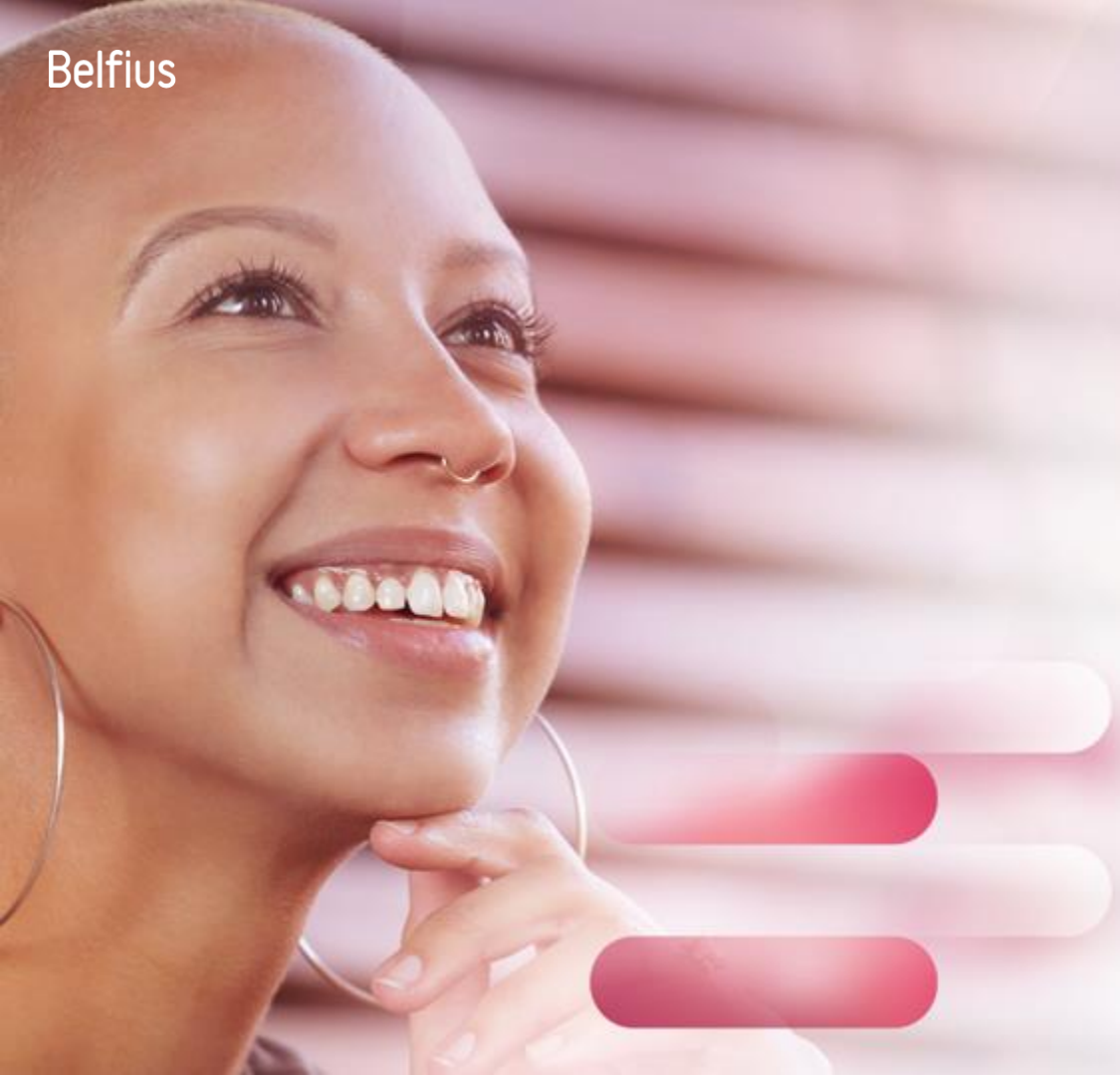
Belfius



Blockchain

04.05.2022

Blockchain Categorization

Permissionless

Open to anyone publishing blocks, without needing permission from any authority: any blockchain network user (even malicious) within a permissionless blockchain network can read and write to the ledger

To prevent this, use of multiparty agreement or 'consensus' system is foreseen

Permissioned

Only authorized users are maintaining the blockchain, it is possible to restrict read access and to restrict who can issue transactions.

The establishment of one's identity required to participate as a member of the blockchain.

Permissioned blockchain networks support the ability to selectively reveal transaction.

There should be a shared business process with natural disincentives to commit fraud or behave as a bad actor (since they can be identified).

