Ben Yu

Jun 24, 2017
·
75 min read

Cryptocurrency 101

Ever since Nas Daily's video came out about how I earned over $400,000 with less than $10,000 investing in Bitcoin and Ethereum, I've been getting hundreds of questions from people around the world about how to get started with cryptocurrency investment.

First: I'm *super* glad there's so much interest in cryptocurrency right now. I firmly do believe that cryptocurrency and blockchain technology has the potential to fundamentally change much of the way our world currently operates for the better. It reminds me a lot of the internet in the 90s.

Second: 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. Countless speculators and day traders have lost their entire fortunes trading cryptocurrency. I was no different when I first started investing in crypto. The first $5000 I put into crypto fell almost immediately to less than $500 — a net loss of over 90%.

Third: All of the following words are entirely and solely my own opinion, and do not reflect any objective truth in the world or the opinions or perspective of any other individual or entity. I write them here merely so people can know how I personally approach cryptocurrency, and what I have personally found helpful in my foray into this realm.

I'm firmly of the opinion that one should never invest in something one doesn't thoroughly understand, so I'm going to split this article into three parts.

The first part will speak to a broad explanation of what bitcoin and cryptocurrency at large are. The second will discuss my personal investment philosophy as it pertains to crypto. The third will show you step by step how to

actually begin investing in crypto, if you so choose. Each section will be clearly delineated, so feel free to skip parts if they're already familiar to you.

Part I: What is Bitcoin? Why is it useful?

Great question. If you want the full story behind the advent of bitcoin, I highly recommend the book Digital Gold. It traces the entire history of bitcoin from its inception all the way up to 2015. It's an engrossing read, and highly informative.

For now, let's start with a quick history lesson about bitcoin. Bitcoin was officially unveiled to the public in a white paper published October 31st, 2008. The white paper is actually extremely readable, very short (just 8 pages), and incredibly elegantly written. If you want to understand why bitcoin is so compelling straight from the horse's mouth, you must read this paper. It will explain everything better than I or anyone else likely ever could.

I won't delve too much into the technical details of how bitcoin works (which are better elucidated in the white paper), but will instead focus on a broader exploration of its history and implications.

Subpart: The Background Context of Bitcoin

Bitcoin was invented in the aftermath of the 2008 financial crisis, and the crisis was a clear motivating factor for its creation.

Numerous banks and other financial institutions failed across the world, and had to be bailed out by governments at the expense of their taxpayers. This underscored the fragility of the modern financial system, where the health of our monetary system is reliant on banks and other financial institutions that we are forced to trust to make wise and prudent decisions with the money we give them. Too often for comfort, they fail to carry out this fiduciary responsibility to an adequate degree.

Of particular note is fractional reserve banking. When you give a bank $1,000, the bank doesn't actually keep all that money for you. It goes out and is legally allowed to spend up to $900 of your money, and keep just $100 in the off chance that you ask for your money back.

In the most simplistic case, if you are the only depositor at this bank, and you ask for more than $100 back at once, the bank won't be able to give you your money, because it doesn't have it any more.

Shockingly, this is actually how banks work in reality. In the United States, the reserve requirement, or the percentage of net deposits banks are actually required to keep in liquid financial instruments on hand, is generally 10% for most banks. This means that if a bank has net deposits of a billion dollars, it needs to only keep 100 million on hand at any given time.

This is fine most of the time, as generally the customers of that bank won't all try to cash out at the same time, and the bank is able to stay liquid. However, the moment customers start to question the bank's financial stability, things can go south very quickly. If just a small number of customers begin asking for all their deposits back, a bank can rapidly become depleted of all its liquid funds.

This leads to what's known as a bank run, where the bank fails because it is unable to fulfill all the withdrawals customers demand. This can escalate quickly into a systemic bank panic, where multiple banks begin to suffer the same fate. Each successive failure compounds the collective panic, and quite quickly, the whole system can begin to collapse like a house of cards.

This is what led in large part to the Great Depression, for instance. The whole system is fundamentally predicated on trust in the system, and the second that vanishes, everything can go south incredibly quickly.

The financial crisis of 2008 highlighted yet another risk of the modern banking system. When a bank goes out and spends the 90% of net deposits it holds in investments, it can often make very bad bets, and lose all that money. In the case of the 2008 crisis, banks in particular bet on high risk subprime mortgages. These were mortgages taken

out by borrowers very likely to become delinquent, to purchase houses that were sharply inflated in value by the rampant ease of acquiring a mortgage.

When those mortgages were defaulted on, the artificially inflated values of the homes began to collapse, and banks were left holding assets worth far less than the amount they had lent out. As a consequence, they now had nowhere near the amount of money that customers had given them, and began experiencing liquidity crises that led to their ultimate bankruptcy and demise.

After the Great Depression occurred, the government attempted to address this issue by creating the Federal Deposit Insurance Corporation (FDIC), which technically guarantees all customer deposits in participating banks up to $250,000 per account.

Unfortunately, the FDIC is just as dramatically underfunded as banks are. As the FDIC itself acknowledges, it holds enough money to cover just over 1% of all the deposits it insures. In other words, if banks reneged on any more than 1% of all their deposits, the FDIC itself would also fail, and everyone would yet again be left in the dust without recourse.

In fact, this has already happened. The FDIC used to have a sister corporation that insured savings and loan institutions, as it itself at the time only insured bank deposits, and not savings and loan institution deposits. This was known as the Federal Savings and Loan Insurance Corporation, or FSLIC.

In the savings and loan crisis of the 1980s, over 1,000 of the 3,200 savings and loan institutions in the United States failed in rapid succession. The FSLIC almost immediately became insolvent itself, and had to be recapitalized several times with over $25 billion dollars of taxpayer money. Even this didn't even come close to being sufficient to solve the crisis, and the FSLIC managed to only resolve the failure of less than 300 of the 1000 bankrupt institutions, even with all the handouts from taxpayers, before it just flat out gave up and dissolved itself.

For the most part, things generally work fine on a day to day basis. This belies, however, the true fragility of the system. It's hard to anticipate these things before they happen, because it's so easy to fall into the trap of assuming

that things will always be as they mostly always have been. If things have been fine yesterday, and the day before, and the few years before that, or even the few decades before that, we just naturally assume that they will continue to be fine for the indefinite future.

History has proven this to be an often fatal assumptive error. The second things start to stop working, they tend to stop working in an extremely rapid, catastrophic fashion. There's very little, if anything, stopping us from seeing another Great Depression sometime in the future, be it the near or longer term future. When that does happen — and it almost certainly will, sooner or later, if history is any good teacher — those who haven't adequately prepared for it and taken appropriate prophylactic measures may very well find themselves in a bad spot.

Subpart: Fiat Currencies Compound the Dilemma

Mistrust in fiat currencies, or currencies created and backed solely by faith in a government, both because of the modern banking system and because of the inherent nature of fiat currency, has in large part been why gold has been used as such a reliable store of value over millennia.

Fiat currencies are the world's predominant form of currency today. The US dollar or the British pound, for instance, are fiat currencies. These are currencies that are entirely controlled in their supply and creation by a national government, and are backed by nothing but faith in that government.

This has proved a mistake countless times throughout history. Zimbabwe is a classic example, where the Zimbabwean dollar, thanks to an incompetent government among other factors, experienced enormous levels of hyperinflation. At one point, inflation was estimated at almost *80 billion* percent in just a single month.The following image gives an idea of just how rapidly and absurdly a fiat currency can spiral out of control, once it reaches the point of no return.

TABLE 1
ZIMBABWE'S HYPERINFLATION

Date	Month-over-month inflation rate (%)	Year-over-year inflation rate (%)
March 2007	50.54	2,200.20
April 2007	100.70	3,713.90
May 2007	55.40	4,530.00
June 2007	86.20	7,251.10
July 2007	31.60	7,634.80
August 2007	11.80	6,592.80
September 2007	38.70	7,982.10
October 2007	135.62	14,840.65
November 2007	131.42	26,470.78
December 2007	240.06	66,212.30
January 2008	120.83	100,580.16
February 2008	125.86	164,900.29
March 2008	281.29	417,823.13
April 2008	212.54	650,599.00
May 2008	433.40	2,233,713.43
June 2008	839.30	11,268,758.90
July 2008	2,600.24	231,150,888.87
August 2008	3,190.00	9,690,000,000.00
September 2008	12,400.00	471,000,000,000.00
October 2008	690,000,000.00	3,840,000,000,000,000,000.00
14 November 2008	79,600,000,000.00	89,700,000,000,000,000,000,000.00

Lest we think this an isolated instance, Venezuela is experiencing incredibly similar hyperinflation in the present-day, right this moment. The Venezuelan Bolívar inflated over 800% in 2016, and shows no signs of stopping in 2017.

The US hasn't been immune to these crises, either. The US began its foray into fiat currency with the issuance of Continental Currency in 1775. Just three years later, Continental Currency was worth less than 20% of its original value. 13 years later, hyperinflation entirely collapsed the currency, and the US had to pass a law guaranteeing that all future currencies would be backed by gold and silver, and that no unbacked currencies could be issued by any state.

