THE LUNCHTIME TRADER PRESENTS

PROFITING FROM CRYPTOCURRENCIES

How to Profit from Bitcoin & Other Cryptocurrencies in Just 20 Mins a Day

MARCUS DE MARIA

Profiting From cryptocurrencies

How to profit from Bitcoin and cryptocurrencies in just 20 mins a day

(Includes section on How to Invest in Initial Coin Offerings – ICOs)

Marcus de Maria

Risk and Disclaimer:

These Terms and Conditions form a part of Investment Mastery Enrolment agreement with you (this 'Agreement') and apply to all online Membership courses YourCryptoBook that are specified below and for which you wish to enrol ('YourCryptoBook' or 'YCB'), to the exclusion of all other terms and conditions issued or stipulated by anyone else other than Investment Mastery. The information presented by Investment Mastery or any of its staff is for educational purposes. Any examples used are for educational and illustrative purposes only. Investment Mastery is not a stockbroker, broker dealer, or investment advisors. They are not recommending particular stocks, options, forex, CFD, Cryptocurrencies. The names of any firms of Crypto Exchange, stockbroker, stock exchange, financial institutions, financial planners, bookmakers, or financial websites mentioned are for illustrative purposes only. The decision on which company to use if any is at the total discretion of each individual person. It is recommended that you seek a professional licensed broker prior to implementing any investment programme or financial plan. The world of Cryptocurrenceis is HIGHLY speculative and you can lose all your investments. Investment Mastery cannot guarantee any results or investment returns based on the information you receive. You must read and understand the above and be aware of the risks of all trading and investing and be willing to accept them before investing.

Table Of Contents – Chapters and Headings

Foreword

I am not going to print this book

The changes that are happening on an almost day to day basis means that if I print it, parts of the book will be redundant within a few months

Cryptocurrencies and the Blockchain will change the way we see the world.

It cuts out middlemen, fees and timewasters.

And at the same time, fortunes will be made.

Not just by the owners of the companies, but by those individuals who are brave enough to get involved at this early stage in investing in Cryptocurrencies, ICOs and companies set to benefit from blockchain technology.

This book was written for you, the beginner, in mind.

I hope it helps.

The best is yet to come.

To your success

Marcus de Maria

1. Introduction

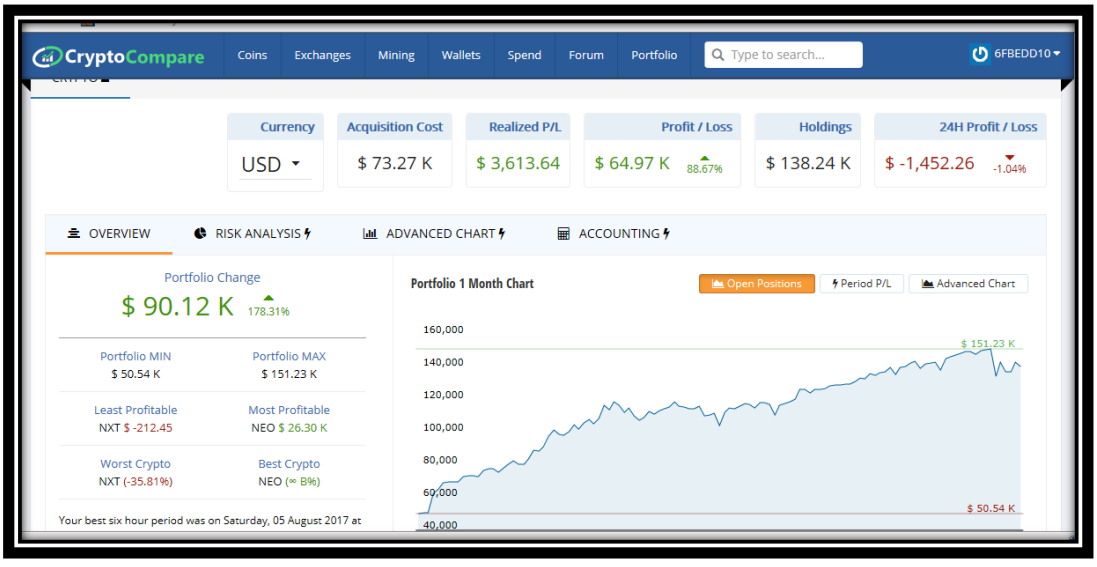
"Science-Fiction is now Science-fact"

- Unknown

At the end of 2016 I read that some cryptocurrencies had gone up by 5000% in just 12 months. I decided to do some research, fast. This is what I found: $100 worth of Bitcoins bought in 2010 would be worth well over $27 million today. How could I have missed out on those returns? It was time to get in.

A few weeks of research later and I had bought 15 different cryptocurrencies using speculation money. Most of the coins quickly went into profit, some substantially. I decided I needed to take this more seriously and really do some research. If not me then who? If not now then when? You have to be in the game to win it!

I paid several thousand dollars for the best crypto subscription service I could find, and started buying more and more cryptos based on their recommendations. I got obsessed – I was even listening to it while going running. At the time of writing, I now own more than 36 different cryptos and over 50+ positions, have banked some profits and am still up over 70% on my entire investments. Not a bad start.

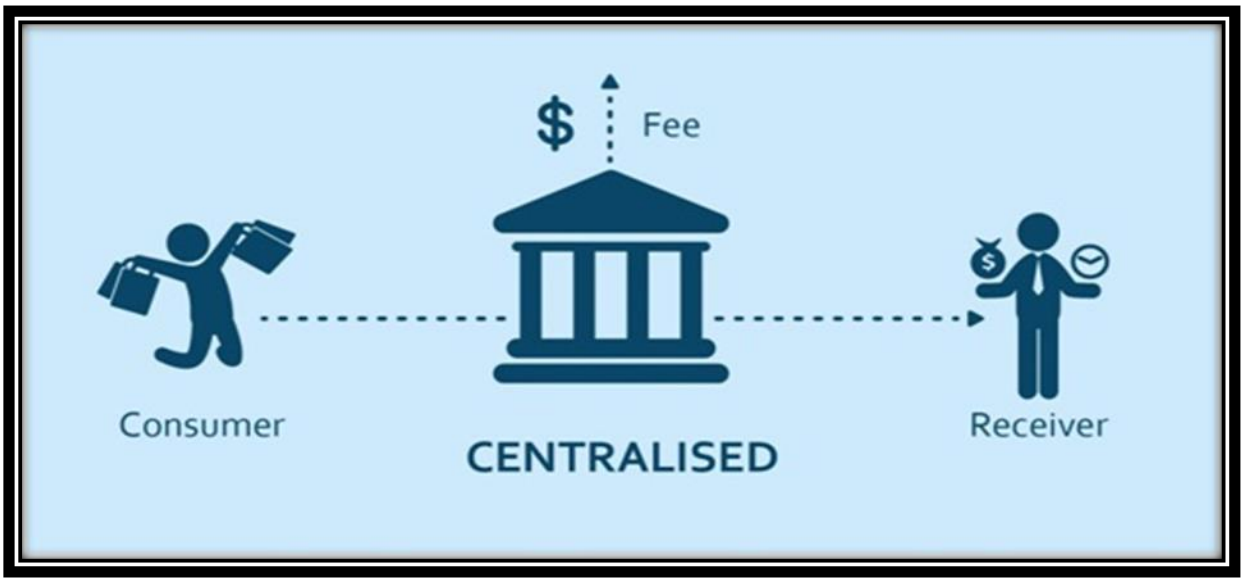


As you can see, I invested $73,000 and made a profit of $64,000 which is an 88% gain. This happened in as little as just 3 months. This was definitely helped by a fast growing Altcoin called NEO. I invested just $850 and turned that into $26,300 profit! I am not sure where else you can do that at the current time but it is possible with cryptocurrencies.

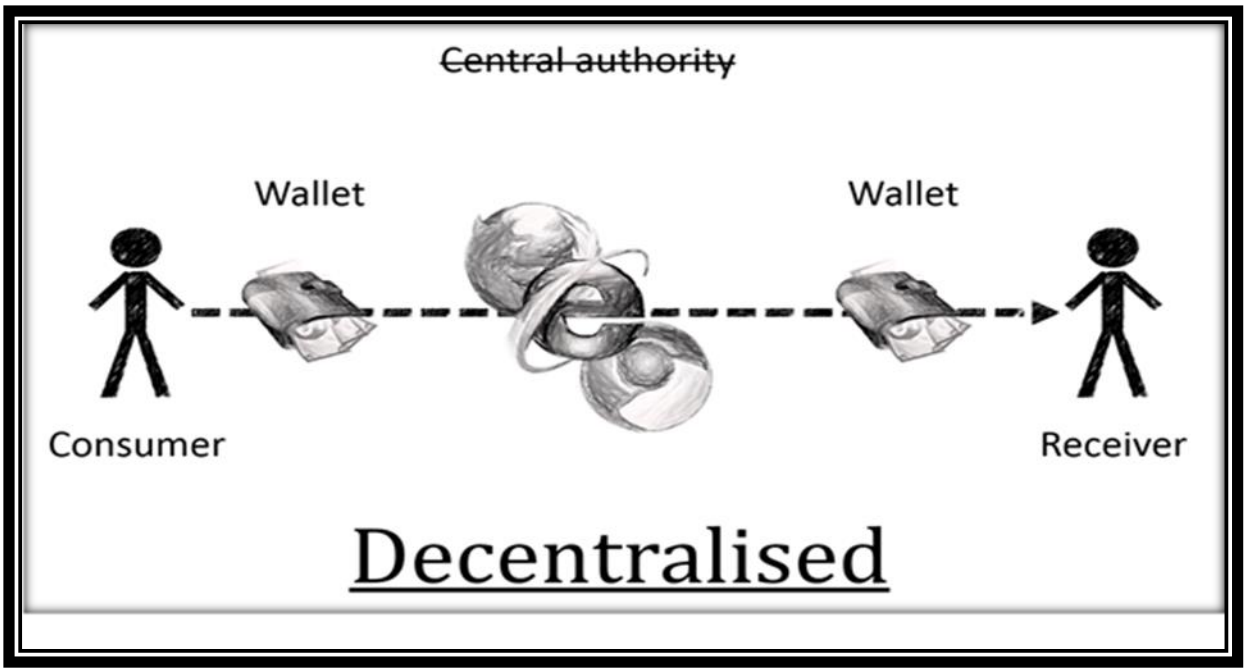
So what are cryptocurrencies and where did it all start?

1. A decentralised system for sending money to other people

Most payment systems run on a centralised network. The problem with this is that you have to incur unnecessary and expensive transaction fees. Usually, this is done by a central server that keeps track of your balances i.e. your credit card and/or the banks. It can also take several days for one bank to talk to another bank and so sending money becomes both expensive and takes too long.



A programmer calling himself Satoshi Nakamoto successfully found a way to build a decentralised digital cash system, thus avoiding the need for a centralised system. He describes it in a surprisingly simple way in his White Paper for Bitcoin, which I have added in the Appendix. You should read it before buying Bitcoin.



A decentralised system means the network is powered by its users without having any third party, central authority or middleman controlling it. Neither central banks or Governments has power over this system.

2. What are cryptocurrencies?

Cryptocurrencies are digital currencies which can be used to digitally transfer money to another person safely, without having to use intermediaries or trusted third parties, like a bank or Visa, e.g., to verify that you have sent the money and the money is now no longer yours. You might want to read that sentence again, slowly. In addition, it does it much faster at a fraction of the cost because it does away with unnecessary and expensive transaction fees.

Why 'crypto'?

The way digital currencies provide safety is two-fold. The first is that it uses Encryption technology (hence the name cryptocurrency).

What is the blockchain?

The second way is to have a public ledger, where all the transactions are kept. Thousands of computers around the world are linked together to display this ledger. They refresh and update every few minutes. This network of computers all linked together in this way is called the blockchain. You can trust it because it means that each transaction has been verified again and again by all the computers (the blockchain). With thousands of computers linked up all over the world saying the same thing, the ledger's integrity is upheld. Each cryptocurrency can have its own blockchain, although some are shared.

How does this work?

Imagine I send you 10 dollars and you send the 10 dollars to someone else. Somehow someone has to keep track of these transactions, to avoid forgeries or anyone claiming they haven't received the money. In the past, Central Banks or banks have kept details of the transaction on something called a ledger. This is based on a centralised system. With Bitcoin, currently the main digital currency, the whole system was turned on its head. Instead of a centralised system controlling the ledger, now thousands of computers, all around the world, each keep a copy of this Ledger. Every single transaction is kept there, from the beginning to present day. This is a decentralised system, called the 'blockchain'.

Please note that money in itself does not have any intrinsic value – it is only because we believe that it has value that it is worth anything. Money is just a tracking system – we track what we own and what we owe. This is called a ledger. Whatever form of money exists, we give it value because of its utility as a ledger (or tracking system of who owes what). That's what the blockchain is – a giant decentralised ledger.

Why are so many computers necessary?

The idea comes from airplane safety. If you have one computer flying the plane and the system crashes, the airplane could crash. The thought was that if there were three computers, and one crashed, then the fact that two computers were saying something different to one meant that the two outweighed the one and the plane would continue even if one crashed. The inventors of the blockchain took it one step further and wanted as many computers as possible to be in on it. So if there is a disagreement on a few computers of the blockchain, whatever the majority e.g. 51% are saying will win and that information is put on the ledger on all the computers.

A particularly brilliant analogy for this comes from Nick Szabo, the inventor of Bitgold, which many view as the precursor of Bitcoin. Imagine a fly trapped in amber. If there is only a small layer of amber, we know that the fly has not been trapped for very long. But if there is a big block of amber, we know that the fly has been trapped for a long time – no one can dispute that.

The blockchain computers are forming a layer of amber every time a transaction occurs. Once the amber covers the transaction, it is very difficult to change. Each layer of amber on top makes it more difficult to change. Each day more information and more amber are layered on top.

In other words, millions of small transactions, i.e. me sending you some money in another country, are documented on the blockchain, locking them in for good, so that they can't be changed afterwards. The information (or fly) is trapped as irrefutable evidence and the transaction can't be undone. That's the whole point of the decentralised system – the computers allow it to remain decentralised and in the hands of many as opposed to the hands of a few who are trying to control the many.

What are miners?

There are two ways of getting Bitcoin. You can either buy one at the current price (today's price is $4,200 for one Bitcoin) or you can 'mine' it. The analogy is like mining for Gold. However, with digital currencies it is slightly different, as you don't have to go down a mine to do so. With cryptocurrencies, you have to do it through something called, 'Proof of Work'. Proof of Work refers to the fact that if you want a Bitcoin, you have to literally prove that you have done work and in return you get paid in Bitcoin tokens.

In cryptocurrencies this is done by creating a scenario where if you want to get paid in Bitcoins, you have to do something which is not easy to do i.e. you have to commit your computers to solving puzzles or mathematical functions. If the computer solves the puzzle then it proves that you have dedicated power, time, effort, heat and computation to solve the problem. The more you do this the more of a 'vote' you are allowed to have. This vote is embodied in a Bitcoin token. You receive a token of Bitcoin (a fraction of a Bitcoin) in return for mining it.

Only miners are able to confirm a transaction. This is their role in the cryptocurrency network. They record transactions, verify them and disperse the transactional information in the network.

For every completed transaction monitored and facilitated by the miners, they are rewarded with a token of cryptocurrency, for instance with Bitcoins.

What this does is introduce scarcity into the system. Scarcity is important because the only way anything has any value is because it is scarce. If Gold, like pebbles, were to be found everywhere, it wouldn't have any value. But Bitcoins are not easy to mine – it takes computational power and time to do it AND there are a maximum of 21 million that can ever be mined. This creates instant scarcity.

Terms

An Altcoin (Alternative coins) is the name given to coins which were set up to compete with Bitcoin, like Dash, Litecoin and even Dogecoin. The term 'crypto', short for cryptocurrency, is used for all coins.

A digital currency is a virtual currency. It is unregulated, issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community. It is a medium of exchange that operates like a currency in that specific environment but not necessarily outside of it.

A cryptocurrency is a currency based on certain principles of cryptography. It is a type of digital token that relies on these principles to chain together digital signatures of token transfers. It is based on a peer-to-peer network and it is decentralised.

In most situations, cryptocurrency is also a digital currency, though, in even more cases, digital currency is not a cryptocurrency.

Summary:
Bitcoin is a software program that allows people to securely transfer money over the internet without a bank.

It does this by replacing the function of a bank with a network of computers running the software that verifies and transfers the money.

These computers, known as miners, maintain a global ledger of transactions that is used to validate, verify and transfer money.

2. What are the benefits of Cryptos and what problem do they solve?

The new digital revolution of money.

Cryptocurrency has many appealing benefits. Some of this is thanks to the blockchain technology previously mentioned. It is a strictly monitored process with encrypted transaction and control.

A quick history of money

Since the beginning of human time, people have used something scarce as a source of value. At the start they used bartering one object for another. But how can you buy a cow if you only have two chickens? A third entity was needed, so they used the scarcest of seashells. Then came coins made of precious metals. At the beginning, coins did not have a value stamped on them, rather the coins were weighed. Only later was an actual value stamped onto the coin.

Next was paper money backed by precious metal e.g. Gold. The idea was that you could literally walk into a bank and ask for the equivalent of your bank notes in Gold. Then paper was taken off the Gold Standard and was not backed by anything, allowing the printing of money to flourish. This is the current 'fiat' money.

The problem is that fiat money is not scarce. More money can be printed and so every year it is worth less and less. The only store of value that retains its value is Gold. But Gold is not easy to store, not easy to sub-divide and not easy to transport.

For a full breakdown of the timeline of the History of Money, see Appendices.

Scarcity is an essential part of cryptos. Take the largest, Bitcoin for example. As already stated, only 21 million will ever be made, so scarcity is part of the system.

1. No Third-Party Involvement

There's always a process you go through when using traditional money to buy yourself a new property, set up your own business or buy a new car etc. One way or another, the process requires a third-party involvement. We are talking lawyers, owners and some other external factors such as delays, documentation, extra fees etc. This in general will consume unnecessary time, money and energy to the point of giving up in some cases.

Recently, I wanted to send some money over to the USA. In order to do that, I had to pick up the phone to my bank. I was stuck in a queue listening to music for over eight minutes just to start the process. I was then charged for sending the money plus an extortionate Foreign Exchange rate which did not resemble the real rate. Finally, since the transaction was via something called an intermediary bank, I was told that they would likely charge me as well, although they could not tell me how much. The money, I was told, would be there within 3-5 working days. Since it was a large amount of money the whole thing probably cost me over $200 if you include the Foreign Exchange spread, maybe more. I agreed to everything because, well, I didn't have many alternatives.

With cryptos, I can send Bitcoins directly to the other person from my computer to theirs online, within 10 minutes. There is no spread, no Foreign Exchange (Forex) charge, intermediaries etc. And the whole thing might cost me $10 maximum.

So if you want to save a lot of time and money then cryptos are the way to go.

In short, you are in control of your own money using cryptocurrency. This is what we call the ‘decentralised’ system. It is possible to be able to pay and receive money anywhere in the world at any given time. Your transactions are practically immune to any influence from your Government, with minimum processing fees, thus preventing users from having to pay extra charges from banks or any financial institutions.

Now imagine this in EVERY part of society – from legal contracts between two companies to sending money across the world; from keeping money in escrow when buying a house to online payments. Basically, anywhere where there is currently a ’middleman’ who is either 1. Slowing it down, or 2. Making it more expensive.

2. Lower risk than traditional currencies

In this era, most people rarely have their cash in their possession now. Instead, they have an array of credit cards, debit cards and other payment cards available as their nation’s method of payment. Nothing’s wrong with that, however if the store’s connection to the server is disconnected or their machine is out of service, and you do not possess any cash, you cannot pay.

