TUTORIAL ONE

CRYPTO 101 BEGINNERS

What we'll cover in this Tutorial:

1. Creation – 2008 – 2009 (Satoshi Nakamoto – Bitcoin)
2. Cryptocurrency – What is it?
3. Fiat Money & Cryptocurrency – Understanding the difference?
4. Public & Private Keys – What are they?
5. Blockchain – What is it, and why is it important?
6. What is Mining? – How does it work?
7. Coin v Tokens
8. Beginners Tips

1. Creation – 2007/2008 (Satoshi Nakamoto – Bitcoin)

The original Cryptocurrency – Bitcoin was created by someone called Satoshi Nakamoto. Satoshi' vision from his whitepaper was to create - "A purely peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another ***without going through a financial institution***"

Nakamoto is has been credited with the creation of Bitcoin and released a Whitepaper called **Bitcoin: A Peer-to-Peer Electronic Cash System** which has been credited with solving the problem of double spending electronic money. Double spending occurs when someone tries to spend the same money more than once (Yes…people do try to do that!). Satoshi managed to solve this problem by creating a network where multiple computers (Miners) had to agree on the same information before committing that information to a Blockchain (a 'chain' of databases linked together)

In 2008 this whitepaper started conversations amongst cryptographers as to whether a peer to peer (person to person) electronic network could actually work, as groups took this whitepaper and started to created models which evolved into test networks, attempting to prove the validity of the whitepaper. The first ever commercial Bitcoin transaction occurred in 2009 when Satoshi sent 10 Bitcoins to another cryptographer. In 2010 the first Bitcoin was spent buying a pizza which cost $10,000 Bitcoins (Roughly $40 at the time…now that Pizza cost would be **one billion, one hundred eighty-five million dollars**)

Throughout its history Bitcoin has faced many regulatory challenges from governments around the world primarily from its perceived threat to Fiat currency (paper money) and the fact that Bitcoin is not owned by any one nation. An attraction for many people.

Whilst Bitcoin was the first, it is not the only Cryptocurrency to make its mark with the popularly coined phrase 'Altcoin' being one that you will hear a lot. Altcoins are coins that are not Bitcoin,

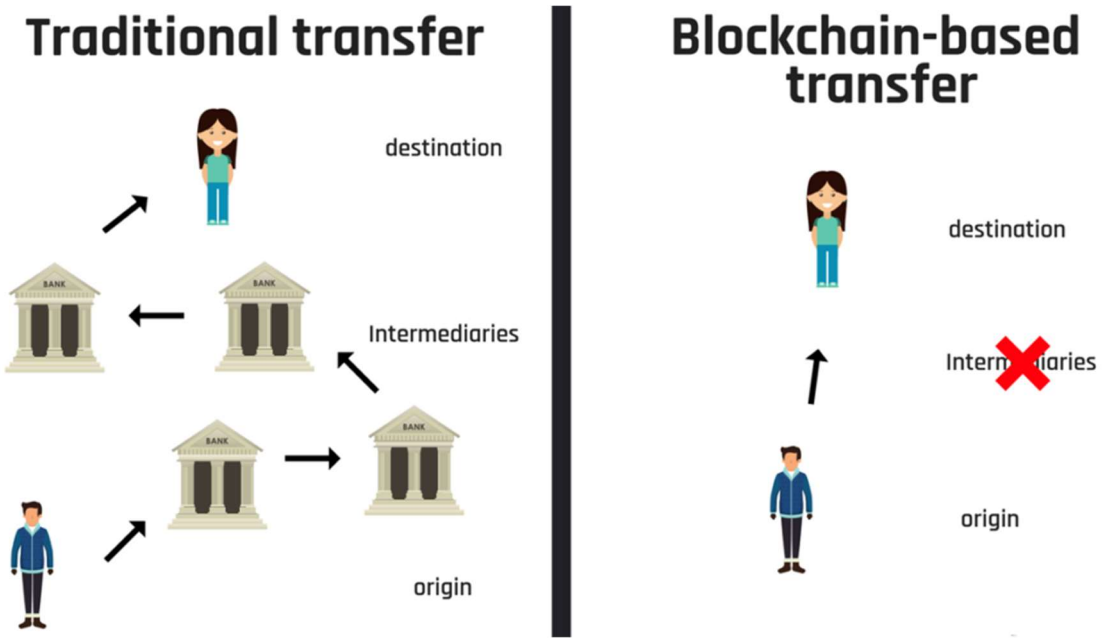
although Ethereum could perhaps lay claim as a founding coin, considering that most coins are 'forked' from these two. The main methods how transactions are verified are:

1. **Proof of Work** - Proof of work is provided by sending the information in a block through an algorithm. The 'Miner' proves they have done the work through this algorithm, which is then verified by other Miners, and they get paid
2. **Proof of Stake** – Proof of stake require 'Validators' to hold and stake tokens for the privilege of earning transaction fees. I.e. They get paid

There are literally tens of thousands of Altcoins in the Cryptocurrency space, with a majority having little or no utility value. OPINION: In many cases their creators have issued these coins or tokens in the hope of creating a lot of interest and value, whereby they as the principal coin owners, can sell off these coins at a premium (Often then exiting) This is commonly called a 'Pump and Dump'. If you are interested in any coin then it is suggested:

1. You make sure that you have read any whitepaper describing how the coin works, it's benefits etc
2. Review the creators themselves, check out their backgrounds and where possible confirm any financial/company documents available
3. Verify how you can convert any coins or tokens to either other coins i.e. Bitcoin or to Fiat currency. NOTE: There is little value to you in owning a coin or token if you have no way of converting that to something that you can use! You'll end up owning a coin that has no other value than the value its creator nominates (even though the creators of the coin may seek to persuade you otherwise.)

It will help you greatly if you understand that due to its decentralised nature, cryptocurrencies do not work like banks, in that there are no intermediaries. If you lose your cryptocurrency on a blockchain then it is literally gone. With traditional banks there is a centralised process in play. Their software running across their terminals with their rules. On a blockchain there can be literally thousands of different databases in play and no one single intermediary.

