*****Go to www.bitgoldwallet.com for information on what bitcoin is and how to safely buy, use and store it, and how to choose a secure and memorable password*****

# THE ALTCOIN INVESTMENT – CRITICAL ANALYSIS

**(3 January 2019)**

by Bitgoldwallet.com owner

DISCLAIMER: All the usual disclaimers apply. Under no circumstances whatsoever am I or anyone affiliated with this work, liable for any outcome arising from it. The opinion expressed in this article is purely my own and may change in the future dependent on the future evolution of the asset class. Absolutely no assurance whatsoever is given to the accuracy or truthfulness of any information stated in this article. In fact, it is explicitly stated here now, that some or all of the information presented, may be incorrect. Readers are strongly advised to do their own research on any statements made to ascertain any similarities it may have to real world facts, and then form their own opinion.

## OPENING COMMENTS

Take a look at these figures below:

Top 21 cryptos (excluding stablecoins, that have been around 14 months or more) >>>> All time high (counted as 100%) >>>> Subsequent low (approximate value counted as percentage of all time high rounded up to the nearest percent)

| | | |
|---|---|---|
| Bitcoin | 100% | 16% |
| Ethereum | 100% | 6% |
| Ripple | 100% | 7% |
| Bitcoin cash | 100% | 2% |
| EOS | 100% | 7% |
| Stellar | 100% | 10% |
| Litecoin | 100% | 7% |
| Tron | 100% | 4% |
| Cardano | 100% | 3% |
| Iota | 100% | 4% |
| Monero | 100% | 8% |
| Binance Coin | 100% | 17% |
| Dash | 100% | 4% |
| NEM | 100% | 3% |
| Ethereum classic | 100% | 7% |
| NEO | 100% | 3% |
| Zcash | 100% | 6% |
| Waves | 100% | 6% |
| Tezos | 100% | 3% |
| Dogecoin | 100% | 11% |
| Bitcoin gold | 100% | 2% |

All coins listed are still trading near the same price range as the lows shown above.

Conclusion solely based on the above data: Only buy and hold bitcoin and be very cautious of investing in any coin that has dropped to 12% or below of its all time high, unless you are buying crypto as part of a gambling strategy (as opposed to a buy and hold strategy). Only buy altcoins if you want to have that particular cryptocurrency in order to

use the developers platform or some other similar reason. Do not buy it because you want to hold onto it for investment purposes, with the aim of selling it when it appreciates in value.

Definitely however read on for more details. A very comprehensive, and some might say, 'penetrative' look at altcoins is now offered…

And in the following sections, I have avoided naming many specific altcoin cryptocurrencies or giving precise examples, even though doing so would have been easy and would have more clearly highlighted the points.

## THE 3 MAJOR DEFICIENCIES OF THE ALTERNATIVE COIN (THE ALTCOIN) FROM AN INVESTMENT PERSPECTIVE

### MAJOR DEFICIENCY 1

ALL ALTCOINS (BESIDES STABLECOINS WHICH CAN'T REALLY BE REGARDED AS CRYPTO) SUFFER FROM NARROW DISTRIBUTION LEADING TO HUGE DUMPS AND MASSIVE PRICE DROPS. MASSIVE PRICE DROPS OCCUR ESPECIALLY EASILY DURING A MARKET DOWNTURN WHEN THESE LARGE HOLDERS DUMP THEIR COINS. EVEN AFTER A DUMP, THE ORIGINAL OWNERS CAN STILL RETAIN THEIR MAJORITY OWNERSHIP OF THE CIRCULATING SUPPLY AND HENCE DO ANOTHER DUMP WHEN THE MARKET RECOVERS AGAIN IN RINSE AND REPEAT FASHION. THIS IS POSSIBLE BECAUSE MOST ALTCOINS ARE PROGRAMMED TO VERY STRONGLY REWARD INITIAL INVESTORS OR THE ORIGINAL CREATORS/ OWNERS OF THE COIN.

NOTE: BITCOIN DOES NOT HAVE THIS DEFICIENCY AS WILL BE EXPLAINED

Most altcoins were and still are developed and managed by a small group of individuals or an alliance of companies. This centralized control has meant that they can and have designed into the structure of their cryptocurrencies qualities that strongly benefit initial investors. For one thing, they have almost always given themselves (or a small number of early investors), most of the initial coins that were circulated, and this initial circulating supply is a large percentage of the overall amount of coins that will ever enter circulation. This distinctly differs from bitcoin in that bitcoin was originally born (or mined) by individual people all over the world on their own personal computers, before gradually being mined from a broad range of increasingly larger organizations. On top of this, with bitcoin the amount of coins that entered circulation did so gradually over a period of many years before reaching its current amount which is about 80% of its theoretical limit. This longer period of time has not only allowed bitcoin to become much more widely distributed than all the other cryptocurrencies, but has enabled it to go through multiple market cycles of highs and lows leading to even broader distribution.

Distribution matters because the buying and selling decisions of a small number of people can dramatically alter the value of the crypto. In particular, if large holders of a particular cryptocurrency decide to all sell at the same time, the price of the cryptocurrency will drop dramatically. For many altcoins, this process can repeat itself several times because these initial owners simply have so many of the coins in circulation and it will take multiple dumps before they deplete their holdings (if they ever deplete their holdings).

Most altcoins came into existence through an initial coin offering kind of distribution. This by its very definition makes them very centrally owned or distributed. Not to mention, many initial coin offerings required id verification and KYC (know your customer) processes which would have further reduced the distribution of the new coin. All this basically means that a small number of people own most of the altcoins that were ever created by this method. This is an unavoidable and indisputable aspect of these altcoins.

The other main way altcoins came into existence was when people forked the bitcoin blockchain or the blockchains of other cryptocurrencies, thereby creating the new coin which inherited the distribution of the original coin, at the

time of the fork. This method is better in terms of distribution, however, only moderately so since many of the users of these kinds of altcoins may have not been aware of the fork and may have discarded or lost the private keys to these altcoins through neglect or theft after they spent their bitcoins. Or these users simply might never have sold their coins, until the recent cryptocurrency growth spurt of late 2017. And even when they did sell their coins, they may have done so for bitcoin.

Another big issue narrowing distribution of these hardforked kinds of altcoins may have been programming changes in the altcoin before it got launched that dramatically benefited the development team (such as an extra mining session after the hardfork, but before its release to the public, which would have simply given the developers a lot of new coins; or a post mine airdrop that was launched shortly after the creation of the new cryptocurrency which only awarded altcoin addresses which held large amounts of the coin, the large holders being early investors and members of the development team).