In comparison, the early history of the US dollar makes the relative volatility of bitcoin in these first 9 years look like peanuts.

Once adopted out of necessity, the gold standard became part and parcel of US currency, just as it was with most other currencies from around the world. The gold standard removed some of the need to have pure faith in US

dollars in of themselves, as it guaranteed that all paper money the US issued would be exchangeable at a fixed rate for gold upon demand.

Naturally, you still had to believe that the government would actually keep enough gold to fulfill all these demands (déjà vu and foreshadowing, anyone? Any flashbacks to fractional reserve banking yet?), but it was certainly better than nothing.

Gold, unlike fiat currencies, requires no trust and faith in a government to responsibly manage its money supply and other financial dealings in order to believe that it will retain its value well over time. This is because gold has no central authority that controls it and effectively dictates its supply and creation arbitrarily. Gold is fundamentally scarce, and only a small amount of it can be mined every year and added to the whole net supply. To date, the estimated total of all the gold ever mined in the history of humankind is only 165,000 metric tons. To put that in perspective, all that gold wouldn't even fill up 3.5 Olympic sized swimming pools.

No government, no matter how much they wanted to or needed to, could simply conjure up more gold on demand. Fiat currencies, on the other hand, can and often have been printed on demand by governments whenever they happened to be short on cash and needed a quick infusion.

This printing of more money generally leads to inflation, as the total *value* of all the money in existence rationally should stay the same, no matter how many dollars are printed. Hence, if more dollars are printed, each dollar is worth fractionally less of the total money supply.

In fact, governments *design* their currencies and monetary policies to inflate intentionally. This is why $100 US dollars in 1913 (when the government officially started tracking inflation rates) is equivalent to $2,470 dollars today, just over 100 years later.

In fact, the average inflation rate of the US dollar over that time period was about 3.22%. This seems low, but in reality means that prices *double* just every twenty years. In other words, your money becomes half as valuable if you keep it in US dollars every twenty years. Doesn't seem ultra cool to me.

Gold, on the other hand, doesn't inflate like fiat currencies do. That's because there's an intrinsically limited supply, and consequently, things tend to cost the same in gold over long periods of time. In fact, 2,000 years ago, Roman centurions were paid about 38.58 ounces of gold. In US dollars today, this comes out to about $48,350. The base salary of a captain in the US army today comes out to just about the same at $48,500.

This makes gold, in many ways, a better store of value based on fundamental principles than fiat currencies over time. You don't have to trust anyone to trust that your gold will retain its value relatively well across the sands of time.

Unfortunately, the gold standard collapsed multiple times during the 20th century and was ultimately abandoned altogether by almost every nation in the world, because governments effectively played fractional reserve banking with their gold reserves. Who could blame them? It must be irresistibly tempting, knowing that in all likelihood, the vast majority of the time, only a fraction of people will ever want to trade in their dollars for gold. Why hold all that gold when you could hold just a fraction of it and get to spend the rest with no consequences in the short term?

Inevitably, this caught up with each and every government over time. For the United States, the gold standard was suspended in the aftermath of the Great Depression. The Bretton Woods international agreement instituted in the aftermath of World War II restored the gold standard to the US dollar, but this was short lived.

Under the Bretton Woods system, numerous foreign governments held US dollars as an indirect and more convenient method of holding gold, as US dollars were supposedly directly exchangeable at a fixed rate for gold. However, by 1966, gold reserves actually held by the US were already pitifully low, with only $13.2 billion worth of gold being held by the government.

By 1971, other governments had caught on to this, and began demanding the exchange of all their US dollars for gold, as was promised to them. Naturally, the US had nowhere near enough gold to fulfill their promises, and this became a government version of the bank run, essentially.

The US chose instead to fully renege on their promised exchange rate, and announced in what was known as the Nixon shock that the US dollar would no longer be redeemable for gold, and would henceforth be backed solely by faith in the US government (very faith-inspiring, no?).

Almost every nation quickly followed suit, and since then, fiat currencies have been allowed free reign to grow as they please with no accountability whatsoever in how much a government chooses to expand their money supply.

This, thus, requires anyone holding fiat currencies to have extreme trust that their government will manage their money supply responsibly, and not make poor financial decisions that will severely devalue the currency they hold. This compounds with the trust one must hold in the banks in which one deposits their fiat currency, to create an ultimate monetary system that has multiple points of very real possible failure, as history has shown time and again.

Holding gold privately removes the need to trust either of these points of failure in the modern banking system, but comes with its own host of problems. Namely, while gold has proven to be an excellent store of value over time, it is incredibly poor for actual day to day use in the modern economy. To transact with gold is excessively cumbersome and inconvenient. No one would consider walking around with an ounce of gold on them, measuring and shaving off exact portions of gold to pay for a cup of coffee, groceries, or a bus ride. Worse, it's even more difficult and time consuming to send gold to anyone who isn't physically in the same exact location as you.

For these reasons among others, fiat currencies have traditionally been preferred for everyday use, despite their many shortcomings and associated inherent risks.

No solution to this tradeoff conundrum has heretofore been discovered, or even necessarily possible. Bitcoin, however, with the aid of recent technological advances (computers and the internet), solves all of these issues. It takes the best of both worlds, and puts it into one beautiful, elegant solution.

Subpart: Bitcoin to the Rescue

Holy long-windedness, batman! 2,700 words later, and we finally get to talking about bitcoin. I'm as relieved as you are. Remind me never to write again.

Bitcoin was designed, essentially, as a better 'digital gold'. It incorporates all of the best elements of gold — its inherent scarcity and decentralized nature — and then solves all the shortcomings of gold, in allowing it to be globally transactable in precise denominations extremely quickly.

How does it do this? In short, by emulating gold's production digitally. Gold is physically mined out of the ground. Bitcoin is also 'mined', but digitally. The production of bitcoin is controlled by code that dictates you must find a specific answer to a given problem in order to unlock new bitcoins.

In technical terms, bitcoin utilizes the same proof-of-work system that Hashcash devised in 1997. This system dictates that one must find an input that when hashed, creates an output with a specific number of preceding zeros, among a few other specific requirements.

This is where the 'crypto', incidentally, in cryptocurrency comes from. Cryptographic hash functions are fundamentally necessary for the functioning of bitcoin and other cryptocurrencies, as they are one-way functions. One-way functions work such that it is easy to calculate an output given an input, but near impossible to calculate the original input given the output. Hence, cryptographic one-way hash functions enable bitcoin's proof of work system, as it ensures that it is nigh-impossible for someone to just see the output required to unlock new bitcoins, and calculate in reverse the input that created that output.

Instead, one must essentially brute-force the solution, by trying every single possible input in order to find one that creates an output that satisfies the specified requirements.

Bitcoin is further ingeniously devised to guarantee that on average, new bitcoins are only found every 10 minutes or so. It guarantees this by ensuring that the code that dictates the new creation of bitcoin automatically increases the difficulty of the proof-of-work system in proportion to the number of computers trying to solve the problem at hand.

For instance, in the very beginning of time, it was only the creator of bitcoin who was mining for bitcoins. He used one computer to do so. For simplicity's sake, let's assume this one computer could try 1000 different values to hash a second. In a minute, it would hash 60,000 values, and in 10 minutes, 600,000 values.

The algorithm that dictates the mining of bitcoins, therefore, would ensure that on average, it would take 600,000 random tries of hashing values to find one that would fulfill the requirements of the specified output required to unlock the next block of bitcoins.

It can do this by making the problem more or less difficult, by requiring more or less zeros at the beginning of the output that solves the problem. The more zeros that are required at the beginning of the output, the more exponentially difficult the problem becomes to solve. To understand why this is, click here for a reasonably good explanation.

In this case, it would require just the right amount of leading zeros and other characters to ensure that a solution is found on average every 600,000 or so tries.