Cryptographic Hash Functions

Hashing: method of applying a cryptographic hash function to data, which calculates a relatively unique output (called a message digest, or just digest)

Computationally infeasible to compute the correct input value given some output value:

- find x such that hash(x) = digest

Computationally infeasible to find a second input which produces the same output

- given x, find y such that hash(x) = hash(y)

Collision resistant. one cannot find two inputs that hash to the same output.

- find an x and y which hash(x) = hash(y)

Cryptographic hash functions are used for many tasks, such as:

- Address derivation ·
- Creating unique identifiers.
- Securing the block data – a publishing node will hash the block data, creating a digest stored within the block header.
- Securing the block header –

Transactions

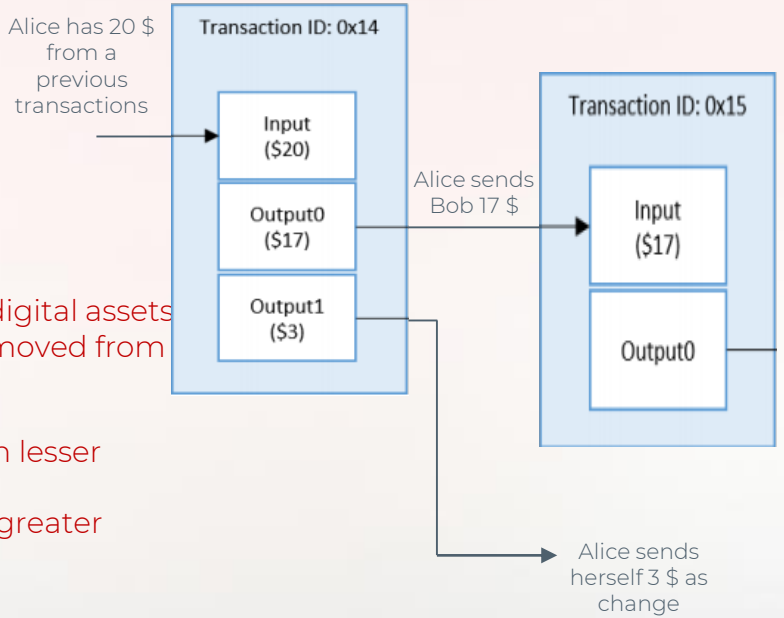
A single cryptocurrency transaction typically requires

Input

Source of the digital asset (providing provenance) –
the previous or if a new digital asset, the origin event.

Since the input to the transaction is a reference to past events, the digital assets do not change. The value of the digital asset cannot be added or removed from existing digital asset.

A digital asset can be split into multiple new digital assets (each with lesser value) or digital assets can be
combined to form fewer new digital assets (with a correspondingly greater value).



Output

Account of the recipient of the digital assets + how much digital asset they will receive.
The output specifies the number of digital assets to be transferred to the new owner(s) + the identifier of the new owner(s)

Transactions are signed by the sender's associated private key & can be verified using the associated public key.

Transactions

A single cryptocurrency transaction typically requires

Address

Alphanumeric string of characters derived from the blockchain network user's public key using a cryptographic hash function

Addresses are shorter than the public keys - are not secret.

Permissionless blockchain networks, a blockchain network user can generate as many asymmetric-key pairs

Addresses may act as the public-facing identifier in a blockchain network for a user (often converted into a QR code)

For Ethereum, smart contracts are also accessible via a special address called a contract account.

A single cryptocurrency transaction typically requires

Private Key Storage

with permissionless blockchain networks, users must manage and securely store their own private keys (in a wallet: more secure ! Or better in a secured hardware

- Emergence of an industry of private key escrow services.

If a user loses a private key, then any digital asset associated with that key is lost, stolen

Transactions

A single cryptocurrency transaction typically requires

Ledgers

Pen and paper ledgers exist for a long time to keep track of the exchange of goods and services.

In modern times, ledgers have been stored digitally, in large databases owned and operated by a centralized trusted third party (i.e., the owner of the ledger) on behalf of a community of users.

These ledgers with centralized ownership can be implemented in a centralized or distributed fashion

Blockchain offer the opportunity of also decentralizing the ownership of the ledger (together with distributed physical architecture)

Transactions

Let’s compare centralized – decentralized ledgers to catch the value proposition of blockchain

Centrally-owned ledgers may be lost or destroyed

Centrally-owned ledgers may be on a homogeneous network,with the same software, hardware and network infrastructure (impact of resiliency)

Every user can maintain their own copy of the ledger.

New full nodes joining request a full copy of the blockchain network’s ledger, making loss or destruction of the ledger difficult.