Yet another closely related attribute of altcoins which affects its distribution is the fact that the people who own most of the crypto originally (the creators) have the ability to easily profit much more from the crypto without ever needing to even sell it. Again this is possible due to the way many altcoins are programmed. It may be possible therefore for them to always retain their majority share of the coin even if they regularly dump a proportion of their holdings. Examples of this can be seen in any altcoin that allows large holders of the coin to award or reward themselves proportionately large amounts of coins due to their large ownership stake of the coins. Or in any coin that has a masternodes or proof of stake or other similar system which gives large holders of the coin the ability to create sizable amounts of new coins or to collect substantial transaction fees. In some cases these masternodes hold 60% or more of all the coins in circulation. These original creators of the coin and majority owners of its circulating supply, can simply hold onto their majority stake almost indefinitely and make a continuous stream of income that way. New participants seeking to buy the cryptocurrency might never be allowed to buy from this large percentage of coins and must instead buy from the smaller percentage of coins in circulation. It is ALMOST like a pyramid style selling operation where the owners or creators of the cryptocurrency make most of the profits from new members while the majority of small owners and users of the cryptocurrency or those who join later, make peanuts. The wealth profit distribution is not as uniform or equal for both small and big holders, or early and late adopters like it is with bitcoin.

For early adopters of bitcoin, apart from creating exchanges, mining new bitcoins, and creating bitcoin related businesses that helped people to make better use of bitcoin (like bitpay or coindesk), the only other main way people could profit from bitcoins they owned and mined was to buy and sell it. They couldn't simply hold onto their bitcoins indefinitely and create residual profit from it like they can with alot of altcoins. To really profit from the actual bitcoins they had to sell it to someone else for fiat and in the process of doing so, made the coin more widely distributed and hence less vulnerable to future market collapses (through pump and dump operations). And miners in particular, were always incentivized to sell at least a portion of their bitcoins for fiat whenever they could because there was a real world ongoing mining cost to the procurement of those bitcoins.

Don't also forget that bitcoin in the beginning faced much more skepticism than it does today and was much more likely to be sold and hence became more widely distributed. Not to mention alot of bitcoins left the circulating supply (often in a random manner) due to the loss of private keys by owners; or confiscation and re-auctioning by government agencies due to crimes; or theft by hackers due to poor security measures, or some other way. Bitcoin personal storage standards of the past weren't as good as they are today.

I would also argue for instance that Satoshi's first 1 million ever mined bitcoins (which has never entered circulation) will never enter circulation because the owners themselves or himself, lost the private keys. All of this not to mention that bitcoin currently stores over 50% of all the investment that has ever been made by people into cryptocurrencies (through direct buying using fiat); and this calculation has not included the numerous other investments that have been made into businesses that revolve around bitcoin like exchanges, payment processors and hardware wallet manufacturers.

Also, as has already been mentioned, bitcoin has been around much longer than any of the alternative cryptocurrencies and has already experienced multiple market cycles of peaks and lows (compared to altcoins single major cycle in 2017 – 2018). This makes it sufficiently well distributed in such a way to benefit new holders of the coin, more or less equally, to old holders and to reduce massive volatility in its trading price.

Another factor that helps ensure this outcome of even distribution of rewards is the specific program parameters used by bitcoin. Bitcoin started out with the vision by its developers to create an alternative form of money that was not prone to the mistakes and vulnerabilities of the current financial system. And it was specifically designed to be fair, particularly in the way it was created and distributed.

One of these program parameters is the amount of profit people can make from bitcoin mining and transaction fees. In this aspect, the scale of the profit with bitcoin is no where near as large as the scale of profit that can be obtained with many or most altcoins. Bitcoins earned from mining and transaction fees are relatively small amounts of bitcoins relative to the total distribution of available coins. You can at most create around 340,000 new bitcoins in 2018 - 2019 if you alone got ALL the mining block reward (and this figure will lower in every halving event, the next one due in 2020). This represents only 340,000 of the estimated 11,000,000 live bitcoins whose keys have not been lost, which is only 3% per year. This is a conservative estimate since the current number of total bitcoins ever mined is currently around 17,400,000 (so I am calculating there to be around 6,400,000 inactive bitcoins). With transaction fees included, this figure would increase by 0.5% per year at most. And remember, in practice this 3.5% profit generated per year from bitcoin mining and transaction fees is shared among many many participants because mining pools are run by many individual people.

You might be exclaiming, "no wait, isn't mining managed by maybe only 20 or so key groups or mining pools?". The answer is yes, however individual miners who work within the mining pool and who receive the payouts of new bitcoins generated are still highly decentralized and globally distributed. People need to make the distinction that the top 20 mining pool operators consist of many separate miners comprising of individuals, groups and corporations from all over the world. The profit from new bitcoins mined and from transaction fees, is more or less, evenly shared according to the hashrate contribution of each miner.

And how about all the altcoins that hardforked from bitcoin, and which do not have these unfair programming and distribution issues. We are talking about the projects whose developers have only made minor changes to the protocol and who have more or less kept most of the positive characteristics of bitcoin. With enough time and enough market cycles, wouldn't their market value and distribution mirror bitcoin's exponential growth curve? The answer is: Not Necessarily. As you will soon see, this is due to Major Deficiency 2 and 3 which are mentioned next.

## MAJOR DEFICIENCY 2

MOST IF NOT ALL ALTCOINS ARE 'SUSCEPTIBLE' TO HARDFORKS BY THEIR DEVELOPERS THAT FORCE USERS OF THAT COIN TO CHANGE TO THE NEW HARDFORKED VERSION OF THE COIN. THE HARDFORK CAN BASICALLY BE PROGRAMMED TO RESET THE SYSTEM TO SEVERELY FAVOUR AGAIN INITIAL INVESTORS OR THE ORIGINAL CREATORS/ OWNERS OF THE COIN. BASICALLY AFTER THEY DUMP THEY CAN STILL RETAIN MAJORITY OWNERSHIP OF MOST OF THE COINS. FOR SOME ALTCOINS THERE HAVE BEEN 'REPEATED' CYCLES OF ALL TIME HIGHS FOLLOWED BY CLOSE TO ALL TIME LOWS WHICH COULD BE EXPLAINED BY THIS.

NOTE: BITCOIN DOES NOT HAVE THIS DEFICIENCY AS WILL BE EXPLAINED

Apart from the concentrated distribution of most altcoins noted above in MAJOR DEFICIENCY 1, many altcoins are suspect in one other major way. This second way called MAJOR DEFICIENCY 2 is double whammy hit on your investment. Basically, since most altcoins are managed by a few all powerful entities or individuals; they have the power to easily HARDFORK their blockchains, and FORCE all holders of the coin to follow along for the ride.