When using your card, you are giving the end-receiver access to your full-credit line. No matter how small the amount of the transaction is, the fact that you are giving someone your card to gain access to your account is already a form of ‘breach’. Most of this ‘breach’ is considered secure nowadays using differing safety measures like ‘PIN enabled’ or other methods. Then the store initiates payment by ‘pulling’ the designated amount from your account using the information provided within your card.

Cryptocurrency doesn’t work that way. Instead of a ‘pulling’ mechanism, it ‘pushes’ the amount that is needed to be paid or received to other cryptocurrency holders without any further information needed. Payments are possible without your personal information being tied to you or the transaction. Your account can be backed up and encrypted to ensure the safety of your money.

By allowing users to be in control of their transactions helps keep Bitcoin, Ether or other larger cryptocurrencies safe for the network.

3. Protection from fraud

We often hear of cases where someone's payment card is being used by other users but not the owner. When contacting his card's service issuer, it is found that the card has made certain transactions without his consent. This is what we call a fraud case.

Most of the time the perpetrators of these fraud cases get away with the crime because it is not easy to trace the fraud back to the perpetrator. What's more it is even difficult to get the attention of law enforcers to launch an investigation.

However, cryptocurrency is not viable to be used for fraud. Due to the fact that your personal information is kept hidden from prying eyes, this protects you against identity theft.

Remember, cryptocurrency is a form of digital money, created from code. Individual cryptocurrencies are, as mentioned, digital and cannot be counterfeited by senders.

Because the transactions cannot be reversed, they do not carry with them any personal information. This ensures security and the merchants are protected from any potential losses that might occur from fraud cases.

It is very hard to cheat using these cryptocurrencies due to its decentralised system and the existing blockchain system. It cannot be manipulated by anyone or any organisation thanks to it being cryptographically secure. All the computers have a copy of all the transactions and the computers are continuously talking to each other. This is the most secure way of doing it as no one can hack in and make changes.

If someone wanted to hack into the blockchain they would be wasting their time hacking into just one or a few computers, since the information on the majority of computers always wins. So in order to hack in they would have to hack 51% of the computers around the world that make up the blockchain to make a change. The computational power required to do this is prohibitive.

Also it would take some time. The blockchain updates or refreshes its data every few minutes, giving a would-be hacker a few minutes window to hack in before everything is reset. After that they would have to start again. So not only would they have to hack into 51% of the thousands of computers around the world that make up the blockchain, but they would also have just a few minutes window to do it in.

4. Universality

Over the course of payment history, nations worldwide had their differing methods of payments. We had bartering or money-goods exchange systems. It wasn't until traders visited other countries that they found out how to trade items with one another.

Thanks to various innovations and developments, we now have multiple methods to trade and exchange moneys worldwide.

But even with all the upgrades, we are still experiencing problems doing transactions across the globe. There are always currency issues, bank authorisations, unacceptable payment methods and some other varying issues experienced by business owners or travellers abroad.

Fact is, not all countries have similar financial procedures. Your card or currency may not be accepted by other countries and that is a major setback for some people. For example, most online banking, payment or cash system requires additional processing fees for their service.

However, cryptocurrencies are not bound by any of the exchange rates, transaction charges, the interest rates or any other fees applied by any countries. They can be used at any time, in any part of the world, without experiencing any problems.

It also saves a lot of your time and money by reducing additional spending over transferring money from and to multiple countries. Which means cryptocurrency operates on an international platform which in turn make transactions easier than your average bank to bank transfer.

Cryptocurrencies have three important properties:

1. Transactional Property

Cryptocurrency transaction is fast and global. Transactions are propagated immediately in the network and are confirmed within minutes. Since the transactions are managed by a global network of computers, they do not take into account your physical location. It is possible for you to send your cryptocurrency to someone in your vicinity, or even if they are living on the other side of the world.

2. Monetary Properties

Some people want to use Gold as a monetary value. However, it is not easy to store, it is not easy to subdivide and it is not easy to send. Because it is heavy, sending it would also be costly. Cryptocurrencies can be seen as digital gold because they are easy to store, easy to subdivide, easy to send & transport and less costly.

The currencies are in controlled supply; thus there is a high chance that the value of the currencies appreciates over time. As mentioned earlier, Bitcoin will somehow reach its final number somewhere in 2140.

3. Revolutionary Property

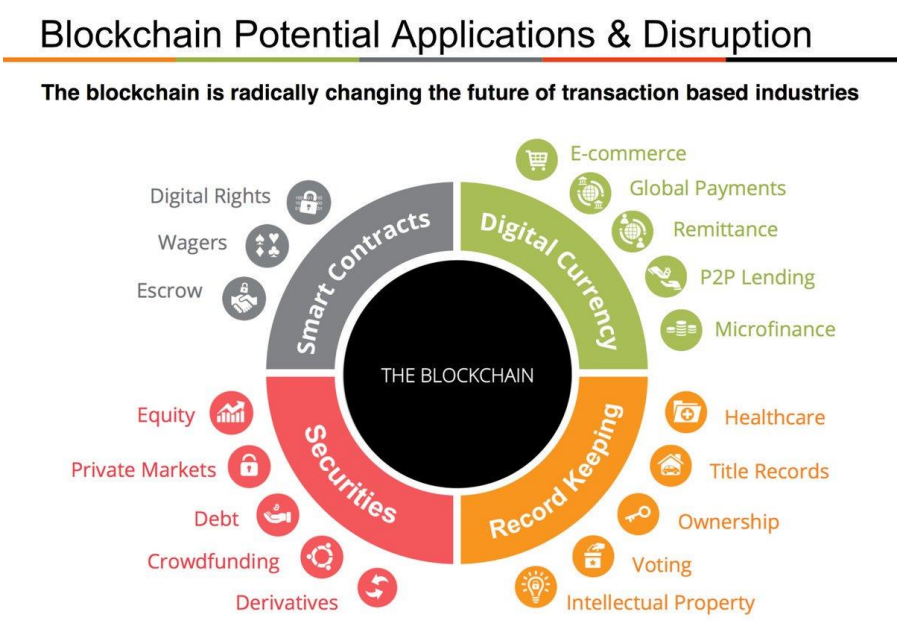
You have more control of what is going on in your account and how the system works and operates. This is due to the decentralised network of peers which keeps a consensus on account balances and the transactions made. As compared to your physical bank account, which can be changed and controlled by people you don’t see and governed by rules you don’t even know (how many of us really read the small-print?).

I attended the 2017 World Blockchain Conference in London. Look, to prove it I have a picture of me in the audience. Can you see me in the red circle? :--)

Two things became clear. Firstly, there is big excitement about Cryptocurrencies and this excitement is growing rapidly. The organisers told me that last year there were only 30 people at the conference. This year there were well over 300 as far as I could see.

Secondly, whether believed in cryptocurrencies or not, everyone believed that blockchain would transform the world.

Even people like Jamie Dimon, Head of JP Morgan, who is a fierce critic of Bitcoin, is heavily investing in the blockchain, because of the many applications of the blockchain and the potential it has to disrupt most industries, including his own.



One strategy I am therefore pursuing is to find current public companies in the stock market which are set to gain from the use of blockchain technology. Some of them are established companies and some of them are fairly new, but you can buy them on the stock market now.

3. Why is it important for YOU?

"Nothing in life is to be feared, it is only to be understood."

– Marie Curie

Like most things tech, the realm of cryptocurrency can be a bit complex to master and is still new to many. But the benefits of purchasing this currency are surely worth your investment in both time and money. Experts have also predicted that it may be the next big thing in finance.

1. Crypto Trading and Investing

Bitcoin trading can be very profitable for both professionals and beginners. The market is new, where arbitrage and margin trading is widely available. The currency's high volatility has also played a major role in bringing new investors to the trading market.

Compared to other financial currencies, Bitcoin has very little barrier to entry. If you already own Bitcoin, no verification is required and you can start trading almost instantly. Moreover, Bitcoin is not fiat currency. This simply means the price is not related to the economy or policies of any single country.

And unlike stock markets, there are no official Bitcoin exchanges. Instead, hundreds of Bitcoin exchanges operate 24/7 around the world. Because there are no official exchanges, this results in no official Bitcoin price andthe currency is known for its rapid and frequent price movements.

2. Personal Spending

Secondly is personal spending. There are millions of items now being sold for Bitcoins and this number is only increasing. You can use Bitcoin to purchase almost anything! From buying cars (Tesla) to travelling the world (Cheapair). From buying a Microsoft product to paying Estate Agents.

3. HUGE potential

We could well be in the midst of the next Gold Rush. If that is the case, do you really want to miss out?

For me personally, I wouldn't want to be the one who said "I knew it was going to be big, but I was too lazy to do anything about it and yet again I missed out while everyone else made a fortune" AND "What if everything I have learned so far has led me up until this point." I even had the thought “What if I become the Warren Buffett of cryptocurrencies? Someone has to – why not me?" LOL.

4. Don't need a lot of money

You don’t need a lot of money to make really sizeable profits – even a few hundred could turn into tens of thousands.

Have you heard of Erik Finman? The teenage Bitcoin millionaire who started picking up Bitcoin at only $12 a piece back in May 2011, when he was just 12 years old. He received the Bitcoin as a tip from his brother and a $1000 gift from his grandmother.

He now reportedly owns 403 Bitcoins, which holds a value of roughly $4000 where it has accumulated to a stash of just over $1.6 million and change.

I personally bought £850 worth of Antshares (now called NEO) and turned that into over £40,000 in three months. Where else can you get 4000% return in three months?

5. Volatility

You might have thought that Forex was volatile. You haven't seen anything yet. There are days when the portfolio is down by -15% and the next up by 15%.

Individual coins can fluctuate by 50% in one week. One of my coins went up over 100% in just one day. In stocks, this kind of volatility would take an entire year!

Volatility is our friend – most people are scared of it because they feel they can’t control it, but it is great. How else can we buy low and sell high? An idea is to wait for the coin to go down and start buying into it in order to lower our average price.

4. We are just at the start

The majority of people haven't heard of cryptocurrencies and even less about the blockchain, meaning the value will increase as they become mainstream.

4. What are the main cryptocurrencies and what do they do?

There are around 1000 coins/Altcoins. Some are legitimate and some may not be. It is imperative that you do your own research before investing

Which ones are the best ones?

This changes all the time – do your research. We will go more in depth into this in the Chapter “How do you make money in cryptocurrencies?”

Below are the largest coins at time of writing in terms of their market capitalisation (price in dollars x number of shares in the market). They are in no particular order:

a. Bitcoin

What problem does it solve?

The first blockchain, solving the problem of duplication and manipulation. It's like Liquid Gold.

This is the first ever cryptocurrency invented and remains by far the most sought after cryptocurrency to date. Bitcoin is known as the digital gold standard in the cryptocurrency network. As explained, Bitcoin is the pioneer of blockchain technology that made digital money possible.

It is the first ever decentralised peer-to-peer network powered by its users without any central authority or middleman which means no unnecessary costs are included in the digital money transaction.

One major advantage that it has over other cryptocurrencies is Bitcoins are impossible to counterfeit or inflate. The reason being there are only 21 million Bitcoins created for mining, no more no less. Therefore it is predicted by 2140, all Bitcoins will already be mined.

Thanks to its blockchain technology, you have ultimate control over your money and transactions without having to go through a third party such as the bank or PayPal.

Interesting fact: WikiLeaks would not be here if it weren't for Bitcoin. When credit card companies stopped their service to WikiLeaks, people used Bitcoin to keep the service alive.

Media companies and investment firms in South Korea, India, Australia, Canada and Japan have started discussing on how Bitcoin may surpass the value of certain fiat currencies in the future as an alternative monetary system. Japan even made it an official currency in April 2017, paving the way for other countries to do the same.

Over the years of Bitcoin's existence, its value has fluctuated tremendously from zero to over $4200 per Bitcoin to date.

Have I invested in Bitcoin?

I buy Bitcoin to then exchange it for other Altcoins, so I hold very few Bitcoins.

b. Ethereum

The second most popular currency is Ethereum. It has scored itself the second spot in the hierarchy of cryptocurrencies. This digital currency, launched in 2015, is predicted to surpass Bitcoin and may be the cryptocurrency of the future.

Is Ethereum similar to Bitcoin?

It is in a way, but not really. Like Bitcoin, Ethereum is a part of a blockchain network. The main difference between the two currencies is that the Bitcoin blockchain focuses on tracking ownership of the digital currency while the Ethereum blockchain focuses on running the programming code or network.

Instead of having to build an entirely original blockchain for each new application, Ethereum enables the development of thousands of different applications in a single platform. In the Ethereum blockchain, miners work to earn Ether. Ether is a crypto token that helps run the network.

Another use of the Ethereum blockchain is its ability to decentralise any services that are centralised. For instance, Ethereum is able to decentralise services like loans provided by banks, online transactions using PayPal as well as voting systems and much more.

Ethereum can also be used to build a Decentralised Autonomous Organisation (DAO). A DAO is a fully autonomous organisation without a leader. DAOs are run by programming codes on a collection of smart contracts written in the Ethereum blockchain. DAO is designed to replace the structure of a traditional organisation and, like Bitcoin, eliminating the need for people and a centralised control.

<u>What problem does it solve?</u>

Ethereum solves the problems of legal contracts online, eliminating middlemen taking fees from transactions.

Firstly, a third party cannot make any changes to the data. The system is also tamper and corruption proof. This is because Ethereum is built based on a network formed around a consensus which, as a result, makes censorship impossible.

Secondly, just like Bitcoin, Ethereum is backed up by secure cryptography. Therefore, the applications are well protected against any form of hacking.

Ethereum went from around $400 to a low of $149 to its current price of $317.

<u>Do I hold Ethereum?</u>

This is my second largest holding. I bought into Ethereum on 10 separate occasions as the price was falling from its high. At time of writing that position is up by 31%.

c. Ethereum Classic

A few years back someone hacked into an Ethereum-based application and stole millions. There was an internal argument about whether this event should be allowed to happen or to go back in time and make good the money so no one loses out. The purists whoargued that there is no going back in blockchain technology broke away to form the new Ethereum Classic.

What problem does it solve?

It is essentially the same as Ethereum, so it is unclear why we need two of the same. However, lately it is looking to distinguish itself from Ethereum.

Do I hold Ethereum Classic?

Yes, I have one position in Ethereum Classic which at time of writing is up 220%.

d. Ripple

Ripple was launched in 2012.

What problem does it solve?
Banks can use Ripple to make payments faster and cheaper nationally and internationally.

If you have sent money overseas, you will have used a SWIFT code which is an entity with a monopoly on border transfers – in 200 countries, with more than 11,000 financial institutions forming its branches.

However, Ripple while working together with financial services, banks and institutions wants to take down SWIFT and disrupt its functionality.

Ripple is actually a technology that has a dual function; as a digital currency as well as a digital payment network for financial transactions.

Unlike the other cryptocurrencies, Ripple operates on an open-source and a peer-to-peer decentralised platform which allows a transfer of money in any form, both fiat and cryptocurrency.

Ripple uses a middleman in the currency transactions. The medium (the middleman) known as “Getaway” acts as a link in the network between two parties wanting to make a transaction.

The way it works is that the Gateway functions as a credit intermediary that receives and sends currencies to public addresses over the Ripple network. This is why Ripple is less popular when compared to the other digital currencies. Also, many people don’t like Ripple because they believe that cryptocurrencies is an answer to the domination of the current banking system and Ripple works with the banks.

Ripple acts as a bridge for other currencies which includes both fiat and cryptocurrencies. In Ripple’s network, any currency can be exchanged between one another.

If user X wants Bitcoins as the form of payment for his services from Y, then Y does not necessarily have to possess Bitcoins. Y can pay X to X’s Gateway using US Dollars or any other currencies. X will then receive Bitcoins converted from the US Dollars from his Gateway.

The nature of Ripple’s network and its systems exposes its users to certain risks. Even though you are able to exchange any currencies, the Ripple network does not run with a proof-of-work system like Bitcoin. Instead, transactions are heavily reliant on a consensus protocol in order to validate account balances and transactions on the system.

But Ripple does improve some features of traditional banks. Namely, transactions are completed within seconds on a Ripple network even though the system handles millions of transactions frequently.

With traditional banks, even a wire transfer may take up days or weeks to complete. The fee to conduct transactions on Ripple is also very minimal, as opposed to large fees charged by banks to complete cross-border payments.

<u>Do I own Ripple?</u>

I have three positions in Ripple due to a Tim Ferris podcast with Nick Szabo, the creator of BitGold. Nick said that the currencies that could cross the bridge between the current banking system and the new digital system would be the winners. Ripple is the first to attempt this.

At time of writing, this position is up by 14%.

e. Monero

What problem does it solve?

The technology solves the problem of privacy. People who might be under dictatorship of governments can use Monero to keep their identity hidden. So it has a real function to help the underprivileged in the world regardless of your creed, colour, sex etc. who might not be able to existing systems, not be able to open a bank account etc.

Monero's main goal was to create an algorithm to add the privacy features that is missing in Bitcoin. Monero invented a system to conceal the identity of its senders and recipients.

The system combines a user's private account keys with public keys obtained from Monero's blockchain to create a ring of possible signers that would not allow outsiders to link a signature to a specific user.

While Monero users have the ability to keep their transactions private, they are also able to share their information selectively.

Monero has received the acceptance of multiple dark web marketplaces and has generated its own fan base due to its privacy settings. Therefore, it is less speculative as compared to other digital currencies and traders purchase Monero as a hedge for other cryptocurrencies.

Do I own Monero?

Yes, I have three positions in Monero which at time of writing are up by 138%.

f. Dash

Dash – Digital Cash is one of the most promising alternative coins to Bitcoin.

Dash is unlike other cryptocurrency projects like Ethereum or Stratis which are more of a development platform.

Dash advocates itself as peer-to-peer decentralised electronic cash. It intends to be as liquid as real cash which we use in our respective countries.

Dash is built upon Bitcoin's core code with the addition of new features (such as privacy and quick transactions).

Like Bitcoin, Dash is open-source and has its own blockchain, wallet infrastructure, and community. But unlike Bitcoin, its transaction fee is negligible.

Moreover, it appears from the attitude of the development community that Dash will only remain as digital money for the Internet, which is a good thing.

Dash is designed to have a total supply of 18 million coins.

At present, the circulating supply of Dash is over 8 million and it will reach 18 million in the year 2300.

<u>Do I own Dash?</u>

I only have one position which is up by 216%. This is one I wish I had more of. I am looking for any weakness in the dollar price to get in again.

g. Litecoin

When the currency was first launched, it aspired to be the 'silver' to Bitcoin's 'gold'.

The main reason of Litecoin's creation is to make up what Bitcoin lacked. The main difference between Litecoin and Bitcoin is the 2.5 minute time to generate a block for Litecoin, as opposed to Bitcoin's 10 minutes.

For miners and technical experts, the Litecoin possesses a very important difference to Bitcoin, and that is a more improved work algorithm which speeds up the hashing power and system altogether.

