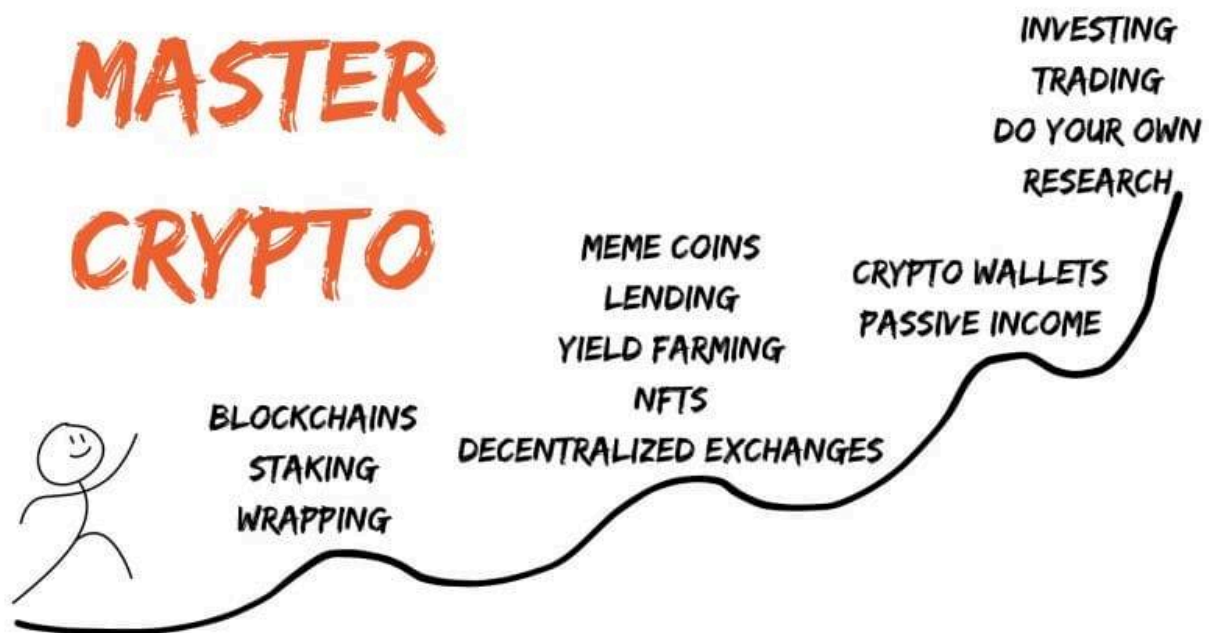


Cryptocurrency for Beginners

This guide is a collection of the introductory articles on ElementalCrypto.com. After reading them you will have a very good sense of what crypto is about.



This PDF cover two fundamental coins which form the core of all cryptocurrencies. If you understand these you have a very good overview of how cryptocurrencies work.

If you prefer you can read the articles directly on my site

- [What is a Bitcoin](#)
- [What is Ethereum](#)

Cryptocurrency for Beginners	1
What Is a Bitcoin and How Does It Work? A Beginner's Guide	4
The three facets to understanding Bitcoin	5
What is Bitcoin?	6
1. Bitcoin, the currency	6
Bitcoin compared to gold	7
Properties that make bitcoin good money	9
Why we don't use bitcoin for groceries	11
#1. You can't price stuff with it	11
#2. It's volatile	12
#3. It's slow	13
#4. It's not an official currency	13
2. Bitcoin, the network	14
How Bitcoin came about	14
The idea for bitcoin is born	15
How does Bitcoin manage without a central intermediary?	18
Private keys and public keys	20
Elliptic curves and public keys	21
How bitcoin uses public addresses instead of names	24
Signatures	26
Wallets and how messages are sent	29
How do messages get propagated?	31
The best way to understand public addresses and private keys	33
#1. Can one person have more than one address?	35
#2. Can an address have more than one person's money?	35
3. Can people see how much money you have?	36
How blocks are stitched together	36
How SHA-256 works	37
SHA-256 examples	38
Connecting data using SHA-256	40
What's a blockchain?	44
Bitcoin Mining explained	45
Incentives and who gets to add the new block	45
Nonces	46
How miners solve the puzzle	48
Proof of work	50
Game-theory-based security model	50
What is a Mempool?	51
How do miners bundle transactions?	52
What happens if two miners solve the puzzle at the same time?	53
What is a coinbase transaction?	55

How do payments work on the Bitcoin network?	55
How an input becomes an output	56
Combining multiple inputs to an output	58
How long do transactions take?	60
Is it possible to change the transaction history?	61
Wait what if I want a cup of coffee? Do I have to wait ten minutes?	61
Isn't Bitcoin slow?	62
What are mining pools?	62
Where do I get bitcoin?	63
1. Cryptocurrency exchanges.	63
2. Bitcoin ATMs	63
3. P2P networks	63
4. In a back alley	64
Who created Bitcoin?	64
The big picture	65
Article Resources	66
What Is Ethereum and How Does It Work? A Beginner's Guide	67
What Is Ethereum and How Does It Work?	68
First: what are smart contracts?	68
Let's see how this loan example would play out.	70
Back to what Ethereum is	71
Ether vs. Ethereum: what's the difference?	72
A small primer on validators	73
Ethereum market cap	73
Token issuance	75
Initial Coin Offerings	75
Why people overreacted to ICOs	76
How the Ethereum consensus algorithm works	77
Proof-of-Work vs. Proof-of-Stake	78
You can participate in Staking	79
Layer 1 vs Layer 2	79
EIP-1559 and its Significance for Ethereum	81
Why is it called Ether / Ethereum?	82
Why do some people think Ether is a shitcoin?	82
What is Ethereum Classic?	83
Forking	84
Back to Ethereum Classic	85
TheDAO Hack	86
Who are the founders and creators of Ethereum?	87
Summary of the rest of the founders.	88
Ethereum ecosystem projects and copycats	89

What Is a Bitcoin and How Does It Work? A Beginner's Guide

In this post, I will explain what a bitcoin is and how it works in as simple a language as possible. I will help you understand how Bitcoin works conceptually without dragging you through complicated maths and terminology. However, I am going to go into detail.

After reading this post you will have an excellent understanding of the mechanics of how the Bitcoin Network and blockchain work and what makes bitcoin, the currency, so special.

Before you move on I ask for one commitment from you: **that you concentrate**. Understanding how Bitcoin works is not easy if you aren't mentally prepared to take it seriously. So I ask you to carry the same attitude to studying for a class. From my side, I pledge to break down the concepts in as simple language as possible.

Table of Contents

1. The three facets to understanding Bitcoin
2. What is Bitcoin?
3. 1. Bitcoin, the currency
4. 2. Bitcoin, the network
5. How blocks are stitched together

6. [What's a blockchain?](#)
7. [Bitcoin Mining explained](#)
8. [How do payments work on the Bitcoin network?](#)
9. [How long do transactions take?](#)
10. [Is it possible to change the transaction history?](#)
11. [Isn't Bitcoin slow?](#)
12. [What are mining pools?](#)
13. [Where do I get bitcoin?](#)
14. [Who created Bitcoin?](#)
15. [The big picture](#)
16. [Article Resources](#)
17. [Up Next](#)

The three facets to understanding Bitcoin

There are **three aspects to Bitcoin** that will both confuse and fascinate you at the same time:

1. The first is **the code itself**. If you are not a coder then this can be scary ground. However, it's not as scary as you think. I am not a coder myself but I have spent a lot of time learning the mechanics of how the code works.
2. The second is **economics**. Suddenly you'll be forced to ask yourself difficult questions like what is money anyway?
3. The third is **political and ideological**. Should a digital currency without a central intermediary be allowed to exist? What are the repercussions of a government not being able to control the printing of new money? Some believe this is the beginning of the end for nation-states. If you're curious about that last statement read the [Sovereign Individual](#).

As I walk you through Bitcoin these facets will come up and distract you as they send you down different thought processes. Your job is to keep your focus throughout.

Let's start with the easy stuff.

What is Bitcoin?

Bitcoin is two things: a currency and a network.

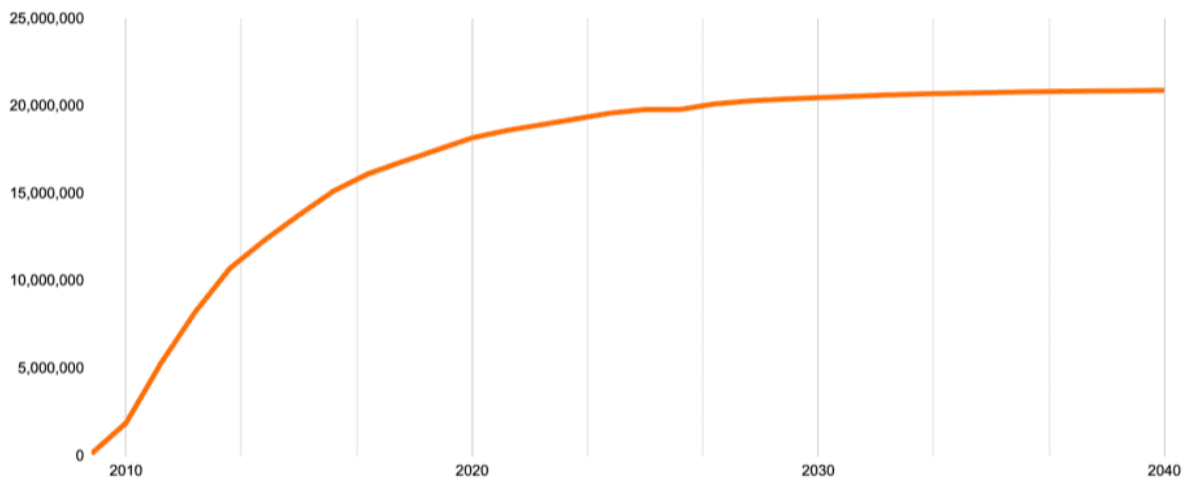
1. Bitcoin, the currency

Lowercase bitcoin is a digital money that has a limited supply of just under 21 Million.

It uses magic called cryptography that prevents anyone from being able to increase the supply. I will explain how this magic works further down.

The point you need to keep in mind for now is that there can only ever be 21 million bitcoins, period.

Bitcoin Supply



elementalcrypto.com

Bitcoin has a geometrically declining supply function. In fact, Bitcoin's supply never reaches 21,000,000 because it approaches that number asymptotically.

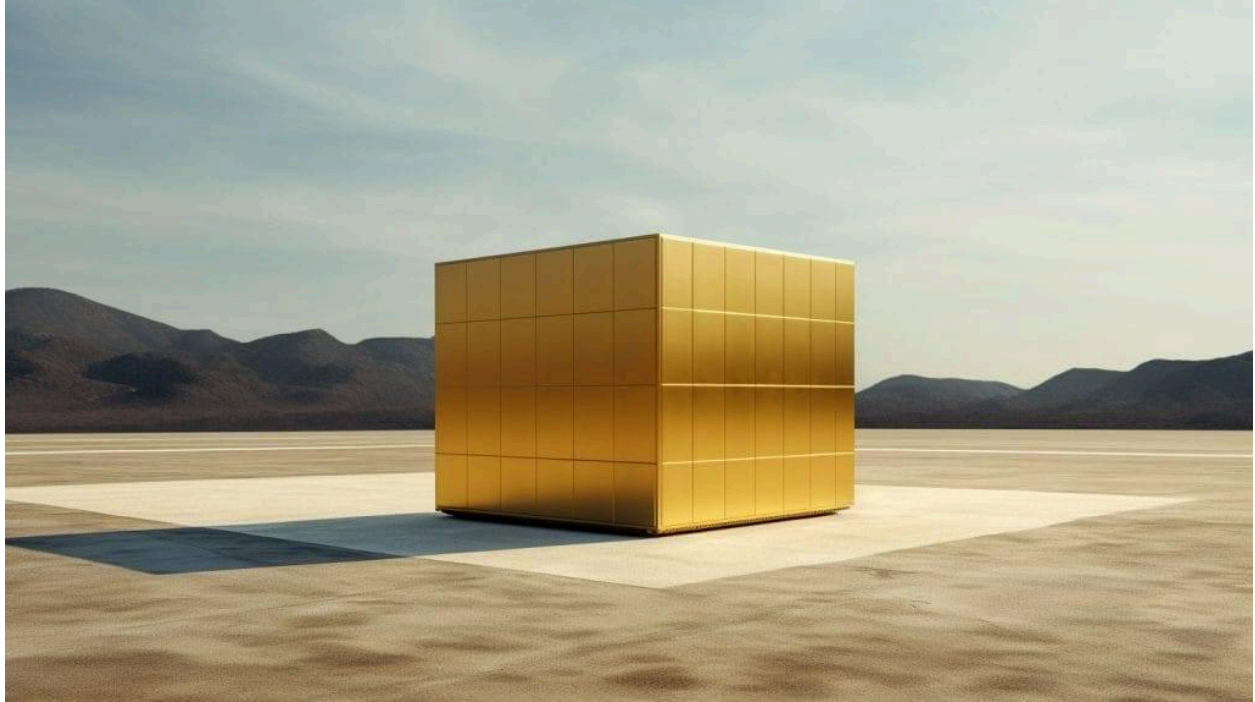
Let that sink in.