The thing to highlight is that they can hardfork and force adoption on their users at the same time; something that is very unlikely to happen with bitcoin.

The ability to hardfork is basically the ability to fundamentally change the programs used in operating the cryptocurrency and its blockchain, in a way that is not backwards compatible with older versions of the program. So anyone who wants to continue using the old version of the currency needs to maintain the old branch of the network themselves. A hardfork of a cryptocurrency can totally change how a cryptocurrency works and introduce unforeseen problems and vulnerabilities to it. It really should only be done as a last resort; and yet many cryptocurrency's development teams seem so willing to do it these days.

Lets more clearly explain this susceptibility altcoins face with more examples. Say you wanted to trade bitcoin for fiat. Currently you can buy and sell it globally from many different places and using many different payment methods. This is distinctly different to a specific altcoin which might only be able to be bought easily from one particular website, or somewhere else. This means that if this website says that they no longer support the old pre-hardforked version of their coin, the value of that preforked coin would plummet. Or it could plummet if the development team of that particular altcoin says that they no longer support the old version of their coin, and that all users are required to upgrade their software and/or hardware and use the post hardfork version. Anyone left with the old coin and who doesn't follow along will be holding a coin that no one supports or mines or processes transactions for on the blockchain, or a coin that rapidly loses all its value. Most altcoins are susceptible to this problem excluding 'maybe' the biggest ones.

The developers and/or early investors of most, if not all altcoin projects usually have the majority control of all the nodes or miners or coins, or operating websites that that particular cryptocurrency relies on. This means they can always get the concensus needed to execute any hardfork they propose, and at the same time get people to abandon the pre-hardforked coin.

During hardfork code changes, a cryptocurrency's circulating supply can fundamentally alter and this can greatly impact its distribution or ownership characteristics. This is possibly the biggest danger of the hardfork since it can alter the all important limited supply characteristic that enables all currencies to retain value. For example, the rate of new coins entering the system could change, or the maximum number of coins in circulation could change, or more coins could be added through airdrops or pre/post-mines. Other ways the distribution could dramatically change is by unintentionally or intentionally opening up vulnerabilities in the system that weren't there before, which may enable hackers to steal or create coins. Or any other possible number of as yet unforeseen things can happen that can steal away or chip away at investors hard earned wealth. This is clever and inconspicuous shifting of wealth at its best. There are countless real world examples of these above things happening.

Developers might even be so blatant so as to simply introduce more coins into their wallets once they have finished dumping their pre-forked coins, through possibly a postmine or airdrop or something similar, WITHOUT letting anyone know. Developers could for example introduce some kind of backdoor or program code that could discretely give them more coins down the road without people realising. Privacy coins are probably the most vulnerable to this kind of action because no one really knows who owns what and how much of a currency is at a particular address.

Granted, you could argue that one of the characteristics of most (but definitely not all) cryptocurrencies which helps to prevent blantant abuse like this during hardforks or even during the ICO stage is that they usually make use of open source programs. And make no mistake, open source is good at helping to secure cryptocurrencies and avoid abuse because it makes the programs freely available to anyone interested and knowledgeable enough to examine the code for bugs, backdoors, vulnerabilities or other potential flaws. The theory is that if there is anything wrong, someone would have already pointed it out and fixed it.

What people should know though is that the amount of review that is actually done on any particular cryptocurrency's open source software varies greatly among the different cryptos. The biggest, and most used, and most invested cryptos which have also been around the longest, are the ones that are logically more scrutinized, audited and peer reviewed. They are the ones whose code has been checked most thoroughly by the most skilled

people, and whose computer bugs and vulnerabilities have most likely been fixed. This is actually how cryptographic systems in general usually develop, where a new algorithm such the AES128 encryption key is introduced into the community, and then audited and nominated by knowledgeable people and groups, before being allowed to prove itself in the gauntlet of time through regular use.

The bottom line is that smaller cap cryptos are usually not scrutinized as much as the bigger ones and this is a point of weakness. As far as cryptocurrencies are concerned, in this aspect as in many other aspects, nothing can match bitcoin. Real world experience has shown that even some top 10 altcoins by marketcap have suffered major security breaches on their platforms or blockchains. If the big ones are susceptible like this, what chances do the small ones have? It needs to be said however, that bitcoin has never experienced a successful blockchain hack.

I emphasize now that I and no one else outside of these projects can know for sure if any of the altcoins actually commit the worst of the offences mentioned above. What I am saying is that it is possible that these things are happening without people really knowing about it. And in my view, knowing just how much of the potential is there, these kinds of things are likely happening.

Even many ecosystems revolving around bitcoin itself, has in its early and less recent history been prone to attacks. If these ecosystems regularly face attacks and breaches, why wouldn't altcoins and their ecosystems face attacks and breaches. These bitcoin related breaches have included exchange hacks, stolen wallets keys, software app bugs and a myriad of other issues. We are after all, skirting on the very forefront of this entire industry, or this very idea of what cryptocurrency is and what it can be used for.

From this necessary position arises a situation where there are few individuals or groups of people who have the knowledge, ability or even will power to safeguard people from scams. In a word, crypto has few friends. Financial establishments see it as a potential threat. Governments are wary of it. Established businesses unrelated to bitcoin but who could have their dominant position challenged by cryptocurrency businesses are not going to want to help. And no one really even knows much about what it is or why it is even valuable in the first place. In this very climate, who is going to protect you from all the new cryptocurrency scams, ponzi schemes, pyramid structures, pump and dump operations or anything else that can make you part with your money? Only yourself and your sense of caution.

How many investors for example actually research on the very important supply and inflation characteristics of the coins they hold. Or how many organizations managing altcoins even reveal this information to investors. Your altcoin could maybe have a rate of new coins entering circulation set at 90% of current coins being added every 2 weeks, and you probably wouldn't know. No doubt most of this new supply would be deposited into initial investors cryptocurrency addresses.

The other major cause of concern with cryptocurrency is that there is not much accountability when things go south. Altcoins have been the wild wild west of the cryptocurrency system in 2017 and 2018 and will likely stay this way for a while. There is an acceptance that crypto prices are inherently volatile and an understanding that it could completely crash at anytime. So even if a 90% drop in the value of a coin is experienced again and again, this scenario will almost certainly be attributed to market forces rather than to anything else. Altcoin company managers, developers, owners and coin-issuers never draw any public attention or scrutiny when the value of their coin goes under.