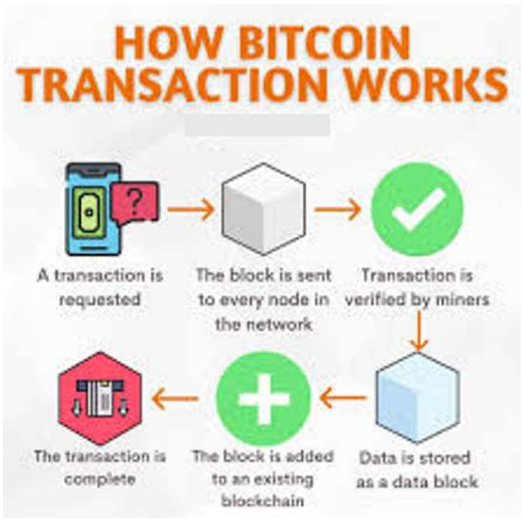


2. Cryptocurrency – What is it?

Here is the standard definition that you will get from the Internet. ***"A digital currency in which transactions are verified and records maintained by a 2nd system using cryptography, rather than by a centralised authority."*** One of the common issues you will find that some financial commentators have with cryptocurrency is their argument that Crypto is backed by nothing. Further, many state that it has few of the 6 common properties of money which are:

A simple search on Internet will reveal that there are literally hundreds of occasions that mainstream media has declared Bitcoin to be dead, only for Bitcoin to resurrect itself. Cryptocurrencies initially suffered this battering from mainstream media. Over the last several years there has been steady and consistent opposition from many governments to cryptocurrencies, with numerous jurisdictions creating legislation to hamper the growth of cryptocurrency withing their boundaries.

Cryptocurrency is a digital payment system that doesn't rely on banks to verify transactions. It's a peer-to-peer system that can enable anyone anywhere to send and receive payments. Instead of being physical money carried around and exchanged in the real world, cryptocurrency payments exist purely as digital entries to an online database describing specific transactions. When you transfer cryptocurrency funds, the transactions are recorded in a public ledger.



Suppose Bob wants to transfer one unit of cryptocurrency to John. Bob starts the transaction by sending an electronic message with his instructions to the network (generally via an Exchange – more on that later) where all users can see the message. Bob's transaction is one of a number of transactions that have recently been sent. Since the system is not instantaneous, the transaction sits with a group of other recent transactions waiting to be compiled into a block (which is just a group of the most recent transactions). The information from the block is turned into a cryptographic code and miners compete to solve the code to add the new block of transactions to the blockchain.

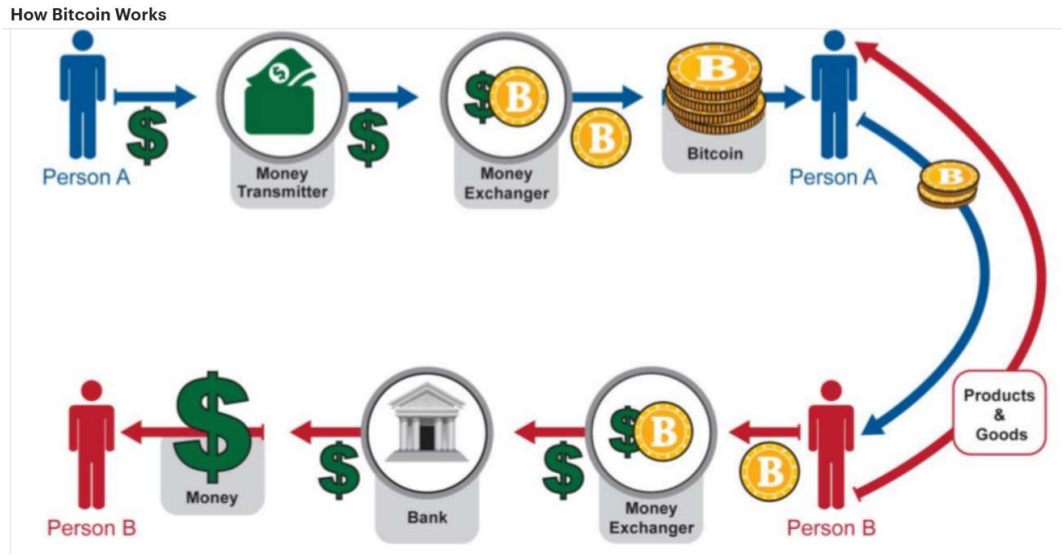
Once a miner successfully solves the code, other users of the network check the solution and reach an agreement that it is valid. The new block of transactions is added to the end of the blockchain, and Bob's transaction is confirmed. (This confirmation is not instant as it takes time for six blocks of transactions to be processed so that users can be certain that their transaction has been successful.)

If you're new to Cryptocurrency then the challenge for you may in understanding how this 'digital' network works and has value compared to the existing Fiat (Paper based) monetary system. In order to establish 'value' our current Fiat based system assigns a monetary value to an item, and a willing buyer and seller can then agree or disagree and complete or chose not to complete that transaction. We're using Bitcoin as the example here as it is the 'Grand Daddy' of Cryptocurrencies – but you could just as easily use Ethereum or Ripple as other examples as they have been ascribed a dollar value.

So, in order to reach consensus on this value its important to use the existing system to establish that value. Even 20 years ago it would have been unthinkable to value a Cryptocurrency in Fiat terms as it was not backed by either government/s or a physical asset like gold. Cryptocurrencies have varying uses and we will discuss Coins v Tokens in this Tutorial as a good starting point on your Crypto journey.

Digitisation of Money is nothing new to the modern world, with most Banks providing electronic payments for many years and with an associated declining use of cash (for a number of reasons). Electronic money that doesn't belong to a centralised authority though, effectively belonging to the people of the world, is something that is new, something uncontrollable, something that has value in a world where Fiat currency is being printed at increasing rates and with declining value.

Cryptocurrencies in general seek to arrest this erosion of value, by limiting their number and increasing demand. We'll use the example of Bitcoin (The original cryptocurrency Blockchain) in the following graphic to get a better understanding of that.