There is no government or other entity that can step in to increase the supply.

Bitcoin compared to gold

In that sense, bitcoin is similar to gold whose supply is very limited.

Humans have found almost all the gold in the world. However, the supply of gold has been increasing by about 1.5-2% per year.



According to the BBC, all the gold in the world would fit in a cube that is 23 meters on each side. That's about the length of a tennis court.

In contrast, there are currently 19.58 million bitcoins in circulation today. But by 2140 we will reach the maximum supply of 21 million after which no new bitcoin will be created.

Know what happens when you make something scarce?

Everyone wants some.

If you reduce the supply of anything no matter what it is I guarantee you people are going to want it. This is a core strategy of luxury brands that will get rid of excess supply or produce limited editions.

For this reason, both gold and bitcoin are thought to be good stores of value.

While bitcoin is very volatile in the short run it has performed exceedingly well in the long run.



Both bitcoin and gold have appreciated over the long run. Sources: [Coinmarketcap](#) and [Goldprice.org](#)

If bitcoin were to completely replace gold as a store of value then it would be worth \$500,000.

To see how I arrived at this number check out [Why Is Cryptocurrency Worth Anything](#).

But bitcoin has some other properties that make it a good candidate for money.

Properties that make bitcoin good money

1. **It's divisible.** Each Bitcoin can be subdivided into 100 million Satoshis just like how a dollar can be divided into 100 cents. So even if the price of bitcoin is high you can still buy 1/100 millionth of it.
2. **It's easy to move.** If I want to send someone bitcoin from the US to Guatemala I can do it in seconds and it will be confirmed

within an hour. Other forms of money such as gold or physical cash require that you get on an airplane. Digital fiat currency can be transferred online but this usually takes 2-5 business days within the country and can take more than 10 when transferring between countries.

3. **It's durable.** Bitcoin cannot break or wear out. Gold and diamonds are also pretty durable. Seashells, feathers, and beads are less so.
4. **It's fungible** i.e. you can exchange one bitcoin with any other and it wouldn't make a difference. Just like how you can exchange one euro coin for another or a bar of silver for another. (See [what is fungibility in crypto](#) for more).
5. **It's easy to verify.** Bitcoin uses cryptography to do that. On the other hand, gold requires an appraiser, and fiat currency bills require special machines like the one depicted below.



6. **It's stood the test of time.** Bitcoin has been around for more than 15 years which gives it a decent footing. Of course, that is

nothing compared to gold for example that has been used as money for thousands of years.

Yet most people's objection to bitcoin being a form of money is that it hasn't replaced fiat for day-to-day transactions.

Why we don't use bitcoin for groceries

The original intention was for bitcoin to be used as a form of payment just like the US dollar.

However, four things have prevented bitcoin from replacing fiat currency.

#1. You can't price stuff with it

The first is that **bitcoin is not a good unit of account**. Imagine you walked into a grocery store and you saw that an avocado costs 0.002346 bitcoin. What does that even mean?

You are used to quantifying groceries in dollars and euros or whatever your local currency is. So Bitcoin fails in being adopted as money for the moment.



What if grocery stores priced their goods in bitcoin?

#2. It's volatile

The second issue is that you would need to keep updating the price of that avocado every 5 minutes because the price of **bitcoin is volatile**.

Of course, volatility is a relative concept.

If you ask someone in Venezuela or Argentina whether they would like to hold bitcoin or their own local currency you will find a strong preference for bitcoin.

Because while bitcoin's price is volatile it's been following an upward trend over time vs, say, the Argentine peso whose value has been nosediving.

Bitcoin price vs Argentine Peso



People in Argentina buy the store of value argument because their currency has seen massive inflation as opposed to bitcoin which has trended upwards overall. Source: Tradingview.com

#3. It's slow

The third issue is that Bitcoin **cannot process transactions as fast as Visa or Mastercard** can.

There are ways around this that are being developed, most notably the Lightning Network, but for the moment the main narrative that has caught on with bitcoin is that it is a store of value.

#4. It's not an official currency

Finally, in most countries, **bitcoin is not legal tender**.

This means you cannot pay your taxes in bitcoin.

So you still use the U.S. Dollar or whatever your national currency is to process taxes even though you might accept bitcoin as payment or invest in it as an asset.

See the [Bullish case for Bitcoin](#) for more reasons why Bitcoin advocates believe Bitcoin is the future. The book by the same title is also pretty good.

Apart from being a virtual currency and store of value though Bitcoin is a network.

2. Bitcoin, the network

Uppercase Bitcoin refers to the Bitcoin Network and the first successful blockchain for digital currencies.

I will spend the rest of this article explaining how the Bitcoin blockchain and network work.

How Bitcoin came about

Imagine it's January 2009 and your name is Satoshi Nakamoto.

You are dismayed by the turn of global financial events.

The US economy has just combusted after several major banks went bankrupt including Lehman Brothers, Bear Stearns, and Merrill Lynch.

The US government and Fed are printing tons of money to bail out the rest of the banks that are “too big to fail”.

As you delve deeper trying to understand how we ended up in this situation you realize that there are two issues at play here.

The first is an issue of transparency. If you, as a customer, were able to see the quality of the assets on banks’ balance sheets they would have never been able to get away with holding so much toxic stuff. Would you give your money to a bank if they said “Thanks for your cash, we are now going to invest in these highly risky mortgages that we don’t think anyone will be able to pay back”.

The second issue has to do with money printing and incentives. In response to the financial crisis, the Fed increased the money supply **massively** and the government bailed out the banks. Some feared inflation which in this case **didn’t materialize**. But if there is going to be someone who will bail you out every time you cheat then you will always have an incentive to cheat again.

The idea for bitcoin is born

So there you are sitting at your desk wondering if you could create an alternative financial system.

One that is transparent and not managed by a central intermediary such as a government or central bank.

And then a spark lights up in your mind: You are going to create your own digital currency.

Here it is:

21 Million FREEDOM COINS

I declare the bytes that form that sentence to be a currency.

Are they digital? Yeah sure they are.

Can you send them to someone? Yup, just copy and paste it into an email.

So what's the problem? You know what I have just proposed is ridiculous but why is that?

Let me help you.

If you send me an email saying "Here are 21 Million FREEDOM COINS" how do I know that you still don't have them?

You can easily type the string "21 Million FREEDOM COINS" as many times as you like.

21 Million FREEDOM coins
21 Million FREEDOM coins
21 Million FREEDOM coins
21 Million FREEDOM coins
21 Million FREEDOM coins
21 Million FREEDOM coins

A key challenge with internet currencies prior to Bitcoin was that someone could spend them again. This is known as the double spend problem.

Your digital dollars, euros, yuan, and pesos are the same thing. They are just strings of numbers sitting in a bank's database somewhere.

Except there is one big difference.

When you wire \$100 to my bank account the bank acts as a referee and deducts \$100 from your account while crediting my account with \$100.

Hence, it's not so much the fact that bitcoin is digital that's fascinating but rather that it manages to exist without a central intermediary i.e. its decentralized.

How does Bitcoin manage without a central intermediary?

Let's make a file and create some digital coins like before. The file will say something like

Markos has 1 FREEDOM coin

Johny has 3 FREEDOM coins

Adanna has 0.2 FREEDOM coins

Priya has 10 FREEDOM coins

....

and so on.

Since this is a digital file I can send it to 10 friends of mine and they can each store a copy of the file on their laptop.



Now if I, Markos, were to update the file so that Markos has 0 FREEDOM coins and Priya has 11 it would be like I have sent Priya 1 coin. I can then send the updated file to all my friends who in turn also update their files to reflect the new state of affairs.



My friends will perform some checks such as:

Did Markos even have 1 FREEDOM coin to send Priya in the first place and

Did he format everything correctly?

Assuming everything is ok then they know it is my wish to send Priya 1 coin so they update their file accordingly.

But how can my friends verify it's me who is updating the file and not Priya pretending to be me and actually trying to steal the coin?

This is where we need cryptography.

Private keys and public keys

In the past people used wax seals or a unique signature to prove it was them sending the message.



In the modern era, we need something equivalent to a signature only it needs to be in digital form and 100% verifiable.

To do that we are going to use cryptography.

Let's give Markos a secret code called a private key.

Say it looks something like this:

4796822caefd3dcf540ebce4abeb7414d95351dda0156bd5ccf02c9611
30a8a2

Elliptic curves and public keys

Now, I can use a special algorithm called an Elliptic Curve Signature algorithm (ECDSA) that converts my private key into another code.

I just plug in the private key and get an output.

Here it is:

```
0466c932ca8b844ef70c5913fd9b5c511b6a241fa8d6e82d00ad9310a9
5b64b5624589a24f01123451b1a680d925b4eea485a4885af103b4608
d1ef50441d9d5f5
```

I will call this code my public key.

HOW PUBLIC KEYS ARE GENERATED

4796822caefd3dcf540ebce4abeb7414d95351dda0156
bd5ccf02c961130a8a2



PRIVATE KEY



Elliptic Curve Signature algorithm (ECDSA)



0466c932ca8b844ef70c5913fd9b5c511b6a241fa8d6e
82d00ad9310a95b64b5624589a24f011...



PUBLIC KEY OR PUBLIC ADDRESS

ELEMENTALCRYPTO.COM

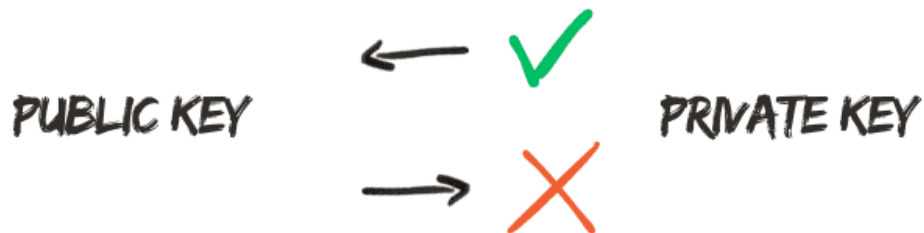
You can play around with [generating signatures here](#).

Here is a key point that needs to stick in your mind.

What's special about this procedure is that while you can derive a public key from a private key you can't do the opposite.

PUBLIC AND PRIVATE KEYS

YOU CAN DERIVE YOUR PUBLIC KEY FROM YOUR
PRIVATE KEY BUT NOT THE OTHER WAY ROUND



[ELEMENTALCRYPTO.COM](https://elementalcrypto.com)

This means that when you share your public keys with someone they won't be able to access your private keys.

How bitcoin uses public addresses instead of names

Now it's time to update the mental model we've created. Remember how I said we had a file with names on it and how many coins each person owns?

Well, instead of names we are going to use public addresses.

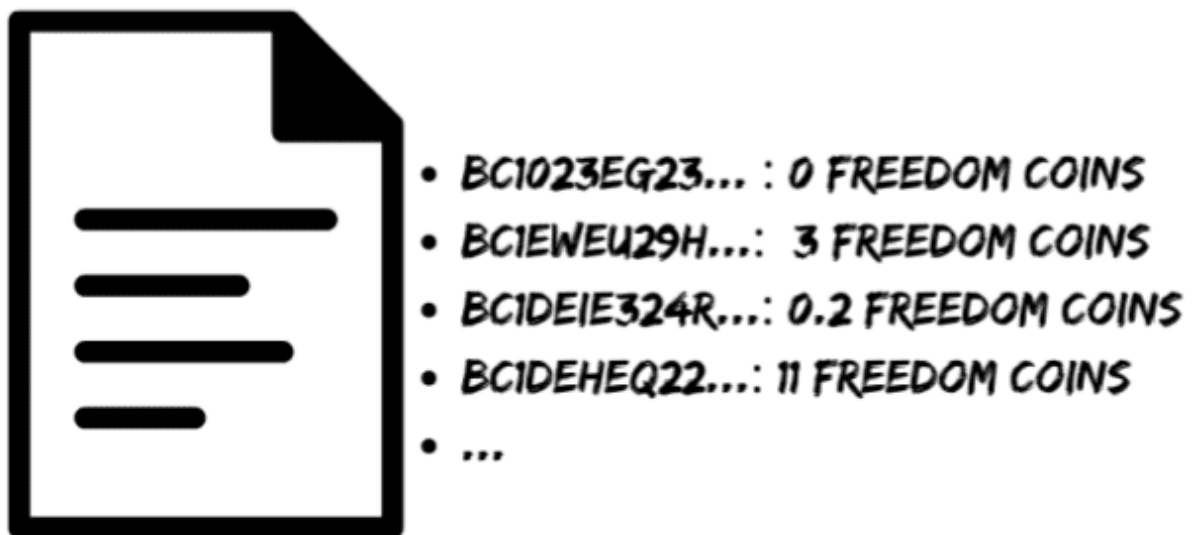
So, Markos will generate a random private key and use the ECDSA algorithm to derive a public address from it.

