return only IP addresses of nodes controlled by the attacker (…)”
  - “For this reason, programs should not rely on DNS seeds exclusively.”