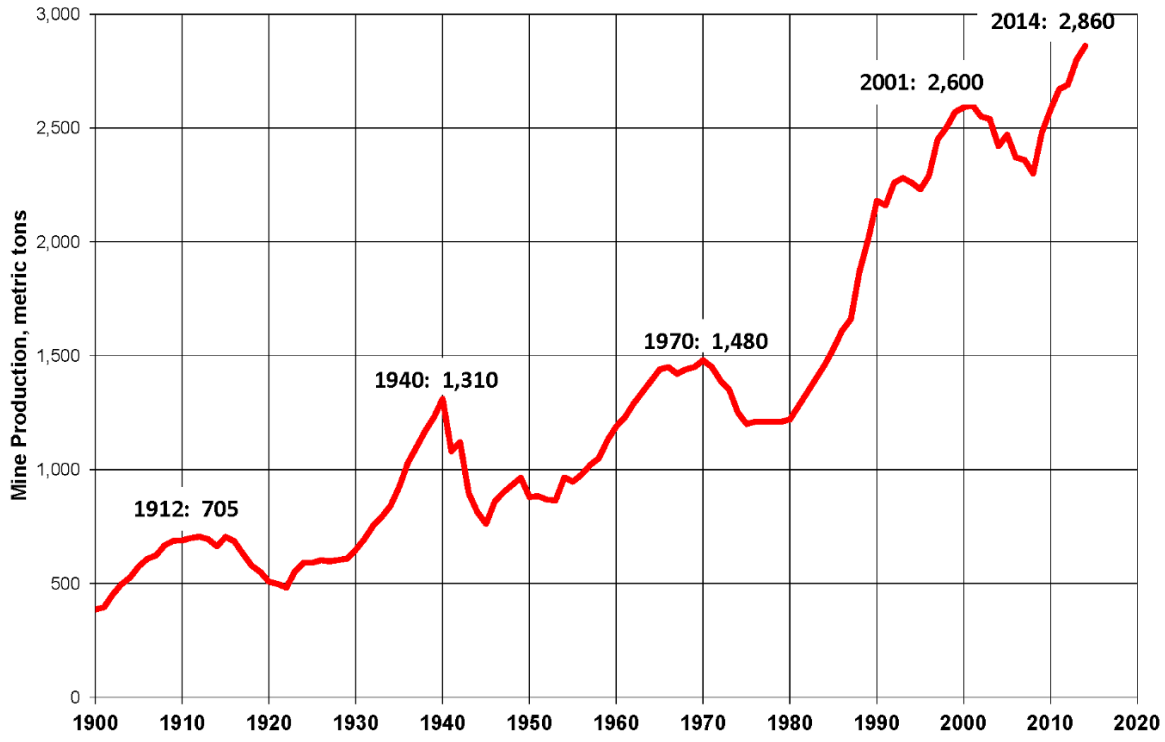
However, imagine now that a new computer joins the network, and this one too can compute 1000 hashes a second. This effectively doubles the rate at which the problem can be solved, because now on average 600,000 hashes are tried every 5 minutes, not 10.

Bitcoin's code elegantly solves this problem by ensuring that every 2,016 times new bitcoin is mined (roughly every 14 days at 10 minutes per block), the difficulty adjusts to become proportional to how much more or less hashing power is mining for bitcoin, such that on average new bitcoin continues to be found roughly every ten minutes or so.

You can see the present difficulty of mining bitcoin here. It should be evident from a half-second glance that the amount of computing power working to mine bitcoin right now is immense, and the difficulty is proportionally similarly immense. As of the time of this writing right now, there are close to 5 billion billion hashes per second being run to try to find the next block of bitcoin.

This system holds a lot of advantages even over gold's natural system of being mined out of the ground. Gold's mining is effectively random and not dictated by any perfect computer algorithm, and is consequently much more unpredictable in its output at any given moment. If a huge supply of gold is serendipitously found somewhere, it could theoretically dramatically inflate the rate at which gold enters the existing supply, and consequently cause an unanticipated decrease in the unit price of gold.

This isn't just theoretical — it's the reality of gold production. This graph illustrates vividly the fact that gold production has been dramatically increasing over time, and is today over four times higher than just a hundred years ago.



In fact, more than half of all the gold that has ever been mined in the history of humankind has been mined in just the past 50 years. The difficulty of mining gold doesn't proportionally increase with the number of people mining it, or with technological innovations that make it significantly easier to locate and mine gold over time.

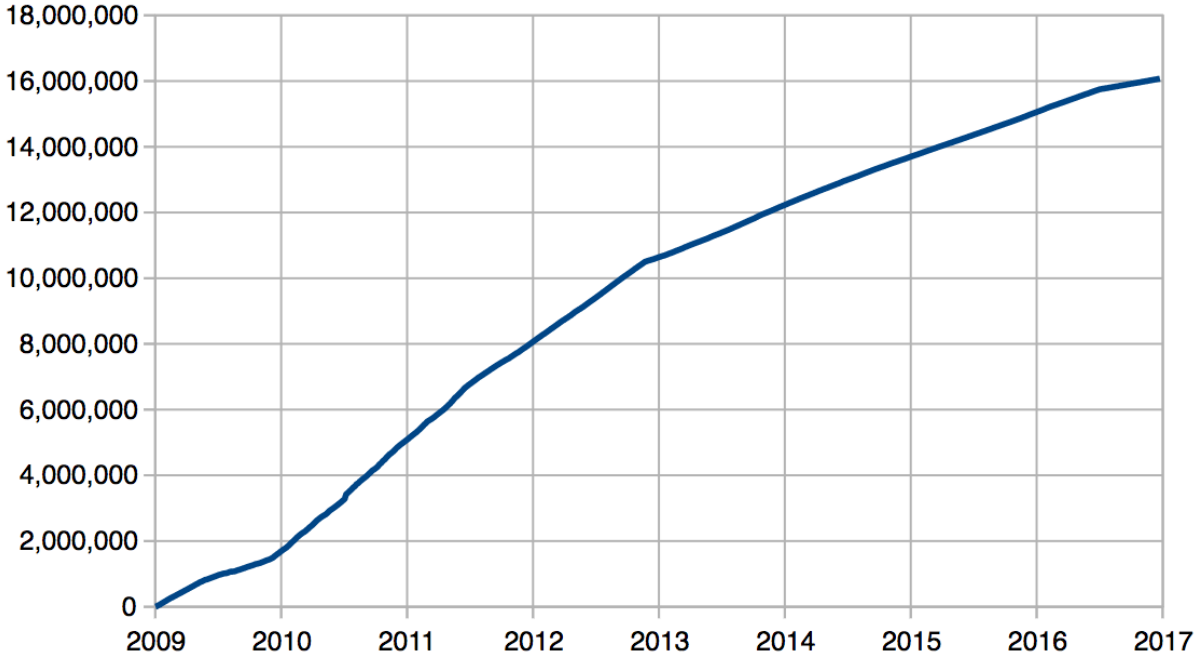
Bitcoin, on the other hand, will always be mined on a carefully regulated schedule, because it can perfectly adapt no matter how many people begin to mine it or how technologically advanced bitcoin mining hardware becomes.

In fact, it's already known for certain that there will only ever be a total of 21 million bitcoins in the world.

This is because the amount of bitcoin that is mined every time a hash problem is solved and a new block is created halves every 210,000 blocks, or roughly every 4 years.

The initial reward per block used to be 50 bitcoins back in 2009. After about four years, this dropped to 25 bitcoins in late 2012. The last halving occurred in July 2016, and dropped the reward per block mined to 12.5. In 2020, this should go down to 6.25, in 2024, 3.125, and so forth, all the way until the reward drops to essentially zero.

When all is said and done, there will hence be 21 million bitcoins. Exactly that, no more, no less. Elegant, no? This eliminates yet another risk with extant currencies, gold included: there are absolutely no surprises when it comes to knowing the present and future supply of bitcoin. A million bitcoin will never be found randomly in California one day and incite a digital gold rush.



The total supply of bitcoin over time. Look how straight the line is getting over time! (Note halvings here too)

On top of this, bitcoin is trivially divisible to any arbitrary degree. Presently, the smallest unit of bitcoin is known as a satoshi, and is one hundred millionth of a single bitcoin (0.00000001 bitcoins = 1 satoshi).

This means that unlike gold, bitcoin is perfectly suited to not only being an inflation-proof store of value, but also a day-to-day transactable currency as well, as it is easily divisible to any arbitrary amount. You can buy a cup of coffee with it just as easily as you can buy a car.

Moreover, bitcoin can be sent incredibly quickly and remotely over the internet to anyone anywhere in the world. This is because when bitcoin is mined, the miners are actually providing a service in powering the bitcoin network.

What happens when a miner mines bitcoin is actually that they add a 'block' to what is known as the 'blockchain'. The blockchain is a ledger that contains a record of every transaction ever made with bitcoins since its inception. When someone decides to mine bitcoin, they must download the entire blockchain as it presently stands.

Then, when they successfully find a solution to the next hash problem and mine a block of bitcoins, something magical happens. They get to add the block they just mined to the end of the existing blockchain — and with it, they include every transaction that was initiated on the bitcoin network since the last block was mined. They then propagate this block they just created to the rest of the network of bitcoin miners, who all then update their own blockchains with this new block, and begin working on solving the next hash problem.

As a reward for providing this valuable service, miners are allowed to add a single transaction to the beginning of the block they mined, called the 'coinbase transaction'. This transaction contains the brand new bitcoin that was created when they mined the block, and allows the miner to claim this bitcoin for themselves.

At this point, a particularly shrewd reader might become concerned with the fact that the reward for mining a new block of bitcoin gradually shrinks to zero. Won't this cause miners to stop mining bitcoin, and consequently to stop providing the invaluable service that allows the bitcoin network to function and for transactions to be sent?

The answer is no, because miners are not solely rewarded by the new bitcoin that is generated each time they mine a block. Users may also send a transaction fee along with their transactions, which is paid out to any miner who decides to include their transaction in a block they mine. Over time, as the bitcoin network becomes used for more

and more transactions, it is expected that transaction fees will be more than sufficient for incentivizing enough miners to continue mining blocks to keep the bitcoin network safe, secure, and robust.

It's important that enough miners keep trying to mine blocks because this is another valuable service miners provide the network. Bitcoin, like gold, is powerful as a store of value because it is decentralized and *trustless*. There is no one central authority who holds all the power over bitcoin, just like no central authority holds power over gold.

No one person or government can decide to conjure up more bitcoin on demand, or to take it away. The only way the rules that govern bitcoin can be changed is if the software bitcoin miners run to mine bitcoin is changed.

