CRYPTOCURRENCY

Our definitive guide to Cryptocurrency

COIN RIVET

Independent British blockchain and crypto news

CONTENTS

CRYPTOCURRENCY EXPLAINED

Most people first heard about cryptocurrencies in late 2017 when Bitcoin and other cryptocurrencies experienced a phenomenal price increase. Suddenly, all mainstream media outlets wanted a piece of the action.

They started using terms like cryptocurrency, digital cash and token interchangeably, often confusing those from outside the industry.

Below, we remove the smoke and mirrors by clearly defining cryptocurrency. This definitive guide will explore what it is, how it can be used, and what the leading cryptocurrencies are.

Cryptocurrency defined

A cryptocurrency is a digital currency that uses cryptography to secure and verify its transactions, recording them in a decentralised and immutable ledger known as blockchain. They can be used as a medium of exchange or a store of value, and are traded in many exchanges around the world.

Cryptocurrency can be viewed as an alternative to standard national currencies, that can be traded in a similar way on dedicated exchanges.

Cryptocurrencies, however, have no physical form and exist only in the digital space. Digital cryptocurrency coins can be bought, sold, and converted back to fiat money on specialised cryptocurrency exchanges.

Cryptocurrencies operate independently from banks and act as an alternative form of payment to cash and credit cards. As such, it's becoming increasingly popular in countries where banking institutions are unstable. This is because people would rather have full control of their money in a digital space rather than rely on the banks to keep it safe.

Unlike fiat currency, cryptocurrency exists in a volatile and unregulated market.

A brief history of cryptocurrency

Cryptocurrencies first emerged with Satoshi Nakamoto's Bitcoin whitepaper at the start of 2009. The paper outlined a clear vision of a **"purely peer-to-peer version of electronic cash** (allowing) online payments to be sent directly from one party to another without going through a financial institution". Since 2009, thousands of cryptocurrencies have entered the market, with stable coins and privacy coins playing a greater role than ever before.

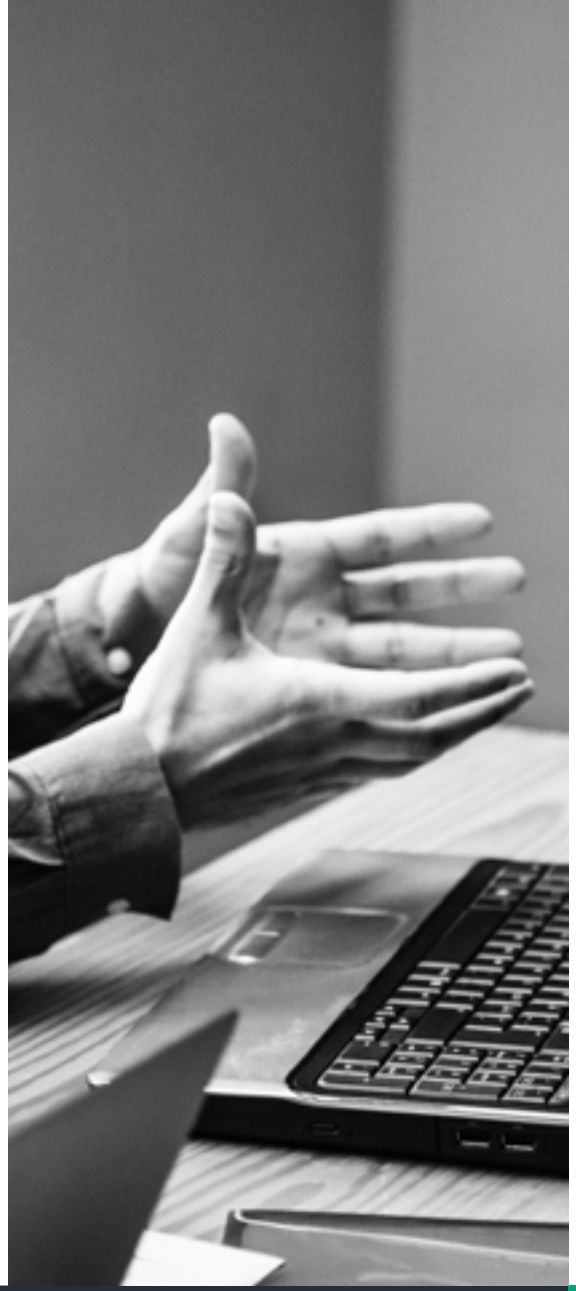
Cryptocurrencies can largely be divided into two categories: those that are supported by their own blockchains, like Ethereum and Bitcoin, and those built on top of other blockchains - also known as tokens.