At least with fiat, drops in the value of a government issued fiat currency is going to be noticed by the population and will generally be seen as resulting from governments excessively printing money as opposed to market forces (although market forces can definitely affect the value of government issued currency as well as cryptos). In this way, it could be argued that there is a higher level of accountability in fiat than there is with altcoins.

So the finishing point being made here is that investing in a cryptocurrency that regularly hard forks and takes you along for the ride is almost the same thing as having to trust that the developers of the cryptocurrency will not print more fiat money for themselves! What is the advantage of cryptocurrency over fiat if you need to rely on

trustworthy humans to make the right decisions. Human monetary policy is always biased towards certain people. The hard coded laws and other characteristics that prevents this deception from happening in bitcoin, cannot be said to exist for all or most altcoins.

What are these hardcoded laws or characteristics of bitcoin?

First and foremost, in all its now 10 year history, bitcoin has never as yet forced a hardfork on its users. It has had its chain split many times into other cryptocurrencies (or alternative cryptocurrencies) which are hardforks in themselves, but it has never fundamentally changed its open source code where everyone in the network is forced to go along with them and where old holders or miners of the coin can no longer use or access their old chain bitcoins. I repeat that it has never hardforked its code and forced everyone involved (miners, nodes, users, exchanges, wallet providers, etc) to follow it and at the same time completely leave the original version lost and unused. There have been numerous times where the temptation and the reasons for doing it were there, however, to date it has still never happened. The level of consensus needed in the community to execute such a dramatic move has never been reached.

Some close calls included the buffer overflow incident of Aug 2010. Or the blockchain temporary split of Mar 2013. Or the bitcoin scaling debate of mid 2017 and subsequent bitcoin cash hardfork. In all these situations, a network wide consensus driven hardfork, with forced adoption was never implemented. The community got together to resolve these issues through soft program changes (soft forks) and community action.

Bitcoin is simply not prone to hardforks like other altcoins' hardforks because bitcoins network is so large and decentralized and dispersed that people are not forced to follow the hardfork in order to use the coin or to retain their wealth. It is almost impossible to completely and totally hardfork bitcoin whilst at the same time totally abandon the old version. During any major change like this, people always have the option to support the pre-forked version or the post forked version as has happened with the bitcoin cash hardfork. There will always be a segment of the community who will stick with the original version of bitcoin and continue to mine and verify transactions for it.

A parallel to this can be seen in Ethereum Classic. Ethereum Classic was the original Ethereum before their big hardfork in May 2016. At the time there was very strong reason for everyone to abandon the old coin completely (Ethereum classic) and follow the new version (Ethereum), and this is exactly what most people did. However, this move did not have participation from 100% of the users in the network and so the original Ethereum known as ‘Ethereum classic’ still exists and still has value because it is still maintained and supported by enough of its users and is sufficiently decentralized.

In a way, because bitcoin is the very first cryptocurrency, it is very difficult to hardfork bitcoin and at the same time have everybody abandon the old chain. It is much easier to simply split the blockchain and create new cryptos and have whoever wanted to follow the new chain to do so while everyone who wanted to stick with the old chain doing the same. Bitcoin in essence, due to its privileged and unique position, is almost unable to be hardforked in this way. This proves that it is not controlled by its miners or developers like a lot of people might think. It is also not controlled solely by its users or exchanges or anything else. The fact is, it is controlled and owned by everyone in the entire network who interacts with its blockchain. Only in the situation where all these many different groups suddenly and completely abandon the ‘first’ cryptocurrency after changing its code and making in non-backwards compatible (hardforking), will it disappear into the new version. Something very very enormous would have to happen for there to ever arise a need for this (like if the SHA256 hash was broken thereby making transfers totally insecure).

Even if all the current core developers of bitcoin try to fork it and force users to change over, all they would be doing is relinquishing their esteemed position for some other group of developers to take their place and continue working on the original version. Over the medium to long run, the current core developer group of bitcoin is a continuously changing group of people anyway. It is actually an opt in system (not a we hire you system) where anybody can propose ideas, after which the majority of users in the network can decide to implement them or not.

This is completely different from the centralised decision making process of most or all altcoins and the rarely changing owner/initial investor type development teams of most or all altcoins.

The overarching point I am making is that the original core Bitcoin implementation is not vulnerable to the dangers of the hardfork. It is unlikely to ever totally disappear from existence or to deviate too much from its original version. Nor does it ever need to.

And if there ever does come a day where this dramatic need does arise and a change is implemented, this would still not negatively affect bitcoin's value because its main value proposition is not purely in its code or even its network. Its main value proposition is what arises as a result of its code and its network. The result is that it offers humans the chance to own and use a form of money that is a better medium of exchange and a better store of value than what is available. As long as these qualities can still be maintained in any new version of bitcoin, then its value will remain the same.

And now for the Third Major Deficiency of the altcoin as I see it.

## MAJOR DEFICIENCY 3

ALL ALTCOINS ARE INFERIOR IN SECURITY TO BITCOIN BECAUSE MOST OF THEM ARE ARGUABLY ALOT MORE SUSCEPTIBLE TO THE 51% ATTACK. NO ALTCOIN HAS BEEN AROUND AS LONG AS BITCOIN HAS NOR HAS ANY OF THEM PROVEN THEMSELVES FOR AS LONG AS BITCOIN HAS. MOST OF THEM HAVE NOT BEEN AS CAREFULLY AUDITED AND REVIEWED BY THE COMMUNITY AND ARE LIKELY TO HAVE MANY MORE CRITICAL COMPUTER BUGS THAN REALISED WHICH OFFERS ATTACK AVENUES FOR HACKERS. AND ANY ALTCOIN THAT DOES NOT IMPLEMENT PROOF OF WORK IN ITS DESIGN LIKE BITCOIN DOES IS USING AN UNPROVEN SYSTEM. LASTLY, ANY MAJOR HACK OF A BLOCKCHAIN LEDGER, SUCH AS SOMETHING THAT RESULTS IN A DOUBLE SPEND ATTACK, WILL RESULT IN A MASSIVE LOSS OF CONFIDENCE IN THE CRYPTOCURRENCY, AND THEREFORE A MASSIVE AND POSSIBLY UNRECOVERABLE DROP IN THE PRICE OF THE CRYPTOCURRENCY.

One of the main reasons I believe why many altcoins hardfork so often is because their blockchains are inherently vulnerable to being hacked or attacked by the notorious 51% attack, and hardforking reduces or fixes this scenario. The 51% attack is a situation where the majority of the computers working to secure the network and mint new coins; disrupts, steals from or otherwise compromises the normal intended operation of the network. Most of the time, this takes the form of a double spend attack where the attackers/hackers send cryptocurrency to a particular organization, then receive the product or service from their payment, before rewriting the blockchain ledger to take back the cryptocurrency they originally sent to that particular organisation. In effect that are spending twice.