A blockchain is a heterogeneous network, where the software, hardware and network infrastructure are all different.

An attack on one node is not guaranteed to work on other nodes.

Transactions

Let's compare centralized – decentralized ledgers to catch the value proposition of blockchain

Centrally owned ledgers may be located entirely in specific geographic locations (e.g., all in one country). If network outages occurs, ledger is down ,

The transactions on a centrally owned ledger are not transparent and may not be valid

A user must trust that the owner is validating each received transaction

A blockchain network can be comprised of geographically diverse nodes which may be found around the world.

Peer-to-peer: ledger is resilient to the loss of any node, or even an entire region of nodes

If a malicious node was transmitting invalid transactions, others would detect and ignore them, preventing the invalid transactions from propagating throughout the blockchain network..

Transactions

Let's compare centralized – decentralized ledgers to catch the value proposition of blockchain

The transaction list on a centrally owned ledger may not be complete; a user must trust that the owner is including all valid transactions

The transaction data on a centrally owned ledger may have been altered

a user must trust that the owner is not altering past transactions

A blockchain network holds all accepted transactions.

To build a new block, a reference must be made to a previous block and building on top of it. If a publishing node did not include the latest block, other nodes would reject it.

A blockchain digital signatures and cryptographic hash functions to provide tamper evident and tamper resistant ledgers

Transactions

Let’s compare centralized – decentralized ledgers to catch the value proposition of blockchain

The centrally owned system may be insecure;

A user must trust that the computer systems and networks are receiving critical security patches and have implemented best practices for security

A blockchain network, due to the distributed nature, provides no centralized point of attack.

Generally, information on a blockchain network is publicly viewable, and offers nothing to steal

Blocks

Blockchain network users submit candidate transactions to the blockchain network via software (desktop applications, smartphone applications, digital wallets, web services, etc.).

The software sends the transactions to a node or nodes (publishing or not) within the blockchain network.

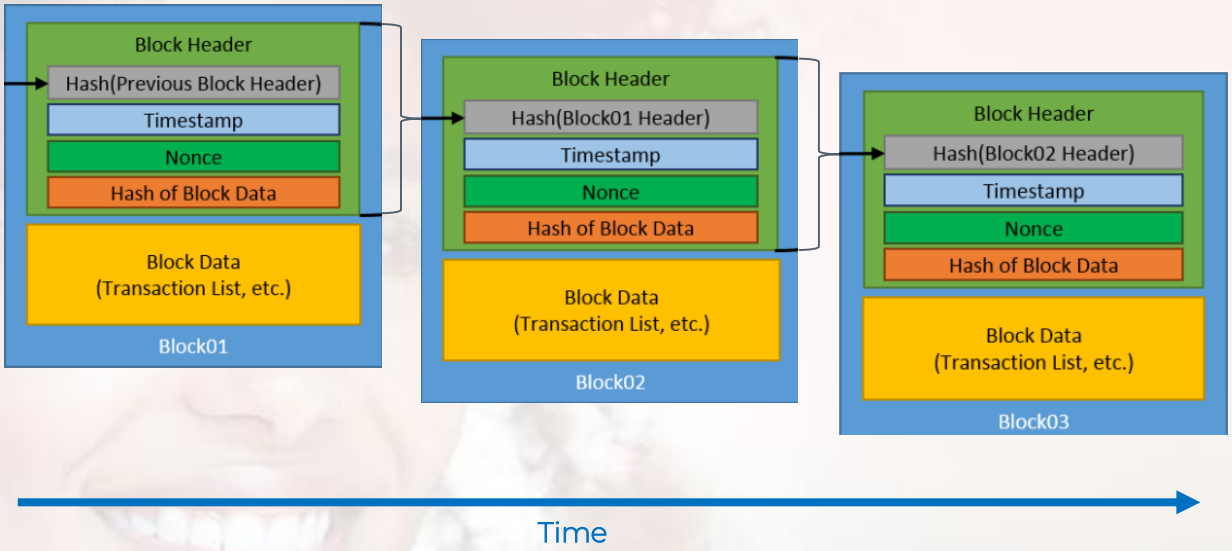
The submitted transactions are propagated to the other nodes, but this by itself does not place the transaction

Once a pending transaction has been distributed to nodes, it must then wait in a queue until it is added to the blockchain by a publishing node.