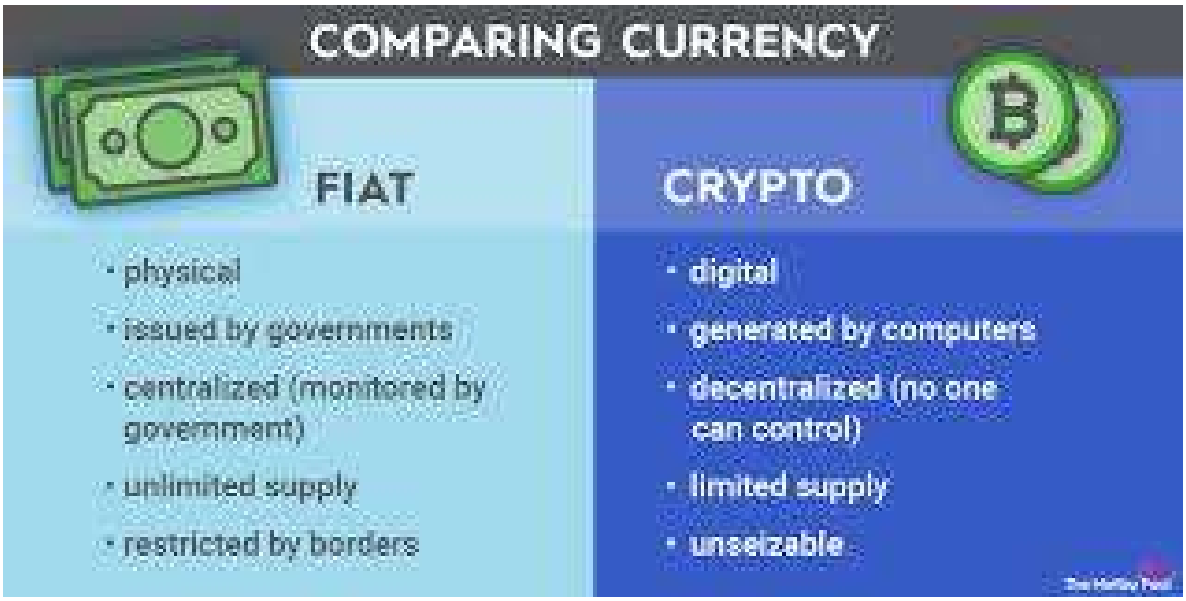


3. Fiat Money & Cryptocurrency – Understanding the difference?

Is Cryptocurrency money? Money/Currency only really has value if everybody accepts that it does. As an example, if you took a $50 note and stripped it of its ink and printed value…what would you have? A piece of paper. That note in your pocket (should you have any) only bears that described value because governments and people agree that it does. Cryptocurrency is no different. Bitcoin only has its current value because people agree that it does, and it is a scarce asset. With 21 million being the maximum amount available there is no opportunity to print more, as is the case for Fiat currency.

When something is scarce and desirable its price increases, with the reverse also applying. If everybody has something then it's easy to get and had less value.

Fiat Currency - (Latin Meaning of Fiat - "it shall be" or "let it be done.")



Fiat Currency is the paper money that governments issue on 'Trust' that they will back its value. Prior to 1972 currencies were generally linked to a 'gold' standard where countries would maintain an identical amount of physical gold that could technically be redeemed on presentation of a fiat currency.

Modern governments however, decided to remove this link opening the door to the potential to printing unlimited fiat currency. The difference between Fiat and Nearly all Cryptocurrencies is that Cryptocurrencies have a finite number of coins or tokens which negates the inflationary aspect one gets from printing more Fiat currency.

But surely most modern money is digital anyway? Whilst this is true, and the physical use of cash has reduced over the past decade due to things like pandemics and the attempt by banks in general to reduce the physical costs of holding and processing cash there are subtle and not so subtle differences between the 'electronic' versions of sending and receiving currencies.

We are all familiar with the use of paper money...we use it every day, but there are some limitations to Fiat currency that you may want to consider:

- **Lack of intrinsic value**

Fiat currencies don't have intrinsic value, so their value can fall quickly if the government's backing or public confidence falters.

- **Inflation**

Governments can print unlimited amounts of fiat money, which can lead to inflation or hyperinflation.

- **Store of value**

Gold has been a reliable store of value for thousands of years, even when fiat has collapsed.

- **Global acceptance**

Gold is universally recognized and accepted, making it a stable medium of exchange during economic crises. Fiat currencies are issued and regulated by governments, while Bitcoin operates on a decentralized blockchain network.

Modern governments continue to print Fiat currencies in an attempt to balance their books. For example, the US dollar, the reserve currency of most of the world, has depreciated around 90% over the past 100 years. (You can prove this yourself by using an inflation calculator). That is nothing of course in comparison to the hyperinflation seen in recent times when considering countries like Zimbabwe or Argentina, where wheelbarrows of Fiat currency were needed to purchase a loaf of bread.

Aside from the fact that Fiat currency is literally backed by the issuer word (Not gold as it used to be) the different between Fiat and Cryptocurrencies is that one has unlimited supply, and one limited – making Fiat inflationary and Cryptocurrencies deflationary – in most instances.

4. Public and Private Keys – What are they?

Getting your head around the difference between Public and Private keys is very important in Cryptography. The Public one is like a security box at your local bank. You want to go down and store something there and lock it away, then you will need to have made that arrangement with your local bank. (In the Crypto space an Exchange provides this service -more on that in another Tutorial).

Your security box is in a place where the bank takes appropriate measures to protect whatever you have stored there. Same deal with Crypto. In a bank your box will be identified by a number…same in Crypto, but it will be a much bigger number! The number of your security box is your "Public Key" Not everyone can just walk into the bank, go to the security area and take a key that unlocks your box. You would be pretty unhappy with that.

Enter the Private Key – Since no one is looking after your decentralised Crypto it's important that your private key is virtually impossible to crack. For example, the probability of guessing a valid Bitcoin private key is 1 in 2^{256}' Lose the Private key and you lose that security box…it's that simple. If you search the internet you'll find countless examples of people who have either through bad luck or inattention, lost their private keys and are no longer able to access their Crypto. In some cases, many millions of dollars.

Once you've gone through the process of registering on an Exchange and downloaded a Wallet (We have another Tutorial on this) then any Crypto you buy will have a public and private key. They look like the following examples:

PUBLIC KEY - 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

PRIVATE KEY - 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

The Public and Private keys work in harmony as the private key is used to validate the public key when it is sent over the blockchain. These keys are generated randomly using blockchain specific code.

4. Blockchain – What is it, and why is it important?

Here's a common definition of Blockchain, ***"Blockchain technology, also known as Distributed Ledger Technology (DLT), is a secure way to store and share information across a network of computers. It's a digital ledger that records transactions in blocks that are linked together in a chain."*** Which of course is correct, but why don't we break it down a bit and take out as much technical jargon as possible. Let's take the 'block' concept and imagine we're going to build a house with that brick – we're going to turn that brick into a house!