Blockchain—the technology powering cryptocurrency

When talking about cryptocurrencies and what a cryptocurrency is, it's important to understand the concept of blockchain technology. Blockchain is the **underlying technology powering cryptocurrencies.** It's used to create, update, and maintain a decentralised, trusted ledger of transactions which occur within a network. This network is made up of independently-owned nodes that use a cryptographic protocol to validate transactions in a cryptocurrency.

The protocol rewards accuracy in a way that ensures the data entered into the ledger cannot be wrong or subject to changes. It's immutable, secure, and completely transparent. Blockchain technology makes it possible to trust the information kept on that ledger without having to rely on a central institution like a bank. A lot of the hype surrounding cryptos comes mostly from the fact that our entire economy does, in fact, rely on centralised institutions.

Analysts look at cryptos and recognise their potential to revolutionise the banking and finance industries. However, it's important to remember these sectors have existed for centuries. In that time, banks have changed but they've primarily remained in control of their destiny. To this end, large financial institutions have been keen to understand blockchain-powered cryptocurrencies. They have poured millions into research and development to understand and integrate the underlying technology, hoping this will allow them to stay ahead of the curve.



CRYPTOCURRENCIES VS TOKENS

Terminology within this space has often been used interchangeably.

However, there are some **distinctions between cryptocurrencies and tokens** that you should make note of. The best method of identifying the difference between an independent cryptocurrency and a token is to ask the question: is this crypto independent from other platforms or does a pre-existing blockchain support it?

An independent cryptocurrency uses its own blockchain while a token is merely a cryptocurrency built on top of another pre-existing blockchain. Tokens are a subset of all cryptocurrencies.

Within the independent ones, there is another difference. They can either be Bitcoin-based blockchains such as Dash or Litecoin, or they can have their own native blockchains like Ripple or Ethereum.

All cryptos in these two categories can also be called alternative coins. Altcoins get their name from being alternatives to the original cryptocurrency: Bitcoin.

DIFFERENCES BETWEEN DIGITAL CURRENCY AND CRYPTOCURRENCY

So now that we've covered the basics of cryptocurrency, we'll explore how it stands apart from digital currencies that already exist.

The entire premise behind a cryptocurrency is that it exists in the digital space and sits directly on a digital ledger. But is a digital currency by default cryptographic?

The core differences between a full cryptocurrency and traditional fiat currencies made through digital transactions represent big differences in end user rights and platform goals. From the unique features of decentralised holding and trading to compatibility when making payments online, the two alternatives are more polarised than you might expect.

A digitised medium doesn't mean a decentralised currency platform. Fiat currencies, whether transferred in cash or online, are still bound to the traditional regulatory oversight and restrictions imposed on any national currency. Although the digital mediums of payment gateways and contactless terminals can be enhanced, the regulatory framework governing modern and traditional fiat transactions is exactly the same. Digital currencies are restricted by these regulations, whereas cryptocurrencies are not.

Digital currencies don't use cryptography, whereas cryptocurrencies do. The majority of cryptocurrencies are decentralised, relying on the power of the people (otherwise known as miners) rather than relying on a central institution that can offer a single point of failure. So what does this mean for trading cryptocurrency?

PEER-TO-PEER TRADING: THE TRUE DEFINITION OF CRYPTO?

One of the central philosophies behind the creation of Bitcoin, the original cryptocurrency, was to create a peer-to-peer electronic cash system.

The intent was to allow people to have self-governance over their finances. To enable peer-to-peer cryptocurrency trading, a system must be decentralised.