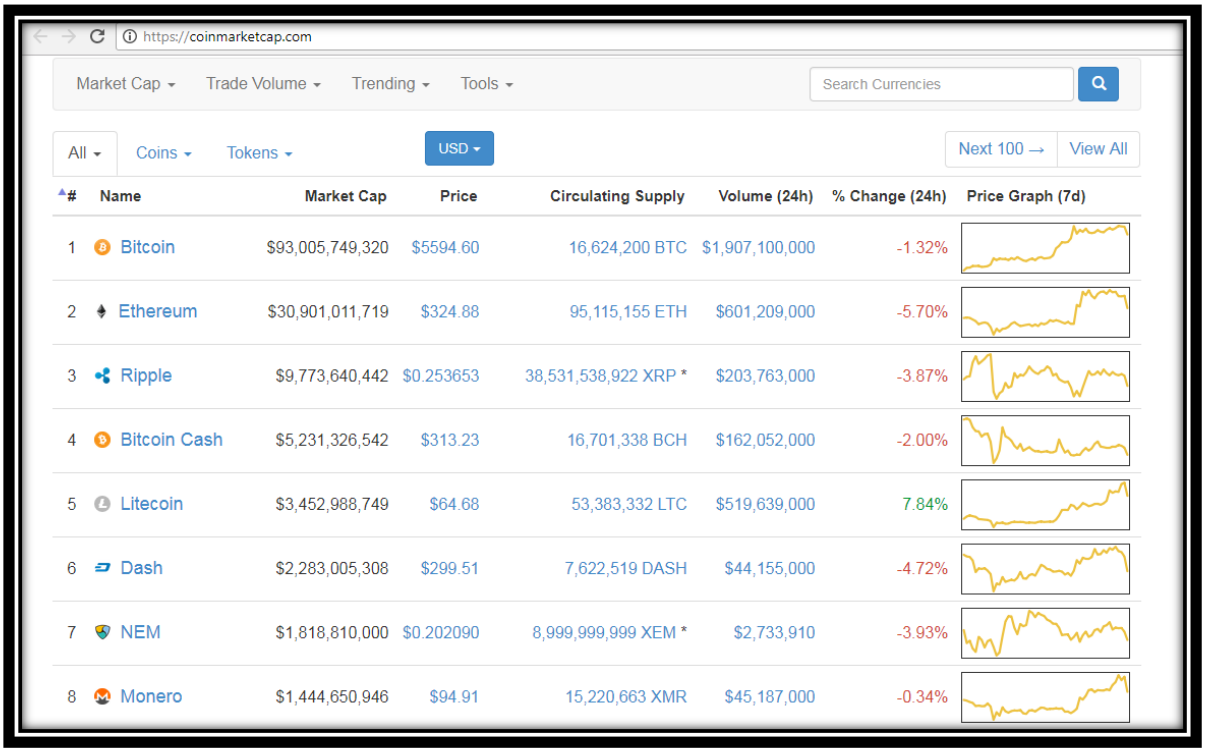
One of the biggest advantages that Litecoin possesses is it can handle a higher volume of transactions thanks to its algorithm. The faster block time also prevents double spending attacks.

While Litecoin failed to secure and maintain its second place after Bitcoin, it is still actively mined and traded and is bought by investors as a backup in case Bitcoin fails.

Do I own Litecoin?

This is an interesting one because it has a lot of promise but it just doesn't seem to be going in the right direction. If it doesn't do something soon it might be overtaken by some of the promising new coins like Dash. I hold one position which at time of writing is up by 22%.

You can look up the market capitalisation and more information on the above on www.coinmarketcap.com



#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$93,005,749,320	$5594.60	16,624,200 BTC	$1,907,100,000	-1.32%	
2	Ethereum	$30,901,011,719	$324.88	95,115,155 ETH	$601,209,000	-5.70%	
3	Ripple	$9,773,640,442	$0.253653	38,531,538,922 XRP *	$203,763,000	-3.87%	
4	Bitcoin Cash	$5,231,326,542	$313.23	16,701,338 BCH	$162,052,000	-2.00%	
5	Litecoin	$3,452,988,749	$64.68	53,383,332 LTC	$519,639,000	7.84%	
6	Dash	$2,283,005,308	$299.51	7,622,519 DASH	$44,155,000	-4.72%	
7	NEM	$1,818,810,000	$0.202090	8,999,999,999 XEM *	$2,733,910	-3.93%	
8	Monero	$1,444,650,946	$94.91	15,220,663 XMR	$45,187,000	-0.34%	

5. Where is the value of cryptocurrencies, how are prices determined and what could Bitcoin be worth in the future?

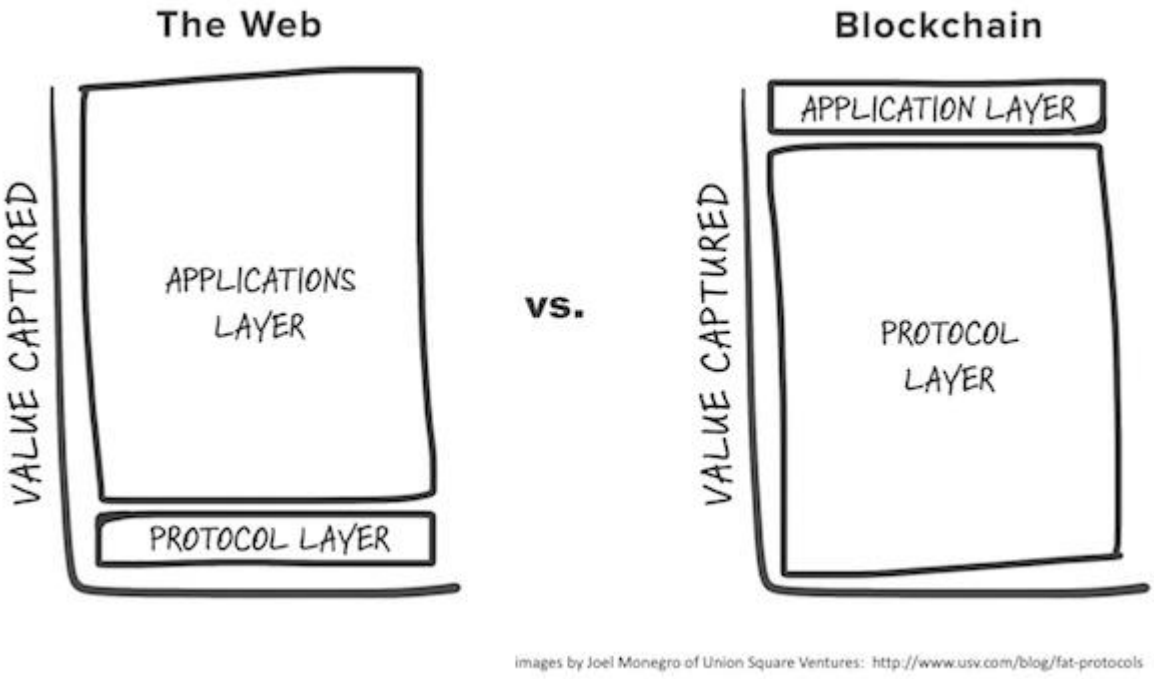
"Bitcoin will go to $500,000 within three years or I will eat my own penis"

- John McAfee, the founder of McAfee software and CEO of MGT Capital Investments and one of the largest Bitcoin mining companies in the world.

5a. Where is the value of Bitcoin and cryptocurrencies?

Some people call Bitcoin and the blockchain 'Internet 3.0'. We understand why they may see it in this way, however, we have to be clear that Bitcoin is a different technology to the Internet. Bitcoin and Ethereum are what is called a 'Fat Protocol'.

For the Internet 'HTTP' is a protocol that defines how information is sent over the Internet. On the back of these protocols, programmers built application like Facebook and Google. While these protocols created an enormous value, most of the value was captured by the applications that were built on top of the Internet. Meaning that the people who created HTTP didn't make money and are relatively unknown. However, the owners of Facebook and Google became billionaires and are celebrated entrepreneurs.



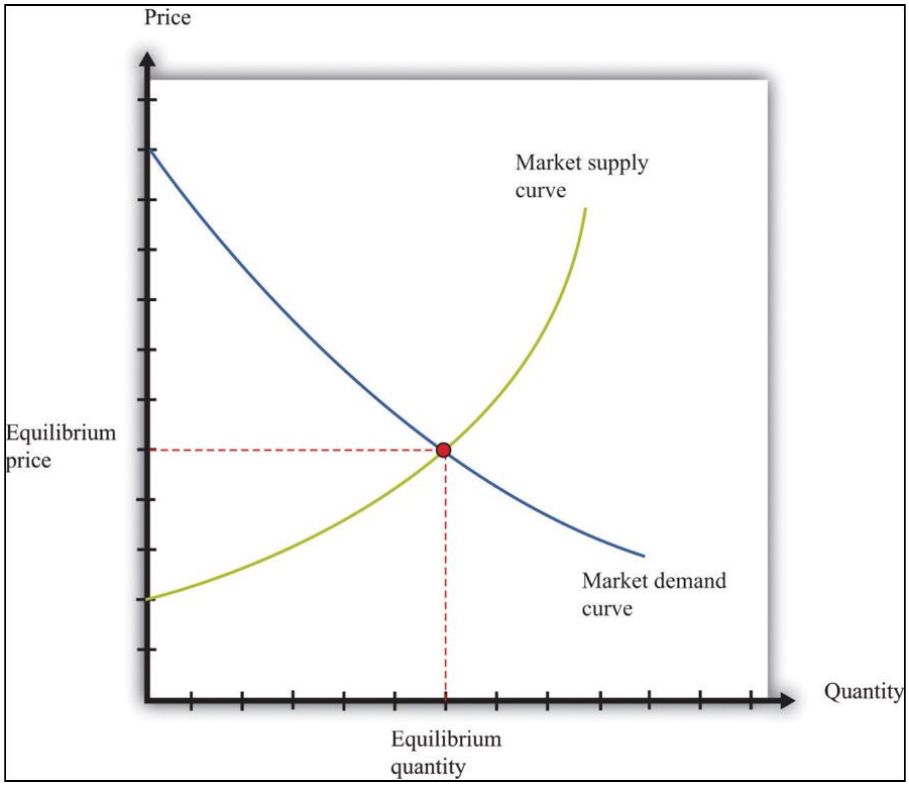
With Bitcoin and a platform like Ethereum, it is the actual network itself that is generating the value. Tokenholders are the ones who are going to benefit. The value will be captured by those building and investing at the blockchain protocol layer because of the financial incentives (tokens) that are part of the network's design.

Participants of the network (users, developers, investors etc) are incentivised to grow the blockchain network because as the network expands the tokens are going to be worth more.

5b. How Are prices determined?

A. The value of cryptocurrencies are dependent on the market, where the prices of various cryptocurrencies vary a lot and it is one of the most fluctuating and volatile markets to date.

B. The price of cryptocurrencies, like any other products, is dependent on demand and supply. If more people demand a particular currency and it is short in supply, then the value increases. More units are mined by miners to balance the flow. However, most currencies limit the supply of their tokens.



C. Scarcity is an important factor when compared to fiat currencies. Fiat currencies can be printed every day, making our money worth less every year. Digital currencies, however, have limited supply. For instance, the total amount of Bitcoin issued is only 21 million. Therefore, Bitcoin's supply will decrease in time and will reach its final number by 2140. It also explains why Bitcoin's value is higher compared to other cryptocurrencies. Dash has the same idea, limiting itself to 18.9 million – this might explain why its price is also doing well.

D. Trust. This one is often overlooked but, like with any currency, tokens will only have value if people have trust in it. Trust comes from a lot of sources such as the credibility of the developers, the kind of service provided etc.

5c. What could the price of Bitcoin be?

Well, this is the 64 million dollar question, isn't it?

A client of mine and I came up with quasi the same potential possible future valuation = $100,000 per Bitcoin. This is how we calculated it – it's not very scientific. If Bitcoin really is Liquid Gold and so becomes the new 'Golden Standard' as a store of value, then you have to figure out the current value of all the Gold in the world that has been mined.

If that is valued at approximately 8 trillion dollars and if Bitcoin reaches that same level and there are only 21 million Bitcoins ever mined, then that would mean $400,000 per Bitcoin. Important here is the scarcity factor – if that ever changed and more were created, then all bets are off.

A multi-millionaire investor friend of mine once told me a long time ago that if you talk to a start up founder and they say their business is going to make x profits in y time, and it would take z costs to do it, then it will probably be half the amount of profits, take double the amount of time and cost double the amount. I have very much taken this to heart throughout my investing career. Therefore, on a potential valuation of $400,000 I would halve it and halve it again. That's how I came up with a potential number of $100,000. I told you, not very scientific. It still leaves Bitcoin with a lot of upside. I just don't know how long it will take. It's going to take longer than you think.

If you feel this valuation is not big enough, then there are others who believe Bitcoin could go to $1 million valuation per Bitcoin. John McAfee, the founder of McAfee software and CEO of MGT Capital Investments and one of the largest Bitcoin mining companies in the world has publicly bet that Bitcoin will hit $500,000 within three years or he will eat his own penis. That's a dangerous

thing to say because I think due to its scarcity it will go up but I don't know WHEN.

There are a few things that could act as a catalyst. China has banned bitcoin before and unbanned it If it were to unban again then prices would explode Also when leverage comes in prices will explode –

Now I hope Bitcoin hits $500,000 within three years for more than one reason…

6. How to make money with cryptocurrencies?

There are many ways to make money with cryptocurrencies. The four most popular ones are:

1. You can mine them

This is where you use your computer(s) to mine for Bitcoin i.e. use the computational power of your computer(s) to help verify certain transactions on the blockchain and be rewarded with Bitcoin or other coins.

In my opinion there is not much money in it for the average person.

2. You can lend them

This is where traders who need margin and leverage borrow your coins to trade with. They have to give them back to you with a % commission.

3. You can buy already established cryptocurrencies

This is the topic of the following chapters.

4. You can buy new ICOs

Recently there have been a flurry of new Initial Coin Offerings where, if you get it right, you can invest £1,000 and turn it into £10,000 or even £100,000 in a relatively short period of time. Therefore, we will also be discussing this topic.

When choosing cryptocurrencies, do your research. Don't get caught up in the hype. When you are researching, remember to ask:

1. "What problem is it solving?" If it doesn't solve a problem then why would anyone use it or buy it? And

2. "Does it have the right team to solve that problem?"

Bitcoin and Ethereum are the most widespread by far. Imagine them like the Reserve Currency of the crypto world – if you wanted to invest in other cryptos, then you have to buy Bitcoin or Ethereum with your local currency first. Then you buy the other cryptocurrencies with your Bitcoin or Ethereum.

If you don't want to buy the cryptocurrencies themselves, you can always buy a Bitcoin fund or Bitcoin tracker. I did this for my daughter in her Junior ISA and it went up 98%, making her just under £2,000 in just three months.

This might not seem like a lot of money but £2,000 in three months isn't bad for an eight year old!

What are the signs of a 'bad' cryptocurrency

Avoid these signs of a bad cryptocurrency

1) **Me-too coins** – these are coins that do exactly the same as already existing coins and don't really add any more benefits or USPs. They are just copying what has already been done. Avoid these. If, however, they are sufficiently different and do the same but do it in a much better or faster or cheaper way etc. then it might be worth considering

2) **Coins for specific industries** – what I mean by this is coins that are designed for just one market. A perfect example is Potcoin. I actually bought some but I regret it now because all they are saying is "here is a market and we are going to create a coin for this market so everyone can use this coin to buy marijuana." But in reality there is no real NEED for this coin. It doesn't solve any PROBLEMS. You can use Bitcoin or Monero or Ethereum instead. Worse still, there are other coins like Dopecoin, Cannabiscoin, Hempcoin doing the same thing. Paragon, on the other hand, is creating a platform for the Marijuana industry – I own tokens in Paragon too.

3) **Teams that are either too small or unqualified** – in reality it is not easy to make a start up successful, and the competition is only going to intensify. It is best to check out the backgrounds of the team and see if they really do have **the experience** to pull off what they are suggesting in their whitepaper. Also, the **team needs to be large enough** to handle this or at least they have to have plans to hire more relevant team members. A one-man band or three people can't dominate an industry.

4) **Low trading volume** – it means that that not enough people are buying and selling. This is not a good sign. You want to see ever-increasing volume as the market is waking up to the opportunity.

If you take care of the above then you should avoid the majority of coins that are scams.

7. How to start buying Bitcoins, Ethereum and other Altcoins

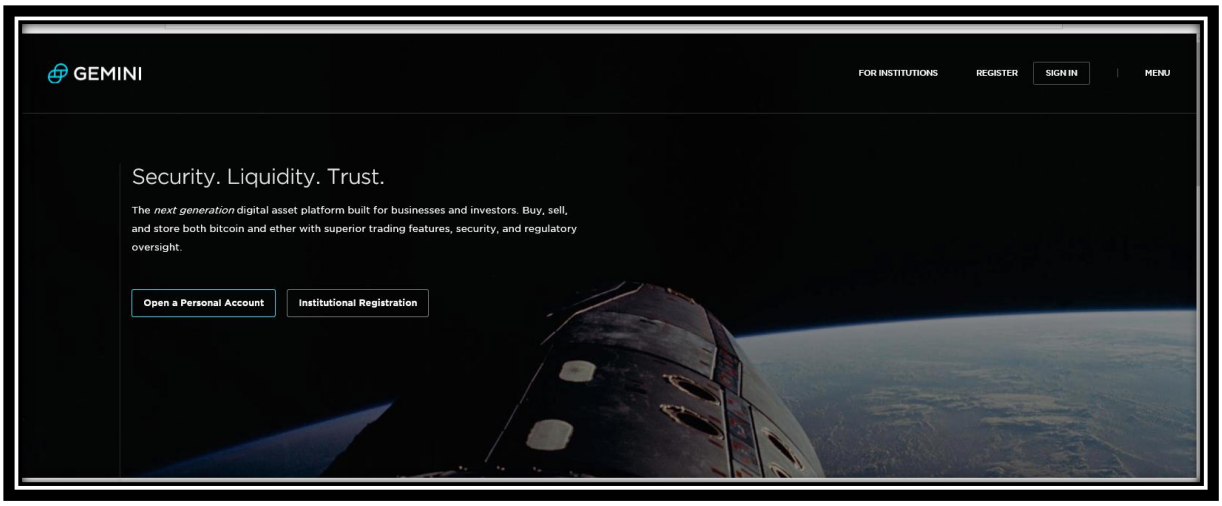
Generally, you have to buy Bitcoin or Ethereum with your fiat money first. Then you can buy other Altcoins with Bitcoin or Ethereum.

There are two ways of buying Bitcoin – through an Exchange or Direct.

1. **Exchanges**

    a. Fiat exchange

Cryptocurrency exchanges are websites which allow you to buy, sell and exchange cryptocurrencies for other digital currencies or fiat currencies like USD or Euro. Kraken is one of the largest. When I started I used Gemini.



The exchanges require you to open an account and verify your identification. Once you have exchanged fiat for Bitcoins, you can then either buy other coins, or in the case of Gemini, you have to then send your Bitcoins to Coin exchanges, like Poloniex, Bittrex or Coinbase (see below).

    b. Coin Exchange

These are websites that connects buyers and sellers where they charge certain fees for a completed transaction.

i. Reputation

Before you start your exchange on your selected site, ensure you've gathered sufficient information regarding the site such as reviews from professional traders as well as well-known industry websites.

ii. Fees

Most exchanges will have fee-related information on their websites. Before joining any sites, ensure you have understood the exchange jargons: deposit, transaction and withdrawal fees. Fees may vary according to the exchange you choose.

iii. Payment Methods

Take note of the payment method available. Does the site use credit and debit card? Wire transfer? PayPal? If a particular exchange has very limited payment methods then it may not be convenient for you. Always remember that purchasing currencies via credit card will always require ID verification and it comes with a premium price to increase the security measures. Always check the fees for using credit or debit cards, as they can be very high.

Meanwhile, purchasing cryptocurrency via wire transfer will take longer as it takes time for banks to process.

iv. Verification Requirements

The majority of Bitcoin's trading platforms both in the US and the UK require a form of ID verification to make deposits and withdrawals. Some exchanges will also allow you to remain anonymous. Bear in mind that verifications may take several days but this is to protect exchanges from any sort of money laundering.

v. Exchange Rate

Do not be surprised that different exchanges offer different rates. Therefore, always remember to shop around and to not immediately settle on an exchange. This makes a big difference on your investment as cryptocurrency rates are known to fluctuate in value up to 10% and even higher in some circumstances.