Bitcoin is much much less susceptible to a 51% attack on the blockchain because there doesn't exist anywhere on the face of planet earth any computers or group of computers which aren't already being used to mine the bitcoin blockchain, that can successfully overpower the bitcoin network or hashrate. To attack the network from outside the network would require a covert operation involving massive investment of capital, and time as well as the theft of the manufacturing blueprints of the latest ASICs mining devices. They would then have to build the manufacturing centres from scratch before beginning work on building the actual mining chips. After this, a game of catch up in manufacturing these devices would ensue, with the goal of the conspirators being for them to eventually own mining devices with more overall hash power than the entire bitcoin network. Remember that while the devices are being created by the conspirators, continuously newer and possibly faster blueprints and devices are being manufactured by the legitimate companies. So production of these devices by the conspirators would really need to be on a giga-normous scale to successfully catch up. And even if they finally manage to do this and execute the attack in such a way so as to succeed, a simple software change can be implemented into the bitcoin protocol by existing miners which will instantly and completely negate the perpetrators attacks (bitcoin might not even need to hardfork).

How about attacks perpetrated by entities already operating within the network. The only chance of this 51% attack happening here is if a large proportion of existing mining pools purposely colluded to effect this outcome. Not only would the attempt at this be at great cost to the perpetrators, but everyone would know who did it (there is complete transparency). It would also only be able to be executed for a short time before the problem is automatically resolved either because the announcement of the attack would lead to all users of bitcoin to temporarily require more confirmations; or because there is a miners exodus from the managers of these mining pools; or due to some other reason such as a software or protocol change. The guilty parties will subsequently permanently lose all their power. Not only this, but any attempt at such a big act of disruption, MAY cause a massive loss of confidence in bitcoin in general (and subsequently the entire crytocurrency industry) which may result in massive and long term drops in the price of bitcoin, leading to even further losses for the perpetrators. These things have already happened before for coins such as Bitcoin gold (51% attack), and Ethereum classic (dao hack). It needs to be emphasized that in the case of a 51% attack on bitcoin from within, absolutely no one benefits, and the only parties that could possibly perpetrate the act stand to lose the most from it.

As you can see, existing managers of mining pools are unlikely to willingly and cooperatively perform such an attack. And if they did, there would likely be criminal prosecutions. If alot of rich people lose their money (or bitcoins) and the culprits are known to everyone, you can bet there will be criminal proceedings.

This strong disincentive to harm the network specifically due to community punishment through a mining pool exodus, applies equally to any other potentially unpopular actions which majority miners may take it upon themselves to impose. The main example being the blacklisting of certain addresses from being used on the blockchain. As a practical example, assume that 51% of bitcoin mining pools try to blacklist addresses. Due to their majority hashrate, this would be possible to do (though impractical over short timeframes) since they will always eventually have the longest chain. However, because this censorship or blacklisting would be counter to what I believe most people in the community would accept, many of the individual miners who power these mining pools might simply move to another pool which doesn't blacklist addresses, thereby removing all the power and influence of those mining pool managers who did blacklist. For this reason, any initial attempts at blacklisting addresses would be unlikely to take off. This same thing doesn't necessarily apply to many altcoins because mining activity is a lot more concentrated for many altcoins, partly represented by the much lower hashrates. A much smaller segment of individual miners can gain and keep majority control of these altcoin blockchains.

So how about the final major scenario often discussed on cryptocurrency forums where bitcoin is compromised by a 51% attack because the managers of these mining pools are coerced or forced (possibly at gunpoint) by criminals, to execute a 51% attack. Although seemingly plausible at first, in practice, this scenario would not be a straight forward undertaking. It would require all the mining managers of all of the targeted mining pools to submit at the same time to the will of the criminals and would need to overcome all the defence mechanisms that may have been built into the mining managers systems. If just 1 of the mining managers succeed in thwarting an attack, this would be enough to stop the whole thing. Think of the idea of multiple fiat central banks being robbed simultaneously of cash at gun point and all the things that banks can do to prevent this from happening and you get some idea of what I mean. There could be distress power switches that suddenly lock access to systems or physical premises. There could be software programs that automatically execute a kill switch or a power off of all the computers running it. There could be time locks used on critical systems requiring the passwords of multiple high level individuals to approve any major changes. There could be loud security alarms that alert police as well as exchanges and everyone else immediately when there is a breach. All this, not to mention the armed security guards that may be patrolling the facilities. Trying to actually attack the bitcoin blockchain through coersion is not as easy as it may initially seem. And once again, even if a blockchain attack is successful, the response to stop it would not be difficult.

So to conclude, the bitcoin blockchain ledger is immune to security breaches in a way that most other altcoins blockchain ledgers are not.

And why exactly are altcoins a different matter entirely?

In simple words, altcoins have much less computational power devoted to their blockchains which make them more vulnerable to a 51% attack from groups of computers outside their network. Bad actors can hire or create mining power from other places that aren't currently being used and then perpetrate the attack much more easily. Many altcoins are mined using general CPU or GPU processors which means that any organisation which manufactures a dedicated mining chip (or an ASIC chip) for these particular altcoins can temporarily obtain proportionately large amounts of hash power. Bitcoin isn't susceptible here because all or most miners in the decentralized network already use ASICs chips. ASICs chips force participants to not only have to invest more of their money into obtaining the hardware needed (which discourages them from harming the network) but also means that large controllers of CPU or GPU processors such as government super computers, leading IT and search engine conglomerates or anyone else with lots of computing power, is unable to harm the network.

And the threat of certain people wanting to harm or steal from the network is always there. Human nature has shown that anything that can happen will happen. It happened once before with 51% attacks on Bitcoin gold and also with Zencash as well as a number of other coins. There are always humans with ill intent in this world who may stand to benefit from certain actions. If it is possible to harm a particular organization to their benefit, even if it is costly to do so, then they will do it.

Now it needs to be emphasized that the likelihood of this kind of 51% security breach occurring on any single particular altcoin varies greatly between the different blockchain ledgers. Smaller, newer and lower market cap coins, as well as coins which share similar hashing algorithms to larger coins, are the most vulnerable. Altcoins that do not have widespread, decentralized use of dedicated ASICs to mine them are in my opinion more vulnerable to attack than those that do (the precise reasons were briefly touched on earlier; the in-depth reasons are reserved for another discussion).

