



# Blockchain Technology

## Beginner

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>What is a Blockchain?</b>	<b>3</b>
Blockchain as a Data Structure	3
The Blockchain is a Type of Data Structure	3
A Database: Efficient but Centralized	4
A Blockchain: Less Efficient, but Decentralized	4
Where does the term Blockchain come from?	5
Summary	6
A Protocol to Transfer Value	7
The Internet - A Protocol to Transfer Information	7
The Mail - A “Protocol” to Transfer Physical Goods	7
Summary	8
<b>How Does a Blockchain Work?</b>	<b>9</b>
The Elements of a Blockchain	9
Nodes	9
Miners	11
But Why Are Miners Doing This?	12
Summary	13
Identity in Blockchain	14
Public-Key Cryptography	14
Your Key Pair is Your Identity	15
Summary	17
<b>Wallets</b>	<b>18</b>
What a Wallet Does	18
A Wallet Acts as a Keychain	19
What If I Lose My Keys?	20
Summary	21
<b>Transactions</b>	<b>22</b>
Intro to Transactions	22
Summary	25
Intro to the Block Explorer	26
Summary	28
<b>Privacy on the Blockchain</b>	<b>29</b>

Why Privacy	29
How to Reclaim Your Privacy	29
Summary	31
<b>Blockchain Technology Summary</b>	<b>32</b>
A Data Structure	32
A Protocol to Transfer Value	32
The Elements of a Blockchain	33
Identity on the Blockchain	35
Wallets	35
Transactions	36
The Block Explorer	37
Privacy on the Blockchain	37
<b>Final Remarks</b>	<b>38</b>

# What is a Blockchain?

Most people have come across the term blockchain but few can tell you what it is, let alone how it works. We will help you understand what a blockchain is and how it works. In the Beginner Level, we will focus on the main ideas and value propositions of Blockchain without getting technical about it.

In this first chapter, we will look at blockchain in two different ways.

In the first article of this chapter, we will look at how a blockchain stores data and why this makes the data secure.

In the second article, we compare blockchains as a protocol to transfer money with the internet as a protocol to transfer information.

## Blockchain as a Data Structure

Welcome to the very first article in the technology section of our Horizen Academy. The first two articles aim to explain what a blockchain actually is. If you have read up on Bitcoin, blockchain, and cryptocurrencies before you may know there is a distinction between:

- Blockchain technology in general
- A protocol (the rules) of a specific blockchain
- The currency that is running on top of this blockchain (if there is one)

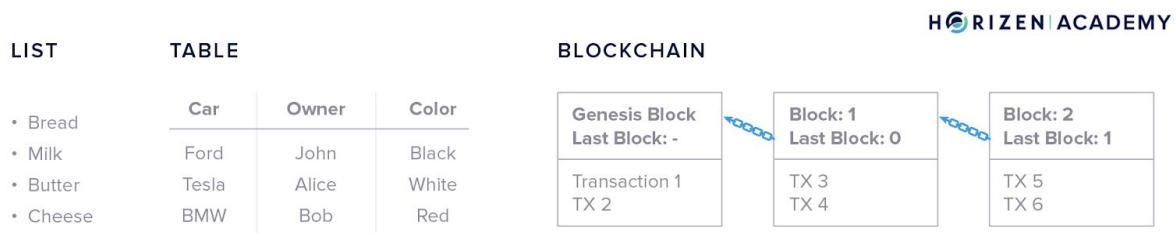
This article provides an introduction to what a blockchain in general is, and what it allows us to do. You can look at it in many different ways, depending on the context, but we want to focus on two very general approaches. On one hand, it is a way to store data and on the other hand a "language", or protocol to transfer value.

## The Blockchain is a Type of Data Structure

A blockchain is a data structure in the eyes of a computer scientist. This structure stores information reliably regardless of being run in a trustless environment. Here trustless means, that you can't trust the other network participants, simply because you don't know them.

A data structure may sound technical at first, but its function is exactly that. It structures your data. Lists or tables are familiar types of data structures. You likely use one of these two structures

anytime you write down something on paper. There are many types of data structures in the digital world, including blockchain. The term blockchain comes from the data being separated into many blocks. Every block states which block came before it, creating a "chain" of blocks. Stating which block came previously is commonly called to as referencing.



## A Database: Efficient but Centralized

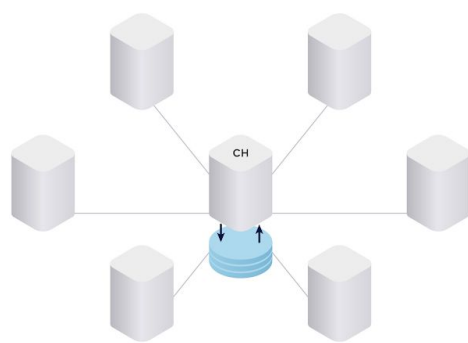
Most traditional databases use very efficient data structures. Databases are an excellent way to store large amounts of data but are usually operated by a central entity. Your bank, your favorite social network, or online merchant, uses databases to store your data.

This entity decides who can add data to the database and who can access it, but it also has the power to change or delete data. You can edit your social media profile. Your friends can see that information, but if you violate the site's Terms of Agreement they can delete your post. The central entity has the last say in what stays on the platform. This can be both good and bad when it comes to a social network, but this would not be a good feature when looking at data structures that store your money. Centralized databases are a lot more efficient not only because of the way they store data but mostly because the database is maintained by a single entity.

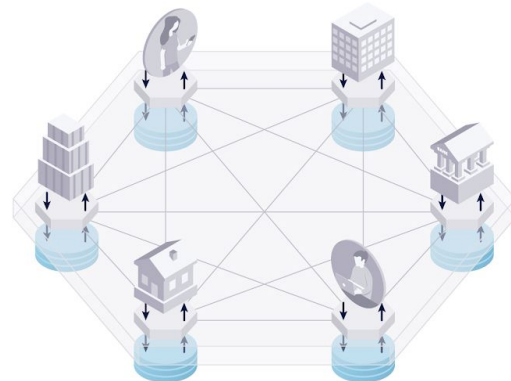
## A Blockchain: Less Efficient, but Decentralized

Many different entities, or *peers*, operate a blockchain. These peers don't know or trust each other (therefore "trustless"). The good thing is that they *don't need to trust each other*. All peers keep a copy of the data and no single peer has the power to change the data or censor what gets added. Participants (or *nodes* in technical terms) communicate constantly to keep each other updated on new events. Events on the blockchain are most commonly transactions.

There is no centralized entity, like a bank or clearinghouse, responsible for accepting and processing new transactions. Cryptocurrencies are permissionless because every individual abiding by the rules of the protocol can create a wallet and send a transaction without needing to sign up to use the service. The transaction is then broadcast to the network and every participant, or node, keeps a copy of it. A node can be operated by an individual person, a store accepting crypto or a bank. It makes no difference who you are. The amount of copies makes a blockchain slower than a database, but a more secure way to store data. For a global and secure type of money, this is a crucial set of traits.



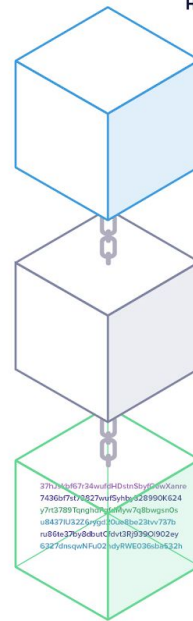
Current Centralized Clearing and Settlement  
used by Banks



Decentralized Clearing and Settlement  
with Blockchain

## Where does the term Blockchain come from?

The blockchain does not keep data in a single huge continuous ledger but separates the data into blocks. These blocks are then connected to each other like individual pages in a book. That is how the term blockchain came to be. Imagine a bookie recording entries using single pages of a book instead of one large scroll. Every few minutes he starts using a new page and adds a reference to the last page - "this page follows page x". The reference he includes "chains" the pages together. He can easily arrange the pages if he ever drops them because each page references its predecessor.



\*Miners\* are the bookkeepers of a blockchain and we will explain their role in the [chapter on how a blockchain works](#). For now, all you need to know is that they are the ones creating new blocks.

The blockchain is simply a way to store information - just like lists and tables. Public blockchains come with powerful features that were not achievable before. It is impossible to change information after the fact. The information is immutable and highly secure. That is why blockchain is perfect for supporting digital money.