Step One when we want to record a crypto transaction is to create that Brick Block. The software on the Blockchain will give that brick and address (A cryptographic one)

When you send your Bitcoin to the network you receive a Public Address:

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

And a Private Address (Your Key)

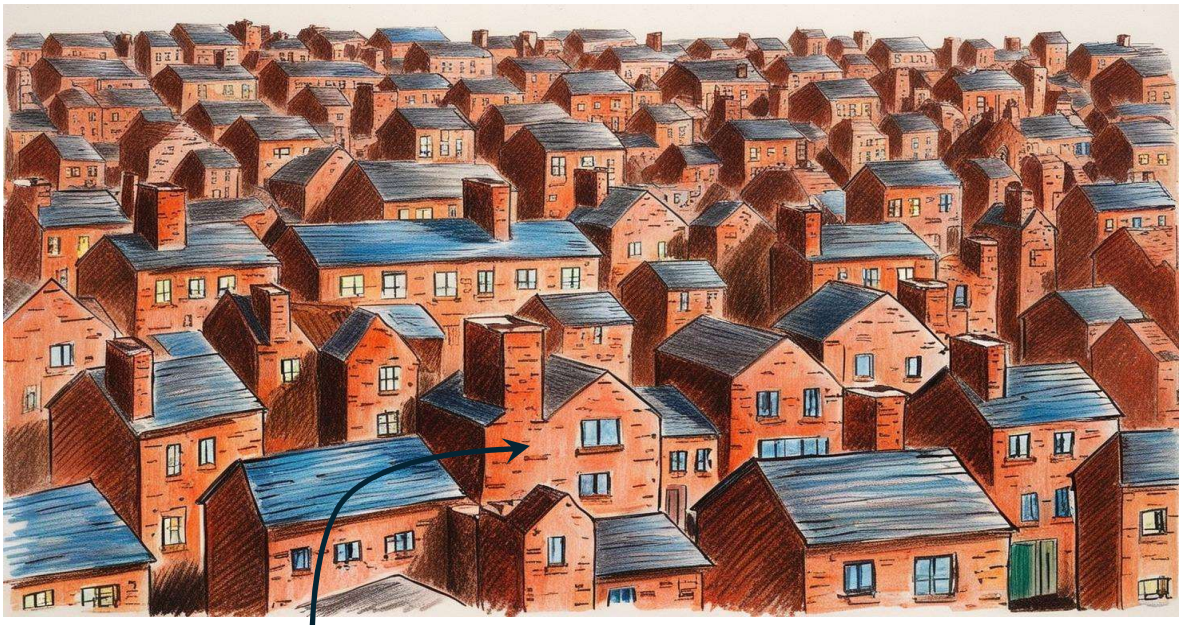
3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

A 'Miner' takes this transaction and adds it to a 'Block'. When sufficient blocks are compiled together by the Miner and Bitcoin' equation is solved, it gets 'cemented' into the block.

Let's Imagine the Block is a house. The Miner is in effect is a builder, and the builder completes the house. (A completed Block!)

That house then becomes part of a new subdivision

That subdivision becomes part of a global network of subdivisions – in effect a 'Blockchain' of completed houses.

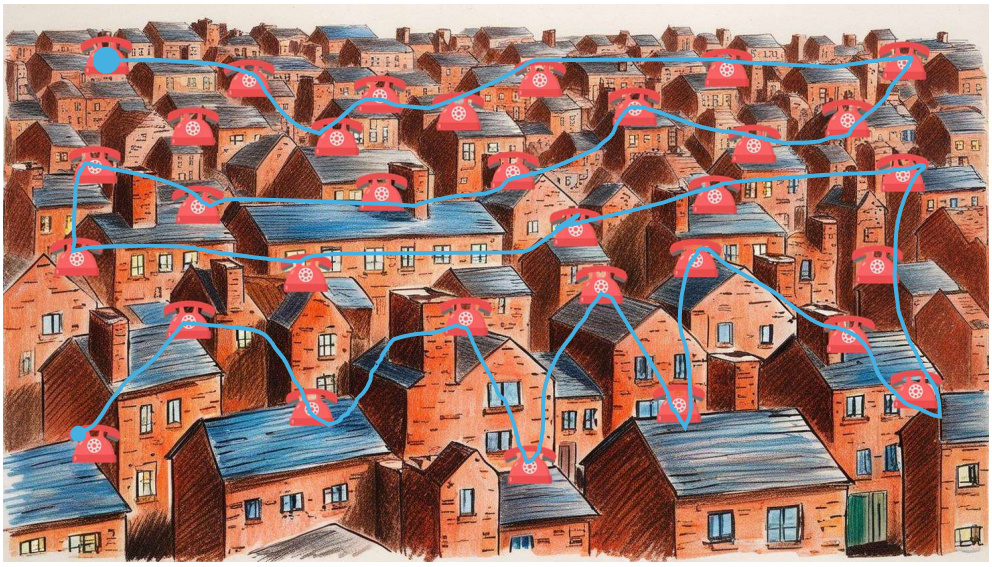


Every brick in each of these houses has its own unique public and private address

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

Now…to get your head around Blockchains and how they work, imagine every house in our global network of subdivisions has a **Telephone in it.**

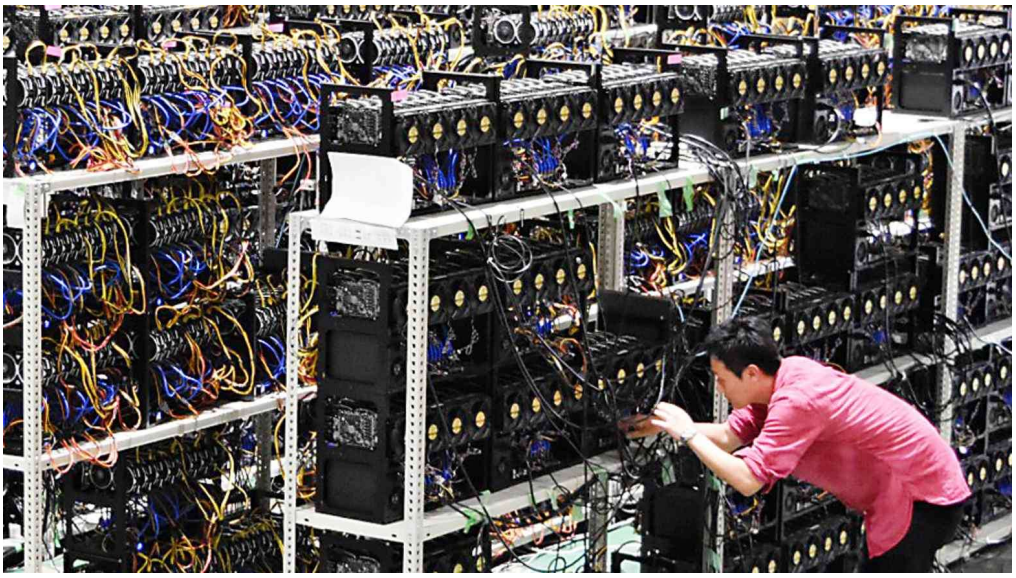


And…all of those telephones are calling each other all the time and sharing the numbers on their bricks and letting each other know when a NEW house and its bricks join! Blockchain!