All of these weaknesses means that the main value proposition of altcoins being 'security', may not be true for most if not all altcoins. Only bitcoin is totally immune cos it has the most hashrate and its hashrate mining is very decentralized. The difference is many many scales of magnitude (in the hundreds of thousands of times difference). If you simply compare the number of hashes computed by the bitcoin network and compare it to the number of hashes computed by its next nearest altcoin Ethereum; you get a good idea of the difference (40,000,000 TH/s vs 180 TH/s as of Dec 2018!).

Not only this but bitcoins security protocols are based on very established cryptographic science created by some of the best minds and organizations on the planet; and these protocols have stood the test of time. Its SHA256 algorithms and other elements of its blockchain systems have for most of its existence had a multi-million to multi-billion US dollar bounty on it for anyone or any organization who could crack it. This exists in the form of the first ever million or so bitcoins still sitting at public addresses that have never been touched. Anyone who can compromise the system can themselves claim to be Satoshi, and would be able to cash in on these coins.

Don't believe in supposedly future susceptibilities of bitcoin such as those arising from quantum computers because these risks are, in my opinion, totally non-existent (quantum computers cannot exist), and in the theoretical thought experiment best case scenario of it possibly existing, is still decades away. Now and into the future, the bitcoin blockchain will be the preferred medium for the big million dollar value cryptocurrency transactions. This is not only because it has and will continue to have the most circulation; and not only because it is the most established, change resistant and decentralized blockchain; but because it is the most secure and least susceptible to double spend attacks.

Anyone who regularly creates, uses, secures or updates computer programs knows that computer bugs are a common, unavoidable part of new programs. Even established programs occasionally have bugs or vulnerabilities discovered. These issues extend to every piece of software, application, web server, website, or interaction people have with a particular program. In the cryptocurrency space, this means that every wallet program you use, every website you interact with, every phone application or online computer you use to interact with the cryptocurrency blockchain may have bugs or vulnerabilities that can compromise your experience or cause you to lose your money.

When the volunteer developers who initially worked on the bitcoin protocol before it launched, collaborated together on the program, they did so while being very careful to avoid making mistakes, or allowing bugs and vulnerabilities to exist in their programs. At least one prominent developer has publicly stated that big mistakes such as these for their cryptocurrency was totally unacceptable (as it should be). The joint contribution went on for months to years. If the design and development stage is counted from when Satoshi published his white paper and started 'toying with code' in October 2008, to when bitcoin was first regarded to have been used as money on 'Pizza day' in May 2010, then this development period spanned at least 1.5 years. Could the same be said to have occurred for most newer altcoins which may have been rushed to market in the 2017 – 2018 bull market. In my opinion, most likely not.

So it just goes without saying that buying and using a cryptocurrency that is the most established and has the most users and developers, is going to be the most secure. It also goes without saying that only bitcoins proof of work architecture can be considered as sufficiently established and sufficiently secure in the crypto-universe due to its program characteristics and proven length of use. Any other cryptographic method used by other cryptocurrencies to secure their blockchains or networks is as yet unproven. And some could be said to be highly experimental.

Finally, I would like to point out again, that this is a space where a lot can go wrong. A lot regularly does go wrong for new and old coins alike. Any blockchain or cryptocurrency that experiences the grand daddy hack of them all which is the attack on their actual blockchain in the form of the 51% attack is likely going to experience a massive and unrecoverable loss of confidence in the community resulting in a quick and possibly unrecoverable downward move in the value of the currency. This has already happened for a number of coins. Since all cryptocurrencies EXCEPT bitcoin are arguably vulnerable to the 51% blockchain attack, your altcoin investment could do everything else right and keep appreciating in value for months and years, and then all of a sudden start to lose 92 – 98% of its value within the span of weeks or months. If you own an altcoin that is susceptible to this; then buying and holding onto it uncompromisingly, may not be a good idea.

SO TO SUMMARIZE IN ONE SENTENCE; THE THREE MAJOR DEFICIENCIES OF THE ALTCOIN ARE:

1. POOR DISTRIBUTION WITH QUESTIONABLE PROGRAMMING CODE FAVORING EARLY OWNERS;
2. EASY ABILITY TO IMPOSE A HARDFORK ON ITS USERS ONCE AGAIN TO THE THE BENEFIT OF EARLY OWNERS; (AND)
3. INFERIOR OR FAULTY SECURITY PROPOSITION IN COMPARISON TO BITCOIN.

## FUTURE STATE AND BANK SPONSORED ALTERNATIVE CRYPTOCURRENCIES

Future government issued cryptos have the same problems and are the same or worse than altcoin cryptos as they will offer even more centralized control to their creators. Some high marketcap cryptocurrencies now currently being bought and traded may have initially been introduced by governments using alias identities. In short, any and all government issued crypto is simply fiat in disguise. If a government tries to issue a cryptocurrency then they will almost surely give themselves between 30% - 50% of the original supply and will program it in such a way to enable them to continuously get and maintain their majority share like many altcoins do now. No way will government issued crypto be decentralized or have any of the other key qualities of bitcoin (like security and censorship resistance or worldwide distribution).

Furthermore, if a government issued crypto is not allowed to roam free and move based on market supply and demand then this means it is a closed system and can't be called a cryptocurrency. If its value is artificially being held up by government forces then the trust must be placed within that government to not abandon the link. It won't offer the value proposition that bitcoin offers naturally due to its inherent program characteristics, broad distribution and strong integration with existing money systems. This strong integration with existing money systems by the way, is another major reason why bitcoin stands out greatly among its peers. I believe many people living in

financially oppressed countries for instance, often buy bitcoin purely so they can convert it into stablecoins, or online gift and money cards, so as to preserve their savings.

If on the other hand, the government issued crypto is sold on the open market and its value is allowed to move with the market, having its price relative to fiat currency being allowed to fluctuate up and down based on market demand, then you can absolutely bet that when market forces go full circle and people start selling their coins, large holders of the currency (mainly government employees) will not be able to resist the urge to also dump their coins into the market, resulting in another 90% crash. After this happens, any purpose for which the coin was suppose to have been designed for would be hard to meet.

All of the statements above that apply to government issued cryptocurrency applies equally to any future bank issued cryptocurrencies, or cryptocurrencies issued by any other major organization or group. Banks that do start their own cryptocurrencies would just be doing so to follow the trend, and will have the aim of replacing their conspicuous control of the financial system with something slightly less conspicuous.