6

## A Protocol to Transfer Value

One of the great innovations of the blockchain boils down to it being a protocol to transfer value. Andreas Antonopoulos calls Bitcoin "a language to communicate value", which feels like a very accurate description.

## The Internet - A Protocol to Transfer Information

When many people want to cooperate there always needs to be a set of standards in place about how to cooperate exactly. This is the same whether they want to exchange information via the internet or cryptocurrency via the blockchain. The internet protocol - TCP/IP - defines standards for how data is split up and transferred from a server to your computer, e.g. when you access this website. A blockchain is defined by a protocol that determines how its participants exchange value.

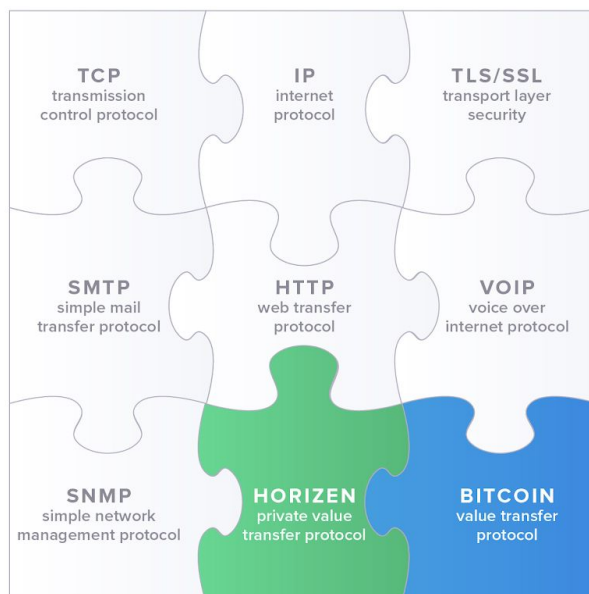
## The Mail - A "Protocol" to Transfer Physical Goods

A very simple analogy would be comparing blockchain to the mail - a "protocol" to transfer physical goods. Let's forget about the post as an entity actually operating the mail service for a minute and think about it this way:

The mail is permissionless in the sense that anybody who wants to send a letter to someone can find a postbox near them and drop the letter in there. It will arrive at its destination a few days later. You don't need to ask for anybody's permission to do so. The "protocol" for sending a letter comprises two things: you must put a stamp of sufficient value on it and you must provide the recipient's address. The standard address format is a name, address and the country if you want to send the letter abroad.

When you are sending some cryptocurrency, the decentralized network transfers your money to the recipient. The protocol requires you to add a small transaction fee - similar to a stamp - and provide the necessary information in a standardized way: the recipient's address, the amount to transfer and your *\*signature\**.





[Wallets](#) make it easy to receive and send transactions. They also create your signature for you, without you even noticing, so don't worry if this sounds complex at first. Addresses on a blockchain are of course a little different to addresses that you are used to - they look like this:

*znWPHuCGsgnJ5nsdu9AJdDcxDPWdrESoMNT.*

Signatures are also different from what you know. We will talk more about addresses and signatures in the next chapter on how a blockchain works.

## Summary

We can consider the mail to be a "protocol" to transfer physical goods and the internet with its underlying TCP/IP protocol as a protocol to transfer information. Blockchain technology and cryptocurrencies provide a protocol to transfer value - from one person to another, without any intermediaries. The protocol of a blockchain defines a set of standards. It determines what a block or transaction must look like to be considered valid.

# How Does a Blockchain Work?

After reading our first two articles about what a blockchain is, you know that in its most simple form it's a method to store data. This method of handling data allows you to transfer value without involving a central entity. We made the comparison of blockchain is a protocol to transfer value with the internet being a protocol that enables you to transfer information. We also compared blockchain to the post being a "protocol" to send physical goods.

In the first article, we want to discuss two important parties that play a part in a blockchain ecosystem: Miners and Nodes.

Next, we talk about where cryptography enters the scene and what this has to do with your identity. Without a concept of identity, there can't be ownership.

## The Elements of a Blockchain

The last chapter stated that on one hand, the blockchain is a data structure, a way to store information. On the other hand, it is a protocol to transfer value. We want to discuss the parties that play a part in the blockchain ecosystem in this article. Let's first talk about the term protocol again.

A protocol is a set of rules. These rules govern a blockchain and restrict what you can and cannot do. They also define standards for how participants communicate. There are rules on what order information must be provided in if you want to send a transaction. Luckily you don't have to know those rules - your [wallet](#) will take care of this. An example of another rule would be the following:

- If you try to spend the same Coin twice, the first transaction that spends it will be valid. The second transaction will be invalid.

Now that you know that a protocol, a term you will hear quite often, is just a set of rules let's take a look at the individuals that play a part in a blockchain ecosystem.

## Nodes

A network of computers - the *nodes* - run a blockchain. They are constantly exchanging information on new transactions and blocks. Nodes make up the infrastructure of the blockchain. A *\*full node\** is a node that maintains a copy of the blockchain. A *light node* does not keep a copy of the blockchain.

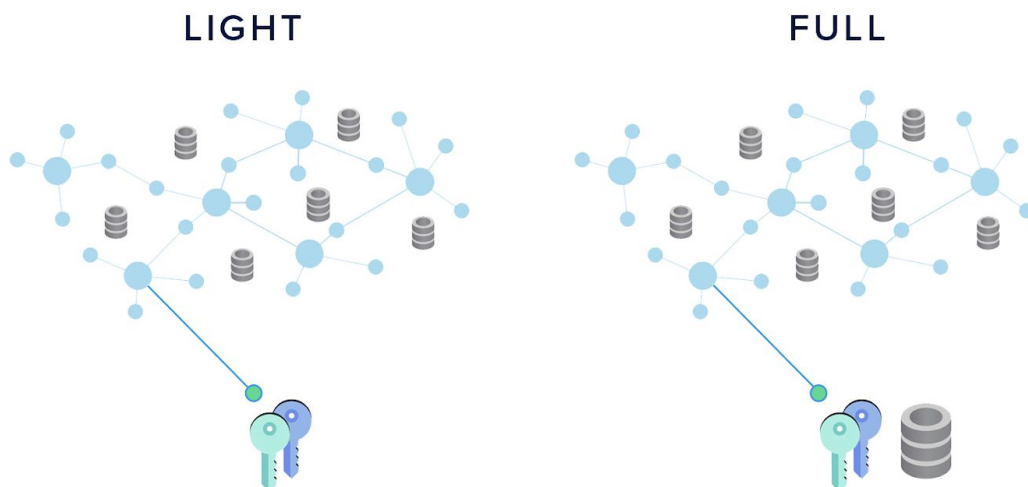
The light node must connect to a full node before it can interact with the blockchain, e.g. to send a transaction. You could compare the distributed network of a blockchain to the infrastructure supporting your mobile phone in this sense.

A *full node* is like a cell phone tower that your phone - the light node - is connecting to. All the antenna stations (full nodes) are connected to each other and make up the communication network infrastructure. If you want to make a call with your phone, you need to connect to a cell phone tower first, before you can interact with any other mobile phone.

Similarly, in the distributed network of a blockchain, the *full nodes* are up and running most of the time and make up the distributed network. They also maintain a copy of the entire blockchain. You are likely using a *light node* if you use a wallet on your phone or computer. In this case, you are going to connect to a *full node* first before you can actually interact with the blockchain.

You can run a full node if you want to contribute to the stability and security of your network, but to use cryptocurrencies you don't have to. Most wallets out there are light nodes, which means they store your keys but don't maintain a copy of the blockchain. With our flagship app [Sphere by Horizen](#), you can choose to run it as a full or light node.