Technically, any bitcoin miner could decide to change the software they run to mine bitcoin at any time. However, this still doesn't have any impact on changing bitcoin itself. What it *would* do is cause a 'hard fork', or a divergence in the block chain.

This occurs because any block that the rogue miner who changed their software mines won't be accepted by all the other miners who are still running the original software. Consequently, all the other miners will begin mining different blocks, and adding those to their blockchain. This leads to a fork in the road, essentially, where two completely different blockchains are formed — one by the rogue miner, and one by all the other miners.

Everything up to the point of the software change remains the same in both blockchains, but after that change, the blockchains diverge. Once diverged, they can never be reconciled and remerged.

This isn't a concern, however, because the bitcoin network runs on consensus, and accepts whichever blockchain is the longest. In practice, this means that whichever blockchain has the most computing power behind it is effectively guaranteed to win, as they'll be able to calculate the solutions to the hash problems and find new blocks faster than their less powerful competitors.

This does mean that in theory, bitcoin is vulnerable to what's known as a 51% attack — an attack in which if a single entity was able to gain control of at least 51% of the total hashing power being directed at bitcoin mining, it could outpace a legitimate blockchain and temporarily take control of the network.

This is an extraordinarily difficult feat to accomplish, however, as the more people there are mining bitcoin, the harder it is to take over the network. At the current worldwide mining rate of almost 5 billion gigahashes a second, it would be extraordinarily difficult for even the most powerful organizations in the world (e.g., large-scale governments) to mount a successful 51% attack. It would be enormously costly, and quite possibly more financially detrimental to the attacker than to the network.

Indeed, the only thing a 51% attacker could really accomplish is destroying collective faith in bitcoin. They couldn't somehow steal and gain all the value of bitcoins for itself. The attacker wouldn't be able to generate new bitcoins on demand arbitrarily, and would still have to mine for them. They also would have no control over taking bitcoins created in the past that didn't belong to them. The only thing they could do, really, is repeatedly spend bitcoin they already owned again and again, but even this is limited in its value, because 'honest' miner nodes would never accept these fraudulent payments.

Hence, no rationally self-interested bitcoin miner would ever try to mount a 51% attack, as in all likelihood, they would lose massive amounts of money doing so and gain almost nothing from the effort. The only reason someone would want to conduct a 51% attack is to attempt to destroy faith in bitcoin — large governments, for instance, who might one day feel that their fiat currencies that presently provide them great value to them are becoming threatened by bitcoin. However, the likelihood even of these enormous entities to successfully conduct a 51% attack is already becoming vanishingly small, as mining power increases.

Thus, bitcoin has perfectly utilized recent technological advances to create something heretofore impossible: an extremely safe, reliable, decentralized, and globally transactable digital and better version of gold, and possibly of all types of extant currency at large.

The advantages don't stop there, however. Bitcoin is also 'pseudonymous', meaning that while all transactions ever conducted on the network are public and known by all as everything is recorded in the blockchain, unless someone knows who owns the bitcoins that are being used in these transactions, there is no way to trace those bitcoins and transactions back to a given person or entity.

This serves a dual purpose of both allowing extreme transparency when desired in making transactions, and also allowing a lot of anonymity when desired. If one wants to ensure that they have perfect undeniable proof of their transactions, all they have to do is prove they own certain bitcoins, and then any and all transactions conducted with those bitcoins are undeniably theirs and most certainly occurred.

If one wants, rather, to keep the movement of their money less overt, one simply needs to ensure that the bitcoins they own are never tied to their identities, and that their transactions on the network are obfuscated. This can be accomplished with a variety of methods, such as using a tumbler, which allows one to send bitcoins to an intermediary service that will mix these bitcoins with bitcoins from numerous other sources, and then send bitcoins forward to the intended destination from sources entirely unrelated to the sender's original bitcoins.

To clarify this a bit more, bitcoins are stored at what are known as 'addresses'. Think of this as an email address or a mailing address. These addresses allow for the storage, sending, and receiving of bitcoin. The blockchain ledger contains a complete record of the movement of bitcoins from one address to another.

A tumbler allows someone who say, wants to move bitcoins from address 10 to address 100, to instead move their bitcoins from address 10 to a totally random address, say 57. In some other transaction, the tumbler has accepted bitcoins from someone entirely unrelated at say, address 20, who wanted to send the coins ultimately to 200 and sent these instead to another completely random address 42. It then sends the coins stored at address 42 from sender 2 to the address sender 1 originally desired, 100, and sends the coins stored at address 57 from sender 1 to the address sender 2 desired, 200.

This is highly simplified, but effectively how a tumbler works, albeit at much larger scale, and with many more senders and receivers of all sorts of varying amounts.

This ability to transact more anonymously in a digital, global fashion than ever before has indeed opened the gateway to some of bitcoin's more infamous use cases. Much illicit activity has been enabled by this pseudonymity of bitcoin, including the sale of drugs and other illegal goods online. A more recent development has also been ransomware, whereby malware can now cut straight to the chase and lock up your computer and demand straight up money in the form of bitcoin in exchange for the release of your computer's data.

These developments have been enabled not only by bitcoin's pseudonymity, but also the irrevocability of transactions. Unlike current forms of digital payment, such as credit cards and bank transfers, bitcoin transactions are irreversible and do not involve any middleman who can mediate between disputes.

This has its disadvantages, but also its advantages, and was indeed one of the primary benefits the creator of bitcoin (a pseudonymous as-of-yet unidentified figure himself, Satoshi Nakamoto) outlined in the bitcoin white paper. In his own words:

> 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 nonreversible 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.

As Satoshi notes, bitcoin's irreversible, trustless nature removes the need for any middlemen to mediate and broker the process of payments from one person to another. Middlemen (e.g. banks and credit card networks) inherently introduce overhead costs and inefficiency into the system, which make transactions — and micropayments in particular — more costly than would otherwise be the case.

Fraud is also inherently eliminated, as any transaction propagated and confirmed by the bitcoin network by 6 or more blocks is generally accepted to be impossible to ever revoke.

Trustlessness in this sense is a huge component and advantage of bitcoin and cryptocurrency at large. Another ground-breaking innovation the blockchain introduces is the concept of a smart contract, or a contract that similarly requires no trust or middleman to mediate, but is rather contractually executed in a deterministic fashion through code run on the blockchain.

Traditionally, with a legal contract, two parties agree to certain terms with the understanding that if one party reneges, the other party can seek legal recourse with the governmental justice system. Lawsuits, however, can often be inordinately expensive, and in many cases the outcome is far from certain. A good or bad lawyer can make or break a case, and one is also at the mercy of a judge and/or jury and their subjective, possibly mercurial whims. Not the most efficient or foolproof system.

A contract written with and enforced by code, however, removes the need to trust a third party arbitrator (such as a court system), in much the same way that transactions enforced by bitcoin's code remove the need to trust a third party financial institution. The code is written in such a way that clearly specifies the conditions of the contract, and will automatically enforce these conditions.

For instance, if two parties decide to make a bet on Donald Trump winning the election, historically, this could only be done by either word of honor or by some ad hoc legal contract. For a say, small $100 bet, it would be absolutely a non-starter to pursue legal action in the case that one of the parties decided to renege on the deal in the aftermath of the election. Normally, the reneged-upon party would simply be left in the dust without recourse.

With the advent of smart contracts made possible by the blockchain, however, this is (soon-to-be) a thing of the past. One can create a simple smart contract at effectively almost no cost that specifies in code that each party will send it $100 in bitcoin, and that upon the completion of the election process, it will either send all $200 to the party that bet on Donald Trump winning the election, or send the $200 to the party that bet on him losing the election. No ifs, ands, or buts. The code is clear, objective, and deterministic. Either the contract is fulfilled in one direction, or it is fulfilled in the other. No need to trust the other party in the bet at all, much less a third party to mediate.

Ethereum, as will be noted later (hopefully in another article because my god I never want to write again), takes this concept to the next level and runs with it.

One further benefit to bitcoin is that it is truly yours to own, and you can keep it yourself, without the need for a bank or any other intermediary, and use it just as easily as you might a credit card. This ensures that you won't fall victim to a banking system collapse brought on by fractional reserve banking or irresponsible government and financial institution fiscal policies in general. It also ensures, however, that no one can take your money from you even on an individual basis, global financial apocalypse aside.

This, like systemic banking failures, is not something most people generally have to worry about 99% of the time. However, in the 1% of cases where this *does* become an issue, it becomes a very serious issue. Refugees and other victims of persecution and oppression are clear examples of this.

As a refugee, generally, if you hope to escape with your money, you have to carry it in physical form on you, either in gold or in paper currency. This is limiting for a few reasons: one, you can only take so much as you can carry or convert to physical form, and two, physical currencies are exceedingly simple to detect and confiscate.

Again, while this all seems incredibly far-fetched today for most people (but not all, as the present day European migrant crisis has made abundantly clear), it happens much more often than one might expect. A little remembered fact is that the United States itself once outlawed the possession of gold, back in 1933 with Executive Order 6102, and forced all its citizens to relinquish all gold to the United States at a fixed price of $20.67 per troy ounce.