As cryptocurrency is gaining more attention around the globe, there is a vast array of exchange platforms to choose from. But not all exchange platforms are created equal.

When I started I transferred GBP from my bank to a Fiat Exchange, like Gemini in USD, where I bought my Bitcoin.

From there I would transfer money to my Coin Exchanges, Poloniex and/or Bittrex.

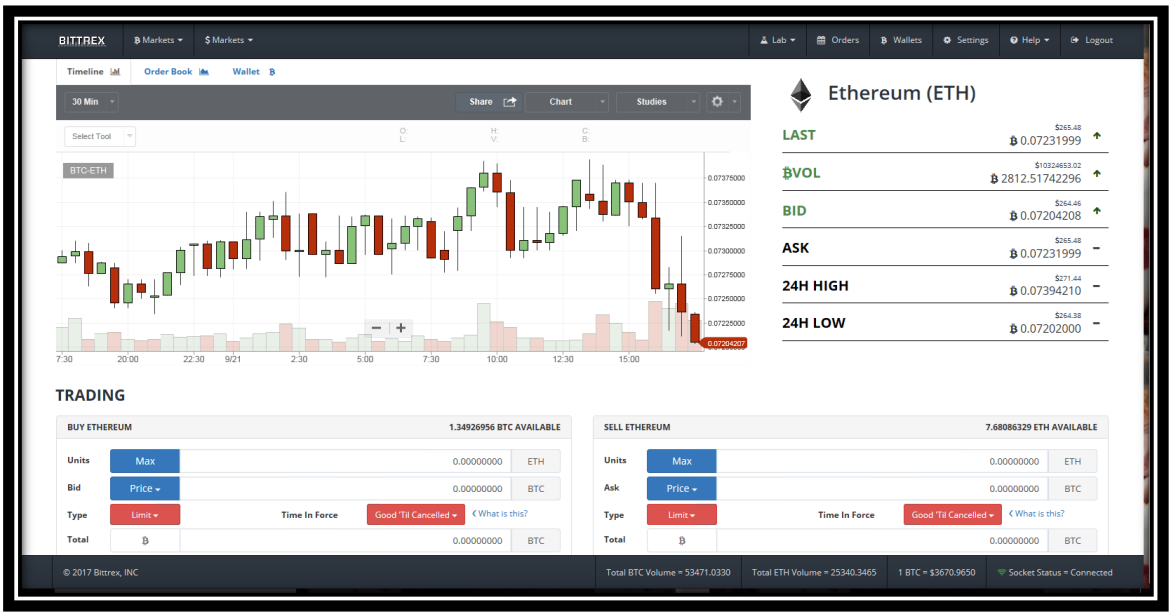
So I decided to open an account with an Exchange that was present in Europe, Kraken. I could send my GBP direct in GBP to Kraken. I would then exchange my GBP for Bitcoin and then send it to either Poloniex or Bittrex. Recently Kraken stopped accepting GBP but people with Euros can still use it.

c. Examples of Coin Exchanges

i. Poloniex: this is the first one I ever used.

ii. Bittrex: this is the second one I opened.

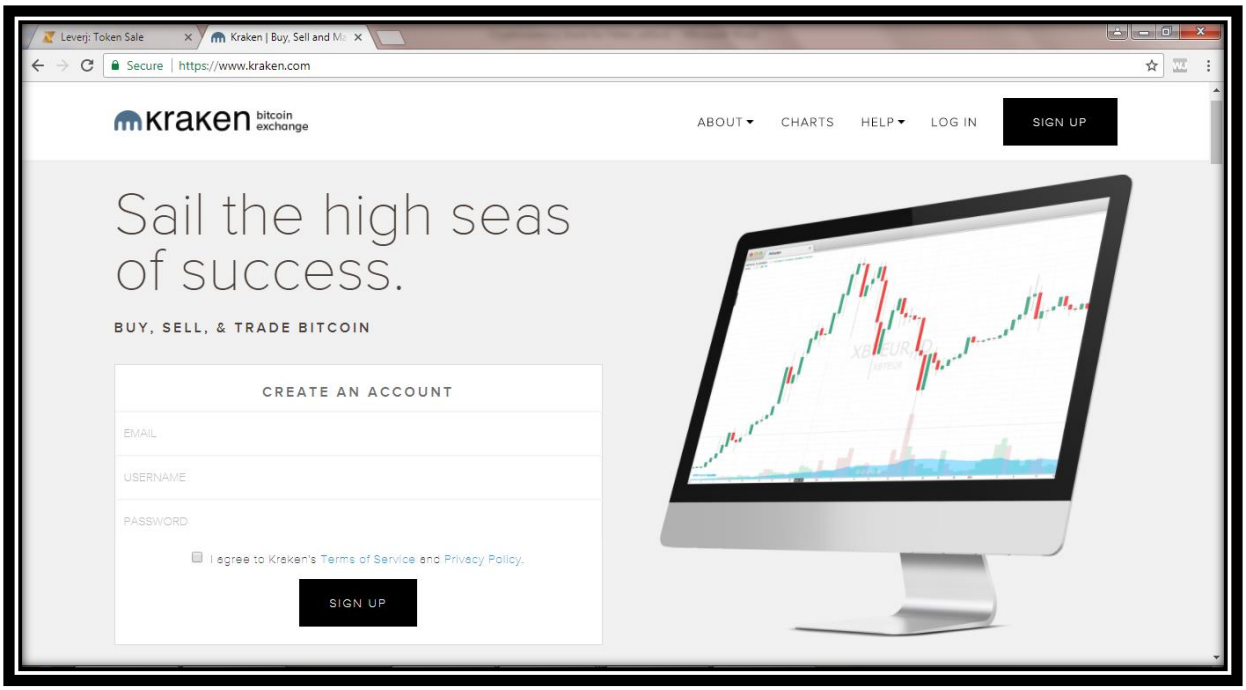
Bittrex has one of the most numbers of coins to trade, that's why I like it so much. This is what Bittrex looks like once you have logged in:



iii. Kraken: The third one I opened was Kraken.

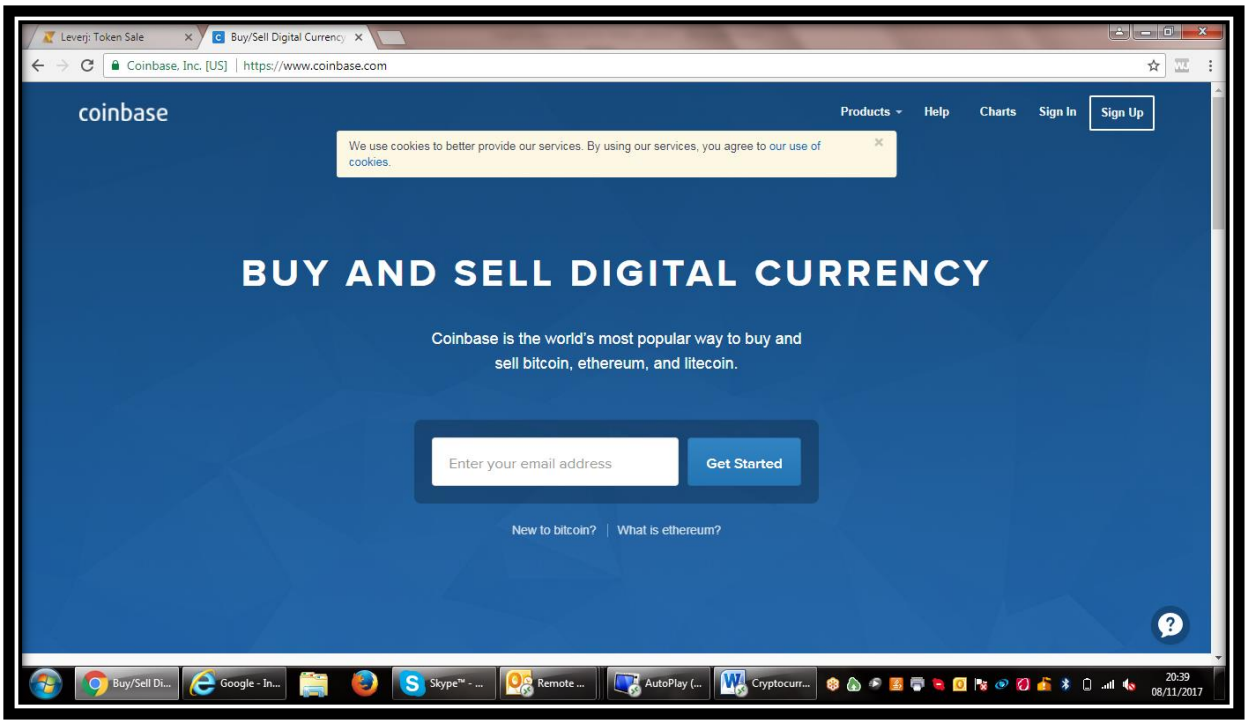
It is one of the largest exchanges in Europe. Now that it no longer accepts GBP I don't find it as useful, however our Continental friends can still use it to send their Euros and purchase Bitcoin.

Since the selection of other coins are limited however, unless you are thinking of just holding Bitcoin, Ethereum and some of the other larger coins, you will probably be sending your money to exchanges such as Bittrex or Poloniex.



iv. Coinbase: this is the best known. No idea why I haven't used it but I haven't :-)

Actually while writing this book I realised that I probably should open an account with Coinbase and have even made a video on how to open the account for the members of our Crypto Club.



An important note: Opening these accounts is simple but it is not easy. We are at the beginning of a new technology here. Things are getting better but as a beginner it might seem very convoluted at first, some might say downright confusing.

This is a GOOD thing. It keeps the masses away while you and I get our positions. Once the doors open, everyone will want to get in. We will be in a great position once that happens. So be grateful that it is not easy to open an account, otherwise everyone would be doing it right now :-)

2. **Direct**

One of our traders here used www.localbitcoins.com to exchange GBP into Bitcoin (BTC). *"I found a seller selling BTC at a predetermined price, got myself verified as per their instructions. And then made a bank transfer to them. The BTC were held in escrow until payment was received. As soon as the payment has been confirmed the BTC are released. I then transferred my BTC from the site into an exchange."*

For an idea of UK exchanges, check out **www.bittybot.co/uk** for a list of all UK Bitcoin exchanges and other exchanges which trade in British Pounds (GBP) ordered by ask price (lowest first).

As always, please do your own research and due diligence.

8. Which strategies do I use?

"After spending many years in Wall Street and after making and losing millions of dollars I want to tell you this: it never was my thinking that made the big money for me. It always was my sitting. Got that? My sitting tight!"

- Jesse Livermore, Millionaire Trader

Once we have opened up our accounts, we can start to invest in the coins.

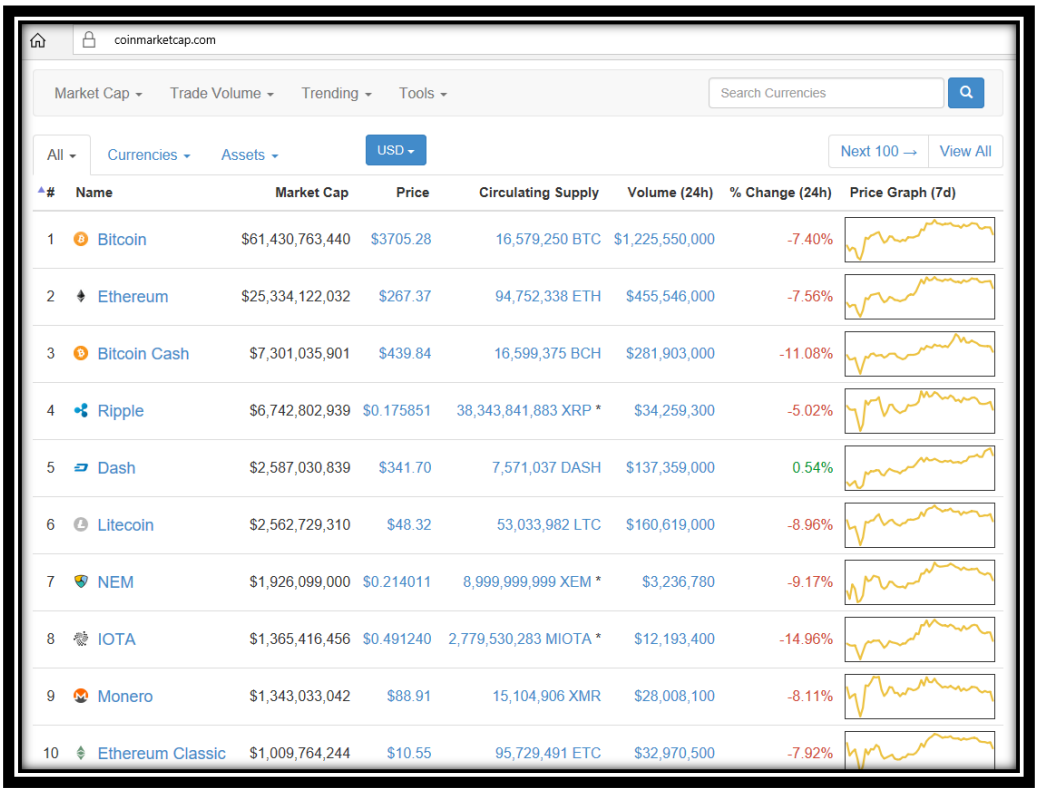
All you need now is a strategy. Most people do not have a strategy which they have thought about in advance, written down and then follow to the letter.

That is the biggest mistake of all. Before we start getting into the strategy, here are a few other mistakes you should try to avoid at all costs:

Mistake 1:

They invest in something they don't really understand or believe in long term. Therefore, they are too easily tempted to sell if the price begins to fall in the short term.

To counteract this mistake, start by sticking to the major ones in terms of market capitalisation ie top ten for safety first while you test the market (www.coinmarketcap.com).

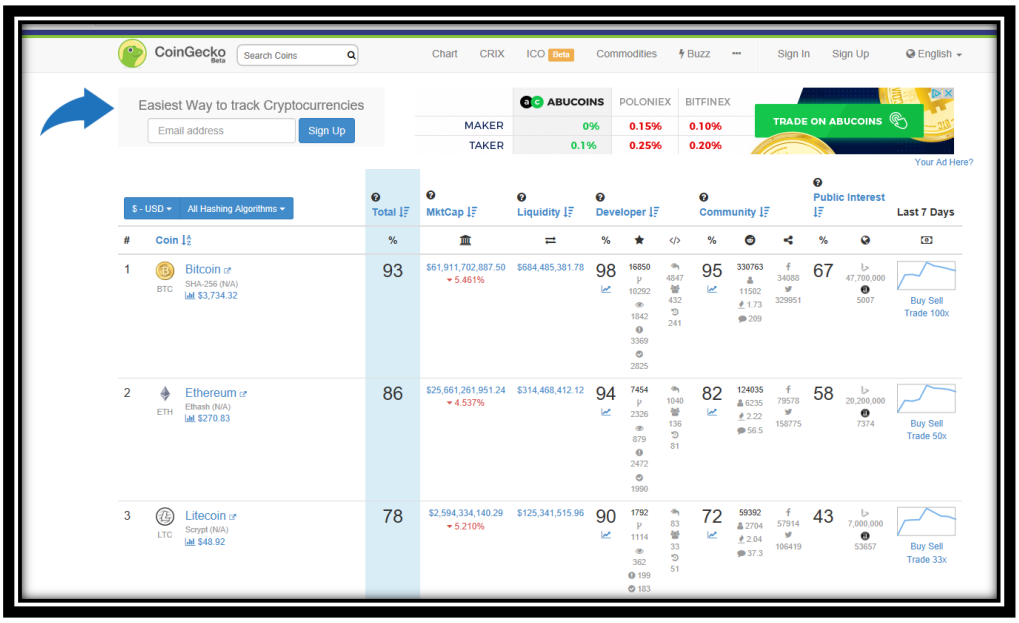


#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$61,430,763,440	$3705.28	16,579,250 BTC	$1,225,550,000	-7.40%	
2	Ethereum	$25,334,122,032	$267.37	94,752,338 ETH	$455,546,000	-7.56%	
3	Bitcoin Cash	$7,301,035,901	$439.84	16,599,375 BCH	$281,903,000	-11.08%	
4	Ripple	$6,742,802,939	$0.175851	38,343,841,883 XRP *	$34,259,300	-5.02%	
5	Dash	$2,587,030,839	$341.70	7,571,037 DASH	$137,359,000	0.54%	
6	Litecoin	$2,562,729,310	$48.32	53,033,982 LTC	$160,619,000	-8.96%	
7	NEM	$1,926,099,000	$0.214011	8,999,999,999 XEM *	$3,236,780	-9.17%	
8	IOTA	$1,365,416,456	$0.491240	2,779,530,283 MIOTA *	$12,193,400	-14.96%	
9	Monero	$1,343,033,042	$88.91	15,104,906 XMR	$28,008,100	-8.11%	
10	Ethereum Classic	$1,009,764,244	$10.55	95,729,491 ETC	$32,970,500	-7.92%	

If you want something a little bit more advanced with more gadgets but that basically does the same thing, then try **www.coingecko.com**

Some people prefer Coingecko because it has its own rating system that takes more information into consideration before ranking, whereas Coinmarketcap only uses the market capitalisation to rank it.

It is up to you which one you want to use but Coingecko does have more functionality:



Mistake 2:

They think they have missed the boat on the most successful cryptocurrencies, whose price has run up – think Bitcoin and Ethereum – and so invest in less established, smaller and more speculative coins just because the price is much cheaper than that of Bitcoin and so have more of an upside.

While you can put a small 10% of your money into speculation, the majority of your money needs to go into any of the pull-backs that occur on the more established cryptocurrencies. A pull-back is a fall in price significant enough for us to enter eg 10% from a recent high.

Mistake 3:

They try to day trade and profit from short term market movements, both up and down.