Johny, Adanna, and Priya will all do the same.

The chances of us generating the same private key are astronomically negligible as the private key is a 256-bit number which means there are 2 to the power of 256 unique private keys which is this number:

115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,
640,564,039,457,584,007,913,129,639,936

So our file will look something like this.



Nowadays Bitcoin addresses start with BC1

Each of those addresses has a corresponding private key but you can't tell whose it is unless they tell you.

Now pay attention as we approach a key point in understanding how Bitcoin works.

Signatures

Using the same algorithm I am going to generate a new code.

Before my input was the private key and the output was a public address.

This time my input is a private key and a message saying “I want to send Pryia 1 FREEDOM coin”.

The algorithm will spit out a new unique code which I will call a signature.

HOW SIGNATURES ARE GENERATED

Private key: MHQCAQEEIJONyLhk6eApShGHAwyio....

Message: "I want to send Pryia 1 freedom coin"



Elliptic Curve Signature algorithm (ECDSA)



Signature: MEUCIAxBWpUbpDt5igwx0K2xWKSom...

ELEMENTALCRYPTO.COM

Next, I send my public key, my message, and my signature to all my friends. They can verify it's me by passing this data through a complex mathematical equation. We're not going to go into that equation here.

The output of that equation will tell them whether it is my signature or someone else trying to fake it. i.e. only one unique signature can be generated from that combination of data and they can confirm it belongs to me without me needing to reveal my private key.

HOW SIGNATURES ARE VERIFIED

Public key: M0466c932ca8b844ef70c5913fd9b5c511...

Message: "I want to send Pryia 1 freedom coin"

Signature: MEUCIAxBWpUbpDt5igwx0K2xWKSom...



Verification Algorithm



TRUE



*ONLY THE PERSON WITH THE PRIVATE KEY TO THIS PUBLIC KEY COULD
HAVE CREATED THIS SIGNATURE FOR THIS MESSAGE*

ELEMENTALCRYPTO.COM

This is the magic of cryptography.

We now have a robust way for anyone with a computer to mathematically verify messages to update the file.

This way I no longer need to collaborate with friends who know me and trust me.

Anyone with a computer anywhere in the world can hold a copy of the file and can verify that the message being sent is from the person holding the private keys.

The private keys are also Bitcoin's Achilles heel as anyone with access to the keys can steal the crypto and send it anywhere they like.

Wallets and how messages are sent

To transact on the Bitcoin network you need a wallet.

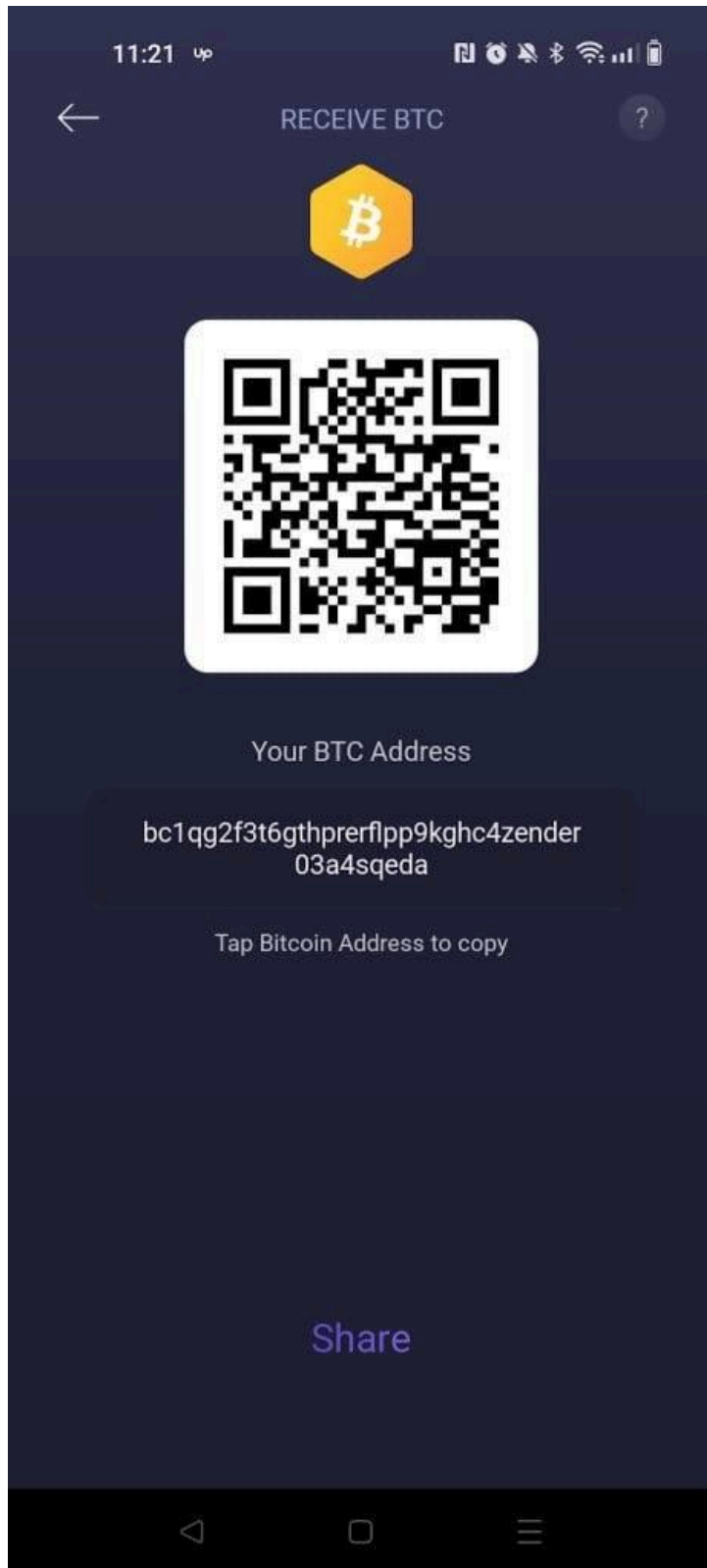
A wallet is an interface that allows you to interact with a blockchain in the same way that a browser allows you to interact with the internet.

Your wallet is a piece of software that generates private and public keys and allows you to send instructions to the blockchain network.

Wallets can have multiple forms.

They can be desktop apps, mobile apps or hardware devices.

In order to make user interfaces easy to use wallets will often allow you to share a QR code that represents your address. This reduces the chances of an error.



This is what a QR code looks like. Others can either copy the public address or scan the QR code to send you bitcoin.

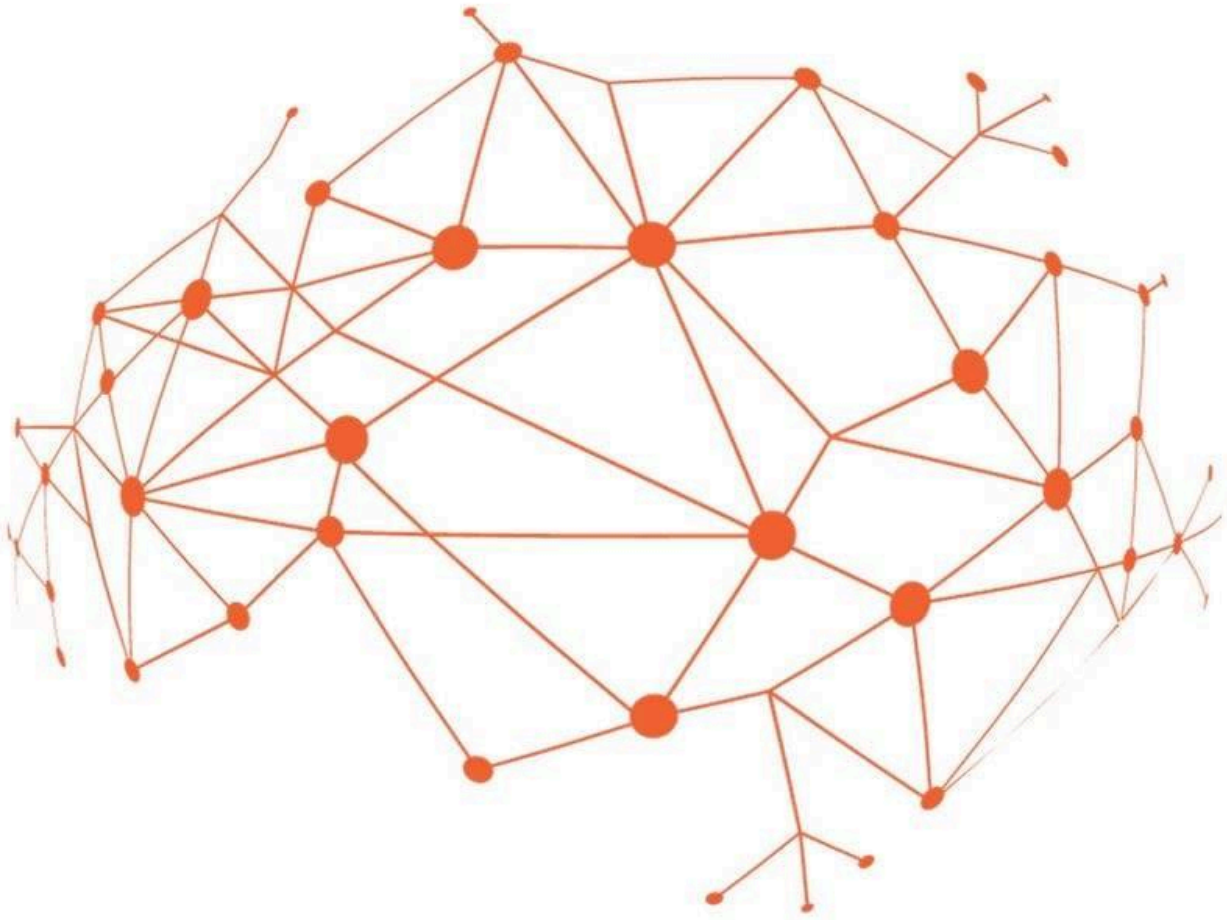
There are two ways to manage a wallet

1. **Non-Custodial wallets.** These generate a seed phrase of 12-25 words that represent your private key and public addresses. You are responsible for safeguarding your seed phrase
2. **Custodial wallets:** Your private key is stored on a central server and managed by someone else such as a crypto exchange. They are responsible for your crypto and execute your instructions but you do not have access to your keys.

Read [Should You Have Multiple Wallets](#) and [10 Ways a Cryptocurrency Exchange Is Different from a Wallet](#) for more on wallets.

How do messages get propagated?

Consider that there are thousands of computers holding a copy of the same file. If you visualize it, it's like a massive network of computers that can communicate with each other.



Each computer is a node in the network

When I send a message anyone can pick it up and verify it to update the file.

They can then forward the message to other nodes which in turn will forward it to others.

Within seconds everyone will have verified the message and updated their files.

This process is known as flooding and takes about 15 seconds.



Here the new message is propagating from one node to another; a process known as flooding.

The best way to understand public addresses and private keys

I am going to use an analogy that I first heard about from Andreas Antonopoulos in one of his classes¹.

Think of a public address like a glass deposit box with a serial code on it.



Imagine the deposit boxes were made of glass so that you could see through them

Anyone can send money or messages to this address if they have the code.

The postman will come and drop an envelope with money or the message through the slit in the box.

Because it's a glass box everyone can see what's inside.

They can see what the messages say and how much money there is.

Now imagine that each of these deposit boxes has a security code. To unlock a safe deposit box you need to know the PIN.

In the case of Bitcoin the PIN, known as a private key, has 77 digits.

The possible combinations of 77 digits is bigger than the atoms in the universe. Hence, they are impossible to guess.

However, if you have the private keys then you are able to access the deposit box and take money out.

You can then drop that money in another deposit box, perhaps in exchange for something you are buying from the owner of that box.

Here are some important concepts to understand about addresses:

#1. Can one person have more than one address?