Immediately thereafter, the US Treasury revalued all their gold at $35 per troy ounce for foreign transactions, and in the process reaped an enormous profit at the expense of all the citizens that were forced to give up their gold at fire sale prices.

It sounds incredible, but this is real life. The government threatened to fine anyone caught possessing gold in violation of this order $10,000 ($185,000 today) and throw them in jail for up to ten years. A famous case involved one Frederick Barber Campbell, who had on deposit at Chase Bank over 5,000 ounces of gold (worth over $6 million today), and attempted to withdraw the gold that he rightfully owned. Chase refused to allow him to do so, so he decided to sue Chase for depriving him of his assets.

In response to his lawsuit (this case demonstrates the value of basically everything about bitcoin, from the ability to store your own money to the ability to not rely on the legal system for recourse), Campbell was counterattacked and indicted by a federal prosecutor, and had to defend *himself* in court for not giving up his gold.

Ultimately, while Campbell didn't end up going to jail, the government did decide to seize all his gold, and confiscated all $6 million worth of gold from him.

It took a full 40 years, or until 1974, before Gerald Ford signed a bill making it once again legal for private individuals and corporations to own gold within the United States.

This underscores the oft mercurial whims of governments, even well-regarded ones like that of the United States, that most citizens heretofore have been subject to without relief or alternative. Most of the time, things run well enough that we all get by without having to think about this fact too much. Sometimes, however, things do go really, really wrong.

Bitcoin fundamentally changes this equation. Unlike even gold, bitcoin is nigh impossible, when stored correctly, for anyone to confiscate without consent. The addresses at which bitcoin values are stored are protected by 'private keys', which can be thought of as a password or a key to a lockbox. Without this private key, it is generally impossible to steal the bitcoins held at the public address to which the private key corresponds. So long as you keep this private key secure, your bitcoins are secure.

With things like brain wallets possible, this means that even in the worst case scenario, you can literally store your bitcoins in your brain and nowhere else, and thereby easily prevent their confiscation. Just yet another fundamental innovation in the evolution of currency that bitcoin has made possible — its fully intangible nature is actually an asset.

The intangibility of bitcoin, however, does seem to hang some people up. It's sometimes difficult to immediately conceive of how bitcoins could possibly hold value, as these people contend, when they are intrinsically worthless. They are nothing but a concept, backed up by some computer code. Gold is a physical, tangible object that you can hold in your hand. It has real uses in industry and as jewelry that lend it value. Even paper money can be used for kindling or toilet paper if the need necessitates.

Bitcoin, on the other hand, is fully intangible. It is just a concept backed by code, no more, no less. It can't be used for anything functional besides being transferred in concept to other people as a store of value. How could something like this possibly hold value like other existing currencies?

It's a good question, and one that underscores just how interesting the concept of money really is, and how rarely we actually think critically about it.

Sure, let's say that you can't compare bitcoin to gold and say it's better because gold has tangible, real-world utility and bitcoin doesn't.

What is the value of that real-world utility? Only about 12% of gold purchased every year is actually used for industrial and medical purposes. If this is truly where gold's value is derived from, gold would be worth dramatically less than it actually is.

To the other point, gold's coveted status in jewelry is merely a derivative property of its perceived value, which leads to its designation as a status symbol. Without that underlying perceived value, it would command far less value in jewelry. Consequently, the question still remains about the gap between the industrial and medical value of gold and the actual value of gold as determined by the market. Where does the value in that gap come from?

This is even more true of paper currency. Yes, you can utilize and reuse the paper for all the intrinsic value paper has. But what is that intrinsic value of paper? This is easy to answer, because we can just see how much the government pays to make paper money. $1 and $2 bills cost less than 5 cents to make on the low end of the spectrum, while $100 bills cost 12.3 cents on the high end.

Even the $1 bill, which seems to be the best deal if one is valuing the worth of one's currency based on its intrinsic 'tangible' value, has only ~5 cents worth of actual paper value behind it, or <5% of its actual denominated value. Where does the rest of that 95 cents of value come from?

It turns out these gaps in value between the worth of the 'tangible' thing itself and the actual value of the currency as it stands on the market today is just as much conjured up out of thin air as a mere concept as bitcoin's perceived value is.

This 'intangible' worth that we ascribe to currency, which accounts for the vast majority of the value of all currencies, not just bitcoin, is ultimately what makes money work. Yuval Noah Harari captures this fact very well in Sapiens, where he lays out the case that the value of a given form of money is essentially an indication of trust in that form of money. It is our shared collective trust and belief in a currency that gives it value, not its intrinsic tangible utility or anything else.

Gold holds its value well because we trust that we will all collectively continue to trust it as a store of value forever, predominantly due to its scarcity and lack of centralized control. Fiat currencies hold their value well when they do because people trust that everyone else trusts the currency as well, and that it is deserving of trust. The moment that collective trust collapses, so too does the currency, no matter what its intrinsic 'tangible' value.

This is why no fiat currency has ever stood the test of time over a long enough timescale, whereas gold has to date always stood the test of time and retained its value well. Collective trust for gold has never collapsed because of its inherent scarcity and immunity to the vicissitudes fiat currencies must endure at the hands of capricious centralized governing powers, whereas collective trust in every historical fiat currency has inevitably failed to date, and collective trust in many present-day fiat currencies continues to fail as we speak.

With this in mind, bitcoin can arguably be seen as the *purest* form of money, as its value is entirely predicated on trust in it, and nothing else. It can arguably also be seen as the most *trustworthy* of currencies, as it was bespoke made by intentional design to exhibit all the best elements of historically trustworthy currencies (e.g. gold), as well as to introduce for the first time a number of characteristics that make it even better than all previously extant currencies.

If people have trusted gold to date as a store of value because of its inherent scarcity and resistance to centralized control and price/supply manipulation, bitcoin does all that and more, and does it all better. Gold's scarcity, as

illustrated above, is anything but constant, and we've more than doubled our world's supply of gold in just the last 50 years. Bitcoin, on the other hand, has a precisely and publicly known proliferation schedule, and will approach the limit of its supply in just a few more decades.

As a thought exercise, imagine a new fledgling nation called the United States came into formation and decided to create their own fiat currency today. At the same time, bitcoin is introduced as a currency.

Which would you trust? My personal bet would be absolutely, wholly, and unequivocally bitcoin. With the new US currency, I would be effectively required to trust that the US government would act without fail over the entire course of its indefinite existence to practice perfect fiscally responsible habits and not screw up its economy in any dramatic ways. I would also be aware that even under perfect circumstances, the currency would be fundamentally designed to inflate, and consequently my money would continue to lose value over time if I decided to hold and save it.

Furthermore, I would be forced to use an intermediary financial institution such as a bank to hold my money for me, and thereby expose myself to yet another layer of required trust and accompanying risk. I would also be aware that these institutions would almost certainly practice fractional reserve banking to the maximum extent they could get away with it, such that they would be extremely fragile to small perturbations and vulnerable to things like bank runs and runaway systemic banking collapses.

On the other hand, with bitcoin, I wouldn't have to trust anyone at all. I would know for certain that my coins wouldn't lose their value due to inflation as a consequence of their designed and indelible scarcity. I would also know that as I stored my coins myself, no one else, not even a bank, could actually go and spend 90% of my money, and fail to give it back to me in the event of a bank run. Furthermore, no one could forcibly confiscate my money under any circumstances, as I could always store it in such a way that it could never be retrieved except with my consent. No one would even necessarily be able to know how much money I held, unless I chose to make that information public.

Remember: just 13 years after its inception, the US currency had already suffered fatal runaway inflation and collapsed. Bitcoin, on the other hand, is worth more than ever just 9 years after its inception, and currently boasts a market cap of over $40 billion. Which would you trust?

The other common argument against bitcoin is that it is useless for any real world functions right now besides ransomware and illegal activities, and is therefore worthless because it has no good use cases.

This is a fundamentally flawed argument that can be lobbied against absolutely any new technology or invention, and fails to take into account the natural process of growth and gradual adoption over time. The exact same argument was used against the internet in its early days, and I find this article from Newsweek, published in 1995, particularly illuminating in this regard.

> After two decades online, I'm perplexed. It's not that I haven't had a gas of a good time on the Internet. I've met great people and even caught a hacker or two. But today, I'm uneasy about this most trendy and oversold community. Visionaries see a future of telecommuting workers, interactive libraries and multimedia classrooms. They speak of electronic town meetings and virtual communities. Commerce and business will shift from offices and malls to networks and modems. And the freedom of digital networks will make government more democratic.
>
> Baloney. Do our computer pundits lack all common sense? The truth in no online database will replace your daily newspaper, no CD-ROM can take the place of a competent teacher and no computer network will change the way government works.

What's striking in this is that while everything he said at the time was true, and certainly none of those things were particularly possible back in 1995, it all came to pass eventually. Today, remote workers are a huge part of the global workforce. Online education is booming. Amazon is taking over all of commerce and is larger than any retail store in the world. Print newspapers and magazines are dying left and right, replaced by a proliferation of online news.