HORIZEN ACADEMY

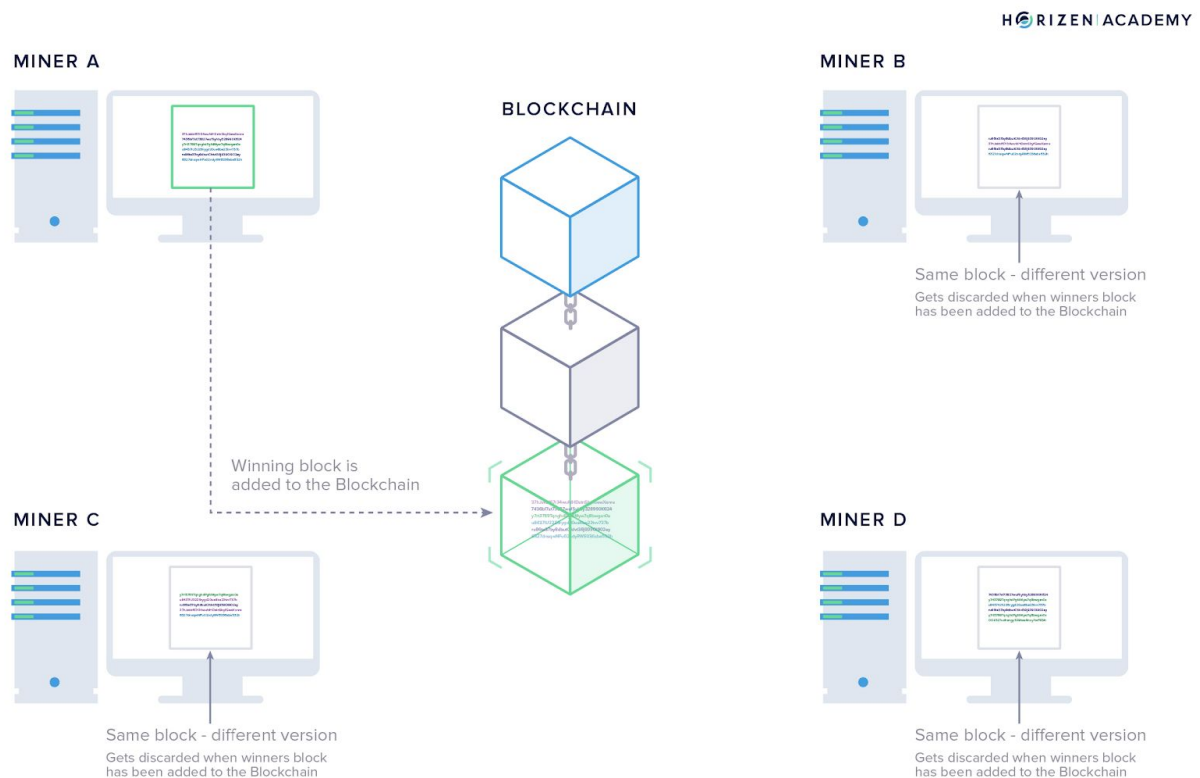


## Miners

Miners are nodes as well. They support the network by forwarding information and maintaining a copy of the blockchain, just like all the other nodes. Additionally, the miners are responsible for creating new blocks.

The purpose of miners for the network is the following: Each new block can be understood as a collective decision on the history of the last few minutes. The network comes to *consensus* on the order of transactions for that time period. For Horizen this time period is 2.5 min on average, for Bitcoin, it is 10 minutes.

Each miner has a slightly different block than the other miners. This is because it takes some time for a new transaction to spread across the entire network, and different miners might receive those transactions in a different order.



Miners have to solve a cryptographic puzzle to create a valid block. The miners start working on a new block - and therefore new puzzle - immediately after the previous block is added to the chain.

They gather all the transactions on the network that have not been included in a block yet and put them in their version of the next block.

The miner who solves the puzzle first gets to add the next block writes the history for the last few minutes. They broadcast their block to the network together with the solution they found for the puzzle. All nodes, no matter if they are mining or not verify if the solution to the puzzle is correct, and if it is they add the new block to their copy of the blockchain. Then the cycle starts all over again.

This is how the network comes to an agreement or *consensus* on what has happened in the past. If you wonder why we said it takes "around 2.5 min" to find a block, this is because it actually varies. All the miners start to solve the puzzle at the same time. The time it takes the miners to solve the puzzle depends on how difficult it is. If there are more people trying to solve the puzzle at the same time they will solve it faster on average.

The protocol increases the difficulty of the puzzle when new miners join the network. It will take the miners roughly 2.5 min again to solve the puzzle. This is another example of the protocol being a set of rules:

- If it takes less than 2.5 min on average to solve the puzzle, make it more difficult. If it takes longer, make it easier.

Miners run the equipment that helps to create consensus among all participants on the order of transactions. Imagine hundreds or thousands of miners in a conference room. None of the miners know each other and must discuss what happened at what time - it would be a disaster. The blockchain introduces a highly efficient way, to reach consensus. Miners propose different versions of the history of transactions. Then they vote on their version with their computing power. The first miner that solves the puzzle determines the version accepted by everybody in the network. Bitcoin actually introduced the first protocol in human history, that could come to consensus in a trustless and distributed environment.

## But Why Are Miners Doing This?

Miners are rewarded when they solve the puzzle first. This creates an incentive for individuals to purchase and run the hardware needed to solve the cryptographic puzzle. The first miner to solve a block receives a reward in the currency that she is mining. She is allowed to send herself a

transaction with a few coins that didn't exist before. It is another example of a rule in a blockchain protocol:

- The miner that solves a block is allowed to include a transaction in his block sending himself some newly created coins.

## Summary

In conclusion, miners and node operators are the two main entities in a blockchain. The nodes make up the infrastructure of the network. Miners are the bookkeepers that make the decisions regarding the order of events.

For performing the valuable task of creating consensus among all network participants miners receive a reward. This reward generates new coins. Every ZEN out there started out as the block reward for some miner.

The next article is going to tackle the question of how [identity works in the context of the blockchain](#). If there is no concept of identity, there cannot be ownership - and wouldn't it be great to be able to own your cryptocurrency when you buy it?

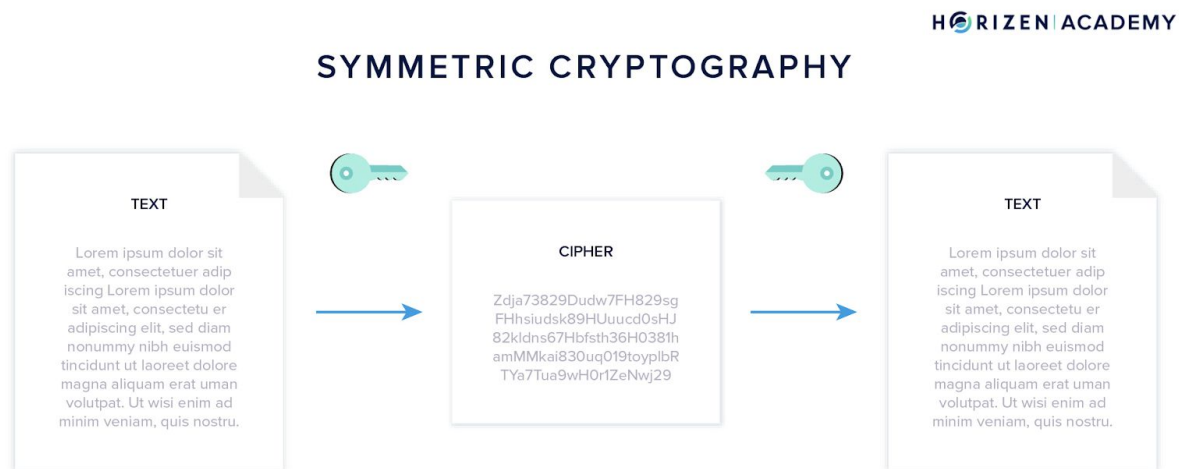
## Identity in Blockchain

In our last article, we talked about the main entities of a blockchain. We concluded that nodes make up the infrastructure of a blockchain and that miners are the bookkeepers of a cryptocurrency. They keep track of how much funds there are and who owns them. We must have a concept of identity to have ownership. You want to be the sole owner of your funds and there must be a way to associate the funds with you. This is where cryptography enters the scene.

## Public-Key Cryptography

One of the core concepts that make blockchains work is the concept of *asymmetric cryptography* also known as *public-key cryptography*.

With symmetric cryptography, you encrypt and decrypt a message using the same key (like a padlock).



With asymmetric cryptography, you encrypt and decrypt a message using two different keys, the public key, and the private key. The keys always come in pairs. If you encrypt a message with a public key it must be decrypted with the corresponding private key and vice versa. This boils down to a simple concept: Your key pair is your identity on the blockchain.

## ASYMMETRIC CRYPTOGRAPHY



### Your Key Pair is Your Identity

The idea in cryptocurrencies is that you are receiving funds with your public key and spending them with your private key. A private key on the Horizen blockchain could look like this

Kz6994Ek9L3uzjQo2wANaHguBbEShoHZo6q1Y3r6rXrHfWka1fnx

and the corresponding public key or address like this

znSrHR9ssjKMSrYfk5fTmKH4LbgDxXJ3s6j.