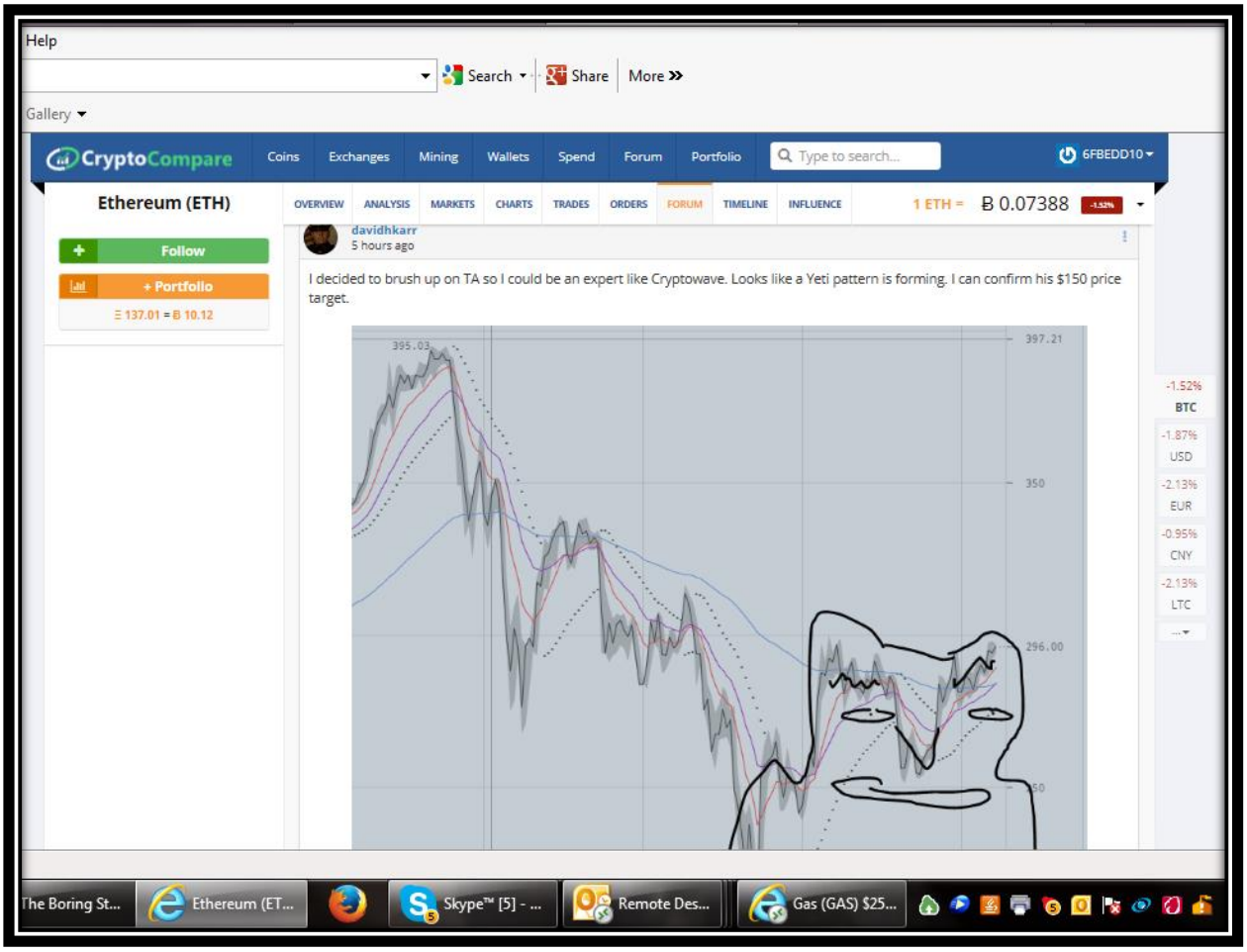
While this can undoubtedly be profitable for someone who knows what they are doing, this is absolutely lethal for anyone who doesn't know proper risk management and who doesn't have a strategy or has a strategy without the proper risk:reward ratios. Anyone who doesn't have this is going to get killed by the volatility.

There are many different strategies you can use. Fundamental analysis relies on data to determine the long term trend of the market and, therefore, there is very little to do. Technical analysis, on the other hand, is the study of short term movements in the price.

Some people claim that technical analysis, often made up of a myriad combination of hundreds of different chart patterns and indicators to help you enter the market, can give you an edge.

Maybe.

I particularly like the picture below where a trader makes fun of technical analysis. It says *"I have decided to brush up on TA (Technical Analysis) so I can be an expert. Looks like a Yeti pattern is forming. I can confirm $150 price target!"* Hilarious!

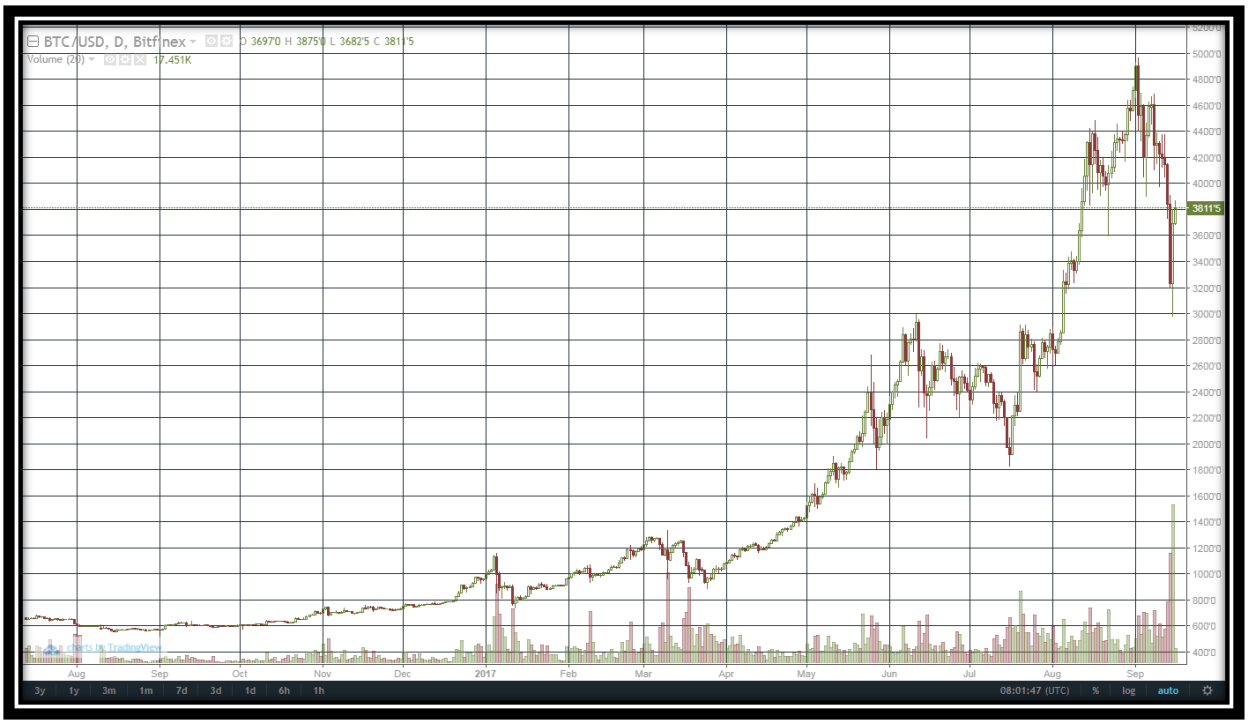


For people starting out, technical analysis can be confusing. So what to do? The answer is: keep it simple.

What do to with a bull cryptocurrency

My advice would be to do as little as possible and allow the market to do the work, especially in a bull market as we have now. I am not advocating buy and hold. Rather, to buy on the dips and sell 20-50% of your profit as it goes back up but hold on to the rest for when the big move comes.

Take a look at the chart of Bitcoin below. There were plenty of opportunities to get in on pull-back in the price and then to gradually sell on the way up.



Just keep doing it. Rinse and Repeat. The only caveat, and it is a big caveat, is that you do need to believe that it is going to continue up.

If it stops going up, then you have to use the following strategy.

What do to with a sideways or slightly down cryptocurrency

When starting out, we suggest you don't try to time the market too much i.e. try to get in and out like a professional trader. Use a simple yet effective strategy like **Value Cost Average™ strategy**. The rules are as follows:

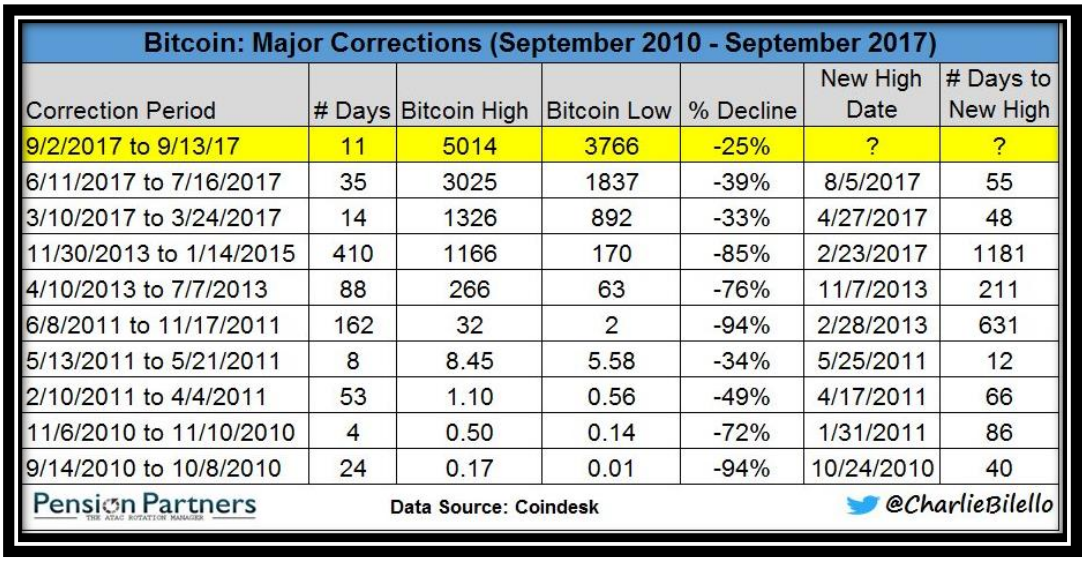
Buy the currency at when it has dropped -10% from a recent high and again at -20% from the recent high and again at -30% from the recent high. Draw your lines in advance, so you get in according to the strategy. Make sure you are looking at a chart which shows the crypto in relation to something stable, NOT in relation to Bitcoin. If you can't find that then write down the price at which you are going to enter in advance. Each time increase the amount you are investing by not more than 25%.

Remember that cryptocurrencies have massive volatility. Do not get emotional about this. Expect it. Embrace it even. Volatility is your friend so you can buy at a cheaper price. While everyone else is panicking, you will be entering again.

Take a look at the chart below of Monero (Ticker XMR)

There were plenty of opportunities to buy on the pull-back and make a fairly fast 10% with this strategy. And Monero is one of the more stable ones. Even the biggest cryptocurrency, Bitcoin, is EXTREMELY volatile.

That is why these strategies work so well – because of the volatility of cryptocurrencies. See the following chart:



Bitcoin: Major Corrections (September 2010 - September 2017)						
Correction Period	# Days	Bitcoin High	Bitcoin Low	% Decline	New High Date	# Days to New High
9/2/2017 to 9/13/17	11	5014	3766	-25%	?	?
6/11/2017 to 7/16/2017	35	3025	1837	-39%	8/5/2017	55
3/10/2017 to 3/24/2017	14	1326	892	-33%	4/27/2017	48
11/30/2013 to 1/14/2015	410	1166	170	-85%	2/23/2017	1181
4/10/2013 to 7/7/2013	88	266	63	-76%	11/7/2013	211
6/8/2011 to 11/17/2011	162	32	2	-94%	2/28/2013	631
5/13/2011 to 5/21/2011	8	8.45	5.58	-34%	5/25/2011	12
2/10/2011 to 4/4/2011	53	1.10	0.56	-49%	4/17/2011	66
11/6/2010 to 11/10/2010	4	0.50	0.14	-72%	1/31/2011	86
9/14/2010 to 10/8/2010	24	0.17	0.01	-94%	10/24/2010	40

Pension Partners THE ATAC ROTATION MANAGER — Data Source: Coindesk — @CharlieBilello

It shows Bitcoins' major corrections. A correction is more of fall then a mere pull-back. When you look at the % declines in Column 4 each time, you will see what we mean by volatility. Let volatility be your friend. Buy on the dips.

Only use this strategy if you are sure your chosen coin cannot go to zero – stick to the top ten with the biggest market capitalisations.

If you are investing more speculatively because you want to take on more risk to make more potential returns then you need to know what you are doing. This is not recommended for total beginners. For example, you could buy others Altcoins that aren't in the top 10 or so. But remember the further down the list you go the more risk you are taking that it could go to zero.

If you are taking on more risk then don't keep buying into it because if it goes to zero all your money will be gone. Here you have to be clever. Try only buying when it has dropped AND you see it going up again.

But remember, this strategy can only work on something you believe will not go to zero. If you believe that Bitcoin or any other Altcoin can go to zero, do not employ this strategy.

Never invest more than you are willing to lose entirely. People always say that but with cryptocurrencies I suggest you heed this advice.

9. How to keep your cryptocurrencies safe and store them

"I threw away $7.6 Million of Bitcoin"

- Campbell Simpson, who bought $25 worth of Bitcoin in 2010, put it on a hard drive but threw the hard drive away by mistake.

To start investing in cryptocurrencies, the first thing you would need is to set up your digital wallet. In the cryptocurrency realm, the term used is "wallet". The wallet can be likened to a bank account, which can be stored in different devices.

The reason you need to do this is because there are countless stories of people losing their cryptocurrencies. Safety is paramount here – you don't want to build up a small fortune only to lose it all.

A cryptocurrency wallet is a software program that functions to store your private and public keys and interacts with various blockchains. It enables users to send and receive cryptocurrencies as well as tracking their balance.

There are many wallets out there for you to choose from, which is all dependent on your security needs as well as whether you wish to be an active trader or a more passive buy-and-hold investor (we recommend you be a mixture of the two, the so-called sweet spot).

Once you have set up your wallet, you can then proceed to purchase and exchange the digital currency of your choice on many platforms.

There are three main ways to store your coins:

1. **An exchange** – this is the easiest way because you are trading your money on there so that is where your money is kept. However, remember that this is an unregulated entity and this is where most of the hacks have taken place. So to date, exchanges have been the worst place to keep your money.

   Make it even safer by using whatever extra security there is available. For example, Gemini asks not just for a password but asks if you want to enable 'Two-Factor Authentication' (2FA). Do it! It makes it even safer. Use 'Google Authenticator' where possible as opposed to text messaging in case someone clones your phone.

   Some of the exchanges actually hold your coins in cold storage for you, so theoretically that sounds a little bit safer than just keeping it on an exchange that doesn't offer that.

2. **An online Wallet** –a.k.a. Hot Wallet. This is more difficult to hack and therefore safer than an exchange. It can still be hacked, however, since it is online. It also means more work because you have to open up several wallets for each of the different coins. This is a pain but do it. Better to be safe than sorry.

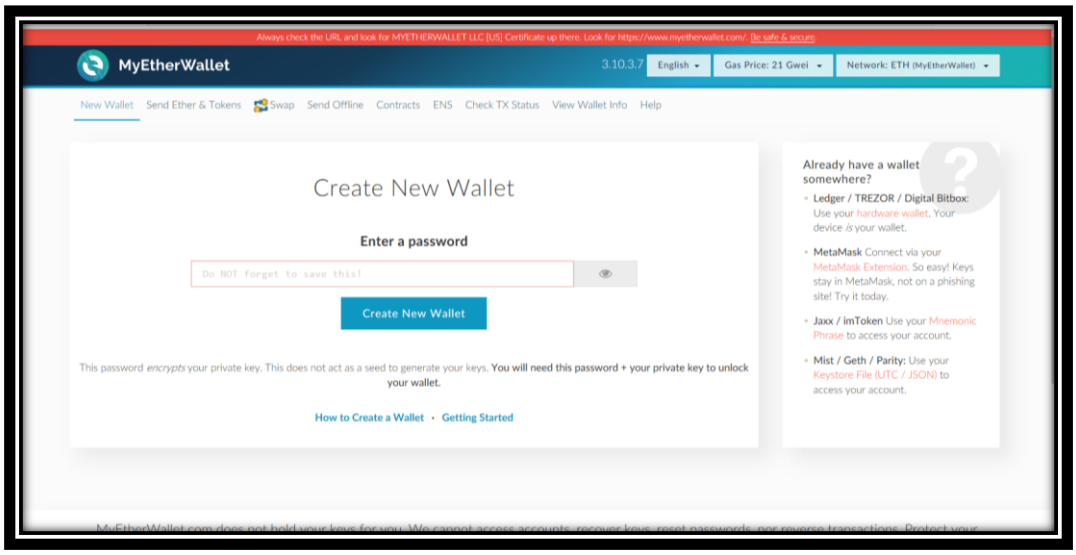
   There are two ways of doing this:

   1. Ones that store your public key and your private key online and

   2. Those that are set up online but then store your private keys on your PC or mobile.

      1. Online or Cloud Wallet

Some examples of these are www.MyEtherWallet.com (which I use) and www.blockchain.info (which I have not used).



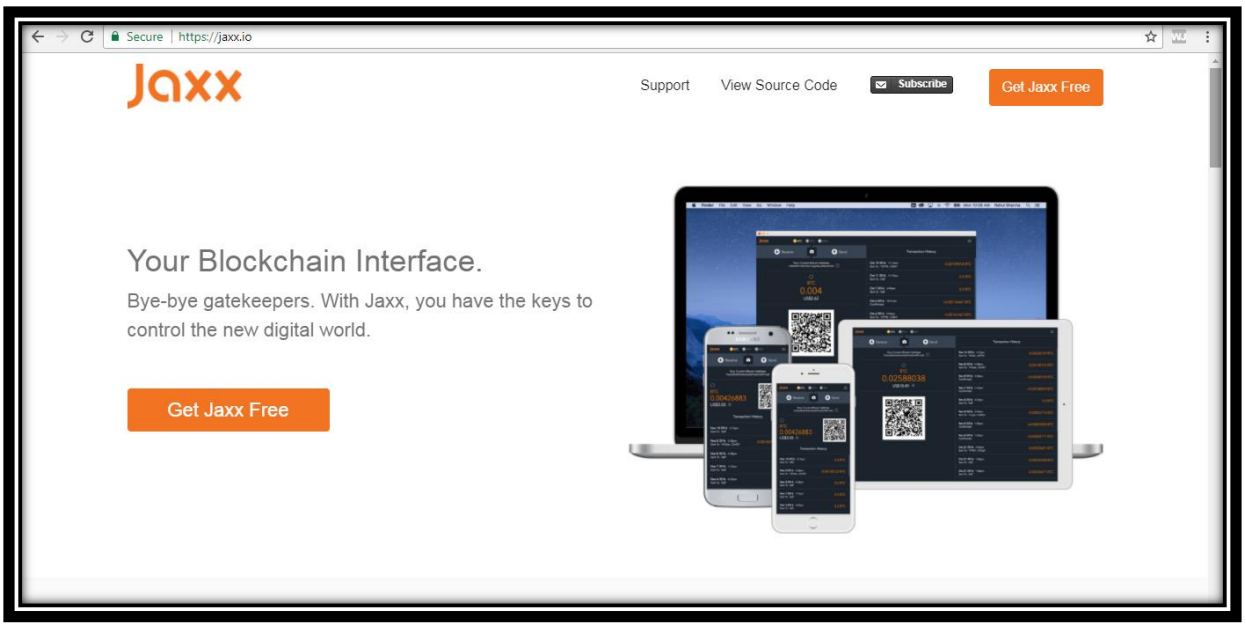
Once you used www.myetherwallet.com there is no turning back. It is extremely simple to use, once you have used it a few times of course :--)

2a. Desktop PC/Mac Wallet

Depending on how secure your desktop is or isn't, this is accessible by hackers i.e. if your PC gets a virus then people can hack it to get your private keys.

2b. Mobile Wallet

The best-known mobile wallet is Jaxx. It syncs to your desktop and your phone so that you can back up the private key. You can download it from the App Store or Google Play. www.jaxx.io

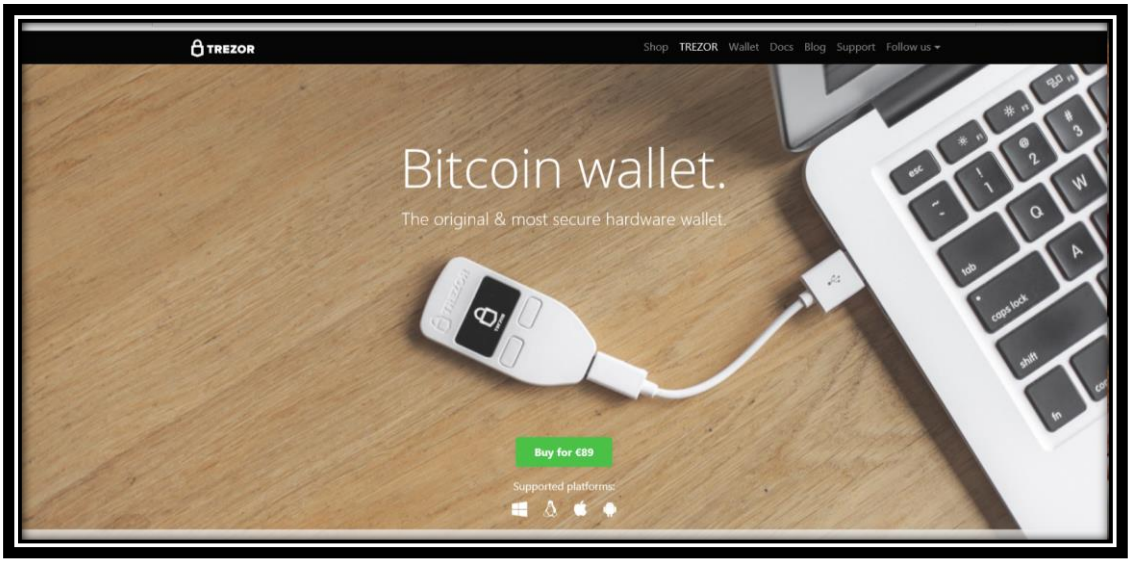


Jaxx is great because it stores a lot of different coins all in one, like Bitcoin, Ethereum, Litecoin, Dash etc.