The same growth trajectory is how I see bitcoin, cryptocurrency, and blockchain technology at large playing out. If all goes well — and there's no guarantee it might, everything indeed might fail and all our hopes and dreams might gang aft agley — there's no reason at all that bitcoin can't one day surpass even our wildest imaginations today, just like the internet did before it, and fundamentally rewrite the script for how we interact with money and the world as a whole.

Yes, today, it is far from this goal, but even now, we make progress in pushing forward the utility of bitcoin in every day pragmatic life. Already, it has proved indispensable to myself and hundreds of thousands of people around the world. I pay many of my employees today in bitcoin, even, because several of them live in Eastern Europe where they're subject to draconian capital controls.

Were I to send them a wire (as I used to), their banks demand a mountain of documentation detailing every last dollar and hold their money for upwards of half a month before ultimately releasing it to them. Naturally, this is a pain in the ass and highly inefficient, time consuming, and resource intensive for all of us. Bitcoin easily sidesteps all of these issues.

Bitcoin is also dramatically cheaper to use than almost any other form of international money transfer today. Already, for this use case alone, it proves its worth over current dominant international money transfer solutions, such as Western Union. I can transfer money to anyone in the world, in any amount, and have them receive it without moving a finger in just a few minutes. For this privilege, I have to pay just a few cents, no matter how much I'm sending, instead of a huge proportional percentage, with hefty minimum fees and surcharges.

It's also extremely convenient and valuable for a merchant to use, and we had great success implementing it for a trial run at my company Sprayable back in the day. In the past, we've suffered from rampant fraud after our site was targeted on a carding forum (a place where people buy and sell and use stolen credit cards). When we were paid in bitcoin, however, these concerns were completely eliminated, as fraud is an impossibility on the bitcoin network with enough confirmations.

This is only the beginning. You don't expect a horse to become a world champion racer straight from the womb. It takes time, training, and a fair bit of luck. The same is true of bitcoin and blockchain technology. But just because a horse may not be a world champion just quite yet, it doesn't mean you shouldn't bet on that horse in the long run. If you see potential in that horse, and are willing to wait it out for the long run, go ahead, bet on that horse. One day, it might just take over the world, and if it does, you might just win big.

Part II: Investment Philosophy

Okay — now that you hopefully have a good grasp of what cryptocurrency is and why it's interesting, we can move on to dipping your fingers in getting some.

We can all be honest — the reason the vast majority of you are reading this is probably because you've heard a lot about just how much money people have made investing in cryptocurrency. Many, if not all of you, are wondering how you, too, can get on the gravy train and start making millions.

This isn't necessarily wrong, or inaccurate. This is the reason I first started paying attention to bitcoin. Countless people *have* made shocking amounts of money investing in cryptocurrency. I've personally made over $400,000 in less than two years. In fact, bitcoin has already proven to be the best investment in all of recorded history by a shocking margin for those who got in at its most early stages.

Here's a story about a completely random Norwegian student who bought 5000 bitcoins for $27 back in 2009. Today, with a single bitcoin pushing past $2700, those 5000 bitcoins are worth over $13.5 million. That's a gain of over 500,000X. No other investment in recorded history that I've been able to discover has ever come close to touching these sorts of gains.

Even the Dutch tulip bubble, which is classically regarded as one of the first instances of massive speculative market mania, saw increases only on the magnitude of 10–100X — not even remotely close to 100,000X+. And even the most successful of extremely risky angel investments in companies, such as Peter Thiel's initial $500,000 seed investment in Facebook, see returns on the scale of 10,000X or so or less — Thiel's $500,000 investment, had

he held it all the way to the present day, would be worth $6.8 billion, or approximately a ~13,500X gain. More incredible than just about anything else, certainly, but still nowhere even near Bitcoin's meteoric rise in price.

What's also striking is that traditionally, these sorts of 'angel or seed' investments in new technologies have been closed off to all but an incredibly well connected inner circle of elite high net-worth individuals and institutions. Peter Thiel, for instance, was only approached to become Facebook's first outside investor because he was already incredibly well known within Silicon Valley for having founded and sold PayPal for over a billion dollars. In contrast, with bitcoin, a random student in Norway was able to invest just $27 and make millions.

That said, just as with everything, there's survivorship bias here. What you don't hear about are the profusion of people who lost their entire fortunes investing in cryptocurrency. While there are a few ways you can beat all the odds and come out vastly ahead in cryptocurrency, there are infinitely more ways you can lose everything you put into it and end up in a much worse place than where you started.

Here, I'll try to cover the most common 'mistakes' people have made. Do keep in mind that this is all entirely my own opinion. Please come to your own conclusions here.

The most common mistake people seem to make is investing solely based on the price alone and its short term historical trajectory, and nothing else. The second mistake is investing in assets that they don't actually understand or believe in long term, are not planning to hold for at least 5 years, and will be tempted to sell if the price begins to fall in the short term. The third mistake is believing that they've already missed the boat on the most established and successful cryptocurrencies, like bitcoin and ethereum, and that consequently they should invest in much less established, much more speculative 'altcoins' to achieve truly outsized gains, for no truly good reason besides the fact that the price/market cap for the altcoin is a lot lower than bitcoin's, and seems like it has more room to grow. The fourth mistake is day trading, and trying to capitalize on short term market movements. I'll address each of these in turn, and why I believe them to be mistakes.

On the first mistake — I made this mistake myself when I first got into cryptocurrency. I first heard about bitcoin from a friend who was raving that we should all get into it just around the time the price of a single bitcoin reached $100. He had gotten in at $30, and was extremely pleased with his gains.

At the time, it was relatively big news that bitcoin had reached $100. I remember thinking to myself that it was clearly too late to get in, and promptly forgot all about bitcoin.

The next time I heard about bitcoin was in the fall of 2013, when it began its last truly meteoric price rise from $100 all the way up to $1200. This time around, I distinctly remembered thinking I'd missed the boat back when the price was just $100, and kicked myself for being totally wrong. I resolved to not make the same mistake again, and tried to get in before I missed out again.

I ended up wiring several thousand dollars to an incredibly sketchy Russian exchange, BTC-E.com, to purchase my first few bitcoins at around $1000 apiece. Before I knew it, I was addicted to constantly checking the price, and spent a full 48 hours doing nothing at the height of the November 2013 bubble doing nothing but refreshing BTC-E.com and seeing how my investments were doing.

I ended up making another big mistake here too, and figured that bitcoin had already gone up way too much, and that my best bet was to invest in some smaller altcoins as well. I made this decision after seeing litecoin (LTC) skyrocket from $4 to $40 in just a few days. The buzz at the time was that litecoin would be to silver what bitcoin was to gold. The price seemed incredibly low compared to bitcoin, and this made a superficial sort of sense (meaning, no sense at all), so I decided to jump in. For good measure, I also decided to jump into a few of the other most popular altcoins of the time — peercoin (PPC) and namecoin (NMC).

The 2013 cryptocurrency bubble burst just a few days later, brought on by the collapse of Mt Gox, the largest bitcoin trading exchange at the time. It was revealed that Mt Gox had either been hacked or embezzled from, and no longer had any funds left to honor customer withdrawals. As a result, anyone who had decided to keep their bitcoins in Mt Gox at the time instead of withdrawing them to their own wallets ended up losing all their money. How much the price of bitcoin rises doesn't mean anything if you lose all your bitcoins, unfortunately.

The price of bitcoin cratered about 80%, falling all the way to about $200, before stabilizing at that price for much of 2014 and 2015. Litecoin, on the other hand, fell from over $45 to about $1, and consequently lost over 97.5% of its value. PPC and NMC suffered so badly that I didn't even bother to calculate how much I had lost, because it was basically everything.

This is when I first saw the light, and realized that investing in altcoins that I didn't really believe in, and that didn't really have any truly compelling reasons they would ever overtake bitcoin or deserve any level of market share, was an incredibly foolish move. It was certainly true that these altcoins *did* often gain on bitcoin and appreciated far more rapidly in many cases while the bubble held strong, but the moment it began to collapse, the altcoins were the first to go, and often fell all the way to zero.

As a general rule, what goes up can come down, and what goes up particularly quickly is privy to come down just as quickly. This is not to say that things *will* come down if they go up, but merely that they can, and certainly have before. This is particularly noteworthy today, with ethereum having seen some truly wild gains this year, all the way up from $7 back in December of last year to over $350 presently — a gain of 50X in just about half a year. Again, this isn't to say ethereum *will* fall, but merely that it very well might, for any host of reasons, and it's very important to keep this fact in mind and not overextend yourself with investments you perceive to be less volatile than they truly are. I'll get back to this more later.

What I ended up learning was something the smartest people in the investment world had learned a long time ago. Benjamin Graham, the mentor of Warren Buffett, who became the richest man in the world by practicing the principle of value investing, has a pretty wonderful analogy that I think is worth repeating here. You should buy your stocks (or any investment, generally) like you buy your groceries — not like you buy your perfume.

What he means by that is that for some reason, people tend to buy stocks when they're going up in price, and sell them when they're going down. At face value, this makes no sense. We wouldn't buy a watermelon when it was $10, and sell it when it was $2. With groceries, it makes intrinsic sense to us to buy watermelons at $2, not $10, but seemingly not so with our investments.