Absolutely, you could have myriads of addresses. Imagine you are a merchant selling laptops and want to accept bitcoin. You could have a separate address for each laptop. That way when you see money come into that address you know you have been paid and you can ship the laptop to the buyer.

#2. Can an address have more than one person's money?

Definitely, imagine you are a crypto exchange. You could put all your customers' money in one deposit box.

As an exchange, you probably shouldn't do this because it would make the box a very attractive honey pot for hackers to try to access but you can if you want to.

3. Can people see how much money you have?

Definitely. If you tell them which box is yours they will be able to check and see how much bitcoin you have.

Congratulations you have understood a major component of how blockchains work.

I hope you have guessed that FREEDOM coins are a metaphor for bitcoins so I am going to use that from now on.

How blocks are stitched together

Now let's say my file fits only 1MB of data.

At some point, after about 1,000 transactions, that file is going to fill up and we are going to need a new one.

But we need a way to connect the two.

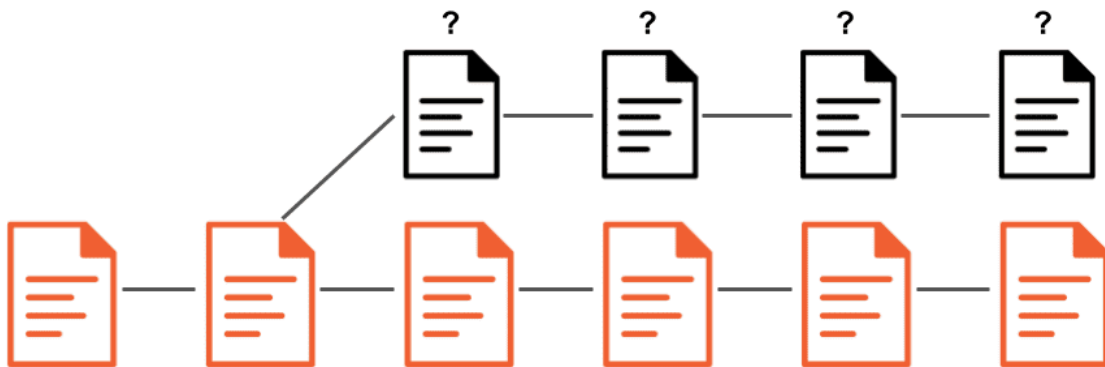
Going back to my previous example, assume the first file is full and I now decide I want to send Priya 1 bitcoin.

Somehow the network of people with laptops needs to be able to refer to the original file and check that I had 1 bitcoin to start with.

After checking the signature, they can then add information in the new file that says, "ok we accept that now Priya has 1 extra bitcoin and Markos is 1 lesser bitcoin."

But how do we stitch the two files together?

What if someone acts maliciously and starts spreading files with misinformation? How do we know which file tells the truth and which one is a scam?



How do you know you should connect to the orange block and not to the black block next?

Let's take another detour into cryptography.

How SHA-256 works

Imagine it is 2001.

See this building? It's the U.S. Government's National Security Agency (NSA).



The NSA has just come up with a pretty cool algorithm called **Secure Hash Algorithm-256** or **SHA-256** for short.

What SHA-256 does is that it takes any piece of data and converts it to a string of alphanumeric characters called a hash.

Here is the SHA-256 hash for different pieces of data:

SHA-256 examples

Hi	8f434346648f6b96df89dda901c5176b10a6d83961dd3c1ac 88b59b2dc327aa4
I am a little fairy	268e13085964a1bbedc1a24eaa77a1c61b5a0052e85600f3 473b24303664b5e5
1+1= 2	9274063a9738f5d43358aaae27111d70bc47e856c18a48ec 9bbb4ab28119a97e
Mark os sent 1 freed om coin to Priya	91e922bc17eb934ffea1521b99c3cc388c6a768583fe5b8b8f e264ea74e9074e

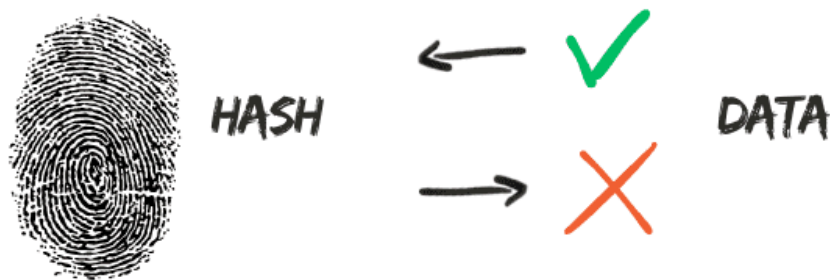
You can play around with your own data [here](#).

Similar to ECSA, using SHA-256 you can derive a unique hash for any data point but you can't derive the data from the hash.

The hash is like a digital fingerprint for the data you have inserted. It's unique to that data.

SHA-256 EXPLAINED

YOU CAN DERIVE YOUR HASH KEY FROM YOUR DATA
BUT NOT THE OTHER WAY ROUND. YOUR HASH IS
UNIQUE, LIKE A FINGERPRINT



[ELEMENTALCRYPTO.COM](https://elementalcrypto.com)

What's cool about it is that anyone can check a hash and data and confirm that the hash belongs to that data.

Connecting data using SHA-256

Here's how we can connect the two files using their hash.

The first file will have data like:

File number

Transaction data on who owns what

A SHA 256 hash that is derived from the file number and transaction data.

Conceptually it looks something like this:

A BLOCKCHAIN BLOCK



ELEMENTALCRYPTO.COM

I'm simplifying a lot but this is what a blockchain block looks like

The second file will have

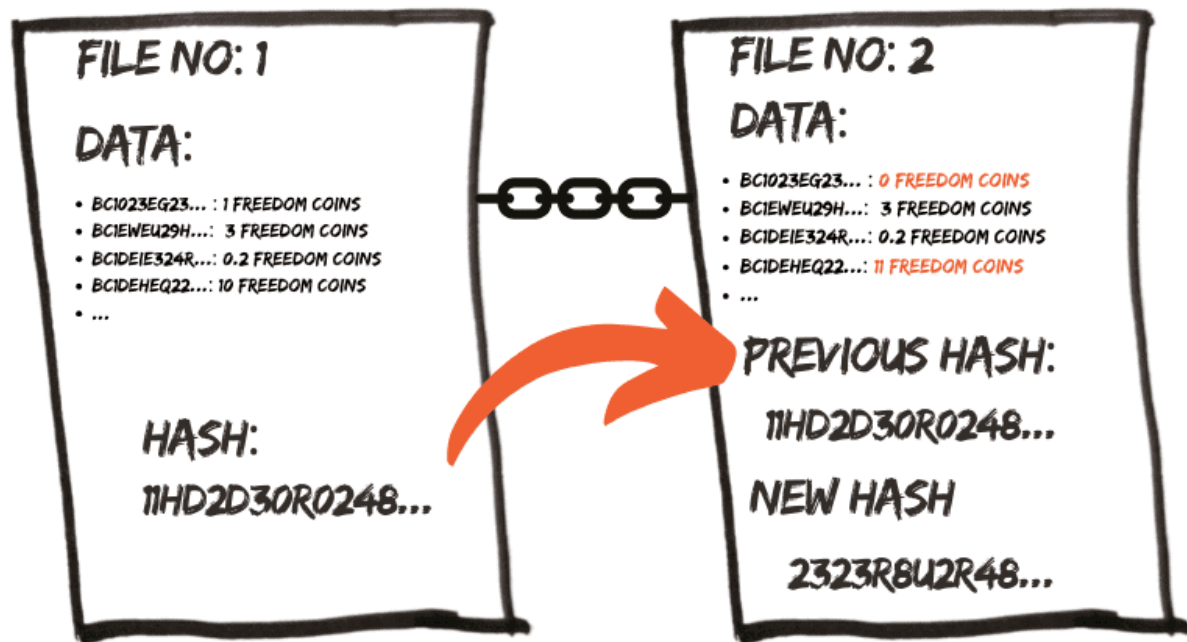
File number

Transaction data on who owns what

The previous hash of file number 1

A new hash for file number 2.

HOW TO FORM A BLOCKCHAIN



ELEMENTALCRYPTO.COM

Now if anyone tries to mess with the data in file number 1 its hash value will change. Anyone will be able to see that the previous hash

value mentioned in file number 2 does not match the value in file number 1.

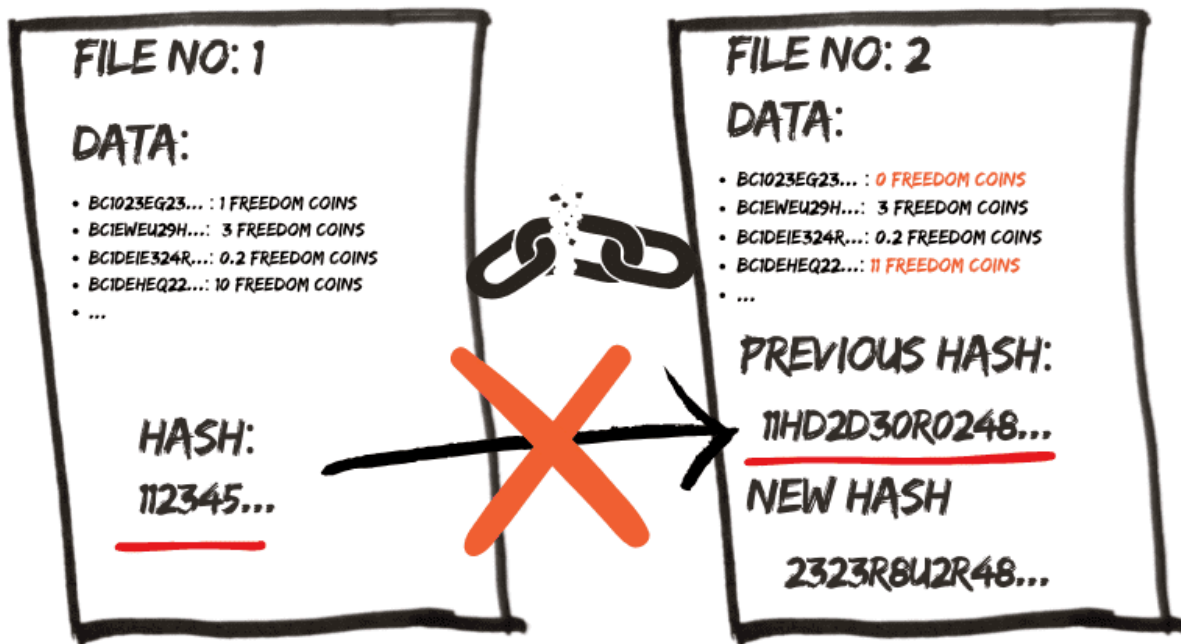
This makes it extremely hard to cheat.

The cheater would have to change file number 2 as well.

At the time of writing, there are more than 825,000 files.

The cheater would need to change all of those files if they wanted to warp reality. I will explain why this is impossible to do shortly.

IT'S HARD TO CHANGE A BLOCK



THE HASHES DON'T MATCH

ELEMENTALCRYPTO.COM

What's a blockchain?

Another way to think of the file is as a block of data.

And because you can use the hashes to connect files you can have a chain of blocks.

Hence the term blockchain.

All clear so far? Good because it's time to understand what Bitcoin mining is.

Bitcoin Mining explained

So now we have a network of computers that can accept messages from others, update their blocks with the new information and string blocks of transaction data together.

But why would you waste your time and energy doing that?

What's in it for you?

Incentives and who gets to add the new block

Bitcoin relies on an incentive structure that rewards participants with new coins for adding a new block to the blockchain.

“Essentially, Bitcoin mining decentralizes the currency-issuance and clearing functions of a central bank and replaces the need for any central bank.”

Andreas Antonopoulos, Mastering Bitcoin²

The participants are known as miners because they are performing certain actions that could result in them being rewarded with new bitcoins plus transaction fees. Just like how a gold miner who discovers a gold nugget is rewarded for the work they put in.



Gold panning during the California gold rush. Source: [wikipedia](#)

Nonces

Let's take a look at block 2 again and add another piece of information to it.

This is called a nonce and it is a number that you can vary.

Block 2 now contains the following information.

File number: 2

Transaction data on who owns what

The previous hash of file number 1

A new hash for file number 2.

Nonce: 1

Now let me run this information through a SHA-256 algorithm. The output I get is:

3862c628e0bcf1b81fa27f0f5053f2221533573c202952637a8bb0fab3131cde

What if I set you a challenge?

Imagine I say you need to produce a SHA-256 that starts with four zeroes by varying the nonce⁵.

So you try:

File number: 2

Transaction data on who owns what

The previous hash of file number 1

A new hash for file number 2.

