**BLOCKCHAIN**

The *blockchain* is a distributed ledger with growing lists of records (*blocks*) that are securely linked together via cryptographic hashes.

Each block contains a *cryptographic hash of the previous block*, *a timestamp*, and *transaction data* (generally represented as a *Merkle tree*, where data nodes are represented by leaves).

Since each block contains information about the previous block, they effectively form a chain, with each additional block linking to the ones before it.

Consequently, blockchain transactions are resistant to alteration because, once recorded, the data in any given block cannot be changed retroactively without altering all subsequent blocks and obtaining network consensus to accept these changes.

Blockchains are typically managed by a peer-to-peer (P2P) computer network for use as a public distributed ledger, where nodes collectively adhere to a consensus-algorithm protocol to add and validate new transaction blocks.

Although blockchain records are not unalterable, since blockchain forks are possible, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance.

**Structure and Design:**

A blockchain is a decentralized, distributed, and often public, digital ledger consisting of records called *blocks* that are used to record transactions across many computers so that any involved block cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently and relatively inexpensively.

A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests. Such a design facilitates robust workflow where participants' uncertainty regarding data security is marginal.

The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double-spending.

Logically, a blockchain consists of several layers:

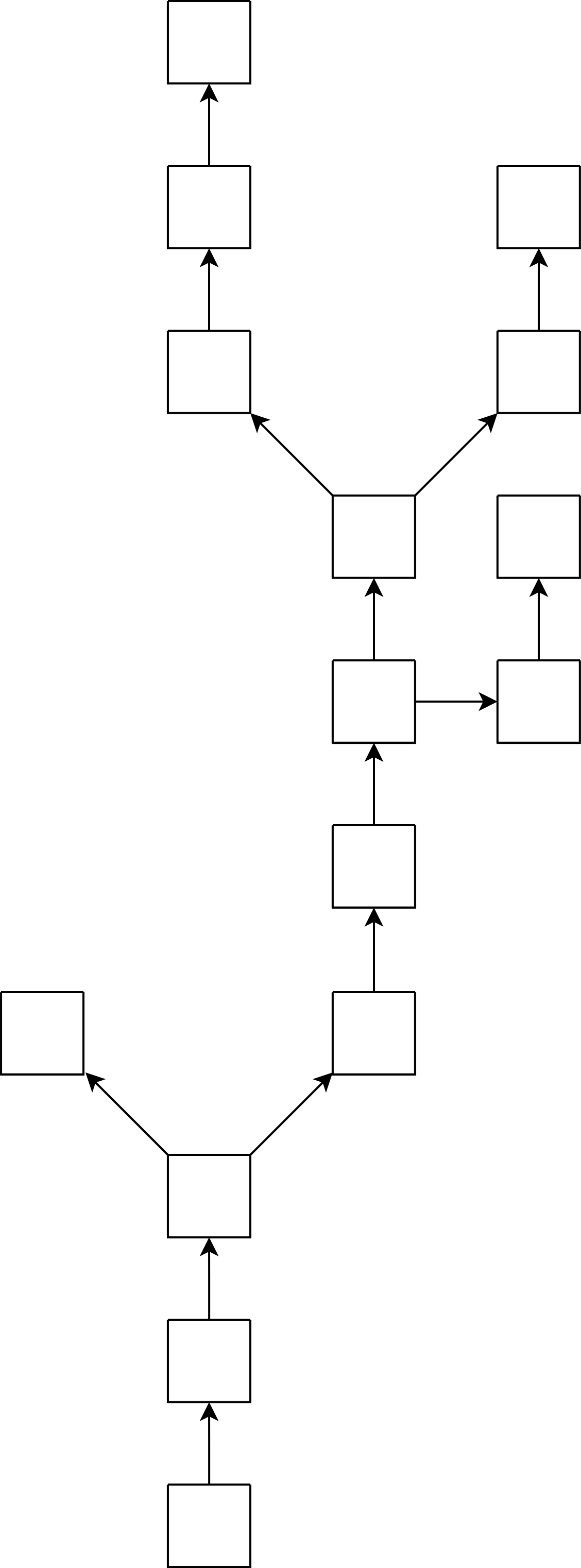
1. Infrastructure – hardware.
2. Networking – information propagation.
3. Consensus – proof of work.
4. Data – blocks and transactions.
5. Application – smart contracts.

**Blocks:**

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree.

Each block includes the cryptographic hash of the prior block in the blockchain, linking the two where the two linked blocks form a *chain.*

This iterative process confirms the integrity of the previous block, all the way back to the initial block, which is known as the *genesis* block (*Block 0*). To assure the integrity of a block and the data contained in it, the block is usually digitally signed.



**Blockchain Formation:**

The main chain consists of the longest series of blocks from the genesis block, to the current block. Orphan blocks exist outside the main chain.

Sometimes separate blocks can be produced concurrently, creating a *temporary fork*.

