What is Blockchain?

Research Report

What is Blockchain?

A blockchain is a publicly distributed general ledger in which all transactions and changes are grouped into blocks. All these blocks in succession form an unadaptable chain, a Blockchain, which together represent the complete history of the general ledger.

Introduction

A Blockchain is a revolutionary digital systematic technology on which it is possible to build applications and services just like the internet. Strictly speaking, Blockchain is a decentralized database, whether public or private. This database functions as an online decentralized general ledger. Decentralized means that all participants can request and keep a copy at any time. So, on a blockchain, we store information, information about who owns what at what time, including the corresponding mutations. In a blockchain, everything is a transaction. It is not the case that you already adapt information that has already been recorded, but you are adding something to the blockchain, such as a transaction from party X to party Z whereby the balance sheets of both parties get an addition, positive or negative. Currently, a blockchain is less suitable for storing larger amounts of information. It is a matter of time before this scalability problem is solved. There are already several competing teams who think they can solve this in different ways. Actually since this 2019 multiple projects solved the scalability problem with success. The blockchain system ensures that the transactions are validated on the basis of predetermined rules. Approved and new transactions are distributed almost immediately to all participants so that the information that everyone owns is the same at all times. There is agreement (consensus) about the truth of the state of the ledger. Where the Internet has become the infrastructure for the transfer of information (communication) and has given us the freedom to communicate with everyone, wherever in the world, Blockchain must be regarded as the infrastructure for transactions (value transfer) that gives us the freedom to exchange value with anyone in the world without restrictions. A Blockchain facilitates transactions between parties without a (trusted) third party being involved. The consensus reached on the 'truth' (or state) of this decentralized organized system, including an overview of all transactions, enables us to do business faster, more efficiently and less costly and to exchange value throughout the world without an intermediary.

Participants in a network

The registers are centrally managed and stored within traditional registration systems. Here, the trust that is based on the manager of the register is fundamental. After all, it is the intention that we can always rely on the 'truth' of the register as it is placed with the administrator, regardless of the situation. Ultimately, the administrator of the register is also the one who has the power over this register and therefore also the truth about it. Because management and storage are centrally regulated in traditional registration systems, a register can be modified relatively easily by a malicious party, internal or external.

With blockchain, we put our trust in mathematics, the underlying mathematical formulas from which a blockchain derives its right to exist. When someone tries to change something in the formula or outcome, this attempt will always be noticed. The network manages and protects the registry together with the corresponding mathematical formulas. The information that is present on a blockchain is therefore not managed by one party but by the participants in the blockchain network.

What is Blockchain?

Participation is simple, anyone with an internet connection and a computer can download and install the required software. After this, you are a participant in the network. Blockchain software contains the rules that everyone who wants to be part of the blockchain network must comply with like specifications, programming languages, settings, and appointments.

Within a blockchain network, everyone is the owner of the information and nobody is absolutely the owner of the stored information. A blockchain is based on shared responsibility and participants have a common goal, namely to maintain the network, to secure it and to validate transactions. This goal is shared because if the blockchain could no longer be trusted, it would lose its (stored) value.

Participants in a blockchain, therefore, all have a copy of the information (the general ledger), have access to the stored information, and can check whether the information is correct.

Registrations immortalized
Changes in a blockchain take place in a unique way. The old data will remain but will be supplemented with extra 'new' data. Changes are added to the general ledger after checking for accuracy by means of transactions and taken over by the network of participants. It is not necessary, as with a traditional database, to synchronize information and so the chance of errors is absent. The new information is copied and added to everyone's own copy of the blockchain. Because a blockchain is set up securely from design, the information on it cannot be adjusted, replaced or removed. Everything that happens on a blockchain is listed next to each other. A participant in the blockchain network can add rules. Each line adds a piece of information to the blockchain, these lines are bundled into a block and added to the chain, hence the name Blockchain. Each block also receives a timestamp so that users can check when a transaction has taken place. As a result, everything on a blockchain can be traced back to the absolute beginning, also known as the Genesis block. This makes it easy to check and understand the entire history of a blockchain.