Transactions are added to the blockchain when a publishing node publishes a block

Validity and authenticity is ensured by checking that each transaction (listed in the transaction's 'input' values) is cryptographically signed

Chaining Blocks



Blocks are chained together through each block containing the hash digest of the previous block's header, thus forming the blockchain

If a previously published block were changed, it would have a different hash.
This in turn would cause all subsequent blocks to also have different hashes since they include the hash of the previous block…..Thus easy to detect and reject altered blocks

Consensus Model

Who (which node) published the next block and place the transaction

Permissionless blockchain networks: many publishing nodes competing
To publish the next block. They compete to win cryptocurrency and/or transaction fees.

No need for a trusted third party provide the state of the system—every user within the system can verify the system's integrity

The consensus model must work in the presence of possibly malicious users

Consensus Model

Proof of Work Consensus Model

A user publishes the next block by being the first to solve a computationally intensive puzzle

One publishing node has performed this work, its send the block to full nodes in the blockchain network.

- The recipient full nodes verify that the new block fulfills the puzzle requirement,
- Then add the block to their copy of the blockchain and resend the block to their peer nodes

Proof of Stake Consensus Model

The more stake a user has invested into the system, the more likely they will want the system to succeed

Consensus Model

Proof of Authority/Proof of Identity Consensus Model

Relies on the partial trust of publishing nodes through their known link to real world identities.

Publishing nodes must have their identities proven and verifiable within the blockchain network.

Applies to permissioned blockchain networks with high levels of trust

Proof of Elapsed Time Consensus Model

Each publishing node requests a wait time from a secure hardware time source (within their computer system)

The latter generates a random wait time and return it to the publishing node software.

Ledger Conflict Resolution

With any distributed network, some systems will be behind on information or have alternative information.

- Due to network latency between nodes and the proximity of groups of nodes.

Permissionless blockchain networks are more prone to have conflicts

- Due to their openness and number of competing publishing nodes.

Due to the possibility of blocks being overwritten (due to a conflict), a transaction is not usually accepted as confirmed until several additional blocks have been created on top of the block containing the relevant transaction

Node in a proof of work blockchain network with enormous amounts of computing power could start at the genesis block and create a longer chain than the currently existing chain

- Thereby wiping out the entire blockchain history.

Forking

Performing changes and updating technology can be difficult

For permissionless blockchain networks (many users, distributed around the world, and governed by the consensus), it becomes extremely difficult.

Changes to a blockchain network's protocol and data structures are called forks

Soft fork: changes are backwards compatible with nodes that have not been updated.

Hard fork: changes are not backwards compatible:

- The nodes not updated will reject the blocks following the changes

With cryptocurrencies, if there is a hard fork and the blockchain splits then users will have independent currency on both forks (having double the number of coins in total).

All the activity must move to the new chain, the old one may eventually not be used since the two chains are not compatible

Smart Contract

Definition of a smart contract:

Satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement),

Minimize exceptions both malicious and accidental,

Minimize the need for trusted intermediaries.

The smart contract is executed by nodes within the blockchain network;

- All nodes that execute the smart contract must derive the same results
- The results of execution are recorded on the blockchain

A smart contract can perform calculations, store information, expose properties to reflect a publicly exposed state, automatically send funds to other accounts.

Smart contracts must be deterministic: the publishing nodes execute the smart contract code simultaneously when publishing new blocks

Immutability

Blockchain uses the strategy of adopting the longest chain (the one with the most amount of work put into it) as truth when there are multiple competing chains.

A longer, alternate chain of blocks could be the result of a form of attack known as a 51 % attack.

- The attacker simply garners enough resources to outpace the block creation rate of rest of the blockchain network (holding more than 51 % of the resources applied for producing new blocks)
- This attack is mitigated for permissioned blockchain: nodes are under control and cooperation can be enforced between nodes.
- Add legal contracts in place for the blockchain network users which may include clauses for misconduct and the ability to take legal action.

Users Involved in Blockchain Governance (1/2)

Common misconception: blockchain networks are systems without control and ownership

- Permissioned blockchain networks are generally setup and run by an owner or consortium
- Permissionless blockchain networks are often governed by blockchain network users, publishing nodes, and software developers

Most blockchain technologies are open source:

- Possible to create separate but compatible software as a means of bypassing pre-compiled software released by developers
- The developer of the blockchain software will play de facto a large role in the blockchain network's governance

Users Involved in Blockchain Governance (2/2)

Developers can design updates to blockchain software to change the blockchain protocol or format.

With enough user adoption, a successful fork can be created.

Permissionless blockchain networks are ruled by the publishing nodes and may marginalize a segment of users by forcing them to adopt changes they may disagree with to stay with the main fork

Beyond the Digital

Oracle Problem:

When blockchains interact with human, input data or sensor input data from the real world: no method to determine if the input data reflects real world events.