Nonce: 2

Then

File number: 2

Transaction data on who owns what

The previous hash of file number 1

A new hash for file number 2.

Nonce: 3

You keep varying the nonce: 4, 5, 6, ... 38901

And keep trying until the SHA-256 output ends up starting with 4 zeroes.

Who adds the new block?



How miners solve the puzzle

Bitcoin miners use powerful computers called ASICs that can run through the numbers fast enough to find a result within about 10 minutes.



The

Antiminer S19, a popular ASIC for hashing bitcoin

If they end up solving it in less than ten minutes the Bitcoin network will automatically increase the difficulty of the challenge.

For example, it might ask for a hash with 5 zeroes.

Nowadays the mining difficulty has increased to such an extent that miners need to find a hash with 17 zeroes.

This means that their machines need to run through billions of calculations.

The only way to do the calculation is to test various nonce numbers.

The first miner to find a SHA-256 with enough zeroes can broadcast the result to the network and add the new block.

Proof of work

Everyone knows that this miner did some computational work to be able to claim the block as they can see it and verify it with the numbers.

This is why this mechanism is known as Proof of work⁴.

The fact that they have added a SHA-256 with 17 zeroes to their block proves to anyone that they have done the work.

This means they have spent a lot of money on electricity.

Now if they try to cheat and add non-valid transactions the rest of the network will reject the new block.

As a result, the cheating miner will have wasted their money.

For a block to be accepted the majority of nodes have to agree that the data is valid and that it has a valid proof of work.

Game-theory-based security model

So we have ended up with an incentive structure to always tell the truth.

If you play by the rules you might be rewarded in new bitcoin.

But if you try to cheat you are guaranteed to lose.

There are no shortcuts to solving the proof of work puzzle.

Putting in the work and being truthful is the only viable economic option which is what guarantees trust in a decentralized manner.

You have just witnessed how a group of people who do not know each other can come to a consensus on what the state of a series of transactions is without the need for a central authority. Anyone with an internet connection can verify transactions.

Congratulations, you have conquered the main concepts of how Bitcoin works.

In this next section, I am going to walk you through some more details worth understanding to take you to an absolute expert level.

The first thing you need to know about is the Mempool.

What is a Mempool?

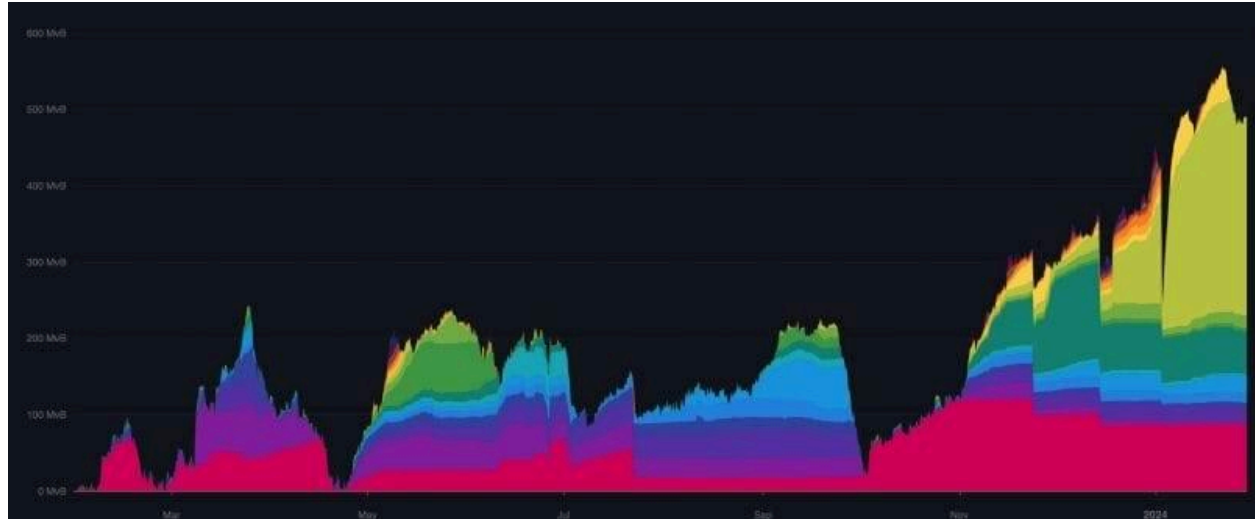
When a user broadcasts a transaction it does not go directly into a block.

Instead, it goes to a **queue called the mempool**.

So when I send out a message saying I wish to send Priya a bitcoin that message is sent to the mempool first.

From there miners will pick my message up along with other transactions and construct a block of transactions.

They will then start trying to solve the cryptographic puzzle so that they can prove they did the work and add the new block of transactions to the blockchain.



Mempool transactions over time. See those dips? That's because data has been removed from the mempool and placed in a block. Source: mempool.space

How do miners bundle transactions?

Each transaction has a corresponding fee.

You can bid as much as you like for the fee.

If it's urgent for you to get the transactions confirmed in the next block then you will outbid everyone else.

Miners will bundle transactions according to who is paying the most. This means that if you pay less you may need to wait for 2-3 blocks before your transaction is added to a block.

Don't worry, eventually your transaction will get added even if you don't overbid.

So now you have multiple miners bundling transactions into new blocks and competing to solve the puzzle so that they can add the new block to the blockchain.

What happens if two miners solve the puzzle at the same time?

Imagine you end up in a situation where two miners solve the hash at almost exactly the same time.

Say one is in the US and one in China.

The US miner starts spreading the new block to nearby computers (nodes) in the network.

They start checking everything is ok and give the green light to add the new block to the blockchain.

At the same time, the Chinese miner started the same process and nodes have started accepting the block as the new block.

What you end up with is a fork.

The blockchain has split in two with one version saying that the last block is what the American miners added and the other saying that it's the Chinese block.

Whose version of the truth do you go with?

The answer is that we don't know yet which version will win. We need to wait for more blocks to get added.

Imagine that as soon as the Chinese block is added another miner finds the next block and adds on top of the Chinese one. Now the "Chinese" fork is longer than the "American" one.

The rules dictate that you need to go with the longest blockchain. This is the chain that has the most proof of work. This way of reaching consensus is known as Nakamoto's consensus.

When a new block gets added to the Chinese fork other miners will see it and say oops I thought the American fork was winning but I was wrong.

They then empty the transactions back into the mempool to be picked up in the next block.

What is a coinbase transaction?

When a miner forms a block the first thing they do is add an entry that rewards them with 6.25 bitcoin plus transaction fees.

This is known as a coinbase transaction and it's why Coinbase, the exchange, chose that brand name.

Anyone who verifies the block will check that the miner submitting the block is rewarding themselves with the right amount.

If the miner is greedy and tries to cheat their block will be rejected.

Everyone knows that the mining reward is currently set to 6.25 BTC.

And they also know that after every 210,000 blocks the reward is halved. This means that at some point in 2024, the bitcoin mining reward will drop to 3.125 BTC plus fees.

How do payments work on the Bitcoin network?

The Bitcoin blockchain is like a digital public ledger except instead of credits and debits you have inputs and outputs.

Here is what happens when I make my payment to Priya.

How an input becomes an output

Priya receives 1 bitcoin as an input from me.

Now say Priya wants to buy a Bluetooth speaker from Vivek's store costing \$50 and Vivek accepts bitcoin.

\$50 is equal to 0.0011 BTC at the time of writing.

So Vivek lists his public address for the speaker on his store.

When Priya instructs her Bitcoin wallet to send 0.0011 BTC to Vivek's address here is what happens:

A BITCOIN TRANSACTION

PRIYA'S INPUT

1 BTC

PRIYA'S OUTPUTS

VIVEK: 0.0011 BTC

CHANGE: 0.99 BTC

(FEES: 0.0089 BTC)

ELEMENTALCRYPTO.COM

When Priya sends 0.0011 BTC to Vivek's address it shows as an output in her transaction. And it will show as an input in Vivek's transaction.

Just like with cash you need to get change though.

So Priya's wallet will construct a change address that will receive the 1 BTC minus 0.0011BTC minus transaction fees.

Now if you are a clever bunny you will have noticed that $1 - 0.0011$ is not equal to 0.99. It is actually equal to 0.9989 which implies that 0.0089 is the fee paid to miners for validating the transaction.

Combining multiple inputs to an output

Now as Vivek collects all these bitcoins from selling stuff on his store he wants to use some of them.

Say Vivek wants to buy a car for \$30,000 in bitcoin (0.65 BTC). He will need to send all of these chunks of payments to the seller's address.

The chunks don't get aggregated beforehand into a single address. Instead you need to send them as individual inputs. It's just how the code works.

So the payment for the car will look something like:

BITCOIN TRANSACTION WITH MANY INPUTS

VIVEK'S INPUT

SPEAKER SALE: 0.0011 BTC

LAPTOP SALE: 0.05 BTC

TV SALE: 0.07 BTC

....

VIVEK'S OUTPUTS

CAR: 0.65 BTC

CHANGE: ... BTC

ELEMENTALCRYPTO.COM

Note that the Bitcoin blockchain does not actually use Bitcoin as its unit of account. Instead, it uses Satoshis where 1 BTC = 100 million Satoshis.

So instead of address xyz input: 1 BTC

it would say:

Address xyz input: 100,000,000

How long do transactions take?

When Priya pays Vivek for the speaker that transaction will appear in Vivek's wallet within the next 15 seconds.

It won't be a confirmed transaction but Vivek's wallet will see it lingering there in the mempool.

To verify the transaction it needs to get picked up in a block that gets added to the blockchain.

Since a block is mined every 10 minutes on average, it is very likely that the transaction will be verified within the hour.

Note that 10 minutes on average means that it's never actually exactly 10 minutes. Sometimes it can be 2 minutes and other times it can be 40 minutes.

But on average it's 10.

For something like a Bluetooth speaker 1 block is enough to feel secure that the transaction is set in stone.

For something like a car, you probably want 3 blocks.

If you are selling a house you probably want it to be closer to 4 blocks.

The more blocks that get added the harder it is for anyone to change the transaction history.

Is it possible to change the transaction history?

Say you want to go back in time and change a transaction in block 2.

To do this you would need to recreate a longer chain than the existing one and solve all the cryptographic puzzles over 800,000 blocks.

And you would need to do this in 10 minutes.

Hopefully, you can see that the deeper a transaction is buried in the blockchain the more impossible it is to change.

In fact, after about 3 blocks I'd say you are pretty much covered for any eventuality and can consider the transaction set in stone.

Wait what if I want a cup of coffee? Do I have to wait ten minutes?

No. You need to think probabilistically vs value.

In the case of the coffee, you can afford to take the risk as soon as you see the transaction in the mempool.

Consider that credit cards don't pay merchants until 30-60 days after the transaction during which time they could reverse the payment.

Bitcoin which will usually confirm your transaction within the hour is looking pretty good in this regard.

Isn't Bitcoin slow?

Yeah, compared to other blockchains Bitcoin is slow. Bitcoin can process about 7 transactions per second.

Compare this against Solana which can process 65,000 transactions per second and it feels awfully slow.

However, Bitcoin has a solution that batches transactions before they get sent to the Bitcoin blockchain called the Lightning Network. Using this hack bitcoin can achieve about 1 Mn Bitcoin transactions per second.

I am not going to explain the Lightning Network in this post.

What are mining pools?

The chances that your machine will solve the cryptographic puzzle are pretty low.

This means that rewards are going to be less frequent while you still need to dole out money to pay for electricity every month as these powerful machines consume a lot of electricity.

To smoothen their income streams miners will often join a mining pool that shares rewards according to the hashing power your machine provides.

The mining pool take a 1-2% cut but this ensures more consistent rewards. You can think of it like joining a lottery pool.

Where do I get bitcoin?

There's a few options

1. Cryptocurrency exchanges.

This is the easiest way to buy bitcoin. Cryptocurrency exchanges are marketplaces where you can use a bank transfer, debit card, or credit card to deposit fiat currency and purchase bitcoin and other digital assets.

The benefit of using a crypto exchange is that they are easy to use and have a lot of liquidity (buyers and sellers).

The drawback, for some, is that you need to upload your personal information and prove your identity.

2. Bitcoin ATMs

With a Bitcoin ATM, you can deposit cash and get bitcoin sent to an address by using a QR code. This address can be your own because you want to convert cash into Bitcoin or it can be someone else's because you want to pay a person in bitcoin.

In the United States you need to go through an ID verification process to use a Bitcoin ATM but in Europe and other countries you can remain anonymous.