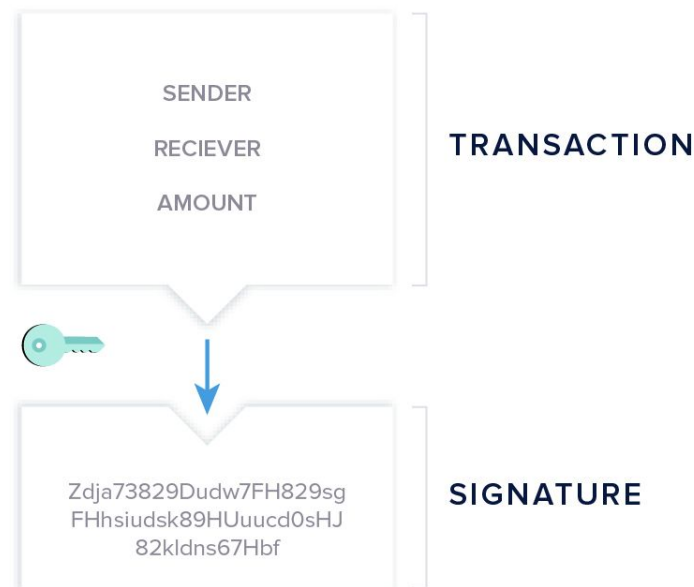
The keys were intentionally named public and private key. You can share your public key with anybody that wants to send you money. Your private key, as the name suggests, should remain private under all circumstances, because it allows you to spend your money. If somebody gets their hands on your private key, they can access and steal your funds.

The real-life comparison you will hear most often is your public key being like your address. You can give it to anybody that wants to send you a letter. Your private key is like the key to your postbox. Only this key lets you access your mail and you wouldn't hand it to a stranger. If you want to learn about this concept in more detail, you will find a more in-depth explanation [in the Advanced Level](#) and an exact description in the Expert Level.



Your keys are important for sending and receiving transactions. Technically, a transaction is a message to all nodes on the network. This message includes how much of your money you want to send, and to whom. This information is then encrypted with your private key, a step we call *signing a transaction*.

## SIGNING



A digital signature works similar to how you authorize real-life transactions using your "analog" signature. Even with modern supercomputers, it is infeasible to forge such a digital signature. The type of public-key cryptography used in blockchains is one of the safest means of encryption available today.

All of this would be cumbersome to do manually and require quite some skill. Luckily there are wallets that help you do all the above. Wallets generate and manage your keys and take care of all the necessary encryption and decryption. What is important, is to understand that your private key authorizes the spending of your funds. Keeping it safe is the first and most important lesson. Nobody can help you recover your keys in case you lose them. If somebody was able to recover it for you, they would also be able to take your money at will.

## Summary

Your key pair is your identity on the blockchain. Your public key serves as your address and is used to receive funds. Your private key is like a password - it lets you (or anybody that gets their hands on it) spend your money. Always protect your private keys and never hand them out to other parties! If anybody asks you for your private key it is most certainly a scam!

# Wallets

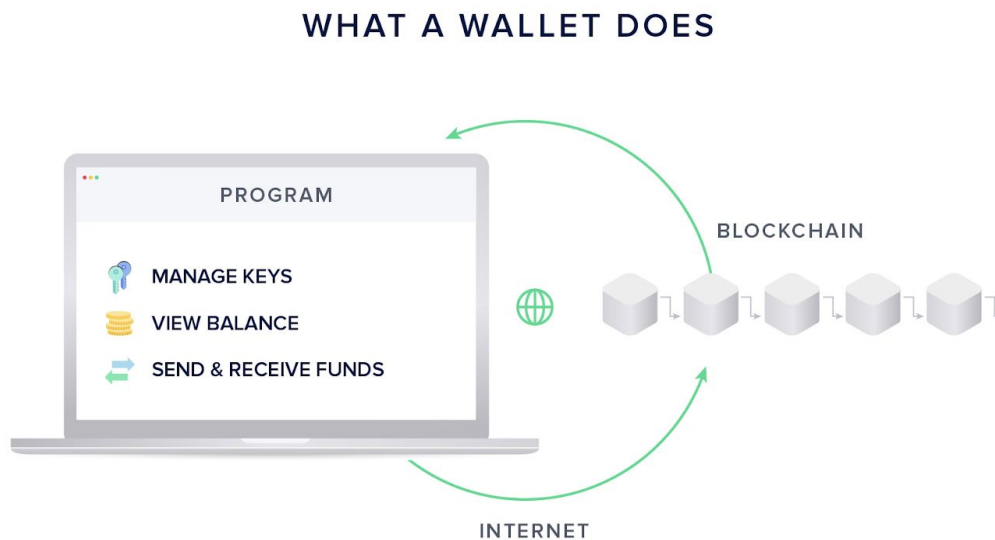
Sometimes there is a little confusion about what a wallet can and cannot do, so we will start with what it can't. Wallets generally don't allow you to buy cryptocurrencies, that is what [exchanges](#) are for. All exchanges provide you with wallets to store your coins in after you buy them, but wallets usually don't provide you with an exchange service.

## What a Wallet Does

A wallet is a program that has three main functions:

- Generating, storing and handling your keys and addresses
- Showing you your balance
- Creating and signing transactions to send funds

HORIZEN ACADEMY



Piece of software that helps you with  
interacting with Blockchain

The first function is the main function and main differentiator of all wallets: generating, storing and handling your keys. As we said in the last article about identity in blockchain, having access to your private keys means to be able to spend your money.

Where you store your keys determines the safety of your funds and at the same time the convenience of using them. With wallets there is usually a trade-off between safety and convenience: Having some funds on your mobile wallet (your smartphone) makes them easy to spend, but not very secure. Keeping larger amounts of money on a hardware wallet is very secure, but not as convenient when you want to spend it. In the Advanced Level, we explain the different [types of wallets](#) out there.

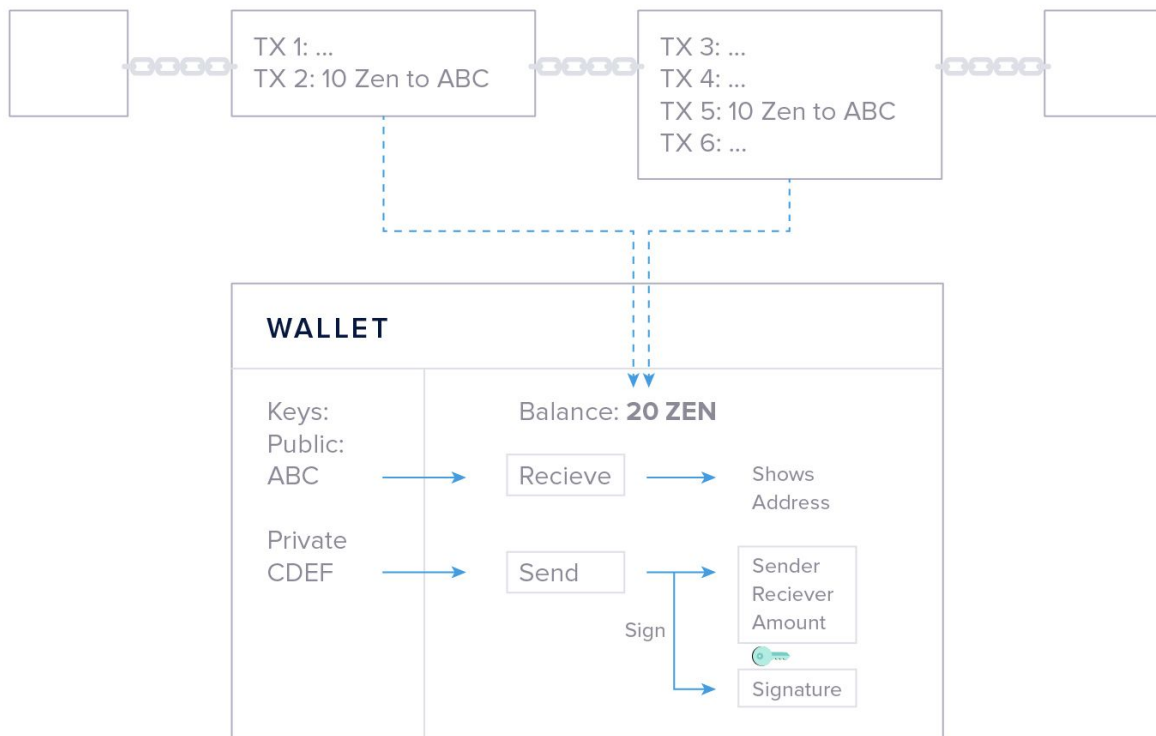
## A Wallet Acts as a Keychain

We would like to introduce an abstraction, that might help you wrap your head around the concept of your keys and the importance of their safety.

