



# What is Cryptocurrency?



## Research Report

# What is Cryptocurrency?

***A cryptocurrency is a digital currency/asset which uses cryptography and is developed as a medium of exchange. The use of cryptography is to secure transactions, to manage the issuance of new units and to verify the transaction of assets, without the need for a trusted third party.***

## **Introduction**

Cryptocurrency and blockchain-technique cannot be seen apart from each other. A digital currency in which encryption techniques are used to regulate the generation of currency units and to validate the transfer of resources, regardless of a trusted third party, is called a cryptocurrency. Cryptocurrencies are being developed by using 'advanced' computers and techniques. This is done by using complex algorithms & mathematical formulas. To develop a cryptocurrency successfully, you need to have a high-level understanding of the matter. Therefore, this is not directly intended for the 'normal' person because of a lack of expertise and resources common people have. As a result, cryptocurrencies seem to be practically inaccessible for a lot of people and only accessible to the 'nerds & tech-savvy people' among us, but in reality, it turns out to be quite different than broadly assumed.

## **Cash(money) and cryptocurrency**

You can easily compare cryptocurrency with cash(money). The value is indicated on the cash(money) and if you take a look at the back, you will find a serial number. This serial number contains information about the origin of the note and other things. This serial number also makes it possible to trace the note. Remember this serial number and put the note in your wallet and we have the basic principle for a cryptocurrency.

## **Digital & encrypted**

With cryptocurrency, this serial number is completely digital and encrypted. The serial number is processed in the network. Network applications enable the value (money) linked to the serial number to be sent to any network participant as long as the sender has the ownership of the asset/money. In this way, we explain the simplest form of cryptocurrency. Of course, the underlying technology is much more complicated, but this is the base.

## **Decentralized approach**

The real power of cryptocurrency lies in the encrypted digital coding where traceability is simple and the transactions (value/money) can take place worldwide in a fast, efficient and above all secure way, all without the need for, usually an (expensive) third party. A complete decentralized approach to transact with each other. With this approach, parties that normally mediate are eliminated, for example, banks, insurance agencies, and payment providers. With cryptocurrency, you have the power over your equity where no (central) authority is needed to move the money. You determine what you do with your money, whenever and wherever. You are in control.

# What is Cryptocurrency?

## **Technically unique**

The potential of cryptocurrency is enormous. Because of the way the technique works, it can count on the sympathy of many. Cryptocurrency makes the difference if we only look at the costs of transporting & sending 'old & traditional' money and the high fees charged by parties such as credit card companies and banks at the moment you make an international payment.

## **Reliability & speed**

Because the stability of this system and the technology is very great, the way we conduct transactions will take place in the same way as we have been sending information since the advent of the internet. Reliable and very fast. Due to the decentralized nature of cryptocurrency, there is no question of a 'single point of failure'.

## **Barter & Cryptos**

The existing fear of the 'unknown' (read cryptocurrency) will gradually give way to curiosity. The best way to approach cryptos is to put it in a familiar light. Cryptos can best be considered as a medium of exchange, just like gold and silver, but think of bread, cheese, and eggs. All to exchange against money. Cryptocurrency can be seen as the next iteration of money.

## **Free transactions(almost)**

Chances are you have ever made an internet purchase through a webshop. In this case both you and the buyer pay, but also the selling party for this. In a lot of cases, this is not immediately visible, but these costs are already included in the price of the product. Do you send money across national borders? Then you have to deal with even higher costs and usually a longer lead time before the transaction is executed. By using cryptocurrency, both you and the counterparty will no longer have to pay any costs for a transaction of value (money) and you will no longer be dependent on, for example, the working hours and availability of the parties.

## **Crypto = Cash?**

One of the strengths of Crypto is that you can transfer value without having to pay a (high) extra fee to a third party. For this reason, the comparison with cash money quickly increases. After all, you do not pay any transaction costs if you give someone cash. It would be absurd if we demanded a fee for withdrawing money from your wallet, transporting it and putting it in the wallet of the other party. All of this sounds strange but is what happens on a large scale by a lot of financial institutions. This is currently still considered, normal. If you think carefully about this, you will most probably come to the conclusion that this is still a very old-fashioned way of working in a digital era. Cryptocurrency is the solution to this way of working.

## **The (unnecessary) intermediary**

With cryptocurrency, you create a wallet on the internet. When creating this wallet, you create (in many cases automatically) a public address and a private key. The public address is an address to share where other value (money/cryptos) can send. The private key is linked to the public address and meant to open your wallet and thus use credits, you must keep it secret.

# What is Cryptocurrency?

## **Decentralized distribution of the general ledger**

A ledger is an overview of all balances and transactions of all accounts (wallets). Maintaining the ledger is a task of the so-called 'miners', they also ensure that the security of the cryptocurrency remains in order because the majority agrees on the state of the ledger. The rewarding of cryptocurrency is also rewarded in the form of the relevant cryptocurrency. This method is crucial because it solves the so-called 'double spending' problem. In other words, because the transaction of the value is recorded in a public decentralized ledger and the majority of the miners recognize this, it is practically impossible to double-spend the same value without being detected by the network of miners. This offers the guarantee that the receiving party is really the owner of the relevant crypto and the sending party did not issue it twice. To keep it simple, see it like a WhatsApp/telegram message that's truly unique and can't be copied, but it can be forwarded. Once you have forwarded the message, it also disappears from your device.

## **Nodes & Miners**

A node is a device or structure that can be considered as an independent unit. Nodes function within an automated system and communicate with each other. A miner is a person or rather a computer that runs specific software to keep the blockchain network, secure and validates transactions. As a reward for the work done, miners have a chance of receiving cryptocurrency (the reward for their work). The nodes within a blockchain reach a consensus. This means that there must be an agreement between the different nodes on 'the truth' or the state of the blockchain network. Mining is important because cryptocurrencies are therefore digitally mined and no transactions/mutations can be added without miners. The valid transactions are recorded in a block. All miners use their computing power to solve a tricky puzzle based on a complicated mathematical formula. Due to the absence of a trusted third party, it is very important that the general ledger in which everything is kept is completely reliable. This reliability is facilitated by the nodes that are all interconnected. One of the most important tasks of the nodes is checking the validity of transactions.

## **Encryption Conditions**

Everyone is equal within a Blockchain network including all the nodes. Everyone has the same odds to find a solution to the mathematical problem. There isn't a node that has the authority over another node. When creating a transaction, you broadcast a message to the network with use of an encryption condition (cryptographic protocol) that requests to transfer value from person-X to person-Z. This message will eventually be sent across the entire network. Because an encrypted signature is added to the message, the network of nodes can ensure that person-X indeed performs a transaction to person-Z.

## **Invalid transactions**

Every transaction can be traced entirely within the public and distributed ledger, whereby invalid and inadequate transactions are rejected by the network without mercy. Finally, all accounts and associated values are kept exactly in the ledger. As a result, it is impossible that new coins are added from scratch, unlike, for example, fiat-currencies such as euros or dollars...

# 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.