## PAYING MY RESPECTS

I am completely of the understanding that publishing this post will likely make me unpopular in the altcoin community including with many large altcoins. This could spell disaster for me, and alienate me from the cryptocurrency community. The altcoin market does after all still make up a large amount of the total marketcap of cryptos, currently close to 50% (marketcap by the way might not be as good a measure of market dominance as 24 hour trading volume).

I believe I am already unpopular with the fiat community, with the banks and probably many governments. Many storage companies and manufacturers of cryptocurrency hardware wallets probably dislike me too because my operations put them in direct competition. Suffice to say, these notes will probably make me unpopular with governments who may be thinking about creating their own cryptos (or have already discretely done so) and even the rare few organisations or jurisdictions that are trying to foster altcoin growth in their communities or economies.

Even so, my primary objective is to help people make informed decisions and to avoid the drastic losses from the last bull run in altcoins (often times 92% - 98% loss from their all time high). This is my priority. Also, these losses just give crypto and bitcoin overall a bad name, which is a shame since bitcoin is distinctly different from altcoins, and bitcoin will benefit everyone.

When cryptocurrencies really do drop in value by 92 - 98% or more from their all time high in the span of weeks or months, then all those doomsayers were definitely right when they referred to some cryptocurrencies as tulip bubbles. Worse still, for a number of cryptos, this cycle of hitting close to all time lows has happened repeatedly! Any mad rush again to buy bitcoins will likely lead to a mad rush to buy altcoins. Then when the altcoin market crashes again due to the inherent design and other flaws described above, it could cause bitcoin to once again drop more severely than it otherwise would and for many people to lose their money. History will repeat itself as it has already done many times before. Is preventing this from happening again such a bad thing? At the end of the day, I want people to make a clear distinction in their minds between bitcoins and altcoins.

Buying and holding altcoins as a long term investment strategy because you think it is going to go up in the long run through a series of massive swings like bitcoin has, is not necessarily a good idea, because altcoins are not bitcoins in several important areas. And recent history has proven many altcoins to be risky investments that can routinely suffer 90% + losses. The long term track record of all altcoins is as yet unknown. Do not rush in with your money blindly trusting in previous, long term bitcoin performance and expecting the same results from your altcoin investments, because I repeat, altcoins are not bitcoins.

And even if we overlook the three Major Deficiencies of the altcoin described above; it is still not clear how many altcoins can succeed in this competitive world of currencies and companies without riding off of bitcoin’s success.

The growth in altcoins experienced in 2017 – 2018 may have originally been due to the piggybacking effect where these coins benefited from the halo, recognition and momentum of bitcoin. Altcoins may not have risen on their own merit and anyone who looks at the price charts of all the different coins, can see the striking similarities of their weekly price movements.

For an altcoin that exists as a currency to excel requires it to be better than bitcoin is as a currency, and better than fiat is as a currency. Maybe you can see now how altcoins are not better than bitcoin and how they are not better than fiat. For an altcoin that exists as a representation of a specific company to excel (and to be regularly used as a token by its owners) requires that particular altcoin company to offer something that is better than what existing competitor companies already offer (and whose users just happen use fiat as their currency). This is required before the crypto-token has any chance of acquiring significant usage and/or value on its own. How else would the native token gain value above that of bitcoin or fiat? Do altcoin companies really do anything better than their fiat currency competitors? Take the word blockchain or cryptocurrency out of the picture and and then see unimpeded whether the project is valuable.

In saying all these things, I am also hoping to encourage developers of altcoin projects to improve their cryptos and their decisions to the greater benefit of everyone who contributes money to their platfoms and who uses their platforms. The focus should be strictly on your users. And I am suggesting that security should remain a priority of all altcoins, as this is one of the core characteristics which give cryptocurrencies value. And I am saying that hardforks are something developers should only make as a last resort. I would also like developers of specific altcoins to openly address (or respond to) these general deficiencies of the altcoin and communicate to their users exactly how or why these deficiencies might not relate to their cryptos, or how they aim to manage or reduce these shortcomings.

## CRITIQUING BITCOIN

In all fairness and in the interest of objectivity, it must be said that Bitcoin itself has dropped alot from its 2018 all time high compared to the subsequent low (notice that bitcoin is the only crypto that is commonly written with both the capital and lowercase b). The drop from peak-to-trough as of this date has been around 84.1% (drop to 15.9%). As stated before though, bitcoin's long term trajectory has always moved in a hugely upward direction, so this current drop is really just down to the nature of market cycles (anyone who wants my view on why bitcoin has kept going high and higher from its very early days, I invite to read my other articles which were published in 2018). The downward price movements from all time high to subsequent low in Apr 2013 ($266 USD) – July 2013 ($70 USD) and Nov 2013 ($1242 USD) – Jun 2015 ($227 USD) can be seen to be similar to the those experienced by bitcoin in 2018 (the previous drops were to approx. 26.3% of all time high and 18.2% of all time high). So this crazy volatility and emotional roller coaster has got its precedents and we may very well, have hit the lowest value bitcoin will ever be in its entire history from this point on.

Looking closely at the older figures, we can see that bitcoin has never had a more than 100% to less than 15% move from its all time high to subsequent low since before 2012 (in 2011 its peak-to-trough drop was about 92% - a drop to about 8%). This shows that its cycles of volatility have reduced over time (unlike many altcoins). Some people might think that there isn't much difference between a drop to 16% as opposed to a drop to 2% - 8% and this simply isn't correct. For something to get from 16% to 2-8% requires a further 50-87% drop in its value from that point in time (not a further 8-14% drop) and a 50-87% drop is like the scale of another market crash.

I believe also that this most recent drop in 2018 was fueled by the run of the altcoins since the drop from the altcoins possibly spooked alot of bitcoin investors. This altcoin add-on makes it a unique situation compared to previous drops. If many investors see altcoins as being the same as bitcoin (which it is not), then this could partly explain the movements. Arguably, this same scenario is now significantly less likely to occur because the mania and novelty of altcoins has dropped which means they are less likely to skyrocket and plummet as before.

Even with an 84% bitcoin drop though, how does this compare to some other asset bubbles that have occurred in recent history such as the sub prime morgage crisis of 2006 - 2008 where the non-inflation adjusted price of house prices in the US plummeted by 70% - 90%? If inflation was accounted for, it would have been significantly worse (governments printed heaps of cash to try to stem the effects). In any case, alot of properties simply could not be sold at even 5% of the original price. Property is suppose to never crash and governments and banks always try to keep it this way. And yet it still did. At least with bitcoin's super duper global liquidity, there is always a buyer of your bitcoin if you wanted to sell it. You could and can ALWAYS exit the market easily and quickly. So, bitcoin's price drop doesn't compare too badly it seems.