3. P2P networks

Using a peer-to-peer network such as [Paxful.com](https://paxful.com), [Bitvalve.com](https://bitvalve.com), [Bitcoin.org](https://bitcoin.org) you can buy bitcoin directly from another person.

Buy from	Pay with	Avg. trade speed	Price per Bitcoin
SavorySiamang102 👤 202 ● Seen 4 minutes ago	PayPal Honest Instant release friends and family	New offer	41,793.18 USD 1 USD = 1.02 USD of BTC ↓1.96% ⓘ Min purchase: 20 USD Max purchase: 200 USD
BestChat639 👤 202 ● Seen 5 minutes ago	PayPal Fast and honest no receipt needed	New offer	43,054.99 USD 1 USD = 0.99 USD of BTC ↑1% ⓘ Min purchase: 20 USD Max purchase: 100 USD
SnazzyKokanee949 👤 204 ● Online	PayPal Fast and honest no receipt needed	New offer	43,481.27 USD 1 USD = 0.98 USD of BTC ↑2% ⓘ Min purchase: 20 USD Max purchase: 245 USD

In this screenshot you can see all the people willing to sell me bitcoin and their price. Source: Bitvalve.com

The p2p platform acts as a third-party referee and holds each person's value in escrow until both sides confirm the transaction.

4. In a back alley

In the early days of crypto people used to exchange bitcoin for cash face to face. I wouldn't recommend you do this in a back alley. A public space such as a police station would be much better.

Who created Bitcoin?

The legend behind Bitcoin is known as Satoshi Nakamoto.

We don't know if this is a single person or a group of people and their last publicly available message is from December 2010.

Since then many people have turned up claiming they were Satoshi but none of them have been able to prove it; something that would be easy to do since the original Satoshi would be able to sign a transaction to prove it was them.

Satoshi didn't invent anything new.

All of the individual technologies that we have talked about here already pre-existed.

But Satoshi was the first to stitch them all together into the network solution that we know as Bitcoin.

The big picture

You now have, for the first time in history, a global, borderless, decentralized open form of money.

Traditional financial institutions are conservative and one of the least innovative industries.

But with Bitcoin and crypto more generally there is nothing stopping anyone from building new financial products.

The applications built on this new system of financial rails will grow exponentially over the coming years.

In 20 years time blockchain technology will be a core part of how financial services work⁷.

Looking back we will look upon the current system like how the automobile industry looks upon the horse buggy.

If you want to understand the potential of this technology I recommend you start reading my [Crypto 101 guide](#) on how to learn about crypto.

Article Resources

At ElementalCrypto we adhere to the highest standards when it comes to our editorial guidelines. We use original sources such as whitepapers, academic research, books and interview with specialists to compile our data.

1. If you want to understand the mechanics of how the Bitcoin network works: [Bitcoin Explained in the Bitcoin Basics Workshop CBP Prep](#) by Andreas Antonopoulos
2. [Mastering Bitcoin book](#) by Andreas Antonopoulos
3. [Satoshi Nakamoto's white paper](#)
4. A good explanation of [Proof of work](#)
5. [Blockchain 101 – A Visual Demo](#) and [Blockchain 101 – Part 2 – Public / Private Keys and Signing](#) by Anders Brownworth are some of the best explanations of how blocks connect and how the verification process works.
6. [How blockchain works](#): Introduction to Blockchain Technologies, INSEAD, Coursera.
7. Non-technical big picture: [Introduction to Bitcoin: what is Bitcoin and Why does it Matter?](#) by Andreas Antonopoulos

What Is Ethereum and How Does It Work? A Beginner's Guide

In this article, I will walk you through all you need to know about Ethereum. What is Ethereum and how does it work? Why is it so important? Who are the main characters and why is it more important than Bitcoin in some ways?

I will also introduce you to key concepts such as mining, ICOs, smart contracts, and the main characters involved in Ethereum.

After reading this article you will understand everything there is to know about the Ethereum platform.

This article is foundational. As you embark upon your crypto journey you will find that Ethereum is the source of all inspiration. It has played an instrumental role in morphing the crypto space into what it is today.

Table of Contents

1. [What Is Ethereum and How Does It Work?](#)
2. [Back to what Ethereum is](#)
3. [Ether vs. Ethereum: what's the difference?](#)
4. [Ethereum market cap](#)
5. [Token issuance](#)
6. [Initial Coin Offerings](#)
7. [How the Ethereum consensus algorithm works](#)
8. [Why is it called Ether / Ethereum?](#)
9. [Why do some people think Ether is a shitcoin?](#)
10. [What is Ethereum Classic?](#)

11. [Who are the founders and creators of Ethereum?](#)
12. [Ethereum ecosystem projects and copycats](#)
13. [Summing up what Ethereum is and how it works](#)
14. [Up Next](#)

Now pay attention.

What Is Ethereum and How Does It Work?

Ethereum was the first cryptocurrency that successfully used smart contracts and the second-largest cryptocurrency by market capitalization.

When you hear Ethereum you should immediately think of smart contracts. So before exploring Ethereum let's first understand smart contracts.

First: what are smart contracts?

A smart contract simply refers to coding language for "if...then..." statements.

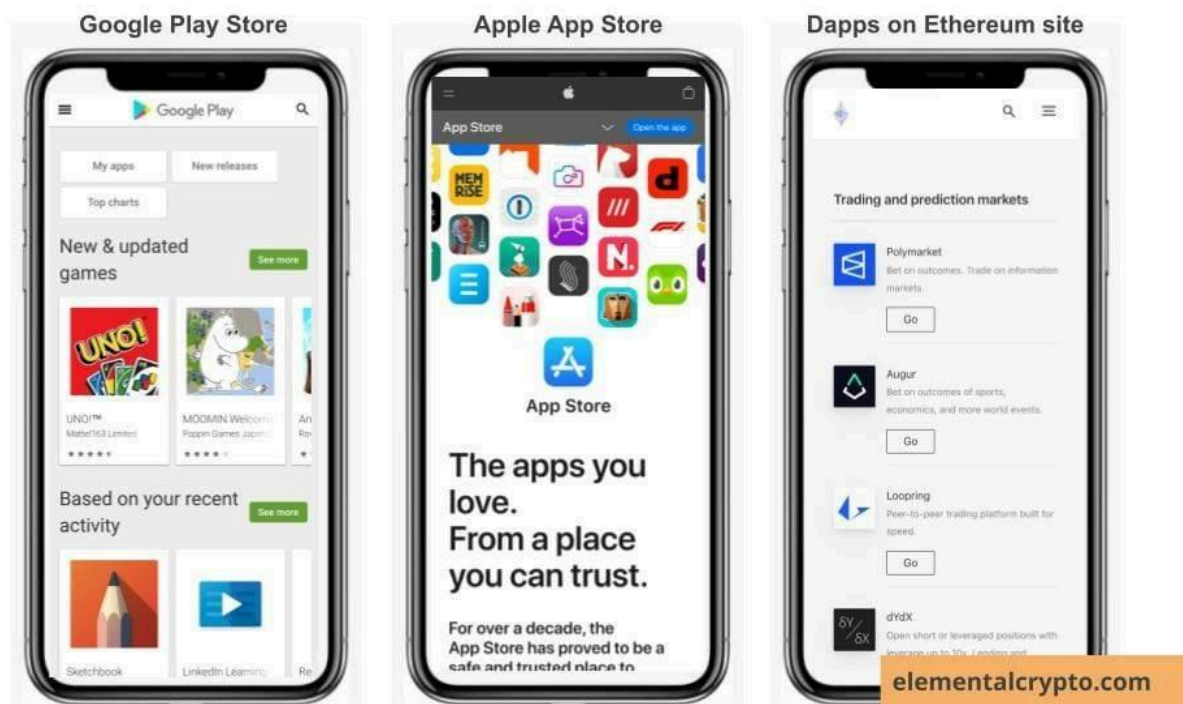
If you ever started a coding course on Python or javascript one of the first things you would learn about are "if... then..." statements.

So, for example, you could write something like: "If the price of bitcoin goes above \$30,000 then sell this user's bitcoin."

Ethereum makes use of these self-executing contracts to turn itself into a platform which other developers can build more things upon. In the coding world, they refer to this as a protocol. Imagine it as an iOS or Android platform of the crypto world that allows any developers to build a decentralized application.

These apps are referred to as “Dapps” by the crypto community. The “d” in Dapps stands for decentralized.

In this context, you will also often hear the term DeFi which stands for decentralized finance.



Dapps on the Ethereum Network are equivalent to apps on Google’s Play Store or Apple’s App Store.

And this is what the hype is about.

Because the smart contracts capabilities that are baked into Ethereum allow developers to build apps that can run on their own and offer financial services and more.

The app could, for example, execute a loan transaction without any intermediation from a human.

Let's see how this loan example would play out.

Imagine you sign up and join an app where you are willing to offer your Bitcoin as collateral to get a loan.

The app could accept your Bitcoin and offer you half its value as a loan. If you did not repay the installment the smart contract would instruct the system to sell part of your crypto. If you did repay in full it would return your bitcoin to you.

You see that with smart contracts it is pretty easy to have an automated system that does not require human intervention. It can simply exist on its own.

Since the launch of the Ethereum network in 2015 over 3,000 Dapps have been launched. Some of the most famous ones are

Uniswap: a decentralized exchange for buying and selling digital assets

Compound: a decentralized lending and borrowing platform

Maker and its **DAI stablecoin**. More on stablecoins another time

For example, imagine a social network with no central authority such as Facebook or Twitter controlling it in the background. Or imagine an Uber-like app with no Uber in the middle taking a cut in fees.

You could decentralize any field that has a gatekeeper or middleman managing the process whether that be a government managing a land registry or an internet company managing email. A decentralized app would purely exercise the smart contract baked into it.

Ether vs. Ethereum: what's the difference?

Ether, denoted as ETH, is the cryptocurrency that powers the Ethereum network.

If you want to launch a Dapp you need to pay in Ether. These transaction fees are known as gas fees in the community. Gas fees incentivize developers to write efficient code that does not use up too much of the Ethereum network's bandwidth.

The more clunky or demanding your app is, the more Ether you need to pay. Similarly, any transaction that is broadcast to the network needs to be verified and hence incurs a fee in Ether.

Who does this Ether go to? Why it goes to a group of developers called validators, who, in a similar fashion to Bitcoin blockchain miners, verify and add new blocks of transactions.



Ethereum miners use servers to provide fast computation to validate transactions. Source: [Wikipedia](#)

A small primer on validators

If I send you 10 ETH then this transaction needs to be verified. How does this system deduct 10 ETH from my account and credit 10 ETH to your account?

Well, these transactions are verified by multiple independent groups of people who use their computers to run the Ethereum Network. They all have to agree that this transaction took place.

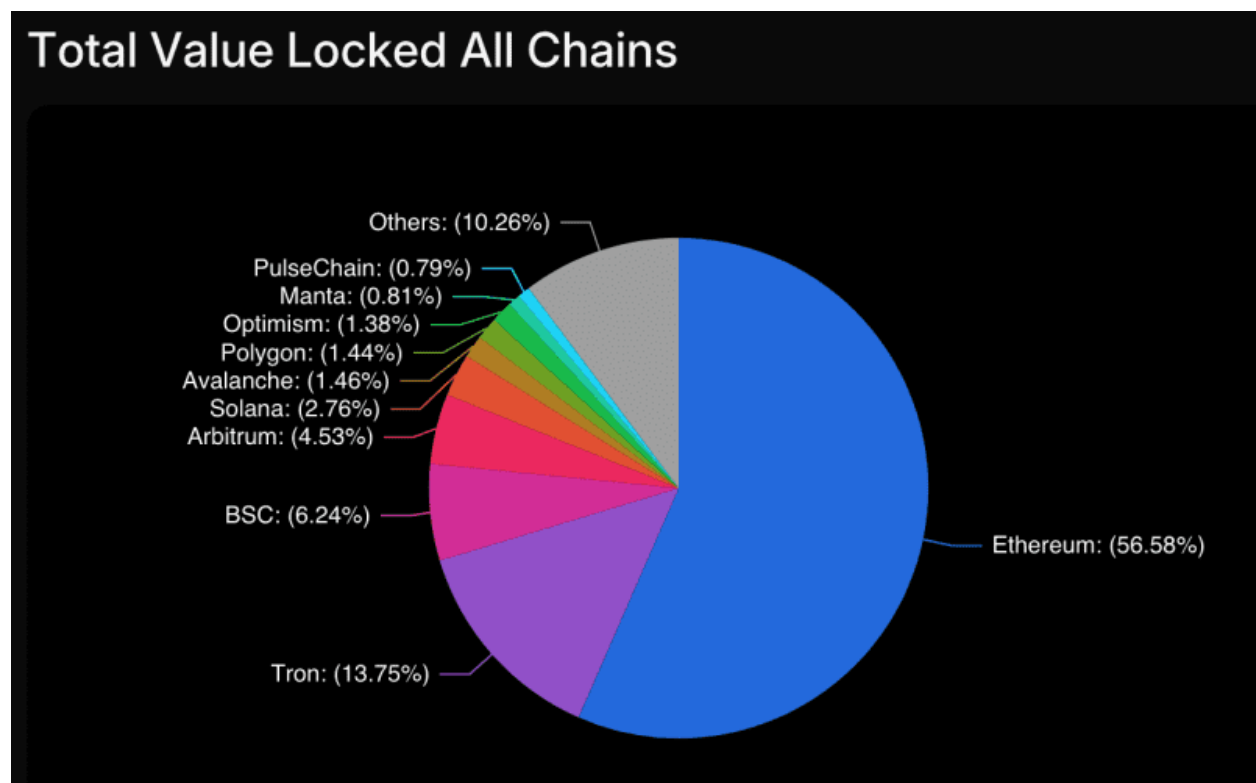
For now, all you need to understand is that developers require rewards for the energy and time they invest in. And the rewards occur in ETH.