5. What is Mining? – How does it work?

Crypto mining is a process blockchain networks, like Bitcoin other cryptocurrencies, use to finalize transactions. It's called mining because this process also releases new coins into circulation. Put simply, crypto mining is really just problem solving with a monetary incentive—proof of work. You need a lot of computing power to do it.

Crypto miners make sure each transaction is legitimate. Traditional banks do this behind the scenes and transactions can take days to fully process. Crypto mining verifies transactions within minutes and makes them visible for everyone to see. The first miner to find the solution to the problem receives bitcoins as a reward. When a transaction is made between wallets, the addresses and amounts are entered into a block on the blockchain.



There is a lot of capital investment made by not just individuals but large companies in many cases that are prepared to invest in order to be the successful 'Miner' and therefore the recipient of brand-new Bitcoin. With the escalating price of Bitcoin in particular it has become commercially viable in many cases for these Miners to make these sorts of investments.

But what about the Power? Much has been made of the power consumption attributed to Cryptocurrency Miners by mainstream media. Does such a large amount of computing power add additional burden to the worlds power requirements? Bitcoin mining's energy consumption accounts for **0.6%** of the world's total electricity use. Many Miners are now also seeking alternative power provision via **Hydropower**: 23.12% of Bitcoin miners use hydropower, **Wind**: 13.98% of Bitcoin miners use wind energy

6. Coin v Tokens

Here's a general description of the difference between Coins and Tokens. ***"Coins are digital assets that operate on their own independent blockchain. Tokens are digital assets that operate on an existing blockchain network. While coins primarily function as a medium of exchange, tokens aim to offer a wider range of functionalities within a specific project's ecosystem".***

If you're new to Cryptocurrencies then it's important that you understand the difference between coins and tokens:

- Cryptocurrency coins are digital assets that have their ***own blockchain***. Tokens, on the other hand, are digital assets that ***rely on another*** blockchain.
- Coins are often used as a store of value, while tokens are used to ***power*** decentralized applications.
- The price of a coin is often driven by demand for the coin as a ***store of value***, while the price of a token is often driven by demand for the ***underlying blockchain***

The best two examples of Coins in Cryptocurrency are Bitcoin and Ethereum coins, both operating on their own Blockchain. Coins function as a form of money, while tokens can be used for a variety of purposes. Tokens are created on top of existing chains (Usually Ethereum).

A key feature of coins is that they are designed to be used as a medium of exchange. That means you can use them to purchase goods and services just like any other currency. In addition to being used as a payment method or speculated upon. That is, you can buy coins in the hopes that their price will go up to sell them at a profit.

If Bitcoin is your principal focus, there are growing supplies of Bitcoin ATM machines appearing in most countries around the world (Check out if there are any near you). At these ATM (Automated Telling Machine) you can buy Bitcoin using a credit/debit card. Funds can be sent to an account or dispensed as a QR code (effectively a paper wallet). Some Bitcoin ATMs allow you to scan a Bitcoin private address - as a QR code - and converted to Fiat for withdrawal.

Stablecoins are slightly different in their approach to value and how they are 'pegged'. Stablecoins are digital assets that are designed to maintain a stable price over time. They are often pegged to fiat currency, such as the US dollar, and backed by collateral. Stablecoins have become an integrated part of the Cryptocurrency marketplace as they are generally not subject to the wild fluctuations you will experience with coins that derive their value from the supply and demand of the day. So lack of volatility is a major bonus within Stablecoins.

Stablecoins usually generate revenue by charging transaction fees when users buy, sell, or trade them on exchanges. Stablecoins are often centralized, which means that they are controlled by a central authority. This centralization can be a disadvantage, as it can make stablecoins more vulnerable to manipulation and hacking.

Tokens can be issued through initial coin offerings (ICOs). During these events, investors purchase tokens using established cryptocurrencies like Bitcoin or Ethereum. Once issued, tokens can be transferred between participants on the blockchain network.

Coins	Tokens
Primary function is to be used as a digital currency or store of value	Diverse range of functions, from representing ownership to enabling access to services
Self-sufficient networks built on independent blockchains	Reliant upon the infrastructure of existing blockchain platforms
Gain value based on their own scarcity, utility and adoption	Derive value from the success of projects upon the network in which they operate
Can be transferred between wallets	Requires wallet compatibility with the platform they operate on

If you want to create your own Cryptocurrency there are multiple options:

1. Create your own blockchain and native cryptocurrency.
2. Modify the code of an existing blockchain i.e. Bitcoin (a hard fork).
3. Establish a new cryptocurrency on an existing blockchain.
4. Hire a blockchain developer to create a cryptocurrency for you

If you're new to Cryptocurrency then you could make your own. It could be very expensive though if you went through the above!

7. Beginners Tips

So, you're new on your Cryptocurrency journey and probably realising that there is a lot to learn to make sure that you're investing wisely and not putting your hard-earned capital at risk. There are a number of steps that you can take to lessen your chances of pushing the wrong buttons at the wrong time (something we all think about!) Here are some tips that you may want to consider as you start down this road. Some of these may have already touched on but it doesn't hurt to re-inforce them.

- **Consider - What sort of Role do you want?**
    - Investor – Hold for longer periods
    - Trader – Trade the fluctuations of the market

- **Consider - What are your goals with Cryptocurrency?**
    - Long Term Gain?
    - Retirement Money?
    - Trade and make margin?