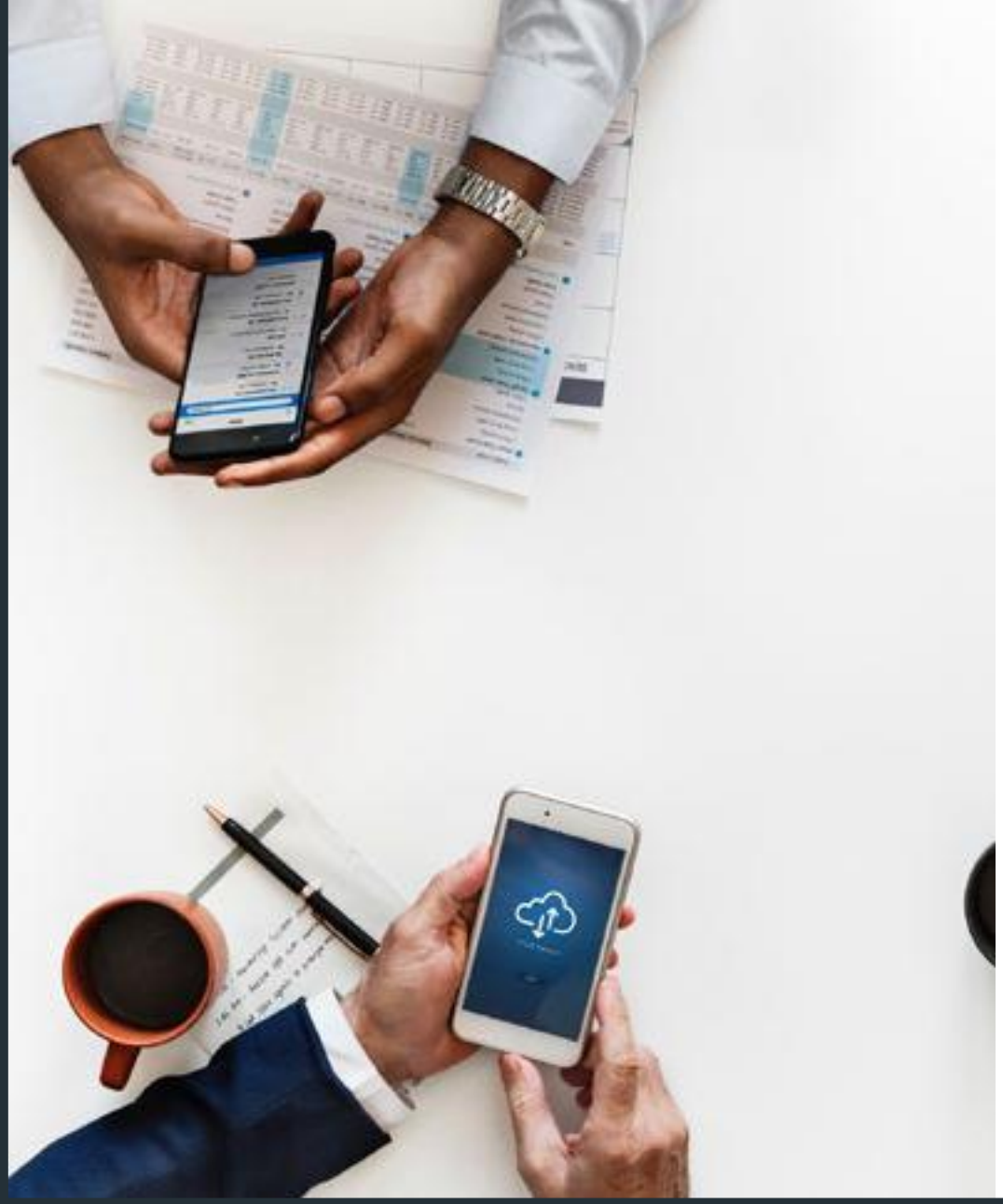
A system that is decentralised has no central server, location, or single authority in charge. Instead, the network is distributed across multiple nodes across the globe. Instead, every person within the network has equal privileges and potency. In the context of trading with cryptocurrency, peer-to-peer refers to buyers and sellers completing transactions directly with each other – with no middle-man needed to facilitate the trade.

Below, we take a look at the benefits of peer-to-peer trading.

Peer-to-peer is private

Since buyers and sellers alike are actively searching for people to match their order, a third party is not needed in peer-to-peer cryptocurrency trading. This provides the benefit of privacy. Since no third party is involved, only the buyer and seller negotiate. Communication between both parties is kept private. Only when the order has been submitted and is ready to be added to the blockchain does it become public. Since the trade will appear on the blockchain, no identifying information is used.