3. An offline Wallet a.k.a. Cold storage or hard storage – this is where you store your private key on a special USB stick and so it is off grid. Once offline, it is almost impossible to hack. However, if the cleaner throws it out, you lose it for good. And yes, this has happened with people losing $millions in hard disks that were thrown out by mistake.

The most popular ones are:

Trezor: this was the first original hard wallet.



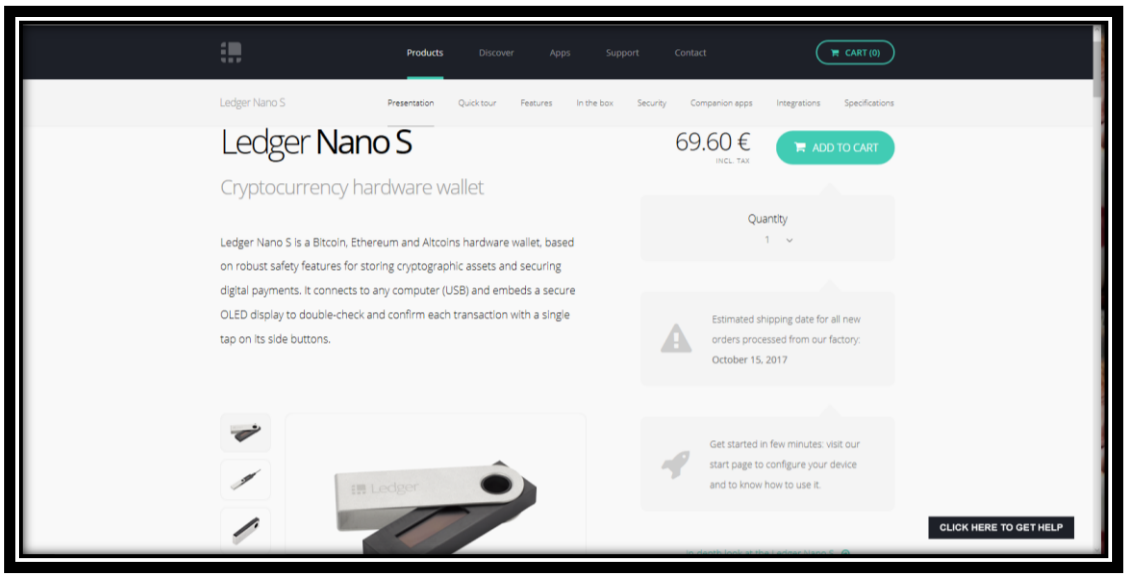
Like most of these technologies, they are SIMPLE to use but not easy. The first time it is like climbing a mountain – but every use after that gets easier and easier.

Before long you will be an absolute expert at it, showing off to all your friends. If you didn't die climbing the mountain the first time around, that is.

Ledger Nano S: one of the most popular.

The Ledger seems to be very popular with people. It is almost the same as the Trezor but looks cooler and is less expensive. I suppose those are two good reasons when buying something, especially since it pretty much does the same thing as the Trezor.

I went for the Trezor because it was more expensive (reassuringly expensive and all that) but now that I have been in the space for a while, if I would start again I would probably go for the Ledger Nano.



KeepKey:

Keepkey aas a larger screen but I have not used it myself

With all of the above, you have to figure out your number that you think it is safer to put on there i.e. any coins worth more than $25,000 in value I use a cold storage wallet.

4. Paper Wallet. This is where you literally write down your private key on a piece of paper. This is, of course, much cheaper than buying one of the above.

Make sure you keep a copy because once the paper is destroyed your private key is gone and your coins will be gone.

With all the above, follow these three Rules:

1. Always back up your wallet, no matter which ones you use.
2. Keep your software up to date if using software.

3. Use whatever extra security there is available such as Two-Factor Authentication. Use Google Authenticator where possible as opposed to text messaging in case someone clones your phone.

Summary: If you are planning to trade with your money (not invest), then leave it on the exchange, but if you are planning to hold it longer term then it is worth keeping it safe in a wallet.

If you have larger investments – you need to decide what that means – it is definitely worth putting into cold storage.

Better safe than sorry!

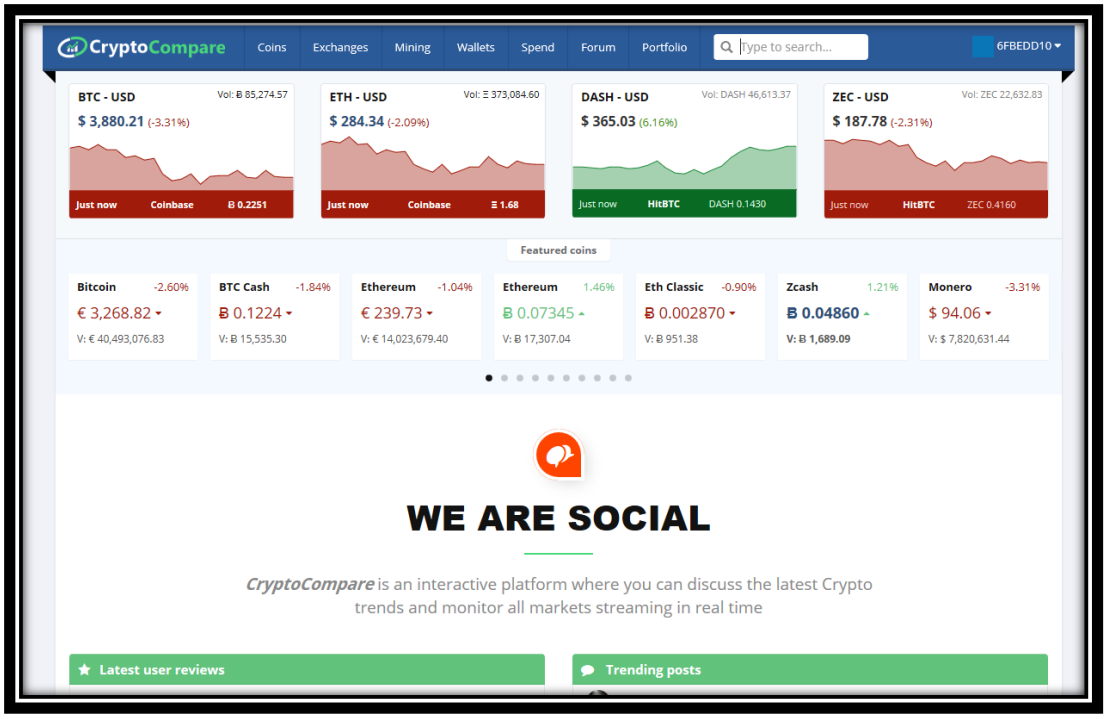
10. How to track them once you have bought them?

"If you can't measure it, you can't improve it."

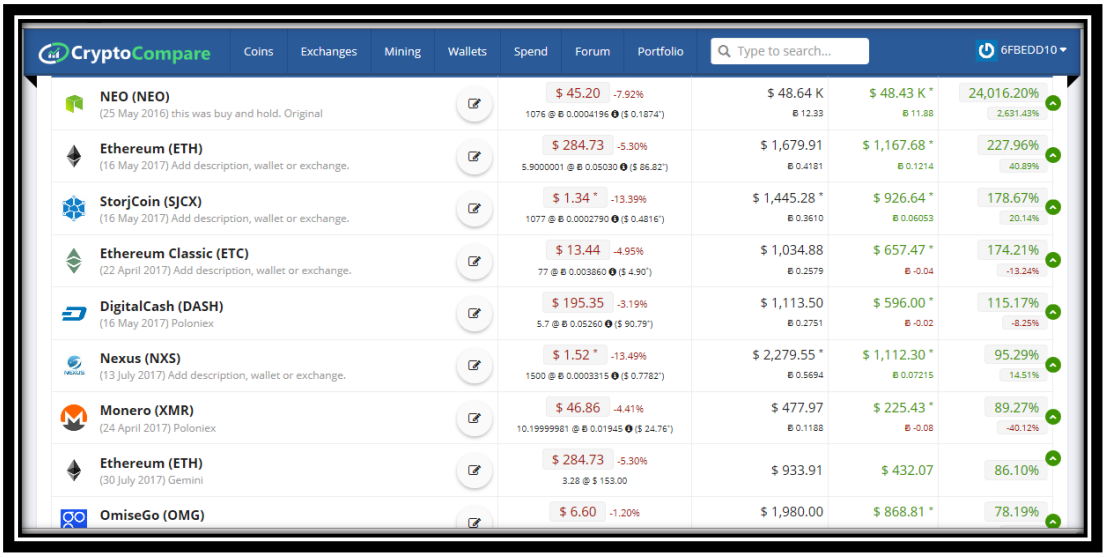
- Management thinker Peter Drucker

There are several sites you can use to track your cryptocurrencies once you have bought them.

The one that I use is www.cryptocompare.com.

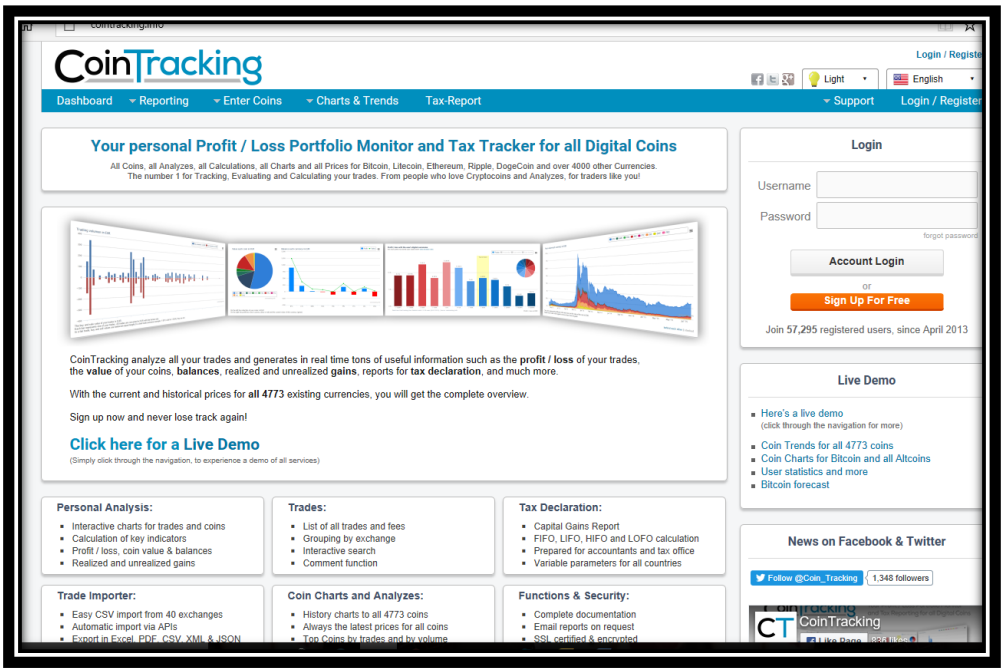


You can either put in what you have bought manually or you cut and paste a code from the exchange in and it does it automatically. This way it has the fluctuations of all the coins on a daily basis:



This is a great way to track all your holdings even if they are on several exchanges or several wallets. You don't want to be logging into several exchanges every day – simply log into your 'Portfolio' in CryptoCompare and everything you want is there. If you have several positions of the same coin, it will amalgamate it and give you the average price.

Another one is www.Cointracking.info.



This has the added benefit of having a tax add on. Again, you can enter coins directly from exchanges such as Bittrex, Coinbase, Kraken etc.

11. How to make money i.e. when to sell them

"The only people who lose money are the ones that have to sell."

- Warren Buffett

This, of course, is the holy grail of trading – WHEN to get out of the trade.

We are at the beginning of cryptocurrencies as a technology, so there could be enormous upside potential. We are looking at the maximum upside. If there is one thing I have learned it is that you have to allow your winners to run if you want to make a lot of money. We are definitely holding for the long-term upside potential.

In this bull market and in the Early Adopter stage of cryptocurrencies, I don't really want to be selling. Why? Unlike other investments, Bitcoin and other cryptocurrencies are currencies and, so if they succeed, you won't have to sell them to gain value from them. You can use them directly, like you can the British Pound or any other form of currency.

I am not even going to buy something with a stop loss to sell, as the volatility is too huge at the moment. I am not really looking at selling at all, since we are in a bull market and if I get out I will miss out on the big moves that comes when you least expect it.

However, to just buy and hold is a pretty lazy strategy too. You don't want to be up massively and then lose all the profits you made. So we have to consider taking some profits now and again in order to take money off the table and rotate it back into other cryptos that might be at a lower price. For example, if you are in profit and have made over 100%, it is time to think about setting a stop loss just below it to sell a part of your holdings and take some profit, say 20-30%.

Another way to make money is a little more advanced and it means watching it on a daily basis if you see the price continuously going up and down i.e. going sideways and not really hitting new highs, then you can start to trade within that 'channel' of high and low prices. So you are getting in near the bottom and out near the top – in effect trading – whilst always keeping your main amount invested but start trading a smaller portion within that range.

It is important to do this but most people do not do this. If you don't do this then you don't make any money while markets go sideways which is crazy when you consider that markets might go sideways for many months, even years on occasions. If you don't trade the range while waiting for the eventual upturn, you have missed out on that time … and profit.

This is the optimal strategy but takes some experience. Not a lot of experience but a little.

Make sure you talk to one of our traders who can guide you and point you in the right direction.

12. Is it too late to get into cryptocurrencies – have I missed the boat?

Get in before the early adoption really starts.

While it might be too late to make 10,000% on the larger coins, it is still very early on and new developments, coins and ideas are being generated almost on a daily basis. We are just at the start. There will no doubt be NEW cryptos that will also have meteoric rises which you can get into. Some haven't even been invented yet. Anything could happen. Get involved.

Whether you are in the know and can buy in time is another matter altogether, so do your research and get going.

A whole generation is looking at Bitcoin as a store of value. The trust is in the decentralised framework of the blockchain, which makes it so difficult to hack into. Anyone under the age of 30 sees Bitcoin as making total sense.

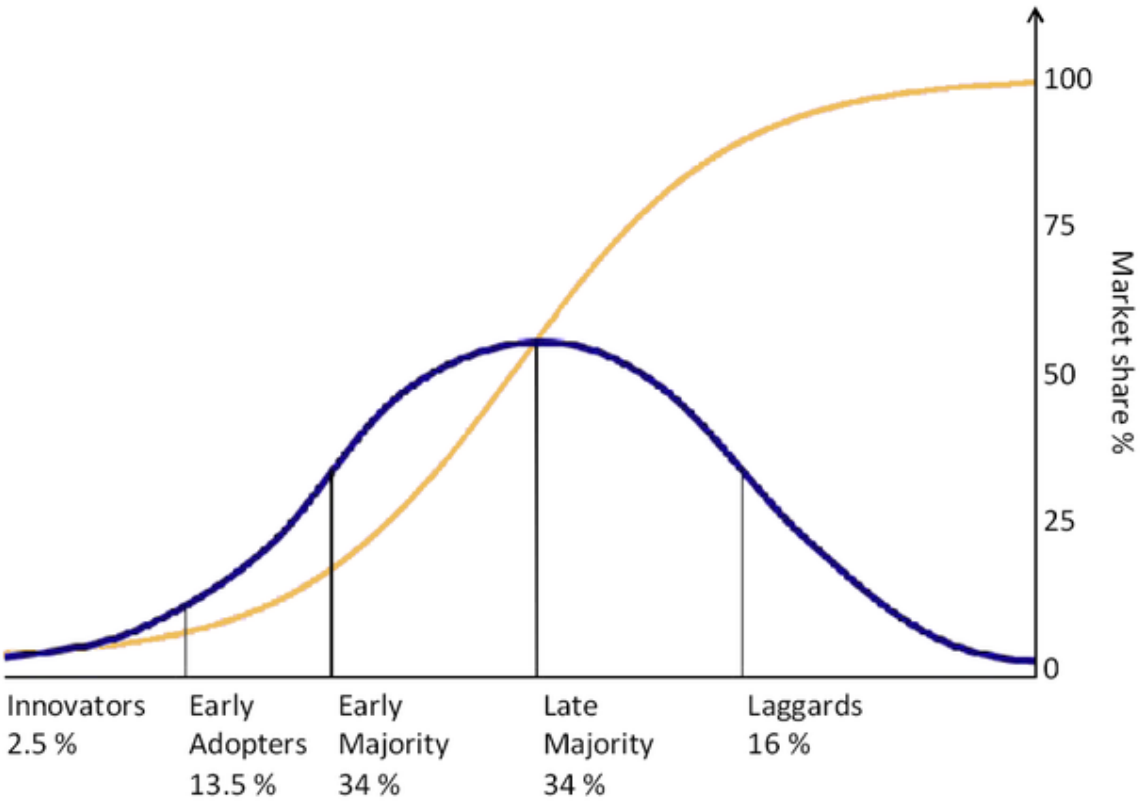
There are generally four phases of adoption according to Everett M. Rogers (1957)

1. Innovators

2. Early Adopters

3. Late Majority

4. Laggards



I believe that we are only now approaching the Early Adopter's stage, so plenty of time to go. At the moment only thousands of people own any Bitcoin or a fraction of a Bitcoin. This is akin to when only hundreds of thousands of people had an iPhone. The real growth came when it started being adopted by everyone and then it grew into the high millions. So get in before the early adoption really starts.

Simon Dixon, CEO and co-founder of BNK to the Future, says that he has seen five waves of cryptocurrencies:

1. The first wave was Bitcoin, which had value because of it being a store of value independent of a central bank.
2. The second was the Altcoins where people were trying to copy Bitcoin. Some of them succeeded, like Litecoin and Dash.
3. Then you had equities in companies, like the exchanges Kraken and Coinbase.
4. Then there was Tokens or 'ICOs' as they are called, where companies create an asset class that trades on a secondary market.

5. The final one is ‘Forks’ – where people have disagreements on how things should be done and split off, for example Ethereum Classic split off from Ethereum and Bitcoin Cash and Bitcoin Gold split off from Bitcoin.

Let us take a look at ICOs in the next chapter.

13. What is an ICO and how can I profit from it?

Let's ICO like it's 1999.

* Important warning before we start: ICOs are a high-risk way of fundraising. Never invest anything you can't completely afford to lose. Keep in mind that due to a lack of regulation, you will have difficulty getting back your lost money in case of any failures.

What is an ICO?

An ICO (Initial Coin Offering) is a fundraising method that trades future crypto coins for cryptocurrencies which have an immediate, liquid value. Much as an IPO is an Initial Public Offering when a private company decides to go public on an Exchange, an ICO is an Initial Coin Offering. ICOs or Initial Coin Offerings are basically crowd sales, the cryptocurrency version of crowdfunding.