The short term price movements of a stock shouldn't concern a long term value investor in the slightest, as a value investor doesn't care about what the market has valued the price of a stock at, but rather only about the intrinsic value of the business behind the stock, and its future potential value. Only after coming to a conclusion about the actual value of a company and its future potential value, should an investor then look to what price the market has assigned a stock, in ascertaining whether or not a stock is a good purchase.

In the case of a watermelon, what we intuitively grasp is that there is some fundamental, intrinsic value to the watermelon, and a 'fair' price for it. We have a general understanding of what this price should be, and are more than happy to buy watermelons when they are on discount relative to their fair price, and are reticent to do so when they are being sold at a premium to their fair price.

If we decide that a watermelon's fair intrinsic value is $6, then we'd be happy to buy watermelons all day long at $2, and reticent to do so at $10.

With investments, it's the same deal. If we decide that Company X is presently worth $100,000 dollars, and that it has strong growth potential in the future, and the market is presently valuing Company X at $50,000, that would probably be a good buy.

On the other hand, if we decide Company X is worth $100,000, and has ambiguous future potential, and the market is presently valuing it at $200,000, it might not be such a good buy.

In a third case, if we decide Company X is worth $100,000 today, and has extremely strong growth potential, and the market is valuing it at $100,000 today, it might still be a good buy to hold and capitalize on that future potential.

In all of these cases, however, a value investor first and foremost must decide, with rigorous analysis and thorough examination, what they believe the fair value of an investment to be, and what degree of future potential it has. Only from there do they then examine what value the market has assigned the investment, in order to ascertain whether or not the investment is a wise one likely to yield good returns. Under no circumstances should one ever

buy into a stock without knowing much, or anything at all about the stock, save for the general market sentiment or hype surrounding it, and its short term price movements. Buying a stock merely because it has seen great gains in the past, without any understanding of why it saw those gains and what gains it might expect to see in the future based on fundamental analysis of the stock, is an inordinately risky and foundationally bereft strategy.

If you're interested in learning more about value investing at large, I'd highly recommend The Intelligent Investor, by Benjamin Graham, who again was Warren Buffett's personal mentor and a professor of economics at Columbia University. He pioneered a lot of the foundational concepts around value investing, and can give you much better and more nuanced advice than I ever could.

All of this said, while these principles can and should be kept in mind at large for just about any investment, cryptocurrencies are dramatically different from stocks, bonds, or any other sort of traditional investment vehicle. They're also so early stage and so volatile that it's a near-certainty that a value investor like Benjamin Graham wouldn't even dream of labeling such opportunities as investments, rather than speculations (at best, they would be labeled growth investments, but I'm working with the Buffett philosophy that there is no difference between 'value' and 'growth' investing, and that good value investing appropriately takes into account growth).

Investments, under this distinction, would be clarified as things that could generally be safely assured not to suffer from dramatic, catastrophic losses in the absence of dramatic, catastrophic situations. Coca-Cola and Walmart might be considered investments. They've been around for well over a century and a half century respectively, are massive, mature companies with a healthy track record of stable, non-volatile growth, and show no general signs of turmoil that might portend a sudden collapse in value.

Speculations, on the other hand, are like the Wild West of opportunities. They're extremely high risk, extremely volatile, and could on one hand multiply one's principal manyfold, and on the other, dissipate it all into thin air. A seed 'investment' in Facebook, for instance, could be considered a speculation. In the vast majority of cases, such an investment is likely to fail outright and lose all of the money invested. In a few instances, however, that investment just might succeed, and return tens, hundreds, or even thousands of times the principal invested.

It's important to note that the mere fact that something *is* speculative does not necessarily mean it can't be a good investment, or that it is merely akin to blind gambling, dependent solely on the luck of the draw. Poker might be a suitable analogy. Poker can be played well or poorly, and skill and calculation lends an incredible degree of advantage to a player's odds of success. However, the game still fundamentally deals with an immense degree of unavoidable variation and unknowns, and even the best poker player is guaranteed to lose many of their games, even if they play each one 'perfectly'. The goal, simply, is to win more than you lose, and with the right amount of skill, knowledge, and preparation, this is a possible feat in poker.

The same might be said of speculative investments such as those in cryptocurrency. You can and absolutely should do your part to learn as much as possible about this field, and come to your own personal conclusions on its current and future potential value. However, no matter how much research you do and how many calculations you make, there will always be a fundamental and inextricable degree of pure luck involved in determining the ultimate outcome of your speculation. Any number of future events could tip the scales for or against cryptocurrency, or more specifically, any one cryptocurrency, and a number of these will be 'black swan' events that are fundamentally unpredictable in their nature and timing, but in aggregate whole, almost certain to occur.

Just because there is this element of luck, however, does not mean that you necessarily shouldn't play the odds, if you so believe with very good reason that those odds are in your favor. What you *do* have to make sure of, however, is that you have such good reason to believe that those odds are in your favor, and that you don't put up more than you can afford to lose, given the odds. The key takeaway and lesson to be learned, again, is to invest, both in speculations and in 'safer' investments, based on firm knowledge of the underlying asset and intrinsic analysis, to the extent possible, and never merely based on price movements.

In the case of bitcoin, my personal belief is that there *is* enough to justify the possibility of long term gain based on fundamentals and first mover advantage. If everything goes right, I do see a future in which it's possible that bitcoin achieves a market cap similar to that of gold's, given that so far as I can see, it provides all the benefits gold does, and a host of incredibly valuable advantages on top of those existing benefits. I even see a future where it *just* might be possible that bitcoin goes even further, and becomes a dominant leading global currency. It's also

possible that bitcoin's blockchain is used to power many future technological innovations, such as smart contracts and even DAOs, and thereby creates and imbues itself with even more value.

At the same time, I also see a million and one ways where bitcoin fails to reach the promised land. Bitcoin has already experienced numerous growing pains, and at the present moment, is suffering most acutely from a huge backlog of transactions that can't be fit on the blockchain. This is because blocks are presently limited to 1 MB in size, and can consequently fit only a small fraction of all the transactions that are trying to be propagated over the network. This forces those who want to have their transactions go through to pay inordinately high transaction fees in order to prioritize their transaction over other transactions.

There are already a number of proposed solutions to this issue, such as the implementation of the Lightning Network, but in order to implement these solutions, the majority of bitcoin miners must agree to update their bitcoin software. Many bitcoin miners are reluctant to do so, in large part because high transaction fees are *good* for miners, at least on a short term basis, as it means they earn far more per each block mined. The implementation of the Lightning Network and other solutions threatens to take away this extra revenue stream. Hence, users of bitcoin and miners of bitcoin find themselves at odds with a very understandable conflict of interest. It's unclear as of yet how this will be resolved, though it seems the community is pushing forward towards a resolution, and I'm of the personal belief that they'll get there eventually.

Similar problems like this are virtually guaranteed to occur in the future as well, and it's simply impossible to predict right now how the bitcoin community might respond to and handle those problems, and if they'll be successful in doing so.

At the same time, it's entirely unclear how governments will respond to bitcoin as it continues to grow, and if they'll attempt to crack down in a very strong way and prohibit the use of bitcoin, or the creation of bitcoin related service companies, such as exchanges. If exchanges were banned from operating, for instance, it could very well make it very difficult for most people to transact between fiat currencies and bitcoin, and render the latter far less useful than it otherwise might be.

On the flip side, if the world suffers a global financial meltdown on the scale of the Great Depression or something similar again, and fiat currencies start to crater, it very well may be such that governments are forced to resort to accepting bitcoin and other cryptocurrencies, if enough people simply flat out refuse to put their stock in fiat. This was exactly what the US government was forced to do just 13 years into their original experiment with Continental currency, when they agreed to promise to back all the currency they issued with hard gold and silver.

These are just a few of countless twists and turns and vicissitudes our much vaunted (and much derided) bitcoin will have to endure before its long journey comes to an end, either six feet under or as an indelible fixture in our global economy. There's no telling which way it will go, and one must come to one's own conclusion on how much faith and conviction one chooses to place in bitcoin.

That's the case as I see it for bitcoin. In the case of most altcoins, however, I don't see remotely enough to even begin to justify the possibility of long term gain in the first place. Even with speculations, or perhaps especially with speculations, it's incredibly important to thoroughly analyze a given investment opportunity for at least the *potential* for long term gain and success, and assess the magnitude of that possible gain, and then to weigh that potential versus the likelihood of outright failure of the speculation. With most altcoins, their value over bitcoin or ethereum is far from clear, and generally superficial or minor at best.

Dogecoin is the most pure example of this. Dogecoin offers just about no fundamental innovations over bitcoin, and is in fact a self-deprecating cryptocurrency premised (initially, at least) entirely on poking fun at itself. The name itself is a reference to the doge meme, and offers little to no further justification for its existence.

Despite this fact, Dogecoin's market cap is presently valued at over $300 million. Come to your own conclusions here.