Granted, the value of property doesn't usually drop quite so much if at all. However, it needs to be said that property also never skyrockets to over 1 million times its initial value over an 8 and ½ year period, like bitcoin has done between May 2010 – Dec 2018. The ability to ride the market roller coaster may be the real price people need to pay for this rare opportunity at exponential growth. Not to mention, unlike property, bitcoin does not need, nor does it have, any major governments or banks supporting it. In fact, it could be argued that most humans on planet earth either have no opinion of it or are in opposition to it. Something with qualities this resilient is not going to stay cheap forever. And anyone with any amount of initial capital can buy bitcoin with their own earnings. They don't need to take on a mortgage or a loan or have heaps of starting capital.

For all we know, there may have also been some active market manipulation by big players which contributed to bitcoin's sharp drop (I remember the time in early 2018 where everything was dropping except Ether making it look like Ether was independent from the other cryptos and was a safe haven, and then all of a sudden Ether dropped heaps as well). Maybe some large players wanted to manipulate the price and cause a crash.

Hopefully, these same players have now come to the conclusion that they can't beat bitcoin and cause it to crash to zero, and therefore may have decided to join the bitcoin party -"if you can't beat them, join them"-.

Barring a massive compromise to the bitcoin blockchain, bitcoin will likely remain the dominant cryptocurrency by marketcap and 24hr trading volume now and into the future. For all the reasons above, this will be true. It will also be true because it is the reserve currency of all the others. It is the only crypto that can claim to have the strongest integration with existing fiat and other money systems. And for another crypto to successfully establish equally strong links on their own at this late stage in the game would require a lot of investment for little benefit, and would also be unlikely to succeed. It is like having different telecommunications companies develop their own cable wires and poles to everyones homes in a given area (or water companies creating multiple underground pipe networks), instead of simply renting or sharing the already established lines.

People usually buy bitcoin first before they buy any other crypto. This among other reasons is because it is the easiest to acquire before any of the others. And this dominant position will likely be true at least until the overall market matures, decades or centuries from now.

## CLOSING COMMENTS

Cryptocurrency should be an object that helps the average global citizen. It should allow anyone to take part in it and to store their hard earned money in it to preserve and grow their wealth. And it should exist as an alternative to current financial systems, especially for those people who really need it. Cryptocurrency must enable people without access to banking services to hold and use digital money, and to transfer value peer to peer without fear of undue financial loss. It should benefit the global citizen in a multitude of ways, including through the fostering of technological improvements and services in existing financial systems (due to competition).

Cryptocurrency should be exactly as its name suggests, a currency that is cryptographically secure. It firstly needs to exist as a "currency" that is widely distributed and owned, with numerous purchase channels and multiple use cases such as international remittances and financial exchange. It isn't simply something that represents company stock or in-store credits offered and managed by a particular organisation. It secondly needs to be "cryptographically secure"

in every aspect, from the way users create their own public and private keys, to the way users interact with the blockchain, to the way people store their information. The most established blockchain, the one with the proven background and the one that hasn't ever forced its users to hardfork because it has never needed to; is the one you should buy and own.

Cryptocurrency should NOT be a way to replicate the current fiat system of the world where the rich become richer and the poor become poorer and where there are any number of gate keepers, middlemen and adjudicators each collecting their own share. It should not be vulnerable to the same flaws of government and bank fiat sponsored money systems that have in the past and present, led to whole economies and livelihoods collapsing and being ruined. It absolutely can not serve as a way for designers and developers of new cryptos to profit indefinitely from unfair design attributes at the expense of the majority.

Which leads me to my final recommendation: **Do not** buy any altcoins at all unless you need to own it to directly use the coin for the specific purpose it was designed for, and do not follow any future bitcoin hard forks. This means, don't sell your bitcoin for the bitcoin forked altcoin (but of course do cash in on the forked bitcoin by selling it immediately for the real bitcoin). Yes, this is a blanket recommendation and there are probably altcoins out there that can avoid some or most of the pitfalls described above however, they still won't be as good as bitcoin for your everyday hodler (hodler = person who wants to simply buy a cryptocurrency and "hold on for dear life" and then not think about it again). Bitcoin grew exponentially because its primary value case is that it serves as an alternative store of value and medium of exchange which existed outside and independently of the current financial system. It succeeded because it emulated gold and because it emulated digital currency. ANY other value case for cryptocurrency like those offered by most altcoins is still, as yet, unproven.

Stick with bitcoin if you are a newbie to this asset class and you cannot go wrong. Yes it is maybe more boring and old and maybe even technologically less advanced than other coins (this simplicity makes it more trustworthy by the way). And yes it seems to offer less profit potential.

But make no mistake... it is the best sure fire bet you can make with your money, now and into the future.

## GLOSSARY

**Altcoin =** any cryptocurrency besides bitcoin

**Coin =** any cryptocurrency

**Crypto =** cryptocurrency

**Hodler =** person who wants to simply buy a cryptocurrency and "hold on for dear life"

**Price of bitcoin =** the price of bitcoin in terms of a fiat currency like the US dollar.

**Stablecoin =** a digital coin backed by a single organisation or various organisations, with the sole aim of tying its value to a particular fiat currency. I don't regard this as being a cryptocurrency for the purpose of this essay. In fact, companies which issue stablecoins wield tremendous power and influence in the cryptocurrency ecosystem because they 'can' create these stablecoins out of thin air, move them onto the exchanges which support them, and offer them up for sale to people to buy using bitcoin. Everytime someone buys a stablecoin with bitcoin, there is a downward pull on the value of bitcoin and power is given to the stablecoin companies. It is easy to see then how bitcoins price can be influenced when stablecoin companies acquire a lot of bitcoin (only possible because people are willing to sell their bitcoins for the stablecoin). When the stablecoin company owns bitcoin, they can influence the market whenever they 'cash out' their bitcoins for fiat via the decentralized exchanges. In a way, stablecoin issuers can become 'whales' in the bitcoin monetary system if a lot of people buy their stablecoins. As of this date, stablecoins cumulatively have the second highest 24hr trading volume of all crypto-assets listed online, the first highest being bitcoin. So, the impact and influence of stablecoins cannot and should not be under-estimated. Even so, individuals who hold onto stablecoins can be seen to be undertaking a risky activity because the major cryptocurrency exchanges can, at anytime, decide to no longer accept deposits of stablecoins, before eventually de-listing the stablecoins, causing any holders of these stablecoins to suffer 100% loss (if the stablecoin issuers don't or cannot honor their link to fiat).