For pseudonymous blockchain networks that are pseudonymous, dealing with data misrepresentation can be especially problematic

- Active area of Research: create reliable mechanisms to ingest external data in a way that is both trustworthy and accurate(e.g. web API data and convert it into blockchain readable byte/opcode)

Blockchain Death

Traditional centralized systems are created and taken down constantly

Because blockcains networks are are decentralized, when it “shuts down” it will never be fully shut down, and that there may always be some lingering blockchain nodes running.

Cyber security

Transactions that have not yet been included in a published block within the blockchain are vulnerable to several types of attacks

- Spoofing time or adjusting the clock of a member of an ordering service could have positive or negative effects on a transaction: time and the communication of time an attack vector
- Denial of service attacks can be conducted on the blockchain platform
- Newly coded applications (like smart contracts) may contain new and known vulnerabilities and deployment weaknesses

Blockchain Limitations and Misconceptions

Malicious users

- Blockchain network can enforce transaction rules and specifications.
- Blockchain cannot enforce a user code of conduct.
- Malicious users can get enough power (be it a stake in the system, processing power, etc.) to cause damage. Once a large enough malicious collusion is created, malicious mining actions can include:

1. Ignoring transactions from specific users, nodes, or even entire countries.
2. Creating an altered, alternative chain in secret, then submitting it once the alternative chain is longer than the real chain
3. Refusing to transmit blocks to other nodes, essentially disrupting the distribution ofinformation (this is not an issue if the blockchain network is sufficiently decentralized

Mitigation: While malicious users can be annoyances and create short-term harm, blockchain networks can perform hard forks to combat them

4. the administrators of the infrastructure for permissioned blockchain networks may also act maliciously.

No Trust

Misinterpretation: there is no “trusted third party” in a blockchain and assuming blockchain networks are “trustless” environment

There is still a great deal of trust needed in:

- in the cryptographic technologies utilized
- in the correct and bug free operation of smart contracts
- in the developers of the software to produce software that is as bug-free
- that most users of the blockchain are not colluding in secret

Inadequate Block Publishing Rewards

Cryptocurrencies that are not able to consistently and adequately reward publishing nodes risk delays in publishing blocks and processing transactions.

Such weakened cryptocurrencies open themselves up to being attacked by nodes with large amounts of resources that may maliciously alter the blockchain or deny service

Application Considerations

The fear of missing out: “we want to use blockchain somewhere, where can we do that?”

Blockchain technology solutions may be suitable if the activities or systems require features such as:

- Many participants or Distributed participants
- Want or need for lack of trusted third party
- Workflow is transactional in nature (e.g., transfer of digital assets/information betweenparties)
- A need for a globally scarce digital identifier (i.e., digital art, digital land, digitalproperty)
- A need for a decentralized naming service or ordered registry
- A need for a cryptographically secure system of ownership
- A need to reduce or eliminate manual efforts of reconciliation and dispute resolutions
- A need to enable real time monitoring of activity between regulators and regulated entities
- A need for full provenance of digital assets and a full transactional history to be shared amongst participants

Application Considerations

The fear of missing out: “we want to use blockchain somewhere, where can we do that?”

Additional factors to check the blockchain is worth it (1/3)

- Data visibility

  Permissionless blockchain networks can allow anyone to inspect and contribute to the blockchain. The data is generally public, so GDPR issue

- Full transactional history

  Some blockchain networks provide a full public history of a digital asset – from creation, to every transaction it is included in.

Application Considerations

The fear of missing out: “we want to use blockchain somewhere, where can we do that?”

Additional factors to check the blockchain is worth it (2/3)

– Fake Data Input –

Since multiple users are contributing to a blockchain, some could submit false data, mimicking data from valid sources (such as sensor data)

– CRUD

Many applications follow the “CRUD” (create, read, update, delete) functions for data.

With a blockchain, there is only “CR” (create, read). There are methods that can be employed to “deprecate” older data if a newer version is found, but there is no removal process for the original data.

– Transactions Per Second –

Transaction processing speed is highly dependent on the consensus model used

Application Considerations

The fear of missing out: “we want to use blockchain somewhere, where can we do that?”

Additional factors to check the blockchain is worth it (2/3)

– Compliance–

> The use of blockchain technology does not exclude a system from following any applicable laws and regulation

– Node Diversity

> A blockchain network is only as strong as the aggregate of all the existing nodes participating in the network.
>
> If all the nodes share similar hardware, software, geographic location, and messaging schema then there exists a certain amount of risk associated with the possibility of undiscovered security vulnerabilities