Ethereum market cap

Ether is the largest cryptocurrency by market cap after Bitcoin.

Market cap is simply the market price times the number of coins or tokens that are available for the respective cryptocurrency at the time. However, this is not the whole picture.

Ethereum also has the largest number of Dapps on its platform. This means that the value of Ethereum is the value of the Ethereum network plus the value of all the crypto assets built on top of it which is the majority of the crypto economy.



Ethereum accounts for 57% of the total value of crypto assets locked on dApps. Source: defillama.com/chains

Some major competitors to Ethereum have risen such as Cardano, [Polkadot](#), Avalanche, [Cosmos](#), and [Solana](#). All are still in their early stages.

Very often people use Ether and Ethereum interchangeably to refer to the currency.

Token issuance

With the launch of the Ethereum network, it became very easy for developers to mint their own digital currency. There is a protocol in Ethereum called ERC-20 that allows you to do this.

With a few lines of code, a group of developers could issue new ERC-20 tokens, give them a random name, and accept Ether in return for it.

There is also another protocol called ERC-721 which allows you to mint non-fungible tokens. If you want to learn more about NFTs I recommend you read my [deep dive on Ape Coin](#).

Initial Coin Offerings

The ERC-20 protocol allows people to raise funds for their projects through Initial Coin Offerings (ICOs).

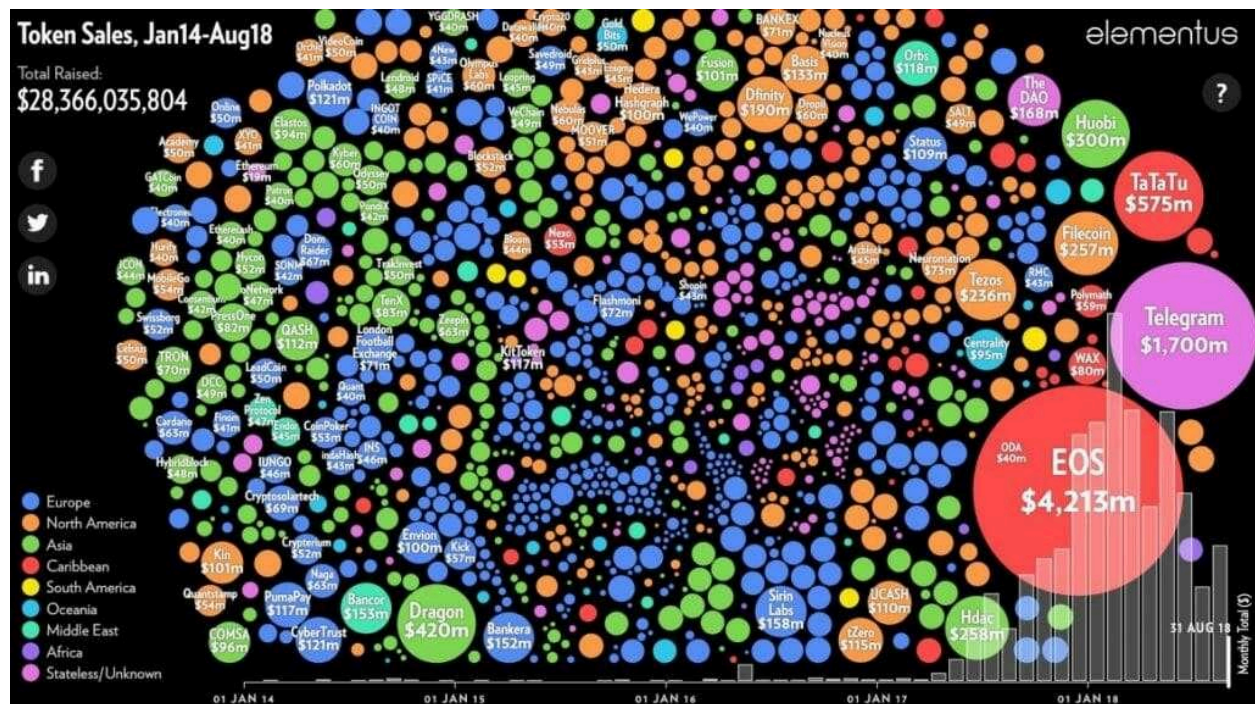
An ICO is a play on words for IPO: Initial Public Offering.

IPOs come from mainstream finance when a company lists shares on the stock market for the first time.

Initial Coin Offerings allowed developers who had written a conceptual white paper of the project they wished to start, to raise capital.

By issuing coins, known as tokens, they could raise capital to fund their project. This way they circumvented the lengthy and costly process of using banks as intermediaries.

ICOs allowed teams of developers to raise capital for projects that were also less fundable via traditional mainstream finance vehicles such as venture capital funds. A lot of the time attracting funds just required a white paper, a sleek website, and some publicity on Reddit and other social media.



Value per coin and total capital raised during the ICO craze 2014-2018. Source: elementus.io

Why people overreacted to ICOs

ICOs were attractive to many people in the crypto community because it was like giving the middle finger to mainstream finance.

It was a step towards the realization of the permission-less self-governed economy they had been trying to create.

Most people however just wanted to become millionaires and fast.

They had seen how Bitcoin and Ether had jumped from a few cents in the early days to thousands of dollars. Now they too wanted to get in early on the next opportunity.

This caused a lot of hype.

Some companies were raising millions in just a few hours. By the end of 2018, ICOs raised more than \$28Bn surpassing total venture capital investment at the time.

The ICO coins were utility tokens in the same sense that you used Ether as gas for running a project on the network. For example, a gaming company might issue tokens that you need to make purchases inside the game.

The token was then able to trade on the market. In contrast to stocks, tokens don't give you the right to own a part of the company.

This allowed them to clear a legal loophole in some countries in that they were not securities and therefore not subject to regulatory restrictions. You could consider them more like arcade or fun fair tokens.

How the Ethereum consensus algorithm works

Proof-of-Work vs. Proof-of-Stake

We already mentioned that for transactions to be validated participants need to be rewarded. These participants are known as miners or validators.

To prove that a transaction is valid miners expend energy to solve complicated algorithms. This is known as Proof of Work and is energy-intensive.

Bitcoin comes under strong criticism by its detractors for its energy usage.

See [What is a bitcoin and how does it work](#) for more on Bitcoin.

To address this issue and scale in a more eco-friendly manner the Ethereum founders proposed an alternative model known as Proof of Stake.

With a Proof-of-Stake consensus algorithm, miners put their own coin holdings up as collateral. The more cryptocurrency a validator stakes, the higher the chance they have of being chosen to create a new block. Rewards are then distributed proportionately to the amount staked by validators.

This requires much less energy consumption.

In September 2022, Ethereum successfully transitioned to a Proof-of-Stake model.

You can participate in Staking

Anyone can delegate their ETH to a validator to be staked. This way they can earn a return on their ETH. If you plan on holding ETH for the long term then this is a good way to earn a yield on your assets.

You can find out more about staking ETH in the following resources

[What does it mean to stake Ethereum](#)

[What is LIDO crypto and How Is it Connected to ETH Staking](#)

[How to Stake Ethereum on Coinbase: A Step-by-Step Guide](#)

Layer 1 vs Layer 2

In addition to making the network more eco-friendly, the founders of Ethereum wanted to make Ethereum process more transactions per minute.

This would lower transaction costs for developers and make the network more competitive against traditional corporate entities such as Visa and Mastercard. One methodology that most Ethereum developers agree on is sharding.

Sharding breaks up a process into smaller components called shards which run in parallel. Ethereum plans to run 64 shards. While we don't need to understand the technical details it is important to note that this solution is planned to be built into the Ethereum blockchain itself.

It is thus known as a layer 1 solution.

Now that Proof-of-Stake is complete, once sharding is complete, Ethereum will be operating an entirely new blockchain known as Ethereum 2.0.

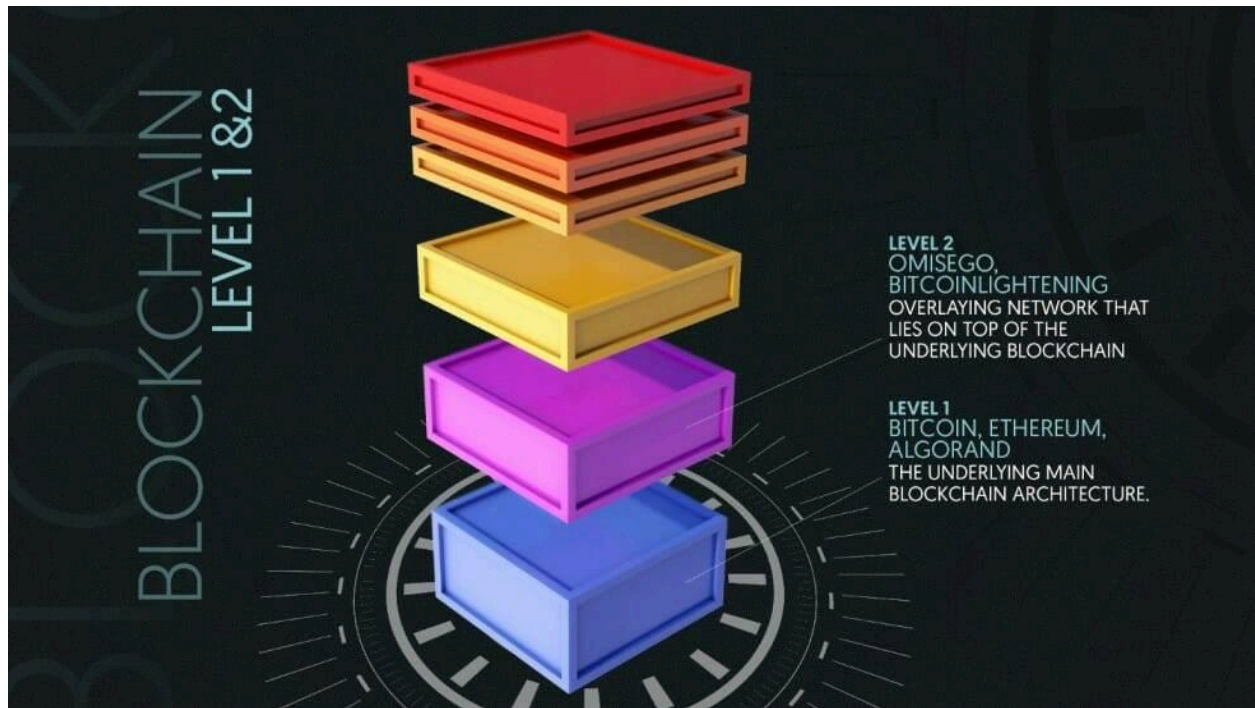
The team believes it will be much more efficient compared to the previous version.

In the meantime, a host of separate entities are building a second layer. These are not part of the core base-level protocol but live on top of Ethereum to scale it.

A [layer 2](#) solution would run transactions on its own blockchain. Subsequently, it would hook up to Ethereum to validate batches of transactions together.

You may have come across the term optimistic rollups or zero-knowledge rollups that do precisely this.

Check out [Polygon MATIC](#) and [Arbitrum](#) for more.



Layer 2 protocols bundle transactions separately before passing them on to the Ethereum Layer 1 blockchain network. Source: coincu.com

EIP-1559 and its Significance for Ethereum

EIP stands for Ethereum Improvement Proposal.

The community voted in favor of EIP-1559 in August 2021.

It was significant because it reduced the amount of ETH in supply by burning a large part of the gas fees. It also simplified the process for paying gas fees thus making them cheaper for the average user.