- **Consider - What is your risk tolerance?**
    - I'm not prepared to lose anything.
    - I'm happy to risk some of my capital
    - I'm shooting for the moon and am ALL in
    - Volatility in the Crypto market – How to deal with that
    - FOMO (Fear of Missing Out)

- **Not in control of your keys? Not your money!** Public keys are called public for a reason and the same goes for private keys. If you are happy to leave your Cryptocurrency on an exchange which also has control of your Private Keys as well and that exchange gets hacked then you'd better hope that exchange is willing to insure that Crypto for you. If not, then your money has gone. Look up Mt Gox on the internet…

- **Larger amounts of Crypto?** Take them off chain. We cover this more in our second Tutorial 'Using Crypto Wallets' if you're interested. Remember, we're dealing with digital code here via wide information networks that operate electronically. There are bad actors out there who are spending a lot of their time trying to hack networks, so having some sort of 'cold storage' (No on the internet makes sense)

- **Dollar cost averaging.** Something for you to have a look at if you have never heard it before. It's a great way of making sure that you're continually investing regardless of the high and lows of any Crypto cycle. If you are like most people its very hard to predict the highs and lows of any market, and given this difficulty may people simply do nothing…as they are afraid to get things wrong. If you are using a dollar cost averaging investment strategy you will buy some coins or tokens at their high and some at their low…but the secret here is to make regular purchases on a consistent basis, as over time the highs and lows will average out.

- **Choose your exchange wisely.** There is no requirement for you to use just one Crypto exchange (Unless you are geographically restricted by some form of governmental censorship) so why not try a bunch of them to find one that you are comfortable with. Some may have different trading pairs (i.e. different coins and tokens) Start small and put a minimum amount on each of these exchanges when you start trading. This has the added benefit of being able to send coins/tokens between different wallets – a great way for you to learn how the whole process works.

- **Join some chat groups.** Seriously, this is a good way to learn how things work and chat with other new people. Just be aware that there may be some 'experts' on there willing to give you your opinion. Just filter out the stuff that may seem a bit heavy.

- **Spruikers.** There will be people talking up a new coin or token. "Hey…you should buy this coin or token because it is going to the moon! "(Going to make a lot of money) Just be careful and do your research, also make sure that you can trade out of that coin/token if you need to (It is convertible to something that has value. – Bitcoin/Ethereum/Fiat etc)

- **Invest/Buy sensibly.** Crypto currency can be VERY volatile. If you want lots of sleepless nights then by all means check your mobile every 5 minutes as it goes up and down. Pick your strategy and stick with it.

- **Scams.** The age old adage "If something looks too good to be true then it probably is."

- **Security.** Yes 2FA (Two Factor Authentication) is a pain in the butt. But, if it saves your Crypto then do it.

- **Research.** Do it. That simple. Don't just listen to some video where something claims something is fantastic and you should get it now…do your research.

- **LASTLY**

Not in control of your keys? Not your money!

This ends Tutorial One. Want more? Go back to www.iamnewtocrypto.com and click on Tutorial Two to learn about 'Using Crypto Wallets".

GLOSSARY

51% Attack

The term given to a malicious attack on a blockchain network achieved by taking control of 51% (over half) of the mining nodes.

Address

An address is an alphanumeric identifier providing a virtual location to where cryptocurrency transactions can be sent. They are intended to be single use and only refer to the destination of a transaction, not where it came from.

Airdrop

The free distribution of a specific cryptocurrency to a targeted group as a means of promoting its adoption or increasing its visibility.

All Time High (ATH)

Refers to the highest price a cryptocurrency has ever reached, commonly abbreviated to ATH. See also ATL.

All Time Low (ATL)

Refers to the lowest price a cryptocurrency has ever reached, commonly abbreviated to ATL. See also ATH.

Altcoins

A commonly used term to refer to cryptocurrencies that came after Bitcoin; literally alternative coins, i.e coins that are designed to work differently from Bitcoin.

Anti-Money Laundering (AML)

Legislation and best practice focused on preventing the laundering of the proceeds of crime.

BTC

Trading abbreviation for Bitcoin. All traded cryptocurrencies have a three letter price ticker to make it more convenient to display on a trading screen or price tracker.

Bit

A fractional unit representing a 1,000,000th of a Bitcoin e.g 0.000001

Bitcoin

A monetary system utilising a novel technology called blockchain. Bitcoin also refers to the cryptocurrency unit (small 'b') supported by the Bitcoin blockchain. Bitcoin's blockchain is maintained by a distributed network with no controlling central authority. It ensures accuracy of user balances (the 'double spend problem) through a process called Proof of Work (PoW). PoW incentivises network Nodes - called miners - to issue new bitcoin and validate transactions, in return for committing computing power to secure the blockchain. The idea for Bitcoin was published in October 2008 under the pseudonym Satoshi Nakamoto; the true identity of its creator is unknown.

Bitcoin ATM

An ATM (Automated Telling Machine) where you can buy Bitcoin using a credit/debit card. Funds can be sent to an account or dispensed as a QR code (effectively a paper wallet). Some Bitcoin ATMs allow you to scan a Bitcoin private address - as a QR code - and convert to Fiat for withdrawal.

Bitcoin Cash

The most significant Bitcoin hard fork, created in 2017 as part of the disagreement over whether to increase block size. Bitcoin Cash was itself forked in late 2018 to create Bitcoin SV.

Bitcoin Dominance

Refers to the market capitalisation of Bitcoin in proportion to the whole of the cryptocurrency economy as measured by the sum of market capitalisation of listed coins on an aggregator such as Coinmarketcap.

Block

The term used to describe the way transactional information is organised within a blockchain - such as Bitcoin - grouped in so-called blocks, each referencing the previous to create a continuing chain of self-referential information. A block will usually be of fixed size, for the Bitcoin blockchain this is currently 1mb.

Block Reward

The reward given to a Miner for successfully mining a block, containing a subsidy and fees for transactions contained within the block. For Bitcoin the subsidy halves every four year and is currently set at 6.25 BTC.

Blockchain

The name given to a decentralised system for storing data across a peer-to-peer network, without a central authority, the first example being Bitcoin.

CBDC

Abbreviation for Central Bank Digital Currency. This term has been applied to a hybrid type of digital currency that has been issued by a nation's central bank. Largely inspired by elements of Stablecoin design, CBDCs enable central banks to create digital versions of existing fiat money where they retain control. Most CBDCs are still in an R&D phase, with an estimated 80% of the world's central banks researching the subject. Read about CBDCs here.