A lot of exchanges usually require users to **complete a Know-Your-Customer test (KYC)**. A KYC test can help exchanges ensure that legitimate traders are using their service. On the other hand, it's also a means to collect data on individuals. This could range from name, ID, phone numbers and so on. Peer-to-peer trading eliminates this data collection, adhering to anonymity.



Peer-to-peer is fair

When using an exchange platform, the prices for cryptocurrencies will be relatively fixed to reflect the pricing on all other exchanges. By opting for peer-to-peer trading, however, you can look for comparable prices and even better prices. With peer-to-peer trading, orders at better prices are more likely to be filled since parties have already expressed their interest. This type of trading also reduces the amount of cancellations on an order book as levels of commitment between traders is arguably higher than between traders using an exchange.

P2P marketplaces are often affordable and secure

One way of engaging in peer-to-peer trades is by using a peer-to-peer marketplace. These marketplaces allow traders to contact each other by signing up and verifying their accounts for free. In comparison, most exchanges may charge a fee to sign up and/or trade.

Unlike exchanges, peer-to-peer networks don't hold any cryptocurrency. Deals are done directly and so the safety of your currency is always protected.

Most importantly, peer-to-peer trading offers a high resistance to transaction censorship. As there is no central authority in charge, or with access to transactional data, trading activity can't be corrupted and your funds can't be stolen.

Will peer-to-peer continue to define crypto?

Peer-to-peer cryptocurrency trading remains faithful to the intent of the original cryptocurrency. As the market evolves, however, crypto users expect more choice than ever before. Some prefer centralised exchanges, some prefer decentralised ones, and some prefer not to trade at all. As always, be sure to do your own research before committing to any decisions relating to investments.

HOW TO MINE CRYPTOCURRENCY

Cryptocurrency mining is the process of verifying transactions on a blockchain ledger. Anyone with access to the internet and suitable hardware can participate in mining.

The participant who first solves the problem gets to place the next block on the blockchain and claim the rewards. The rewards are transaction fees (from the transactions in the block) as well as the newly released cryptocurrency e.g. Bitcoins.

Cryptocurrency mining and Proof of Work

Proof of Work (PoW) is a demonstration of the difficulty in making the new block. The difficulty is in terms of how hard the processor has to work to solve the problem. Costs involved in cryptocurrency mining will be for the hardware (the processor or miner) and the costs associated with the electricity used.

Cryptocurrency mining is resource-intensive and difficult (in the sense of the processing effort required) and this is deliberate. The first miner to solve the next block gets the reward but the amount of processing required to do this is enormous.

How to start cryptocurrency mining

These are the things you will need to start mining:

1. **Mining hardware – a processor**
   You can buy the hardware on Amazon or eBay. In addition, there are lots of other pieces of supporting hardware available – cooling fans, stacking racks, processing boards, cards and chips.
   The basic way to maximise returns is to have your hardware running for as long as possible every day and as efficiently as possible.
   A **mining pool** is the pooling of resources by miners who share their processing power over a network and split the reward equally.
   In return you pay the mining pool a fee (usually a percentage).
   The difficulty (in terms of computer effort) means, realistically, this is the most practical option to mine Bitcoin.
   The hashing power and power consumption will be included in the miner specs. The price of electricity in your country can be easily found via a Google search and you'll know the pool fee when you choose the pool you want to join.

2. **Get a cryptocurrency wallet**
   Selecting the right cryptocurrency wallet will depend on your particular circumstances. If you hold one currency then using that currency's official wallet is probably the easiest option. If you hold more than one currency (or are planning to own more than one) then you will need a wallet that can hold more than one type of currency.

3. **Find a mining pool**
There are a range of mining pools easily found on the web. Most crypto commentators would recommend **Slush Pool** which has been around since 2010 and was the first mining pool.