Although the term wallet might be more intuitive, the function of a wallet is closer to that of a keychain rather than an actual wallet. To make it crystal clear:

**You don't actually store any cryptocurrency in your wallet. You just store the keys to access them on the blockchain.**

The blockchain records the amount of coins associated with a key pair (your identity on the blockchain). It calculates the amount of money the keys have access to based on all the transactions on the blockchain. Remember: the main function of a blockchain is to store all transactions in the correct order. Say you receive 10 ZEN in a first transaction and receive another 10 ZEN later on. It is clear that you, the owner of the key pair, owns 20 ZEN.



To spend your money you need the private key stored in your wallet. This is why a keychain feels like a good analogy for what a wallet does. If you don't control your keys, you don't control your funds. You don't need to understand how public-key cryptography works in detail in order to use cryptocurrencies but the concept of your keys giving you access to your funds is still important to remember.

Wallets create a layer of abstraction and are becoming more and more user-friendly. Wallets show you your balance, generate an address to receive funds by just clicking "deposit" or "receive", and provide you with a simple interface to send funds. All you need to do is enter the address that you would like to send money to and the amount you want to transfer. The signing procedure using your private key will happen in the background when you click send.

## What If I Lose My Keys?

You don't have to ask anybody to join the network and you don't have to register with a central authority to create a wallet. Being able to do this comes at the cost of you being responsible for the safety of your coins. There is nobody that can help you recover your keys if you lose them. If

anybody was able to recover your keys for you, they would also be able to steal your funds. This would eliminate the trustless aspect of blockchains.

You may have heard stories about people searching for old hard drives because they have "lost their bitcoins". More accurately, they lost the keys to access their bitcoin.

But there is a sort of recovery mechanism with many wallets called a mnemonic phrase or backup phrase. A mnemonic phrase usually consists of 12 or 24 words. With these words, you can recover your keys. You receive your mnemonic phrase when you install and set up your wallet. Be sure to write it down on a piece of paper and keep it in a safe place. You should have at least two versions of your backup phrase stored in different locations.

It's essential to understand that your backup phrase is just as important as your private key itself. If anybody gets their hands on your backup phrase, they can access your money. Saving it as a screenshot or text file on your computer is not a good idea!

## Summary

A wallet is a program that helps you manage your keys and create transactions easily. Your wallet looks at the blockchain to determine how much money you own by reviewing the transaction history. To send funds it writes a transaction and signs it, meaning the wallet encrypts it with your private key.

Try our wallet, [Sphere by Horizen](#) to become more comfortable with the concepts we covered in this article. To do a test transaction you can visit our [Faucet](#) where you will get a small amount of free ZEN! You can use it to receive and send your first cryptocurrency transactions without having to buy some coins first.

Simply install Sphere by Horizen, create a wallet (and save your Recovery Phrase on a piece of paper), provide your address to the Faucet and soon you will have your first ZEN to play around with!

You can visit our Advanced Level for an overview of the [different types of wallets](#).

# Transactions

If you have read our prior articles than you already know more about blockchain than most people. We talked about what blockchain is, how it works, and what cryptocurrency wallets do. You know that wallets are programs, that help you create transactions and receive money. In this chapter, we will introduce you to what these transactions look like and how you can take a look at them.

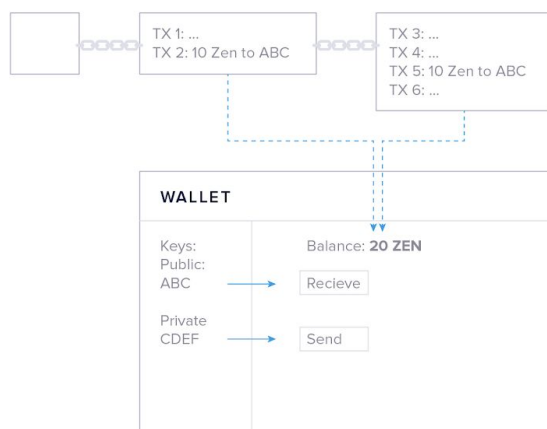
The first article gives you a good analogy to keep in mind when thinking about what a cryptocurrency transaction is and how it works.

The second article introduces the block explorer. A block explorer is a tool that lets you browse the information on a blockchain, just like the internet explorer lets you access the information on the internet.

## Intro to Transactions

Digital money would be pretty useless if there was no way to send it from one person to another. In this article, we want to show you how transactions work and what your keys are used for.

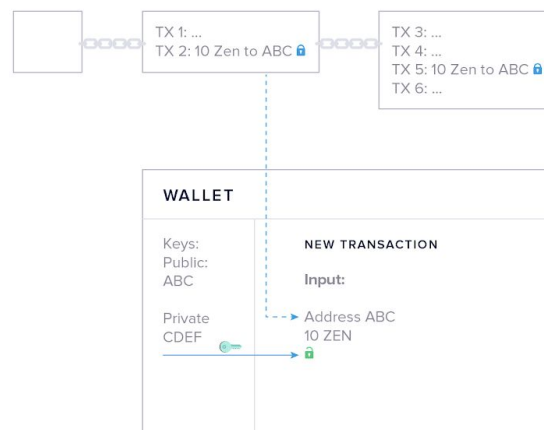
In the very first article of the Technology Section, we said that the blockchain is a public ledger that keeps track of all the transactions that ever happened on the network. In the last article, we stated that a wallet is an app that helps you with managing your keys and creating transactions.



HORIZEN ACADEMY

A wallet gets your balance from monitoring the blockchain for any transactions that involve your address. Initially, all transactions are cryptographically locked. The lock is based on the address the transaction is sent to, and can only be unlocked with the corresponding private key.

Now let's assume this is your wallet. You received a total of 20 ZEN in two different transactions of 10 ZEN each. Now you want to spend 2 ZEN at lunch. Your wallet starts with a blank transaction and in a first step chooses one of your prior transactions to spend. In this case, both transactions are of sufficient value so your wallet might randomly choose the first one.

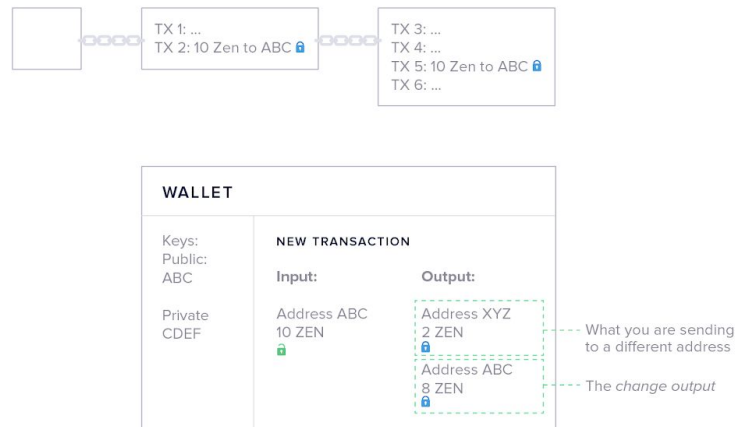


HORIZEN ACADEMY

The money that is being spent in a transaction is called the *input* and the money that is being received is called the *output*.

Your wallet places one of the outputs you own in the empty transaction and uses your private key to unlock it so it becomes spendable - this is what we called *signing* the transaction. The unlocked output is now used as an input to a new transaction.

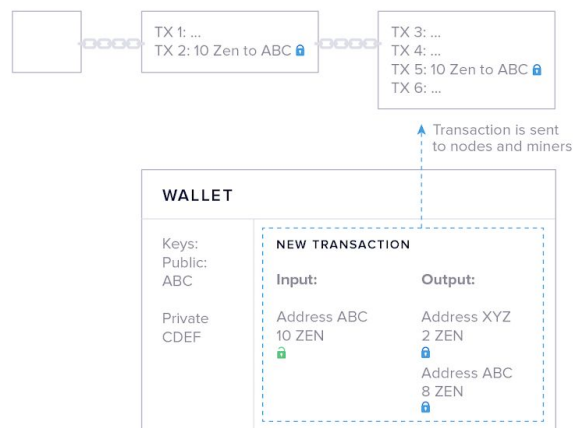




Next, your wallet creates the *outputs*. It asks you for an address to send money to and an amount. You want to send 2 ZEN to address XYZ to pay for your lunch, so your wallet creates the first output accordingly.