Before EIP-1559 gas fees operated on an auction basis. The highest bidder would win the auction and their transaction would go through.

This led to a lot of very large ETH owners, known as whales, being able to dominate transactions. It also pushed gas fees up. The new algorithm for gas prices estimates a base fee.

You can then add a priority fee which is kind of like a tip to make your transaction go through faster. The base fee gets burned while tips still accrue to the validators.

When I say the base fee gets burned I mean it vanishes and no longer exists thus reducing the amount of Ethereum in circulation. While Ethereum does not have a fixed amount of ETH like Bitcoin does burning ETH is thought to be good for its price.

Why is it called Ether / Ethereum?

Vitalik chanced upon the term Ether while browsing online for a name for his decentralized platform. He came across a now disproved 19th-century theory that the air is permeated by a substance called Ether.

He liked the name (it does sound cool) and coined the term Ethereum.

Why do some people think Ether is a shitcoin?

Hardcore Bitcoin believers call Ether and other alt-coins “shitcoins”.

These “bitcoin maximalists” believe that Bitcoin is the only coin worth focusing on since there is a fixed number of bitcoins that can ever exist. This is not the case with Ether.

Because the amount of Ether is not fixed, more could be created in the future thus putting downward pressure on its price.

Another criticism of Ether is that its strength is also its weakness.

Apps on the Ethereum network are immutable. Once developers launch them on the network no one can tamper with them.

The fact that once launched, dApps are immutable is a headache for anyone who needs to change something later. Basically, it cannot be done.

In real life, with central management, there is some flexibility built into the system. You can always escalate things to court or adapt to exceptions.

A smart contract, however, will always execute the contract with no exceptions. Hence, before launching an app, you need to think of all the extenuating circumstances that might occur.

Another criticism is that Dapps needs to appeal to a wider audience beyond geeks. There needs to be someone working on them to improve the user experience such as the packaging and sign-up process.

Hence, dApps are never 100% dis-intermediated. There will always need to be some entity overseeing the process.

What is Ethereum Classic?

Before we go to Ethereum classic we need to understand the concept of forking.

Forking

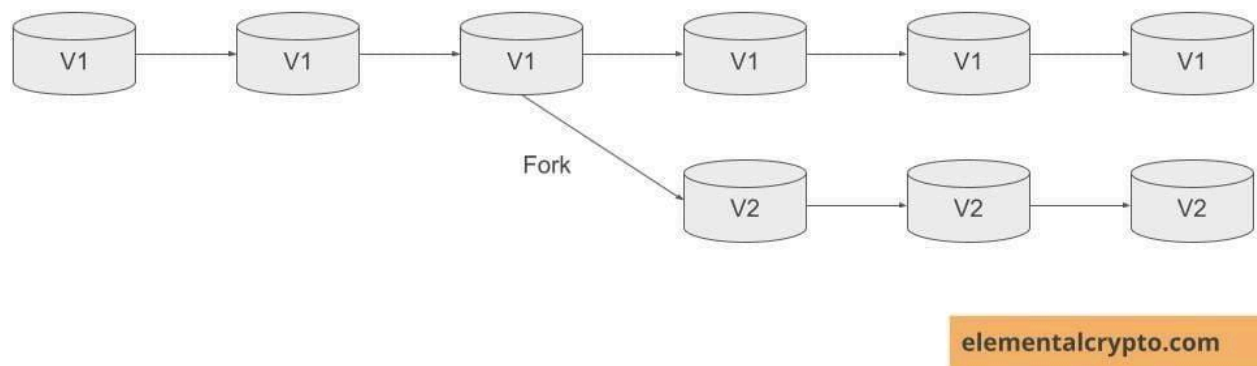
Coders will often host their code on platforms where others can copy and alter or improve it.

So, for example, coder A may write version 1 of a program, and then someone might copy this and branch out to build version 2.

Going forward version 1 still exists and may continue to develop while at the same time, version 2 continues to grow, possibly morphing into something completely different.

So it's like the programs were both the same until there was a fork in the road and each went their own separate ways.

Similarly, cryptocurrencies can also have forks.



How forking on Ethereum works

Back to Ethereum Classic

Ethereum Classic is version 1 of Ethereum i.e. the original version. In the early days, a major crisis caused a hard fork.

During the early days of Ethereum, there was a group of developers who wanted to launch a decentralized fund. They called this protocol a Decentralized Autonomous Organization (DAO) and the fund's name was aptly named TheDAO.

This DAO was the inspiration for many of the decentralized autonomous organizations in existence today.

Participants would send Ether to the fund and the smart contract would allocate them a proportional number of tokens to vote with.

Token holders would then submit proposals or could vote on projects proposed by others. The smart contract would direct the Ether to the winning proposal.

Initially, the creators of the fund expected to raise about \$20 million. However, people in the crypto community were so excited by the idea of decentralized governance that they ended up raising more than \$70Mn.

TheDAO Hack

Soon after raising the money someone managed to hack the fund and started bleeding it of money.

In her book, "[The Infinite Machine](#)", Camilla Russo goes into excellent detail about how the hacker and the Ethereum community were playing a game of cat and mouse.

To cut a long story short the hacker won. In order to save people's money and return it to them and in order to punish the hacker, the community decided to create a fork.

This is kind of like saying: "ok everyone, let's cancel the old path and start afresh on this new path. This way the real Ether is on the new fork and the hacker has worthless old Ether".

Most people accepted this fork.

However, to everyone's surprise, there ended up being still a minority that continued to verify transactions on the old fork. This is a

community of people who believe that Ethereum is immutable and no one should change the rules (create a fork) no matter what. Otherwise, the whole idea of decentralization is a waste.

The old fork, named Ethereum Classic, still retains some value though nowhere near that of Ether. Hence the hacker didn't completely lose as they retained Ethereum Classic tokens.

Who are the founders and creators of Ethereum?

When Vitalik Buterin came up with the concept and wrote the white paper on Ethereum there were 7 other founders who joined him to build Ethereum.

Apart from Vitalik, there are two more people you need to know about. Both play an important role in the ecosystem.



The founders of Ethereum. I'm missing Jeffrey Wilcke. Source:

[Medium.com](#)

1. **Gavin Wood:** allegedly wrote the code for Ethereum in C++ in one night. After reading Vitalik's whitepaper he wrote a "yellow paper" with all the technical details of how the Ethereum network

could be built and designed Ethereum's programming language called solidity. He is now following his own path by developing a new protocol called Polkadot. Polkadot is trying to be the protocol of protocols. So you could use any other protocol on this platform to make Dapps, even Ethereum. You can read a [simple explanation of Polkadot](#) here

2. **Charles Hoskinson:** Appointed himself as CEO when the Ethereum project got started. Charles wanted to run a for-profit model that raised money from venture capital funds. His vision clashed with that of the rest of the team who wanted a non-profit status. Charles ended up leaving to set up a blockchain called Cardano. Cardano is unique in that it uses peer reviewers (just like an academic project would) to progress on its code.

Summary of the rest of the founders.

3. **Mihai Alisie:** was Vitalik's co-founder of Bitcoin magazine. He helped set up the team in Switzerland and dealt with a lot of the legal aspects. He is now focusing on building a Social network Dapp on Ethereum called Akasha.
4. **Anthony Di Iorio:** was one of the first co-founders of Ethereum but later moved on to follow his own path and founded Decentral, a digital wallet.
5. **Amir Chetrit:** a US-Israeli who met Vitalik while working on Colored Coins. This was a project to tokenize stocks and other assets on the Bitcoin network. Vitalik invited him to join Ethereum as a founder. After not being able to contribute to the code development of the project he stepped down. He currently works on various crypto projects but shies away from publicity.
6. **Joseph Lubin:** with a degree in computer science from Princeton and a career in the software and music production industry Joseph was the most experienced team member.

7. **Jeffrey Wilcke**: was so excited about the Ethereum white-paper when he read it that he started writing the code in Google Go code. Later, he met Gavin Wood who had done the same in C++ code. They found that it was good to have a second version as a backup. He quit after the DAO hack and after having a baby and has since set up a gaming company.

Ethereum ecosystem projects and copycats

Ethereum is the original gangster. The “OG” in crypto-twitter speak. From there on you have two major movements.

The first reaction to Ethereum was the development of what we call alt-coins. These were other alternative projects that looked at Ethereum and thought, “Hang on we can do a faster, meaner, better than Ethereum. Everyone, get on the super-duper new shiny thing that I am building”. Here are some major altcoin competitors to Ethereum:

What is Solana

What is Polkadot

What is Fantom crypto

What is Cosmos crypto

The second branch that emerged is what we call DeFi (Decentralized Finance) and Web3. The most famous and usually the largest Dapps to date are built on Ethereum. Some of these are:

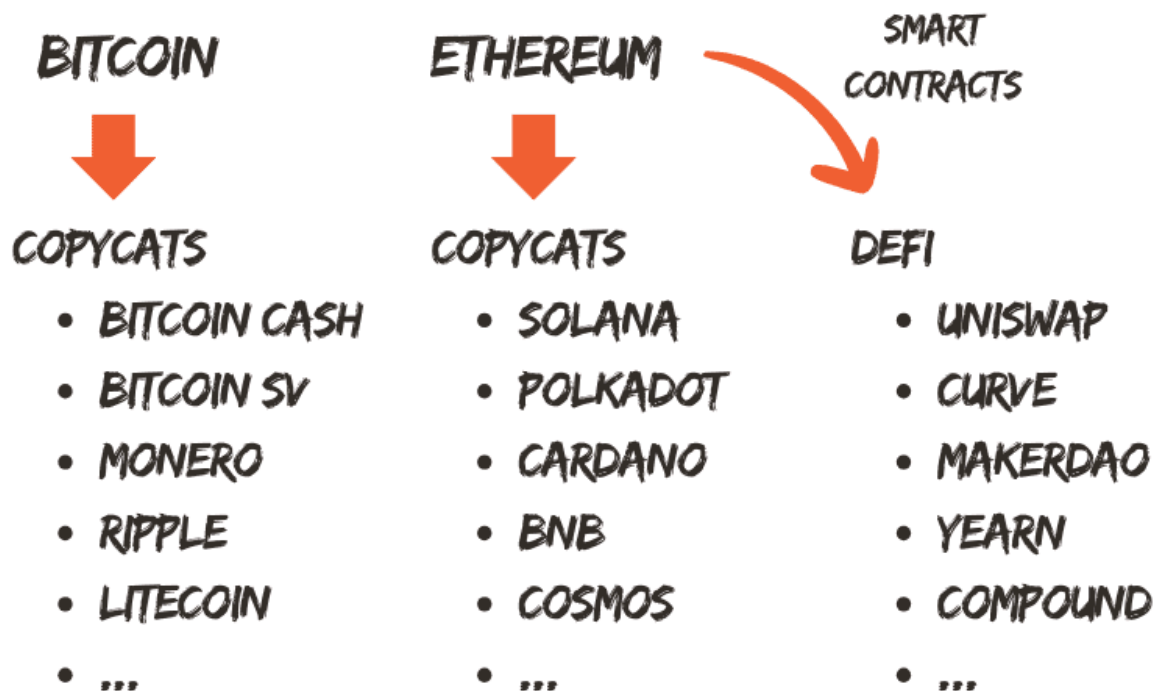
What is DAI crypto

What is Uniswap

What is Olympus DAO

What is Compound crypto
What is Yearn Finance
What is Curve Finance

THE BIRTH OF A CRYPTO ECOSYSTEM



[ELEMENTALCRYPTO.COM](https://elementalcrypto.com)

Summing up what Ethereum is and how it works

All in all, Ethereum is the single most important cryptocurrency.

It was the first to introduce smart contracts and its ecosystem of decentralized apps has scaled massively. This scale has led to sustained demand for ETH.

Despite the presence of multiple alternative layer 1 solutions and despite the high gas fees users have to pay the Ethereum ecosystem continues to grow.

While there are other blockchains that can process transactions faster and cheaper, Ethereum maximalists believe that Ethereum's network effects are so large that it will continue to dominate the crypto market.

Like I said there are some very cool projects that have built products on Ethereum. What's mind-blowing to me is that despite the chaos in the market with multiple crypto projects exploding the core DeFi protocols are still functioning just fine.

The first one you should read about is [Compound a borrowing and lending platform](#) that introduced some mighty innovations in finance.

If you are completely new to crypto then check my [crypto starting guide](#). Have fun!

If you don't want to waste time then you can take my [crash course in crypto](#). It distills over seven years of crypto experience into a few hours of learning, designed to help users understand key concepts, technology, and the overall crypto ecosystem. The course covers topics such as how different cryptocurrencies work, the basics of trading, and how to keep crypto assets safe.