Centralised Exchange (CEX)

A type of cryptocurrency exchange where the trading is facilitated at a central location and subject to the appropriate regulations. A CEX may operate across several jurisdictions complying with the regulations specific to each.

Circulating Supply

A measure of the supply of a cryptocurrency that is in general circulation. Given lost or burned coins, this figure is hard to accurately establish. Circulating supply will function as a proportion of Total Supply.

Coin

Slang term for a cryptocurrency making them more relatable. In reality cryptocurrencies are entirely virtual and have no physical representation. Often used to distinguish cryptocurrency functioning as money rather than tokens with narrow use cases on a specific blockchain.

Coin Burn

Permanently removing tokens or coins from the circulating supply. Coin burning is usually done to restrict total supply and thereby control inflation.

Cold Storage

A secure method for storing cryptocurrency that by default is offline (not connected to the internet) and therefore minimises the threat of hacking. Examples are Hard Wallets or Paper Wallets.

Cold Wallet

A cryptocurrency wallet that by default is offline (not connected to the internet) and therefore minimises the threat of hacking. Examples are Hard Wallets or Paper Wallets.

Confirmation

The process by which new blocks are added to a blockchain, with all nodes confirming the transactions within the block as valid. Confirmations happen as set time intervals which vary depending on the Consensus Mechanism. One Bitcoin confirmation generally takes 10 minutes.

Confirmation Time

The time taken for a new block of transactions to be confirmed and added to the end of a blockchain. The time taken will depend on the Consensus Mechanism employed. A Bitcoin block confirmation takes roughly 10 minutes, while for Ethereum it is around 15 seconds.

Consensus Mechanism

Describes the process by which a blockchain reaches agreement on the validity of new data being added to the existing chain of information. Examples are Proof-of-Work, Proof-of-Stake and Delegated Proof-of-Stake.

Cross-chain

An interaction between different cryptocurrency networks or blockchains. For instance, between the Bitcoin network and the Ethereum network.

Cryptocurrency

A new kind of internet money with no controlling central authority which is instead uses blockchains to record transactions and issue currency. Blockchains are secured by cryptography and consensus mechanisms, hence the term crypto-currency

Cryptocurrency Exchange

An online service, usually website, mobile app or API, that facilitates for a fee, the exchange of fiat currencies for cryptocurrencies, or the exchange between different cryptocurrencies. There are two exchange models CEX (Centralised Exchange) or DEX (Decentralised Exchange).

Cryptography

The use of codes to ensure information is only accessible by a sender and an intended recipient. Cryptography is a central element of cryptocurrency design, providing security in the absence of a central authority.

Custody

The term used to describe who controls the Private Keys for a cryptocurrency wallet., giving them control over funds. Custodial - Controlled by a 3rd party; Non-custodial - controlled by the individual.

Decentralised

The characteristic of a network or organisation that has no central point of authority, decision making is instead delegated to smaller groups or shared across network points (aka nodes). The Bitcoin blockchain enables a money system to be decentralised, taking banks out of the picture, and enabling users to interact directly with each other (P2P).

Decentralised Application (Dapp)

An application built on a blockchain, using Smart Contracts to perform the business logic. They have no single point of authority or control, and rely on the consensus mechanism of the underlying blockchain to process transactions.

Decentralised Autonomous Organisation (DAO)

An organisation that uses the decentralised qualities of blockchains and smart contracts to provide governance (decision making) through aligned economic incentive. DAOs try to solve the Principal-Agent dilemma where agents (managers or politicians) within an organisation have decision-making power but don't feel the consequences of their decisions because they have no skin in the game.

Decentralised Exchange (DEX)

A type of cryptocurrency exchange which has no central trading book but instead facilitates access to liquidity via smart contracts.

Decentralised Finance (Defi)

Offers new crypto-based financial products in a totally decentralised way. There is no bank or business, no formal account creation, just a protocol managed by smart contract, so all interaction is essentially dictated by code.

Double Spend Problem

How to ensure that a balance within any money system cannot be spent twice. In centralised systems there are numerous checks and balances to try to minimise double spend, though it still occurs as charge-backs on credit cards. The biggest achievement of Bitcoin was solving double spend with no central authority.

Dumping

The sudden sell-off of a cryptocurrency causing an immediate and significant drop in its price.

ERC-20

ERC-20 is the technical standard for smart contracts, token issuance and management on the Ethereum blockchain. It is one of the most common ways new cryptocurrencies are created. ERC stands for Ethereum Request for Comment. It is just one of many standards for interacting with the Ethereum Network.

Ether (ETH)

The native currency for the Ethereum Network. It functions both as a money (in a broad sense) and a token for paying for smart contracts execution.

Ethereum

The second most prominent cryptocurrency after Bitcoin. Created by Vitalik Buterin in 2013, Ethereum is a blockchain intended as a base layer for any application (or dApp) to run on top of using the Ethereum Virtual Machine, aka world computer. It also functions as a decentralised digital money.

Exchange Traded Fund (ETF)

A fund that gives an investor exposure to a basket of securities or assets without actually owning them. ETFs can be bought and sold at any time during market trading hours. Approval of a Bitcoin ETF is seen as being a watershed moment bringing in more retail investors.

FOMO

Fear of Missing Out; A description of a type of buying behaviour motivated solely by a desire not to miss out on anticipated further increases in price.

FUD

Fear, Uncertainty, Denial. An acronym widely used to describe unsubstantiated criticism intending to create doubt or generate negative sentiment.

Fiat Currency

The term to describe money created by governments which isn't backed by any asset like Gold. In Latin FIAT means 'let it be done', so Fiat Money is essentially money that functions and has value simply because the government says so.

Fork

A change in the design of a blockchain creating two paths which nodes and miners need to choose, like meeting a fork in a road and deciding which route to take. Each path (fork) is a new blockchain.

Fungible

A property of money, meaning that each unit is indistinguishable and interchangeable. Any Euro can be exchanged for any other Euro. Cryptocurrency has this property.

Gas

The unit for measuring the cost of executing Smart Contracts on the Ethereum Network. Gas is paid for in Ether and denominated in Gwei, one Gwei being equal to 0.000000001 ETH (10-9 ETH) so instead of a Gas Fee being 0.000000001 Ether it would be written as 1 Gwei.