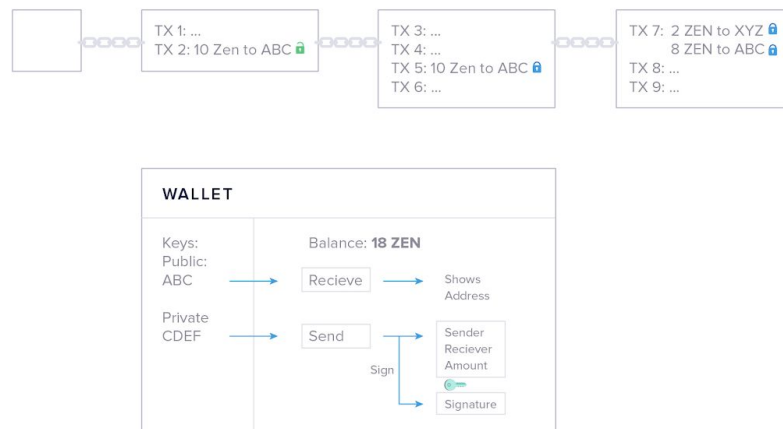
The second output is generated automatically - its called the *change output*.

Outputs are similar to cash denominations. If you need to pay \$2 USD but only have a \$10 bill, you expect to get \$8 in change. Your wallet automatically includes the change in the transaction. The newly generated outputs are locked by default.



Lastly, your wallet broadcasts the transaction to the network, where all nodes and miners will verify if the signature you used to unlock your money is valid. If it is, miners will include your transaction in the next block. The output of 10 ZEN you used is from now on publicly visible as *spent*. The to newly created outputs of 2 and 8 ZEN are included in a new block and locked - or *unspent*.

Then you come across the term *UTXO* - Unspent Transaction Output - this is what it refers to.



When you own 10 ZEN, it means you received 10 ZEN in a transaction and you have not unlocked and spent that output, yet.

## Summary

A *transaction* is a single entry in the blockchain. To receive a transaction you need to provide your *address* to the sender. A cryptographic lock is automatically placed on every *transaction output*. To spend your money - the output of a transaction - your *wallet* uses your *private key* to unlock the output and uses it as an *input* to the new transaction. The outputs to your transaction are generated by your wallet based on the address and amount to transfer you provide. Once the transaction is sent to the network, verified and included in the next block the output you used up is publicly marked as *spent*.

# Intro to the Block Explorer

An often-cited benefit of blockchain technology is the transparency it offers. Transactions, blocks, and addresses are publicly auditable and the tool you use for that job is called the block explorer.

A block explorer lets you browse the blockchain, like how a web browser lets you access the information on the internet. You can review the transaction history of a given address, the set of transactions in a block as well as the status of transactions. Let's take a look at a real-life example:

## Address 42.0002 zen


Address znf7vPwiAAFFoDikV5DU

Bobs Address

Summary

confirmed

Total Received	42.0002 zen
Total Sent	0 zen
Final Balance	42.0002 zen
No. Transactions	1



This is what you can expect when you are searching for an address with a block explorer. Block explorers usually work the same, no matter what blockchain you are looking at. The address that was looked up for this example on a Horizen block explorer is at the top: znf7... Let's say this is Bob's address.

On the top of the page, you will find a summary of the addresses activity. The information provided here will include the total amount received and sent from this address, as well as the current balance. The address we are looking at received a total of 42 ZEN. Bob didn't send any ZEN to other addresses yet and therefore still has a balance of 42 ZEN.

## Transactions

Transaction ID

a46f51cf4d9a4af98587101c2376bdb8c5f919ba4f88152d1

mined Sep 1, 2018 8:17:39 AM

No JoinSplits

1 Input

znd3nr1pqXnfJryA3A2o4 Alice' Address 46.66798506 zen

2 Outputs

znf7vPwiAAFFoDikV5DU Bobs Address 42.0002 zen (U)

znd3nr1pqXnfJryA3A2o4i Alice' Address 4.66768506 zen (U)

FEE: 0.0001 ZEN

5427 CONFIRMATIONS

46.66788506 ZEN

You will find all the transactions that this address was involved in below the address summary. This particular address was only part of a single transaction thus far. Every transaction is characterized by its identifier - the transaction ID - which is the blue string at the top of the grey box. The transaction we are looking at had one input (left) and two outputs (right). The input is what is sent, and the output(s) is what is received. If inputs and outputs are new to you, you can find out about them in our last article explaining transactions.

Let's say Bob received his funds from Alice. Alice's address is next to the input on the left, znd3... Alice had an output of 46.6 ZEN in her address, but only wanted to send 42 to Bob. Alice did this by using her entire balance of 46.6 ZEN as an input (left) and creating two outputs: one output of 42 ZEN she wanted to send to Bob, and one with the remaining 4.6 ZEN going back to her own address as change.

We will take an in-depth look at inputs and outputs in the Advanced Level with a dedicated article about the [UTXO model](#) (Unspent Transaction Output model).

Now there are three pieces of information left uncommented:

- The sender added a transaction fee of 0.0001 ZEN. Transaction fees are a measure to prevent spam. When sending only a few transactions the fee is negligible. If you were to send large amounts of spam transactions though, the cost would quickly add up and become prohibitive.
- The number of confirmations is a measure of how old a transaction is. Every block that is created after a transaction is included in the blockchain is called a confirmation of that transaction.
- There is the total volume of the transaction.

We encourage you to go to our [block explorer](<https://explorer.zen-solutions.io/>) and start playing around with it yourself. The landing page will show you the latest blocks in real-time. If you do not have an address yet, that you can use as a starting point to explore the blockchain, you can pick a recent block, choose a transaction and take it from there.

## Summary

The block explorer does for the blockchain what a web browser does for the internet - it lets you access the data. The things you are likely to look up in a block explorer are your addresses and your transactions. Additionally, you can open entire blocks and see all transactions contained.

When you send a transaction to a merchant or exchange and don't get a notification right away about them receiving your funds, it can feel a bit scary. By using the block explorer to look up your transaction you can verify that it is on its way and everything worked out.

# Privacy on the Blockchain

It is a common misconception that Bitcoin and other cryptocurrencies are an anonymous means of payment. In fact, they are anything but. The blockchain is a public, fully transparent ledger. Anybody can browse the data of a blockchain using a block explorer and see which addresses transferred how much money at what time.

While this generally holds true for most blockchains, there are several ways to achieve financial privacy - even on a fully transparent ledger.

To transact privately, there can't be any information about the sender and receiver of a transaction. You need an address to transact on a blockchain. Because this address doesn't carry any information about their owner we say they are pseudonymous. Your address acts like a pseudonym, similar to how you pick a username in a forum.

Through increasingly more powerful data analysis, it is possible to link real-world identities to cryptocurrency addresses. The more transactions you have received and send, the more metadata there is. This metadata can include the IP address a transaction originated from or frequent transaction partners. Exchanges also log the addresses you use to withdraw funds and can thereby link your addresses to your identity.

## Why Privacy

There are many legitimate reasons to create private financial transactions. If you have a medical condition and need to purchase your prescriptions on a regular basis you have good reason to conduct these transactions privately. If you have a business, you don't want to reveal your revenue streams to your competition and if you are buying a present for your spouse, you might not want him or her to see it before they actually get the present. There are many good reasons to transact privately, and we believe that privacy is and should be treated as a basic human right.

In our privacy section, we take a close look at the ["I've got nothing to hide"](#) argument.

## How to Reclaim Your Privacy

The first step towards increased privacy is the use of a new address for every transaction you receive. Most wallets will automatically generate a new address for you every time you click

"receive". This makes it significantly harder for an adversary to group your payments and ultimately link them to your identity.

If you wish to transact with absolute privacy, you should use a cryptocurrency providing special privacy features. Horizen offers one of the strongest privacy tools possible - Zero-Knowledge Proofs.