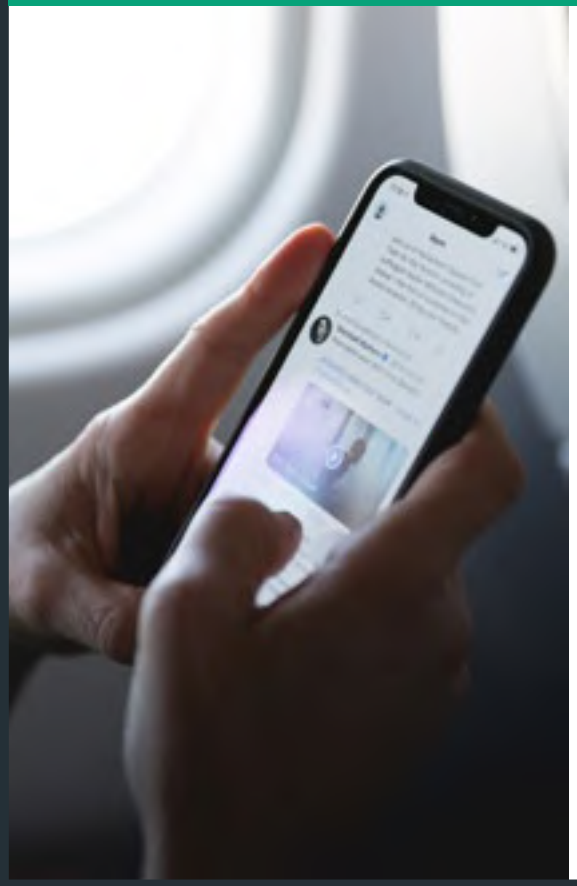
The kind of things you should be looking at when considering your pool are: the reward method (e.g. proportional, pay per share), any fees charged for withdrawal, how frequently is a block mined, how stable the pool is and how easy it is to withdraw money

Once you've selected your pool it's normally straightforward to sign up and add a "worker" that will have its own ID so the pool can keep track of your miner and its mining efforts.

4. **Get a mining programme**
Your miner will already have the appropriate software loaded but you will need a programme for your computer to measure, control and monitor your miner. Many mining pools have their own software but if you need to find your own then it's easily found with a Google search.

HOW TO EARN CRYPTOCURRENCY

If mining isn't for you, there are other ways that you can earn cryptocurrency. In fact, it is becoming a somewhat gamified industry. Below, we take a look at some of the different ways you can earn cryptocurrency



You've probably heard of the old expression 'time is money.' This sentiment certainly pertains to the crypto world. The crypto industry has created a market where people can offer their services in exchange for crypto.

Job boards

Reddit is one place you could go to do this. There are a couple of subreddits that have several thousand subscribers, such as r/Jobs4Crypto and r/Jobs4Bitcoin.

These boards advertise different ways of earning money. As an example, you could complete microtasks such as retweeting businesses in return for crypto.

This method of earning cryptocurrency could be useful for people who are not at work, work part time, or are freelancers.

You could also offer your services on a weekend basis to earn a little extra on the side.

Completing surveys

Websites have long asked for your time in exchange for a potential reward like vouchers or cash.

Sometimes, it is a simple case of answering a survey. The good news for you is these type of sites exist in the cryptosphere too.

Just by answering a quick survey or providing feedback to a company, you can earn yourself a small amount of crypto. This is one avenue you can use to enter the crypto markets.

Still, if you ever have a spare five minutes you could fill out a survey, and after several surveys your Bitcoin stash will grow.

Contribute to an ecosystem

Some cryptocurrency companies encourage developers to take part in their ecosystem. In doing so, the developers are rewarded in crypto.

One example of a company that promotes this engagement is the Kin Foundation. Currently, Kin is undergoing a phase where developers can submit creative ideas to the ecosystem. If successful, the developers will be awarded Kin, the native token for the Kin ecosystem. Kin is just one example of many available ecosystems in the cryptocommunity.

What could you earn?

It's possible you might only receive a few satoshis. A satoshi is the smallest unit of Bitcoin, a bit like the penny to the pound. To be exact, a satoshi is only worth 0.00000001 Bitcoin..

AN OVERVIEW OF CRYPTOCURRENCY EXCHANGES

Whether you mine for cryptocurrency or decide on a different method to earn them, you'll want the ability to sell, trade, or store your funds. Just like on the stock market and in day-to-day life, exchanges and wallets play a critical role in cryptocurrency. We take a look at the role of each below.

If you've dabbled with investing in one form or another, you're probably familiar with the concept of an exchange. Entities such as stock exchanges and foreign currency exchanges allow customers to trade their stock or currency for other assets. On stock exchanges, you typically have the opportunity to convert between shares of stock and fiat money. Through foreign currency exchanges, you can convert your money from one nation's fiat currency to another.