Refers to the backing of notes and coins in circulation with an equivalent of gold lodged with a central bank. Money supply can only grow if an equivalent amount of gold is added to bank reserves. The Gold Standard was finally abandoned in 1971 by the USA's decision to stop converting dollar reserves to gold at a fixed value.

Halving

Name given to the halving in the block reward paid to Miners for completing the Proof of Work and adding and a new block to the Bitcoin blockchain. It halves every four years and is currently set at 6.25 BTC

Hard Wallet

A physical device with USB connection that enables non-custodial management and storage of cryptocurrency. Hard wallets by default are offline making them a safe storage option. Common manufacturers are Ledger and Trezor.

Hash

The unique identifier given to every cryptocurrency transaction, which enables you to view all input details.

Hodl

A slang term used within the crypto community meaning to steadfastly hold on to your crypto assets especially through big price dips. Hodling is a mentality driven by belief in the underlying use case for crypto. Read about the story of hodl and its origin in our blog.

Hot Wallet

A cryptocurrency wallet that by default is online (connected to the internet). Hot Wallets are convenient for transacting and trading but are more susceptible to the threat of hacking. Examples are hot wallets are Mobile Wallets and Web Wallets.

Initial Coin Offering (ICO)

When a cryptocurrency's creator offers some of the tender at a discounted price or even for free as a means of raising funds and attempting to generate exposure to the market.

KYC

Abbreviation for Know Your Customer, generally relates to the information new customers must provide to open an account with an exchange and prove their identity. A Centralised Exchanges (CEX) is required by local regulation to collect KYC whereas a DEX isn't bound by the law of any specific location.

Leverage

A high-risk trading approach where exposure to a given trade can be multiplied by an agreed Margin - essentially on credit - thereby increasing both potential gains and losses. A 50x leveraged position will increase profits/losses by that amount e.g €200 price increase on €10,000 trade at 50x leverage will generate 100% profit, while a €200 decline will wipe out your entire investment.

Mining

The name given to the process by which new cryptocurrency is issued. Miners use specific computer hardware - mining rigs - to run arbitrary hashing algorithms (SHA-256 for Bitcoin) with the aim of finding a specific output (like a lottery) which allows the Miner to add new transactions - grouped into a block - to the existing blockchain. In return, successful miners earn a mining reward. This process is known as proof-of-work, as it requires computing power to be committed. The cost of performing the work ensures only valid transactions are added to the blockchain and secures the bitcoin network in proportion to the total computing power of all active miners.

Mobile Wallet

A cryptocurrency wallet functioning as an App on a mobile phone; can be either custodial or non-custodial.

Non Fungible Token (NFT)

A type of digital token that is verifiably unique and can therefore be used to assert rights to ownership of digital collectibles like art or in-game items. NFTs are generated on the Ethereum blockchain using the ERC-721 or ERC 1155 standards.

Paper Wallet

Permissionless

Used in reference to a public blockchain where no permission is required to participate, for example by downloading the relevant network software and running a node. Bitcoin is an example of a permissionless blockchain. The opposite to Permissioned.

Private Key

A 64 character alphanumeric string which controls the movement of unspent funds associated with a cryptocurrency address. Modern HD Crypto Wallets use Seed Phrases rather than requiring the handling of private keys, but the term Private Key is widely used to underscore the importance of being in control of your funds.

Proof of Stake (PoS)

A blockchain consensus mechanism where the ability to mine or validate blocks is in proportion to funds staked.

Proof of Work (PoW)

A blockchain consensus mechanism where the ability to mine or validate blocks is in proportion to the amount of work committed, measured in CPU power.

Public Key

A 64 character alphanumeric address which allows view only access of unspent funds and used to receive funds. The equivalent of bank account details, the address to which crypto can be sent, and the balance seen by anyone.

Pump and Dump

Describes the coordinating buying of a cryptocurrency (Pump) to create a short term increase in price, followed by coordinated selling (Dump).

QR Code

A Quick Response code is a machine readable two-dimensional bar code with specific information about the product or service it is attached to. In crypto QR codes are used for addresses and within the Lightning Network, generating Invoices.

Ripple

A real-time money settlement system, currency exchange and remittance network that uses the token XRP as part of its function.

Satoshi Nakamoto

The pseudonym of Bitcoin's creator. Their real identity is not known. Remaining anonymous enables Bitcoin to function without a controlling figure or someone that could be a point of weakness/attack.

Sats

Abbreviation for Satoshi, the smallest unit of Bitcoin i.e 0.00000001

Seed

A collection of unique phrases that act as the security layer protecting a HD (hierarchical deterministic) crypto wallet and all associated addresses without needing to access individual private keys.

Shitcoin

Slang term for a cryptocurrency with no perceived real world use case.

Smart Contracts

A set of rules defined in code that can be executed by an underlying blockchain for a fee e.g smart contracts on Ethereum or Binance Smart Chain.

Stablecoin

A type of cryptocurrency specifically designed to avoid volatility by pegging their value relative to an external asset or group of assets. For example USDT (Tether) retains a value pegged to the US Dollar.

Staking

Depositing a specific amount of cryptocurrency with a provider or protocol under specific conditions and in return for specific rights or rewards.

Token

A type of cryptocurrency that has a specific use case within a blockchain ecosystem, rather broader use as money.

Transaction Fee

The cost of sending a cryptocurrency transaction; Fees are collected by miners who validate transactions grouped into blocks. Fees are relative to the specific cryptocurrency, the data size of transaction and the network congestion at the time. As miners earn fees for the blocks they mine (in addition to the block reward) they prioritise transactions with higher fees.

Trezor

A popular brand of hard wallet, a device for securely storing cryptocurrency offline.

Trustless

Describes a system that does not require participants to know or trust each or a third party in order to function.

Two-Factor Authentication (2FA)

An extra layer of protection for online accounts - in addition to username and password - requiring the input of code generated by SMS or ideally an authentication App like Google Authenticator or Authy.

Tx

Abbreviation for transaction, the collective term for all of the details associated with a specific movement of funds or information on a blockchain.

Unconfirmed

When a proposed transaction cannot be added to the blockchain, usually because it is yet to have the process of broadcasting to the blockchain network and verification from miners.

Wallet

A means of storing cryptocurrency balance ownership. Made visible on the blockchain by its unique code, or public key, a wallet's function is to store private keys and is available in several different forms.

Whitepaper

Offers a thorough overview of a cryptocurrency, outlining details including an explanation on programmed purposes, technical information and its potential future to lure buyers.