A Zero-Knowledge Proof lets you prove to a verifier that you know something, without revealing that knowledge. When you create a private transaction you generate a proof that you show to the nodes and miners instead of sending them the actual transaction data.

An intuitive, non-digital example of what this might look like can be constructed with a seeing person as the prover, a blindfolded person as the verifier and two balls of different color.

The seeing person (prover) wants to convince the blind person (verifier) that the two balls are of different colors, without actually revealing the colors.

They sit down at a table and the blind person shows the prover one of the balls. The blind person continues to put both balls under the table and chooses to show one ball in a second round - either the same one as before or the other one. If he chooses to show the same ball, the prover knows because he sees the same color and he tells the blind person. If the blind person were to switch them under the table and show the other ball, the prover could tell with certainty that the verifier (blind person) switched the balls.

HORIZEN ACADEMY

## ZERO KNOWLEDGE PROOFS



In the second round, the prover would have a fifty-fifty chance of getting the right answer if he had to guess. He would have to guess in case the claim that he is trying to prove (the balls are of a different color) was false. At this point, the blind person cannot be sure if the claim is correct, or if the prover got lucky.

If they repeat the game several times, the chance of getting the answer right every time through guessing decreases exponentially. After just ten rounds of the game, the chance of calling the right ball every time through pure luck has decreased to 0.1%. The blind person can be pretty sure the two balls are really of different colors although the prover has not shared any information about the colors themselves.

The idea of using Zero-Knowledge Proofs for cryptocurrency transactions is the following: You construct a proof that the transaction you want to send would be considered valid by a verifying node, without revealing any of the actual transaction data. This allows the sender, receiver as well as the amount to be kept private. Another use-case that is perfect for the application of zk-Proofs is identity verification. You can, for example, prove to an entity that you are of a certain age without revealing any personal data like your date of birth.

To use private transactions with Horizen, you will use a different address type. In your wallet, you can either generate t-Addresses (transparent addresses) or z-Addresses (shielded addresses). When you sent funds to a z-Address, the amount and sender are recorded on the blockchain, but not the receiving address. If you forward the funds to a second z-Address no information about the transaction gets publicly recorded. You can try this feature with our flagship app [Sphere by Horizen](#). Make sure to activate full mode in the settings, otherwise, you won't be able to generate z-Addresses.

## Summary

While cryptocurrencies are not anonymous by default, some of them offer features that allow you to transact privately. To increase the level of privacy, you should use different addresses for every incoming transaction. This makes it harder for an adversary to track your transaction history. Most wallets will do this automatically for you.

You can also use cryptocurrencies with enhanced privacy features, like Horizen, to transact completely private.

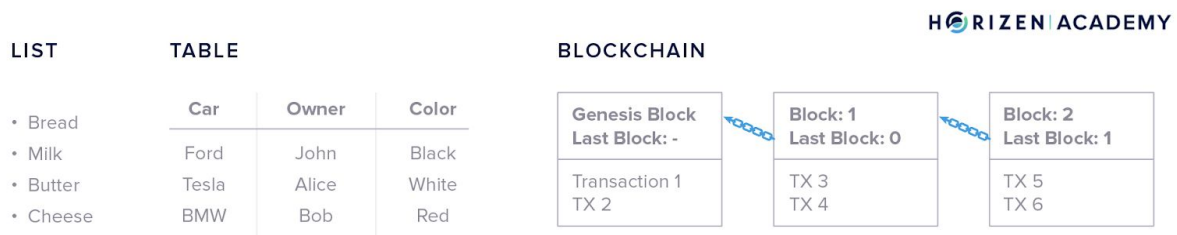


# Blockchain Technology Summary

This is the last article of our technology series for beginners. We hope that the previous articles have helped you understand what a blockchain is, how it works, and how to use it. Here we would like to summarize what we have covered in the Technology Section for Beginners.

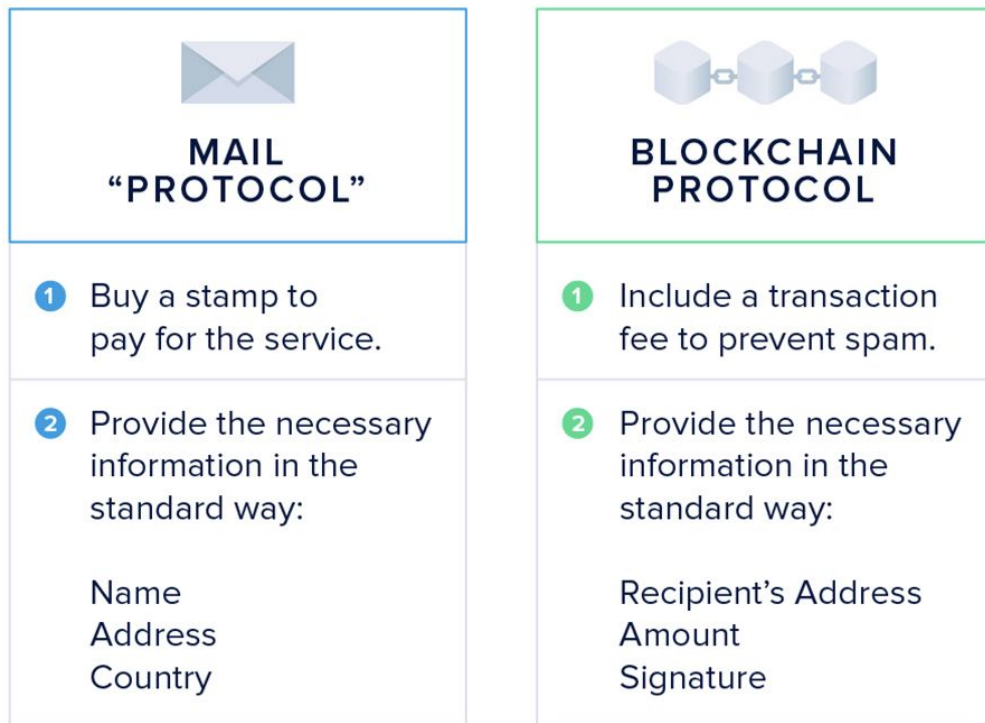
## A Data Structure

A blockchain is a method to store data just like you store information in lists and tables. The special method of handling data allows you to transfer value without involving a central entity.



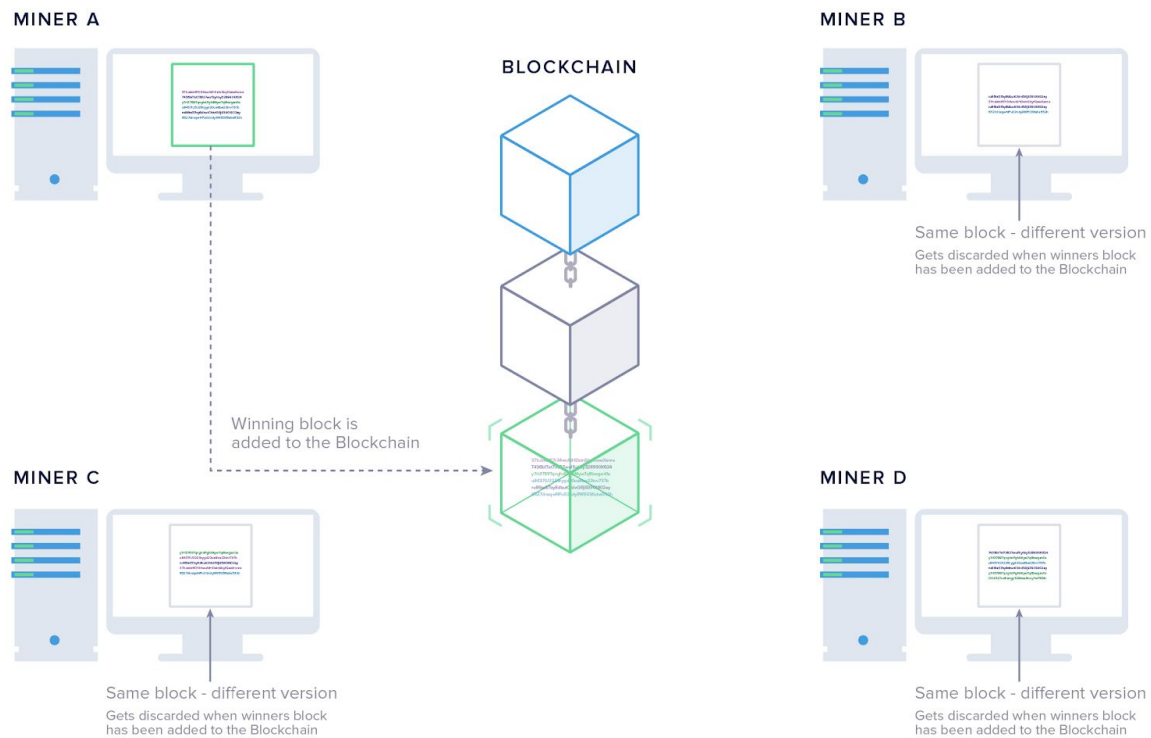
## A Protocol to Transfer Value

We made the comparison of blockchain being a protocol to transfer value with the internet being a protocol that enables you to transfer information. We also compared blockchain to the post being a "protocol" to send physical goods. A protocol is just a set of rules and standards which are defined, so all participants can communicate and collaborate efficiently. The protocol is run on a large number of computers all around the world. Because the data on a blockchain is very secure and all the nodes communicate in a predefined way no middlemen are needed to ensure safe transactions with digital currencies.