How a cryptocurrency exchange works

A cryptocurrency exchange works in a similar way. A cryptocurrency exchange, or digital currency exchange (DCE), is an online platform that allows you to buy and trade cryptocurrency or digital currency, then sell it to convert it back to fiat money. These exchanges will either take a commission or simply charge usage fees for their service.

If you're familiar with placing buy and sell orders through stock brokers, you can safely assume cryptocurrency exchanges function in a similar, third-party manner to these brokers. Brokers take your desired cryptocurrency price and order quantity, wait for an order to be completed, and then typically collect a percent commission (plus an upfront fee) on your order.

Similarly, a cryptocurrency exchange is usually programmed to accept your digital buy and sell orders (along with price and quantity), waits in a similar manner for your order to be triggered (met by a buyer or seller on the other end), completes the trade, and then updates your on-exchange holdings, all without human brokers.

Another of the unique aspects of cryptocurrency exchanges is the ability to exchange one cryptocurrency directly with another. This is something you can't do with stocks, where you'd need to liquidate shares to fiat money before using those funds to buy new stock shares. Be aware though that you won't necessarily be able to trade one cryptocurrency with all other cryptocurrencies under the sun.

Cryptocurrency exchange nuances, such as the absence of human brokers and the ability to trade between small, relatively rare and unheard of digital assets, bring a unique flair to investing. Exchanges can be centralised or decentralised, so be sure to research the options and choose an exchange that works best for your needs.

AN OVERVIEW OF CRYPTOCURRENCY WALLETS

You'll need a cryptocurrency wallet to store your funds. Below, we take a look at the different types, how they work, and what their benefits are.

Cryptocurrency wallets explained

A cryptocurrency wallet is a digital wallet for holding digital currency. Cryptocurrency wallets rely on cryptography for security. The role of public and private keys is critical here.

Cryptography keys

Public key cryptography is any cryptographic system that uses pairs of keys. A key is a piece of information that unlocks or decodes a cryptographic algorithm.

There are two types of keys – public keys which may be spread widely and known to many people and private keys which are only known to the key owner. The use of public and private keys accomplishes two functions – authentication and encryption. Authentication is where the public key verifies that the message was sent by the holder of the paired private key. Encryption is where the paired private key holder (and them alone) can decrypt a message encrypted with the public key.

Now we completely understand public and private keys, let's think about how this works in a cryptocurrency wallet. Obviously, there is no cryptocurrency actually stored in the electronic wallet.

In the case of Bitcoin (and cryptocurrencies derived from it), the cryptocurrency is stored and maintained in a publicly available ledger. Every piece of cryptocurrency has a private key. With the private key, it is possible to write in the public ledger, effectively spending the associated cryptocurrency.

Your wallet stores your private and public keys. This allows and facilitates the sending and receiving of coins. It also acts as a personal ledger of transactions.

Types of cryptocurrency wallets

Wallets come in different formats with a range of features and benefits.

Here are some of the main types with brief explanations.

Multi-currency cryptocurrency wallet

A wallet that supports different types of cryptocurrencies that can be "stored" at the same time.

Software cryptocurrency wallet

This is the main type of wallet as you might expect with a digital currency. It's worth briefly considering the different types of software wallets. They come in different forms like:

- An application installed locally on a computer or device
- Some web-based wallet's use additional security – you may have come across two step verification like Google authenticator. The main benefit of this additional authentication is it prevents a hacker using keystroke logging to try and gain access to the wallet.

- A cryptocurrency exchange (for example the Kraken exchange) links the user's wallet to the exchanges centrally managed wallet. Any trades are written in the exchanges ledger as an off-chain transaction. When a user enters their cryptocurrency into the exchange or takes it out of the exchange then the transaction is written into the blockchain.

Hardware cryptocurrency wallet

A hardware wallet is a small digital device that can be plugged into a computer to be used to authenticate cryptocurrency transactions. The rationale is to provide added security. Some types of wallets require the user to physically press or touch the wallet in order to sign a transaction.

When the user of a wallet requests a payment, the wallet creates the transaction and provides a public key which is sent to the network. In effect, the signing keys never leave the wallet.

Watch-only cryptocurrency wallet

With a watch-only wallet someone can keep track of transactions but transactions can't be initiated since there is no private key stored in the wallet. The private key can be kept safe in another location.