Transactions, Transactions, and Transactions
Because the definition of a transaction can be explained in several ways, it is important that we see this in the right light. A transaction of ownership or value from party X to party Z is called, a transaction in consultation with blockchain. Everything that is added to a blockchain is a transaction. The record-keeping of value-transfers is useful if we want to see who the actual owner of a value object is. We can state that the registration of such a transaction is, therefore valuable. Creating a transaction is not free on a blockchain. Because the network makes it possible for transactions to take place, they also expect a reward. The network would not do this work without a reward. For this reason, it is essential that every transaction on a blockchain is one of value. That's why the transactions are not completely free of charge on a blockchain. Partly because of this property, a blockchain is less suitable for storing large amounts of data that do not necessarily have to represent a (substantial) value in a traditional database. We could say that the perpetuation of information on a blockchain may cost something, in order to prevent 'system pollution'. We primarily use a blockchain for the transfer of value or whether a transaction actually took place, now or at any time in the future.

What is Blockchain?

Decentralized security

Because with a blockchain each participant has a copy of the general ledger with all transactions, this is also safer than a traditional centrally managed database. An additional advantage of the decentralized aspect of the blockchain is that it is a lot less sensitive to a complete outage of the network. For a centrally managed database, a disruption means a complete failure of the database 'service'. Simply put, in a blockchain, there is no single point of failure. The network and thus also the decentralized database will continue to function if there are one or even multiple disruptions. It also holds that the more participants there are, the safer and more robust the system. Because a blockchain consists of several participants, the setup is also more complicated than that of a traditional database, which makes potential attackers virtually impossible to change or delete information. Finally, the registry must be adjusted simultaneously by each administrator by the attacker. The amount of computing power and energy required for such an attack does not make this attractive. Because you no longer depend on the trust in one registry administrator who manages the data, a blockchain offers better protection against internal and external attacks. The remuneration structure in a blockchain network ensures that participating parties have an incentive to continue to act correctly.

Distributed trust

Do we trust 'everyone'? By validating at the gate if the owner is really the owner of the given 'value object' it will be prevented that everyone can perform a mutation on a blockchain. Again, it comes to see that the entire network validates whether the owner is really the rightful owner. In a blockchain, we call this distributed trust. This means we do not trust in one party but in the shared trust across the network, by using a consensus mechanical to agree on the truth. If the majority of the network agrees with each other, a transaction will be validated and added to the blockchain (and will be executed accordingly). So, you do not trust the people or companies behind the computers but in the software of the mathematical formulas that make the blockchain network what it is. Fundamentally, of course, you are familiar with that software with predetermined rules and agreements (and yourself of course). That's why we say, **blockchain is trustless**.

Disclaimer

The information contained in this document is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of TheCrypto.Community. The content in this document is solely the property of TheCrypto.Community.

Any partial, complete, or public access to a third party of the content in this document, TheCrypto.Community reserves the right to pursue legally. And request its confidentiality to the acquiring part, in order to hold the information on the document private.

The opinions and information expressed in this document are in good faith, and while every care has been taken in preparing the document; TheCrypto.Community makes no representations and gives no warranties of any nature in respect of the investment the acquiring party decides to take over the information stated in this document or the reviewed project.

TheCrypto.Community Research Report is not limited to the accuracy or completeness of any project it reviews nor is responsible what the researched project does in a certain period of time.

TheCrypto.Community is not affiliated or economically compromised with the projects it reviews, all information is researched on an unbiased way, in order to provide the clearer pros and cons of any project is reviewed.

This document facts and opinions are TheCrypto.Community alone and are not to be considered investment advice for the acquiring party nor TheCrypto.Community will be responsible for any outcome the acquiring party might have upon taking action with the information contained in this document. Sources are available on request, we reserve the right to refuse such requests.

The acquiring party hereby declares that is completely aware there is no commitment from TheCrypto.Community in any action it takes upon this Research Report. Nor any compensation will be made to any loss of assets, goods or services the acquiring party does upon the reviewed project.