The only difference is that in an ICO the startup sells tokens on a blockchain while IPO is selling shares. It usually takes place before the launch of a coin's blockchain, and involves the public sale, or crowdsale, of a percentage of the coin's initial supply. ICOs are sometimes referred to as ICPOs (Initial Public Coin Offerings) or ITOs (Initial Token Offerings) or even a 'Crypto Crowdsale'. The startups themselves are called 'Blockchain Startups'.

Many of the companies performing ICOs aren't offering coins, but rather tokens. And tokens and coins are very different things. Coins, like Bitcoin, are a way of transferring monetary value. Tokens, on the other hand, can store complex and multifaceted data streams that can be used for endless functionality.

Many of the new companies that are holding ICOs are not currencies and are instead technology companies that will be built on the blockchain. So, they can't be judged solely on their monetary value, but rather they need to be evaluated based on their business model and potential solution.

What is the so-called 'white paper' within an ICO?

Every ICO should have a white paper or manifesto. For example, the original Bitcoin white paper is at the back of this book (see appendices). This details how the technology is intended to work, how the tokens are designed within it, and how users could acquire and use the tokens. A white paper shows whether the founders have thought through the project, what problem it solves and how they mean to solve it. Crucially, it must also show how the tokens they are giving out will be used to solve the problem, since you will own some in exchange for investing.

How does an ICO work?

1. A startup advertises that it will be selling the initial coin supply of their new cryptocurrency.
2. Investors read the 'white paper' of the startup and on that basis exchange Bitcoin or Ether for these new coins.
3. The startup can then exchange your Bitcoin or Ether into normal fiat currency to spend on building out the technology, pay for costs etc.
4. If the project is a success, ie it launches and starts being adopted, then the value of the new currency rises and investors of the ICO make a profit.

Why do companies do them?

ICO provides them a simpler and quicker way to do fund-raising for new blockchain projects than a traditional method. It is also border-free that it can connect to every investor in the world.

Usually, a percentage of the tokens is sold to ICO participants and a percentage kept for the company's needs (private investors, etc. Terms differ from one ICO to another).

Bancor raised $150 million in under 3 hours. BAT raised $34 million in literally under a minute. The ICOfor Status was in such a high demand that it jammed the Ethereum network for an entire day. The highest value raised by an ICO is Tezos, which raised a record breaking $232 million in less than a month!

How do you make money in an ICO?

Most investors speculate that the startup will be successful enough to launch on an exchange, so that they can sell their tokens or coins as soon as possible, at profit. They don't necessarily believe in the company itself, or they might believe in the idea, but are not willing to risk staying in for the long term if they can make 100-1000% in the short term.

What does the new token/coin represent?

The coin/token issued in an ICO has three roles, depending on the goals of the company:

- It represents the company's product – the coins can be used as a medium of exchange for a certain amount of product or services. It could also be used for trading in a project.
- It represents the right of profit sharing – like normal shares, the coins could be thought of a certain percent of a company's shares you own and profits could be shared if the company wishes to do so.
- It represents corporate bonds – the coin is like a loan. The coin owner is able to receive interest based on the pre-set rate.

Those that believe in the company will hold on for the long term. If the startup is successful, fortunes will be made. Even if you invest just £500-5,000. This is unprecedented.

Are there drawbacks to investing in ICOs?
Yes, there are many.

The idea for the startup is written on a 'white paper' – often even without any proof of work – and people invest on the basis of what they read in the white paper. Since investors are pouring in their money in the hope of becoming rich through ICOs, some of these ICO startups are taking advantage of this situation. They collect the money but don't actually get to the work of creating the product, yet alone actually turning the business into a profit-making enterprise. Then they just disappear into the ether.

Mycelium ICO was a particularly bad example of this. Its team members just disappeared after raising the money, and later it was reported they used the funds to pay for their own vacation.

This is why there is so much talk of regulation and self-regulation.

The ones that are legitimate and really do want to create a product may have the problem of insufficient technical knowledge or support. They may be underqualified and lack the experience of building up a blockchain business.

This is not the only way investors have lost money. $7 millions were stolen as CoinDash's ICO started. Right before the start of the token sale, their website was hacked and the ICO wallet address was changed to the hacker's address.

How do I go about investing in an ICO?

1. Research, research, research

Unlike an IPO where the company is normally successful and profitable, an ICO is a startup and needs the funds to get from the white paper theory to develop the actual product or service. So you must do your research by trawling the Internet and asking all your questions on ICO, cryptocurrencies and Bitcoin forums. Remember, you could lose 100% of your investment.

1. Can the team deliver based on its experience?

Read their white paper and go straight to the founding members and the team. Look at their profiles on LinkedIn. See how much history they have in the space – we are looking for people who can deliver on their promise. If not, don't even bother continuing. Find out if the team has any crypto experience and – more importantly – which projects, or ICOs, they were involved with and the impact they had. If you are satisfied that they can deliver, continue your research.

Take a short cut and go to BitcoinTalk.org, because you can see what the experienced investors are saying.

Watch out for the words like ‘scam’ and how the community responds. Give more weight to the answers of experienced investors. Investor’s concerns will be answered (or may be unanswered) in this thread.

Also, it is a bad sign when the developers avoid answering certain questions or aren’t collaborating. Sending them a personal message to see how responsive they are is also a good idea.

2. Does the idea solve a problem/is the idea needed?

Is there any validity in their idea? Is it solving a problem? Is there a potential hungry market for this? Does it have a chance of succeeding? What does your gut instinct and experience tell you? After reading it, you should be able to answer a simple question – what kind of value does this project bring to our world?

Next, is it a totally new concept or are they developing something that someone else already has developed. Don’t get duped into a new Amazon for this new market or an Uber of that new market. It can’t just be a ‘me-too’ product – don’t invest unless you believe that this company can do it much better.

3. What is the Token for?

ICOs mean the creation of a new dedicated token for the project. One of the most important questions each project needs to answer is what is the token for? Why isn't Bitcoin or Ethereum enough to serve as the project's token?

4. How much money is being collected?

Some of the earlier ICOs were unlimited. An open cap allows investors to send unlimited funding to the project's ICO wallet. The more coins are circulating, the less unique your tokens become for trading afterwards – through less demand.

5. What are they using the money for?

Next, what are they using the money for? What percentage will go to the development budget, the marketing budget, and other essential allocations. In the past, many ICOs have not given this level of transparency but in the end don't you want to know where your money is going to be allocated to and if this makes sense to you?

6. Token value

Next, look at the Token value – is the current value worth it? Do you think it has a chance of growing in value to make you enough profits? Do they have too many tokens on offer which will saturate the market? Are there really any incentives to use their tokens – because in the end, even if it is a great idea, you will only make money if the tokens you have will increase in value over time? Etc.

If you can answer these questions as best you can, then you have done the work required to lower the risk of investing. Remember that your risk is 100% and with several of them, this is likely to happen.

7. Token distribution – when and how

Greed can be defined by a high token distribution to the team members, let's say, more than 50% of the tokens is suspicious. A good project will link its token distribution to the roadmap,because each phase or milestone of the project requires a certain amount of funding.

Watch for the token distribution stage. Some projects just release their tokens hours after the ICO has ended. Some projects need to develop a beta version before sending out the tokens. This is good to know but doesn't necessarily have to impact your investment decision

2. Exchange your fiat money for cryptocurrency

You will need cryptocurrency, usually Bitcoin or Ethereum, to participate in an ICO. Remember the startup will then exchange your investment money for fiat money to pay for its development, costs etc.

3. Invest in ICO

Simply send the cryptocurrency the startup asks for to the address they ask you to send it to. Please note that most startups won't accept Bitcoin or Ether from an exchange. Several exchanges won't send Bitcoin or Ether to an ICO startup. Normally it is sent from an online wallet e.g. www.myetherwallet.com

4. Follow the development of the startup

Many people just leave their money in the startup and pray it all works out. I am not one of those people. I try to get involved and see if I can help. After all, this is my money I have invested and I want to ensure that it works for me. I even spent six months in a startup manning the phones. Tell everyone about it, be a walking, talking advertisement for them. You just never know the impact this could have.

Remember, investment in cryptocurrency isn't something to be taken lightly. It's extremely risky, extremely speculative, and extremely early stage still at this point in time.

I have now invested in over 30 ICOs. I am spreading my risk because I don't know which of them will be successful, if any. This is pure speculation. But I

also swore that I would not miss out on what so far looks like a once in a generation opportunity.

I attend as many conferences as I can so I can talk to the team. I read the whitepaper. I might send them an email to see how they react.

I have even managed to get in on a pre-sale where it is possible to get discounts. They were asking for a minimum of 100 ETH but when I reminded them that we had met at the conference and of the conversation we had, they came down to 50 and then finally 25 ETH.

Morale of the story?

If you don’t ask you don’t get.

And attend conferences to meet the team. There’s only so much you can glean from a Whitepaper.

14. Asset allocation – how much to invest in cryptocurrencies?

Overall, there is a school of thought that says that investing in ICOs is not investing at all – it is pure speculation and it is best to wait until after the ICO ie after the coins have gone public. I certainly agree with the first part of that statement – it is speculation to invest in a brand new startup that hasn't even built its product at the start of a new technology revolution. I also agree that you would be better of looking at the ones that have gone public as they have more chance of not being scams.

However, I don't believe that is all we should be doing. I believe that in terms of asset allocation a tiny amount of your portfolio should be invested on ICOs because the returns could be gigantic. So what's the ideal percentage? This will, of course, depend on how old you are, how much risk you are willing to take and how aggressive/conservative you want to be. However, for me, it is the following:

In terms of asset allocation I am looking at putting 5% of my capital into ICOs. The reason is that we have no idea:

1. Where this industry is heading.
2. Which ICOs are going to be successful.

Therefore investing in ICOs is EXTREMELY speculative.

However. I am still open to putting in a small amount every month, say £500+. I am looking to spread my risk among a minimum of 20 different ICOs. I will put more in if I have met the people and get a good feeling about it, or the white paper makes a lot of sense and it is really solving a problem and has the team

to build the required solution. So if I bought into 20 of them and they all failed but one of them exploded, then I would risk £10,000 to make £50,000 or even more.

For example, I might invest:
0.5% of my capital into an ICO where I am not sure but want to be in because I don't want to miss out.
1-1.5% of my capital into an ICO where I feel good about it.
2.5-5% of my capital into an ICO where I really have a very good feel about the problem, solution and the team.
The most I have invested into one ICO is 12.5% of my crypto capital. This was at the beginning of my journey and it was, in hindsight, too much in terms of asset allocation.

Let's break this down:
25% = £2,500 into the top 2 Ethereum/Bitcoin.
40% = £4,000 into established coins e.g. top 20.
20% = £2,000 into up and coming coins ie outside the top 20 but coming up fast.
10% = £1,000 into new coins that have gone public onto an exchange.
5% = £500 into ICOs.
100% Total

This is just a guideline on what I am doing – you need to come up with your own system that works for you.

Remember that this 100% is the 100% of the total of my pot allocated to cryptocurrencies. Since cryptocurrencies are speculative, this '100%' shouldn't be more than 10% of your entire portfolio. So if you lost the entire 100% then you would have only lost 10% of your portfolio. Again, none of us know what the future is of cryptocurrencies (see next chapters). Buyer beware!

15. Are there any drawbacks to investing in cryptocurrencies?

"Where there's blockchain there's also bullshit"

Overheard at a Blockchain Conference

There are several drawbacks to cryptocurrencies, especially with ICOs. This is a totally new and unregulated industry, meaning if you are hacked and someone takes your Bitcoins, you will not be compensated. Also, new launches of coins are increasing and no one knows which ones will vanish and which ones are here to stay. Due to this uncertainty, price swings of 30%+ in a single day up or down are not uncommon. Therefore, at the moment, only invest money you are willing to lose.

Overall, there are four disadvantages of cryptocurrencies. There is a lack of understanding towards this digital currency. Plus, there's minimum protection and guarantee when using is. Because it is mostly operating online, it is bound to experience all kinds of technical flaws and it is still developing.

1. **Lack of understanding about cryptocurrency**

In most cases, people are still unaware of the digital currency world and the potential it holds. This is similar to when the usage of credit card was first announced and the reception towards it was fairly similar to cryptocurrency. Back then, people wouldn't even think that paying for things using a mere card was possible, yet alone a whole new digital currency.

Because it is different, and it doesn't involve cash directly, people shy away from it and constantly doubt its effectiveness. Additionally, it involves online access to make it work. The idea of having to pay for things or transfer money online is convenient to some and is catching on but some people are still sceptical about it.

In order to make cryptocurrency acceptable around us, the people need to be educated about it to be able to include it in their daily lives. But the effort to learn a whole new world of currency requires a lot of time and energy. Most would think it is not worth their time because it is not commonly known anyway.

Even though some businesses are accepting Bitcoins, the list is significantly small compared to traditional currencies. This is probably due to the lack of knowledge. Both businesses and customers need to be educated. Imagine having to teach your customers a new way of paying for something. This will take a longer time and effort.

2. **Lack of consumer protection and guarantee**

In the case of traditional currency, Central Banks govern the authority of a nation's money. No higher authority can suddenly decide that they no longer want to use their country's currency to trade without protest and rejection. There are procedures to follow, documents to file, approvals and many other protocols to follow.

However, that is not the case with our digital currency. There is no Central Bank who governs Bitcoin, which means no one can guarantee its minimum valuation.

The value of Bitcoin, for example, will fall tremendously should a major group of merchants decided to just 'discard' Bitcoins and leave the system. This will inevitably leave other users who have invested thousands of dollars into Bitcoins in a major loss position. There is no one to contact to file these losses, or rules to help compensate it.

Another example is that if you get charged but didn't receive the online movie tickets or flight tickets, you can always call bank service provider, or go to the physical bank instead and declare your case. If you pay via Visa and can prove you didn't get your service, the credit card company will give you your money back. I remember paying £2,000 for a course that was not delivered – the guy just ran away with our money. Visa compensated us fully because we used their credit card. I was actually pretty impressed at the time … and horrified, as I can imagine a lot of people putting in false claims.

That is not how it works with cryptocurrency. First of all, this currency does not have a bank to negotiate and help you. There is no number that you could call and ask to speak to someone or email address.

So, if you bought your goods using Bitcoins, for example, and the merchant didn't send the items you purchased, there is nothing you can do to reverse the transaction or refund. You can't complain to the police or any relating authority for that matter.

Cryptocurrency transactions are typically not reversible. Once you have sent the money to an address you can't get it back. So make sure you double check that you are sending coins to the right address and in the right currency.

Therefore, the very appeal of the decentralised system of Bitcoin is a double-edged sword.

3. **Technical shortcomings**

When online banking made its way into our lives, there was always the risk of a sudden server failure, power shortage, and even hardware lags.

Similar to data corruptions or virus infections, if your hard drive crashes and your wallet file is corrupted your Bitcoin is lost forever. There is nothing you can you do restore it and those 'coins' will be 'orphaned' in the system.

So remember, always make a back-up to prevent this from happening.

4. **The industry is still developing**

When things are still developing, they are prone to many risks. There are so many incomplete features that can be improved but it takes a longer time to finalise them, especially if they have no physical form.

With traditional currency, despite the method of payments being performed online, and without us actually seeing the physical money being transferred from one account to another, we still end up holding the physical cash at the end of the day. We can use the physical cash to buy things from the stores, physically and online.

Since cryptocurrency does not have any physical form i.e. we will never be holding the physical cash, its usage is obviously restricted.

In the end it more often than not – and I hope this changes soon – but Bitcoin needs to be converted to traditional currency to enjoy its worth.

16. The future of cryptocurrency

Lunatic fringe or serious business?

I do think cryptocurrency is here to stay. To suggest otherwise would be like saying the Internet was a fad when it first started. Of course, hindsight is a great thing.

Which cryptos are here to stay, however, is almost impossible to guess.

These digital currencies have been said to be able to capture the world of online finance. With the blockchain technology behind it, the future of cryptocurrency is showing enormous potential.

Although the mechanism behind Ether prevents it from being used as a direct payment method, this cryptocurrency seems to have a bright future ahead. This is all thanks to its smart contract concepts.

On the other hand, cryptocurrencies solving the problem of privacy are starting to gain more prominent favour amongst users.

The growing level of acceptance of Bitcoin is clearly bringing this alternative currency to the mainstream. Some companies are genuinely considering investing in this currency, further fuelling its journey to the world of financial currency.

Consider this:

Ten times more money was raised for ICOs than Venture Capital in 2017.

More than 50 Funds concentrating on cryptocurrencies have sprung up.

All major VS are now on board and investing before ICOs.

Countries such as Japan have even formally accepted it as a currency.

However, we need to differentiate between cryptocurrencies and the blockchain. Cryptocurrencies have entered a speculation phase where people want to make 1000% within days of buying a coin. But that means we are departing from the fundamental assumption of what a cryptocurrency originally is – a scarce digital commodity where the value derives from that scarcity.

Simply put, if more than 100 new sources of this digital commodity have been launched since the summer of 2017, then the entire concept of scarcity, and therefore value, begins to erode. In fact, many of these new cryptocurrencies will need to fail in order to maintain the viability of the best-known currencies, Bitcoin and Ether.

Most of the recent ICOs are based on the ERC-20 Ethereum token, and the primary purchasing mechanism for new cryptocurrencies has been Ether, the currency of the Ethereum network.

Therefore, an investor often needs to buy Ether in order to buy into any of the new ICOs.

But the crypto bubble of lesser-known currencies will have to pop at some stage, and some people are going to get burned. Despite this, the core technology behind it all – the blockchain – will provide value as a hidden infrastructure underlying future applications.

A small number of currencies – likely Bitcoin and Ethereum – and utility tokens where genuine value is created, will remain viable over the long term – although at what price no one knows.

It is interesting to note that the Enterprise Ethereum Alliance is gaining traction. The Enterprise Ethereum Alliance (EEA), the world's largest open-source blockchain initiative, is an industry-supported consortium that aims to bring Ethereum to an enterprise-grade level by supporting, promoting, and building Ethereum-based technologies. The Alliance has recently announced the addition of 48 new members, including Sberbank, Russia's largest bank, and Hewlett Packard Enterprise (HPE).

Governments are going to be embracing the power of the blockchain. Microsoft Opens Blockchain Door to the government. Companies like Microsoft are working with government organisations: "*Blockchain makes it much harder for fraud and waste to exist, makes it much more visible if it does exist and potentially gets rid of a lot of layers of bureaucracy that are designed simply to ensure that waste and fraud [don't] exist.*" Microsoft

Are we going to witness a new norm of currency through cryptocurrency one day? Researchers concluded that it is still too early to predict that it would, but one thing is for sure that this currency is slowly making its way in the world.

The most targeted group of all would be the technologically savvy individuals and most of us are already part of this group. Less than 50% of our time is spent online and this % is growing.

One day, we might even consider using cryptocurrency as our standard currency for a more universal transaction.

17. Cryptocurrency Frequently Asked Questions (FAQs)

The New Liquid Gold?

Why is Bitcoin called 'Liquid Gold'?

Money in itself does not have any intrinsic value – it is only because we believe that it has value that it is worth anything. Money is just a tracking system – we track what we own and what we owe. This is called a ledger. Whatever form of money exists, we give it value because of its utility as a ledger (or tracking system of who owes what).

Gold has been the Standard for over 5,000 years. Then came coins in different metals and finally paper money. All paper money was backed up by real Gold, so real Gold equivalent to the amount of money on the paper had to be stored in the bank. That means if someone were to go the bank and ask to exchange their money for Gold, in theory they would have received it. All this has changed. After Nixon abandoned the 'Gold Standard' in 1971, the US Dollar was cut loose from Gold. Other countries followed suit.