In addition to a secure hash-based history, any blockchain has a specified algorithm for scoring different versions of the history so that one with a higher score can be selected over others.

Peers supporting the database have different versions of the history from time to time. They keep only the highest-scoring version of the database known to them. Whenever a peer receives a higher-scoring version (*usually the old version with a single new block added*) they extend or overwrite their own database and retransmit the improvement to their peers.

There is never an absolute guarantee that any particular entry will remain in the best version of history forever. Blockchains are typically built to add the score of new blocks onto old blocks and are given incentives to extend with new blocks rather than overwrite old blocks.

Therefore, the probability of an entry becoming superseded decreases exponentially as more blocks are built on top of it, eventually becoming very low.

**Block Time:**

The *block time* is the average time it takes for the network to generate one extra block in the blockchain.

By the time of block completion, the included data becomes verifiable. In cryptocurrency, this is practically when the transaction takes place, so a shorter block time means faster transactions.

**Hard Forks:**

A *hard fork* is a change to the blockchain protocol that is not backward compatible and requires all users to upgrade their software in order to continue participating in the network.

In a hard fork, the network splits into two separate versions: one that follows the new rules and one that follows the old rules.

**Decentralization:**

By storing data across its peer-to-peer network, the blockchain eliminates some risks that come with data being held centrally. The decentralized blockchain may use *ad hoc* message passing and distributed networking.

In a so-called "51% attack" a central entity gains control of more than half of a network and can then manipulate that specific blockchain record at will, allowing double-spending.

Blockchain security methods include the use of *public-key cryptography*.

A public key (*a long, random-looking string of numbers)* is an address on the blockchain. Value tokens sent across the network are recorded as belonging to that address. A private key is like a password that gives its owner access to their digital assets or the means to otherwise interact with the various capabilities that blockchains now support.

Data stored on the blockchain is generally considered incorruptible.

Every node in a decentralized system has a copy of the blockchain. Data quality is maintained by massive database replication and computational trust.

No centralized "official" copy exists and no user is "trusted" more than any other. Transactions are broadcast to the network using the software. Messages are delivered on a *best-effort* basis.

Blockchains use various time-stamping schemes, such as *proof-of-work*, to serialize changes. Later consensus methods include *proof of stake*.

The growth of a decentralized blockchain is accompanied by the risk of centralization because the computer resources required to process larger amounts of data become more expensive.

**Finality:**

Finality is the level of confidence that the well-formed block recently appended to the blockchain will not be revoked in the future (*is "finalized"*) and thus can be trusted.

Most distributed blockchain protocols, whether proof of work or proof of stake, cannot guarantee the finality of a freshly-committed block, and instead rely on "probabilistic finality": as the block goes deeper into a blockchain, it is less likely to be altered or reverted by a newly found consensus.

Byzantine fault tolerance-based proof-of-stake protocols purport to provide so called "absolute finality": a randomly chosen validator proposes a block, the rest of validators vote on it, and, if a supermajority decision approves it, the block is irreversibly committed into the blockchain.

**Openness:**

Open blockchains are more user-friendly than some traditional ownership records, which, while open to the public, still require physical access to view.

**Permissionless (*public*) Blockchain:**

An advantage to an open, permissionless, or public, blockchain network is that guarding against bad actors is not required and no access control is needed.

This means that applications can be added to the network without the approval or trust of others, using the blockchain as a transport layer.

**Permissioned (*private*) Blockchain:**

Permissioned blockchains use an access control layer to govern who has access to the network.

It has been argued that permissioned blockchains can guarantee a certain level of decentralization, if carefully designed, as opposed to permissionless blockchains, which are often centralized in practice.

**Public Blockchains:**

A public blockchain has absolutely no access restrictions. Anyone with an Internet connection can send transactions to it as well as become a validator.

**Private Blockchains:**

A private blockchain is permissioned. One cannot join it unless invited by the network administrators. Participant and validator access is restricted.

To distinguish between open blockchains and other peer-to-peer decentralized database applications that are not open ad-hoc compute clusters, the terminology *Distributed Ledger* (DLT) is normally used for private blockchains.

**Hybrid Blockchains:**

A hybrid blockchain has a combination of centralized and decentralized features.

The exact workings of the chain can vary based on which portions of centralization and decentralization are used.

**Sidechains:**

A sidechain is a designation for a blockchain ledger that runs in parallel to a primary blockchain.

Entries from the primary blockchain (*where said entries typically represent digital assets*) can be linked to and from the sidechain; this allows the sidechain to otherwise operate independently of the primary blockchain.

**Consortium Blockchain:**

A consortium blockchain is a type of blockchain that combines elements of both public and private blockchains.

In a consortium blockchain, a group of organizations come together to create and operate the blockchain, rather than a single entity.

The consortium members jointly manage the blockchain network and are responsible for validating transactions.

Consortium blockchains are permissioned, meaning that only certain individuals or organizations are allowed to participate in the network. This allows for greater control over who can access the blockchain and helps to ensure that sensitive information is kept confidential.