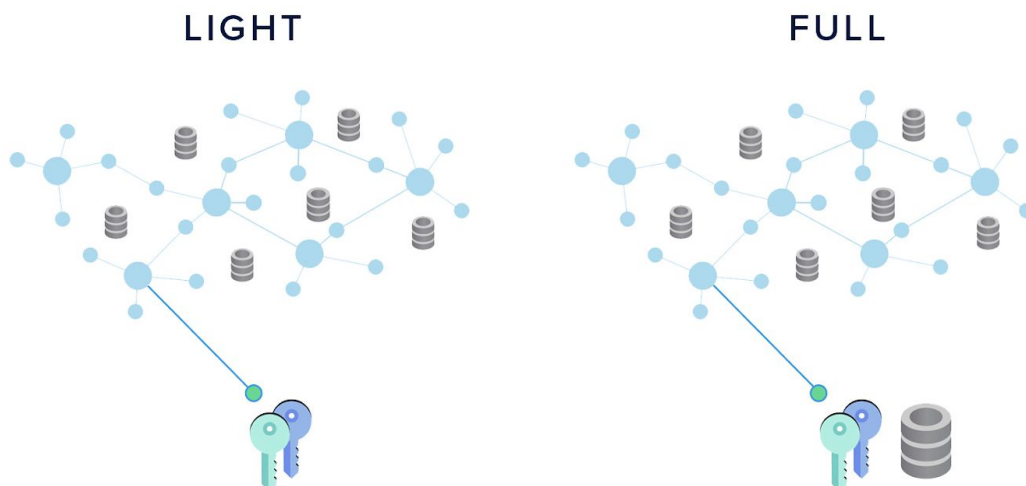


## The Elements of a Blockchain

Miners are the bookkeepers of a blockchain. They collectively make decisions on what happened in the past, allowing the network to reach consensus on the current state. Miners require special hardware and electricity to solve a computationally hard puzzle. The miners are in a competition to find the next block the fastest. In turn, they receive newly created coins if they finish the task first. This is how a decentralized cryptocurrency protocol can pay for its own maintenance.



The nodes make up the infrastructure of the network itself. Full nodes maintain a copy of the blockchain and verify all the transactions and blocks on the network. Light Nodes only store a pair of keys. Most mobile and desktop wallets are light nodes.



## Identity on the Blockchain

Your public key is like your address on the blockchain and your private key is the password to access your address and the money within. You use your public key to receive money and your private key to authorize spending your money. As a pair, they represent your identity on a blockchain. The key pairs are part of an encryption scheme called public-key cryptography or asymmetric cryptography, which is one of the main pillars of blockchain technology.

HORIZEN ACADEMY

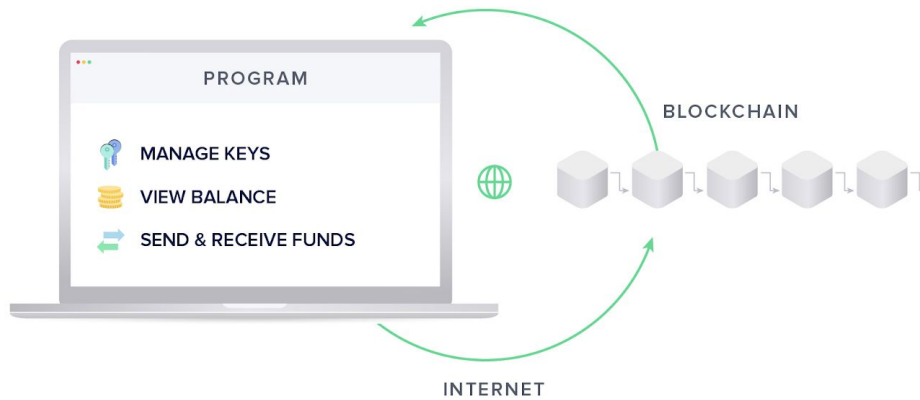
### ASYMMETRIC CRYPTOGRAPHY



## Wallets

Wallets are apps that generate and manage keys for you, show you your balance by finding all the transactions you received on the blockchain, and help create new transactions.

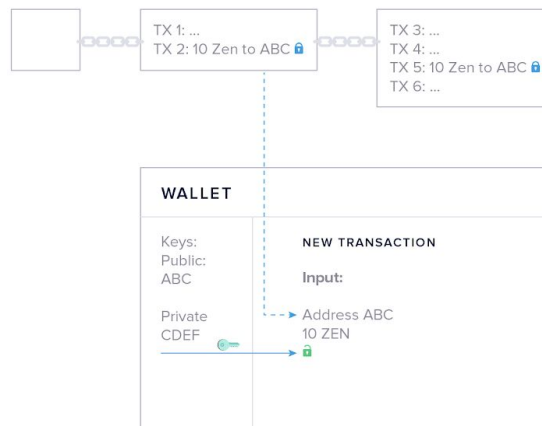
## WHAT A WALLET DOES



Piece of software that helps you with  
interacting with Blockchain

## Transactions

A transaction is a message to the network informing all participants that some money has changed hands. If you want to send a transaction you must unlock your money with your private key first. Then you what address(es) will receive how much of your money. The transaction is basically a message saying "Alice sent Bob 10 ZEN". This statement is what represents Bob's coins.



## The Block Explorer

To access the information stored on a blockchain you use a block explorer. Like how a web browser lets you access information on the internet, the block explorer lets you access information on the blockchain. You can look up addresses, transactions, or entire blocks.

### Address 42.0002 zen

Address znF7vPwiAAFFoDikV5DU

Bobs Address

### Summary confirmed

Total Received	42.0002 zen
Total Sent	0 zen
Final Balance	42.0002 zen
No. Transactions	1



## Privacy on the Blockchain

While cryptocurrencies are not anonymous by default, some of them offer features that allow you to transact privately. To increase the level of privacy, you should use different addresses for every incoming transaction. This makes it harder for an adversary to track your transaction history. Most wallets will do this automatically for you. You can use cryptocurrencies with enhanced privacy features, like Horizen that offers Zero-Knowledge Proofs, to transact completely private. By using a different address type (z-Addresses) within the same wallet your transactions become private.

HORIZEN ACADEMY

## ZERO KNOWLEDGE PROOFS



# Final Remarks

Cryptocurrencies and blockchain are not an easy topic. In this line of articles, we were trying to explain it in intuitive ways without sacrificing too much accuracy. It takes a while to understand blockchain technology - there is no way around it. I read many articles multiple times until they clicked with me. You can always come back to re-read these articles. It will make a lot more sense reading it a second time with a little break in between.

If you feel comfortable about everything you have just read and would like to keep learning: there is more! Move up one level and see our [Advanced articles](#). We have structured them the same way we did in the Beginner Level, but added more detail to all topics and split some of them up to look at the individual concepts more closely.

We designed the content in a way where you can either read it from top to bottom (which we can only recommend) or jump to articles that you are especially interested in.

We hope you enjoyed this series of articles. Please let us know if there is anything that you find confusing. The content provided is and will be work in progress for a while. We are always open to suggestions and constructive feedback so [drop us a message](#) if you want to share your thoughts with us.

**Your Horizon Team**



**HORIZEN**

**ACADEMY**

[academy.horizen.global](https://academy.horizen.global)