Governments were now free to print as much of it as they wanted, as it didn't need to be backed up by Gold. Banks started lending out 5-10 times the amount of money that savers put into their bank accounts. All this caused more and more money to be placed in circulation. This is called 'fiat' money. Unfortunately the more fiat money is being printed ie to fund a war, pay back debt or pump into the economy to stave off a recession, the less value it has. Meaning that the money in your pocket is worth less and less every single year.

So really it would make more sense to use something that holds its value, like Gold for example, and not fiat currency. Gold only has value because it is scarce – it is becoming increasingly difficult to mine and supply is running out. Until Bitcoin and the blockchain, Gold had made for the best form of a ledger devised. The problem is that Gold cannot easily be used for daily buying and selling because it is difficult to store, divide up and send.

This is where Bitcoin and other cryptocurrencies come in, because they are easy to store, divide up and send.

<u>The 5 characteristics of money</u>

1.Scarcity
2.Divisible
3.Transportable
4.Durable
5.Recognisable

5 characteristics of money	Fiat money	Gold	Bitcoin and cryptocurrencies
Scarcity	NO. More and more can get printed every day and the value is falling.	YES.	YES. Bitcoin yes, because there will only be 21 million.
Divisible	YES.	NO. You can't pay for a cup of tea with Gold.	YES. One 'Satoshi' is one hundred millionth of a Bitcoin.
Transportable	YES. Using electronic money systems this is possible,	NO. You can't easily send Gold overseas in	YES. You can send it like a digital file, to another wallet

	but it is expensive and slow.	bulk.	within a few minutes, for a fraction of the price.
Durable	SOME. Coins yes but not notes. New ones have to be printed every year.	YES. It is extremely durable.	YES. You cannot destroy a Bitcoin.
Recognisable	YES – if everyone in that country recognises it, butNO – if you are trying to pay in your own country's currency, then each country will have its own currency so you have to exchange it, meaning costs and time. They are also copied and counterfeited and that is why every few years new holograms and materials are added.	YES. Some countries actually prefer the relative safety of Gold. NO – it is not accepted as a method of payment in most places. It is not easy to copy Gold but how do you really know that the Gold you are receiving is real?	YES. If you have a Bitcoin wallet then that's all you are allowed to put in it. NO – the majority of shops do not yet accept Bitcoin, but the list is growing every day. You cannot copy a Bitcoin and counterfeit it.

This means that Bitcoin, like Gold, is an inflation-proof store of value. However, unlike Gold, it is ALSO a day-to-day transactable currency as well, as it is easily divisible to any desired amount. You can buy biscuits, pay for your utility bills or buy a Tesla car (which you have been able to do using Bitcoin since 2013).

All that needs to happen now is that Bitcoin needs to gain awareness so that people can use it to buy and sell on a daily basis. This is going to take time. Remember when credit cards first came out – it took time for people to use them. Or using the automatic scanning systems at WH Smith or Tesco's? People don't like change, unless they can see the benefits clearly and it is cheaper. Bitcoin fits the bill.

What is Bitcoin Cash and Bitcoin Gold?

In August 2017 a group of miners split off from Bitcoin to create Bitcoin Cash, in the way Ethereum Classic was created by a group splitting off from Ethereum in July 2015.

In October 2017 a group of miners did the same to create Bitcoin Gold.

This is what is called a Hard Fork. A group of miners 'forked' from the main Bitcoin blockchain by switching to a new version of software with greater transaction capacity.

This fork did not affect Bitcoin balances, but millions of Bitcoin users were also given Bitcoin Cash Tokens and in October Bitcoin Gold Tokens as well.

Is there a difference between a Coin and a Token and if so, what is it?

The term "ICO" is now used for any new Coin or Token that comes on the market. However, this is not correct. Coins and Tokens are two very different things. A Coin (or Altcoin) is a variation of Bitcoin's open source code. (Litecoin or Dogecoin are examples of this). A Token on the other hand is a secondary asset for Decentralised Application (DApps) within a blockchain ecosystem –

usually Ethereum. Each DApp uses tokens to run. (Golem is a Decentralised Application within the Ethereum blockchain system. Its secondary asset is a Token called GNT. The Gnosis Token is GNO, etc.).

Confused? Maybe this will help. Bitcoin is a decentralised – not centralised – distributed ledger that performs best as digital money. Bitcoin's consensus process is revolutionary but you can't build much with it. Ethereum, on the other hand, can do what Bitcoin does … and more. It can be digital money too, but unlike Bitcoin, Ethereum is highly programmable — it's designed to accommodate the construction of complex applications. This is where the Tokens come in. A token can do many things while a coin can only do one thing. Coins really only have one utility — to act as simple stores of value with no other functionality. Tokens are a completely different breed all together. They can store complex, multi-faceted levels of value. Ethereum tokens are generated by a Smart Contract System (SCS), are highly programmable and have multi-functionality because of it. Through their functionality they become much more than just a coin – they become "Tokens"...

Bitcoin produces "coins." Ethereum generates "tokens." An "ICO" is a Bitcoin/Altcoin thing. A "Token Launch" is an Ethereum thing. People are mixing up the two and until there is more regulation, it will continue to be mixed up.

Appendix:

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

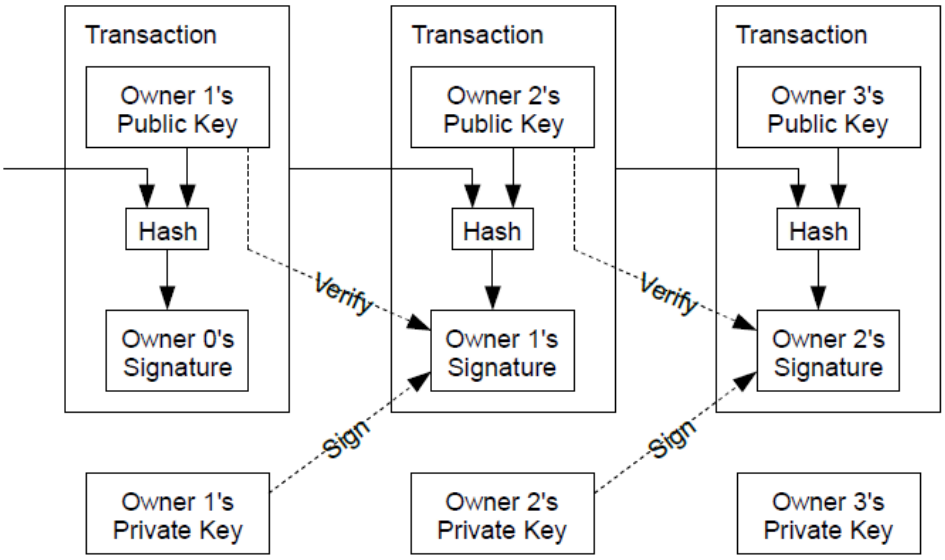
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

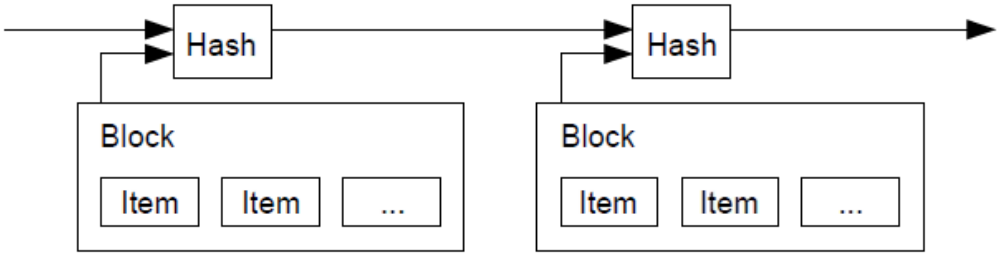


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

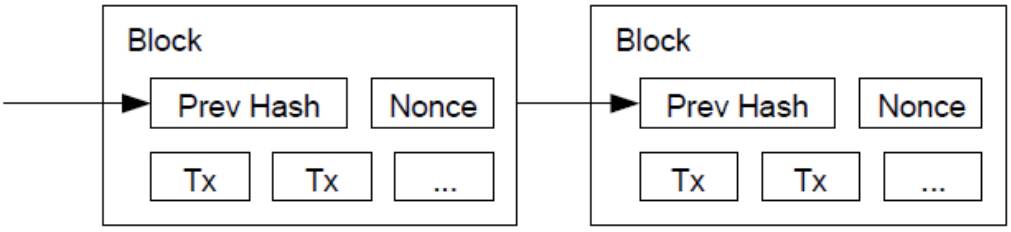
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

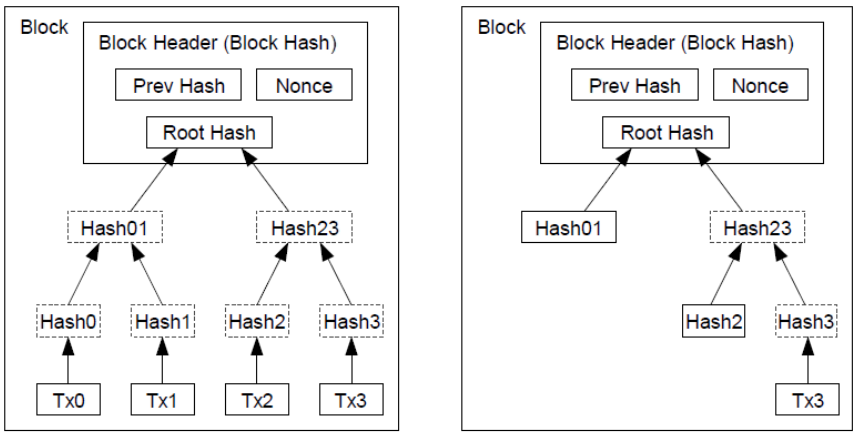
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



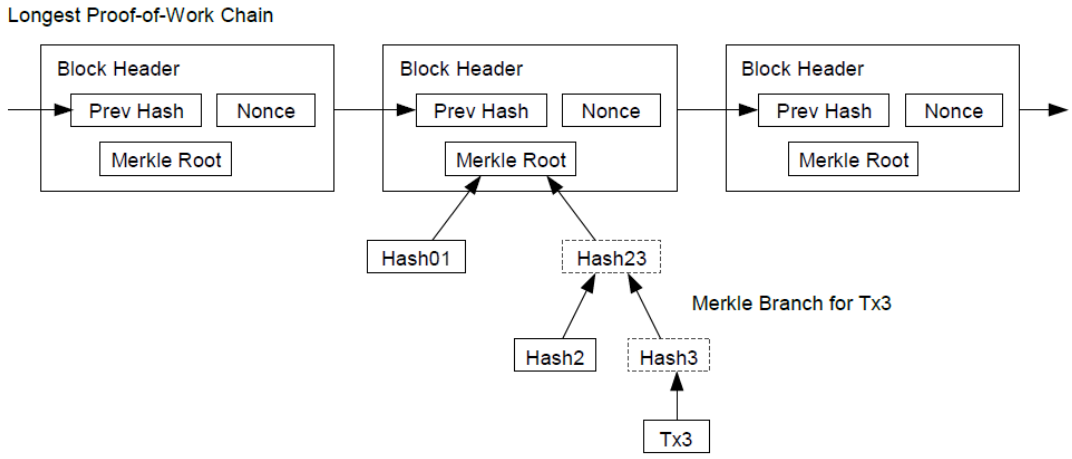
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

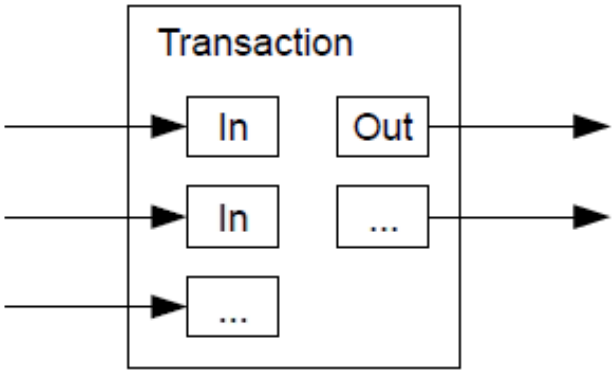
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

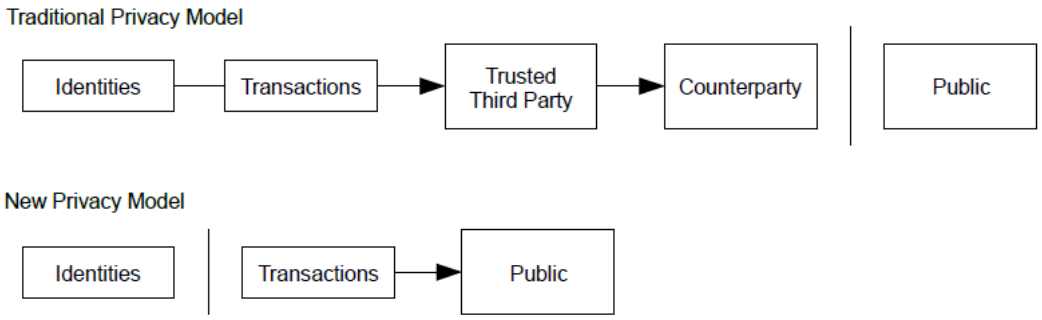
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10.Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11.Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z \frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
	double p = 1.0 - q;
	double lambda = z * (q / p);
	double sum = 1.0;
	int i, k;
```

```
        for (k = 0; k <= z; k++)
        {
            double poisson = exp(-lambda);
            for (i = 1; i <= k; i++)
                poisson *= lambda / i;
            sum -= poisson * (1 - pow(q / p, z - k));
        }
        return sum;
    }
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0 P=1.0000000
z=1 P=0.2045873
z=2 P=0.0509779
z=3 P=0.0131722
z=4 P=0.0034552
z=5 P=0.0009137
z=6 P=0.0002428
z=7 P=0.0000647
z=8 P=0.0000173
z=9 P=0.0000046
z=10 P=0.0000012

q=0.3
z=0 P=1.0000000
z=5 P=0.1773523
z=10 P=0.0416605
z=15 P=0.0101008
z=20 P=0.0024804
z=25 P=0.0006132
z=30 P=0.0001522
z=35 P=0.0000379
z=40 P=0.0000095
z=45 P=0.0000024
z=50 P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10 z=5
q=0.15 z=8
q=0.20 z=11
q=0.25 z=    15
q=0.30 z=24
q=0.35 z=41
q=0.40 z=    89
q=0.45 z=340
```

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and

rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

2.The History of Money

What is money? By definition, it's something of value. But over the last 10,000 years, the material form that money has taken has changed considerably—from cattle and cowrie shells to today's electronic currency. Here, get an overview of the history of money.

Today we value gold Kruggerands and paper Franklins, but cattle and cowrie shells have also served as currency. Enlarge Photo credit: © Steve Sucsy (coin), Skip O'Donnell (bills), narvikk (cow), Steve Goodwin (shells)/iStock

Editor's Note: The dates below mark the approximate start of use.

IN THE BEGINNING: BARTER

Barter is the exchange of resources or services for mutual advantage, and the practice likely dates back tens of thousands of years, perhaps even to the dawn of modern humans. Some would even argue that it's not purely a human activity; plants and animals have been bartering—in symbiotic relationships—for millions of years. In any case, barter among humans certainly pre-dates the use of money. Today individuals, organizations, and governments still use, and often prefer, barter as a form of exchange of goods and services.

9000 - 6000 B.C.: CATTLE

Cattle, which throughout history and across the globe have included not only cows but also sheep, camels, and other livestock, are the first and oldest form of money. With the advent of agriculture also came the use of grain and other vegetable or plant products as a standard form of barter in many cultures.

1200 B.C.: COWRIE SHELLS

The first use of cowries, the shells of a mollusc that was widely available in the shallow waters of the Pacific and Indian Oceans, was in China. Historically, many societies have used cowries as money, and even as recently as the middle of this century, cowries have been used in some parts of Africa. The cowrie is the most widely and longest used currency in history.

1000 B.C.: FIRST METAL MONEY AND COINS

Bronze and Copper cowrie imitations were manufactured by China at the end of the Stone Age and could be considered some of the earliest forms of metal coins. Metal tool money, such as knife and spade monies, was also first used in China. These early metal monies developed into primitive versions of round coins. Chinese coins were made out of base metals, often containing holes so they could be put together like a chain.

500 B.C.: MODERN COINAGE

Outside of China, the first coins developed out of lumps of silver. They soon took the familar round form of today, and were stamped with various gods and emperors to mark their authenticity. These early coins first appeared in Lydia, which is part of present-day Turkey, but the techniques were quickly copied and further refined by the Greek, Persian, Macedonian, and later the Roman empires. Unlike Chinese coins which depended on base metals, these new coins were made from precious metals such as silver, bronze, and gold, which had more inherent value.

118 B.C.: LEATHER MONEY

Leather money was used in China in the form of one-foot-square pieces of white deerskin with colorful borders. This could be considered the first documented type of banknote.

A.D. 800 - 900: THE NOSE

The phrase "To pay through the nose" comes from Danes in Ireland, who slit the noses of those who were remiss in paying the Danish poll tax.

806: PAPER CURRENCY

The first known paper banknotes appeared in China. In all, China experienced over 500 years of early paper money, spanning from the ninth through the fifteenth century. Over this period, paper notes grew in production to the point that their value rapidly depreciated and inflation soared. Then beginning in 1455, the use of paper money in China disappeared for several hundred years. This was still many years before paper currency would reappear in Europe, and three centuries before it was considered common.

1500: POTLACH

"Potlach" comes from a Chinook Indian custom that existed in many North American Indian cultures. It is a ceremony where not only were gifts exchanged, but dances, feasts, and other public rituals were performed. In some instances potlach was a form of initiation into secret tribal societies. Because the exchange of gifts was so important in establishing a leader's social rank, potlach often spiralled out of control as the gifts became progressively more lavish and tribes put on larger and grander feasts and celebrations in an attempt to out-do each other.

1535: WAMPUM

The earliest known use of wampum, which are strings of beads made from clam shells, was by North American Indians in 1535. Most likely, this monetary medium existed well before this date. The Indian word "wampum" means white, which was the color of the beads.

1816: THE GOLD STANDARD

Gold was officially made the standard of value in England in 1816. At this time, guidelines were made to allow for a non-inflationary production of standard banknotes which represented a certain amount of gold. Banknotes had been used in England and Europe for several hundred years before this time, but their worth had never been tied directly to gold. In the United States, the Gold Standard Act was officially enacted in 1900, which helped lead to the establishment of a central bank.

1930: END OF THE GOLD STANDARD

The massive Depression of the 1930s, felt worldwide, marked the beginning of the end of the gold standard. In the United States, the gold standard was revised and the price of gold was devalued. This was the first step in ending the relationship altogether. The British and international gold standards soon ended as well, and the complexities of international monetary regulation began.

THE PRESENT:

Today, currency continues to change and develop, as evidenced by the new $100 U.S. Ben Franklin bill.

THE FUTURE: ELECTRONIC MONEY

In our digital age, economic transactions regularly take place electronically, without the exchange of any physical currency. Digital cash in the form of bits and bytes will most likely continue to be the currency of the future.

This feature originally appeared on the site for the NOVA program Secrets of Making Money.

About the author

Marcus de Maria is an investor and trainer

Since starting in massive debt and turning it around thanks to personal development, his mission is to help as many people do the same.

Marcus in his TV trading and investing series on Sky TV

He is the Founder of Your Crypto Club, where he teaches the general public how to profit from:

1. Cryptocurrencies
2. ICOs
3. Blockchain technology

For more information visit www.YourCryptoClub.com

or email Marcus@investment-mastery.com