TOP FIVE CRYPTOCURRENCIES

So now that you know the fundamentals of cryptocurrency and the role it has in wider society, which cryptocurrency should you choose? Below, we take a look at the five most popular cryptocurrencies and what they are.

Generally, the five most popular cryptocurrencies according to CoinMarketCap are:

- Bitcoin
- Ethereum
- XRP
- Litecoin
- EOS

It is important to note that cryptocurrencies can sometimes fall out of favour, change positions, and that Bitcoin holds that majority of the market.

Bitcoin (BTC)

The **Bitcoin protocol** is an open source software project that was started by the anonymous founder Satoshi Nakamoto. They published the idea in a cryptography mailing list back in late 2009.

By the start of 2010 Satoshi and other volunteers started running the network by becoming miners and writing the software for the wallets to conduct transactions. Bitcoin is completely decentralised, without a single authority having control over this open source protocol.

This decentralised digital protocol is used to transfer value directly between participants without the need for third parties or central intermediaries to come between or govern transactions. Bitcoins are also the name of the token on the network.

Ethereum (ETH)

Ethereum is the name of the public blockchain network. Miners work to earn Ether, which is the name of the crypto token that keeps the **Ethereum network** running. While Bitcoin uses blockchain to track ownership of cryptocurrency (Bitcoins), Ethereum uses the network to run program codes for various online applications. As with other blockchain networks, this is done through smart contracts.

A smart contract is a program that runs exactly as coded by its creator. It is essentially an execution that can be set up ahead of time to trigger automatically once certain conditions are met. While Bitcoin uses smart contracts to transfer currency from one user to another, this is all it's able to do. Ethereum's platform allows developers to write their own scripts and create smart contracts for a variety of uses.

Ripple (XRP)

Originally released in 2012, Ripple is a **real-time gross settlement system** (RTGS), currency exchange, and remittance network. It uses a common ledger which is managed and maintained by a network of independently validating nodes that can belong to anyone from

individuals to banks. Ripple is based on a shared public database which makes use of a consensus process between validating servers to ensure integrity.

The goal of the Ripple network, or RippleNet, is to connect banks and payment providers, allowing one frictionless experience for sending and receiving money globally. The Ripple cryptocurrency, XRP, offers banks and payment providers a reliable, on-demand option to source liquidity for cross-border payments.

Litecoin (LTC)

Litecoin was one of the **first serious altcoin** projects developed with an actual purpose. While Bitcoin was seen as "gold" and a potential long-term store of value, Litecoin was created to be "silver" and used for everyday purposes. So, on October 7th 2011, Litecoin (LTC) was released via an open-source client on GitHub.

Litecoin's goal is to be the decentralised money of the internet – free of censorship, permissionless, and open to anyone who wishes to join. They aim to offer private, secure, borderless payments for pennies – anywhere, anytime, and fully controlled by LTC holders.

Litecoin offers the following:

- Real-time settlement (150 seconds)
- Cryptographically secure transactions
- Payments that move like email
- International reach with a single integration
- The best solution for micro-payments
- Quick and easy LTC payment channel integration

EOS

EOS.IO is a blockchain architecture designed to enable vertical and horizontal **scaling of decentralised applications**. It does this by creating an operating system-like construct upon which applications can be built. The software provides accounts, authentication, databases, asynchronous communication, and the scheduling of applications across many CPU cores or clusters.

The resulting technology is a blockchain architecture that may ultimately scale to millions of transactions per second, eliminates user fees, and allows for quick and easy deployment and maintenance of decentralised applications in the context of a governed blockchain.

CONCLUSION

Cryptocurrency is known to be a volatile market, but one that is continuously evolving. Understnding the basics will put you in a great position to go out and become a skilled trader. Who knows where the industry will head, but one thing for sure is that it's here to stay.

We always advise **staying on top of the latest news**, reading our latest how-to guides, and keeping up with the opinions of experts. We deliver all of this content to you, in a few clicks of a button! Good luck with your cryptocurrency journey and don't forget to download our other guides that can help you along your way.

Bringing you news, analysis, opinion and insight from the fast-moving blockchain world. Our team of journalists and contributors cover the likes of cryptocurrencies, wallets, exchanges and ICOs across a wide range of sectors including retail, fintech, banking and gaming. We go beyond the press releases and marketing hype to tackle all the industry topics that matter.

Featured in

FOX NEWS EXPRESS COINGEEK

coinrivet.com