Less immediately obvious examples include things like Litecoin. Litecoin, too, offers fundamentally no truly great innovations over bitcoin — in short, nothing that bitcoin itself couldn't adopt over time. It uses a different hashing algorithm and just adopted Segregated Witness, the same update that bitcoin is debating adopting that would allow the implementation of layer two protocols such as the lightning network, but beyond this, doesn't have much in the

way of unique differentiation going for it. This said, Charlie Lee, the creator of Litecoin and previously the Director of Engineering at Coinbase, one of the most well respected and successful bitcoin exchanges, just announced his departure from Coinbase to focus solely on improving Litecoin. It remains to be seen what will come from this endeavor, as Charlie certainly is without question one of the most accomplished and formidable players in the cryptocurrency sphere, but largely litecoin appears to be a small hedge in the slight off chance that bitcoin doesn't actually manage to resolve its scaling issues, and begins to catastrophically lose market adoption and faith and crumble into the ground. In a case like that, the notion is that litecoin would be able to quickly take over the ground lost by bitcoin, and become the dominant cryptocurrency.

There are a number of issues with this, however, and a *lot* of things would have to go right before this occurred. There are several cryptocurrencies, for instance, with ethereum being the most notable, that are already far larger than litecoin, and it would have to be demonstrated that there's some reason something like ethereum couldn't simply take the place of bitcoin, and that litecoin would have a better shot at doing so than the larger players that already exist in this space.

Litecoin would then have to deal with exactly the same issues bitcoin has faced at scale, and it's not clear at all that litecoin would fare any better at resolving such conflicts if ever reaches the same scale as bitcoin presently has.

All of this said, it does seem extremely likely to me that there will inevitably be *some* true innovation in this space, and that some cryptocurrencies will be able to carve out niches of varying degrees of value. One might even prove to ultimately demonstrate so many more advantages as to overtake bitcoin one day — ethereum, for instance, is teetering remarkably close to doing just that, at least in terms of market cap, if not quite yet other markers such as developer activity and transaction volume. The true feat here will be discerning those few new technologies with true fundamental potential and innovative advantage (and an incredible execution strategy) behind them, from the vast swaths of similar looking yet ultimately worthless contenders almost certainly doomed to eventual failure.

Expected value is a useful concept frequently employed in poker that also serves to provide utility here. In short, expected value is a way to decide when an outcome is not certain, but a set of outcomes are probabilistically determinable, if a given action is going to be net positive or net negative, and to what degree.

The simplest example is flipping a coin. This will yield heads 50% of the time, and tails 50% of the time. Expected value of betting on the coin yielding heads, hence, is 0. This is because in any one given flip, the coin has exactly a 50% chance of coming up heads. Hence, if you bet $100 on the coin coming up heads an infinite number of times, your expected gain, or value, from such an action, is to be $0.

Conversely, if you bet at even odds that a six sided dice roll would come up 3 or higher, your expected value would be positive, as you would be correct 2/3 times. Hence, if you repeated this bet an infinite number of times, you would be guaranteed to be earning more money than you lost.

Similarly, if you were able to bet at 1:2 odds (meaning if you bet $100 and win, you get $200) that a coin would yield heads, this would also be very +EV (positive expected value). The coin would still yield heads half the time, but that half of the time, you would earn $200, and the other half of the time, you would only lose $100. Hence, repeating this bet an infinite number of times would allow you to dramatically earn more money than you lost yet again.

There are far too many variables and unknowns to take into consideration with most speculative bets, and cryptocurrency in particular, to be able to hope for anything so nice and clean as an exact mathematical probability of how + or -EV a given bet on a given cryptocurrency might turn out, just as there are far too many unknowns to calculate the precise fundamental present and future potential value of a cryptocurrency for the purpose of value investing analysis, but regardless, holding both principles at large as a general guiding strategy in determining one's actions here and elsewhere is a good bet.

Personally, for myself, a quick back of the napkin calculation that I can do to estimate the possible future value of bitcoin is to see what the market has valued all of the gold in the world at, and use this as a rough guiding principle for seeing how much appetite the world currently has for something that can hedge against other currencies and holds similar characteristics to gold as a store of value. I can see that the total value of all the gold in the world is over 8 trillion dollars, and consequently, if bitcoin were to reach that same total valuation, each bitcoin, assuming 21 million eventual bitcoins, would be worth approximately $400,000. Dividing this by bitcoin's current value, I can see that there's still room for approximately 150X gains. This means that if I truly believe this is a possible

outcome for bitcoin, then as long as I believe this outcome has more than a 0.66 percent chance of happening, or 1/150 chances of success, it would be an +EV bet to make.

That said, it's extremely important to keep in mind that one doesn't get infinite opportunities to keep playing this bet out over and over again. There is only one bitcoin in the world, and we only have one opportunity to play out this exact bet. Given this fact, it's important to realize that if this were somehow to actually be a perfectly EV neutral bet, with a possibility of a 150X upside and a 0.66% chance of realizing that upside, it would still mean that we have a 99.33% chance of losing all our money that we place on this bet. It would be *extremely* foolish, therefore, to invest *all* our money into such a wildly speculative investment, even if it is technically EV neutral or even slightly EV positive. What *might* make sense, is to set aside a responsibly proportionate amount of money specifically earmarked for such wildly speculative investments as a part of a holistic investment portfolio, that one is fully willing and able to lose without significant impact to one's well-being or quality of life, and to invest *that* amount of money in a +EV bet like this.

Returning to the question of calculating potential investment upside here, there are countless other ways to make projections on the future potential value of bitcoin, and I encourage you to try to make some depending on your personal beliefs regarding the level of success bitcoin might have, and the ultimate utility it might provide to the world. For instance, if you see bitcoin primarily as a way to simplify making international transactions and cut out inefficiencies there, you might look to see what the overall market size is for a solution that might solve that problem and capture that market. Western Union, as one example, is a company with a market cap of $9 billion. Consequently, it might be reasonable to expect that bitcoin's true ultimate value would be something roughly in that order of magnitude, if this were to be bitcoin's one true long term use case.

If you see bitcoin as most useful for its blockchain, you might calculate hence the value you think can be created through applications, contracts, and other technological innovations run on the blockchain, and use that to guide your estimation of bitcoin's value.

If you think bitcoin will be used to primarily enable black market transactions, same deal. And so on.

I hope that this elucidation provides some insight into why I personally see it as suspect to invest in something based on price alone, and why I urge extreme caution particularly if one is exploring whether or not to invest in an altcoin, especially if one is at least partially motivated to do so because of the feeling that the ship has already sailed for bitcoin, and that there might be better potential for outsized gains with a smaller altcoin. Again, this certainly *may* be true, and often is true even for altcoins destined for eventual failure in the short term while a bubble/bull market continues, but risks are amplified just as much as the opportunity itself when it comes to altcoins, and oftentimes moreso in a bubble than otherwise.

It's easy to be swept away in the fervor of a frenetic market, and the fear of missing out can be overwhelming especially when you see altcoins rising by wild amounts overnight, but my personal guiding philosophy is to always try to keep in mind fundamentals to the maximum extent possible, to never invest in anything I don't actually understand or see long term value in, and to only invest in things I intend to hold very long term (for at least 5 years), especially in such a volatile market.

Speaking to that last point now (the 'second' mistake I mentioned at the beginning of this part) I'm of the personal opinion that it is incredibly important to not only invest solely in things that I truly believe have the real potential to succeed in a big way long term, but to actually commit and hold to that investment, once I make it, no matter what happens with the price short term. If some fundamental fact underlying my investment changes, I can certainly re-evaluate it, but if the price drops 90% or even 95% in the short term for no particular reason except a collapse of a local maximum in price speculation (e.g., a bubble popping), I must never be tempted to sell and try to 'time' the market in any way. Instead, I have to hold that investment with firm conviction in what I believe the eventual price based on fundamentals is worth, regardless of how the market values it in the present moment.

This is critically important precisely for incredibly volatile speculative investments such as cryptocurrency, and plays into the fourth mistake I mentioned above, day trading, as well. More than possibly any other market I've seen, short term price movements for cryptocurrencies are oftentimes absolutely mystifying and nothing short of mind boggling. Highly anticipated events, such as halvings in bitcoin's reward per block mined, come and go without any real perturbation in price. Other times, things rise when reason seems to suggest they should fall, and fall when they seem to have every reason to rise. For instance, bitcoin's price collapsed to $200 after the bubble

popped in 2013, and stayed stagnant at those levels, despite massive development in bitcoin infrastructure and significant growth in the adoption and usage of bitcoin over that same period of time.

More recently, the approval or rejection of a bitcoin ETF was widely touted as being the contributing factor to a bitcoin bull run from under $1000 to over $1200. It was speculated that if the ETF were to be rejected, that naturally the price would fall to where it was before the bull run began. Indeed, the moment the ETF was announced as rejected, the price did momentarily fall to almost $1000. However, it just as quickly recovered, and began an inexorable climb all the way up to over $2700, where it stands to this day.

Consequently, with the short term price movements of bitcoin and other cryptocurrencies being incredibly volatile and oftentimes nothing short of inexplicable, I highly caution anyone against making decisions such as selling their bitcoins on the way down in anticipation of a market crash, so as to either avoid the crash or to buy their coins back at a cheaper price at the bottom of the crash.

This goes hand in hand with mistake number four I mentioned above: day trading. This is absolutely number one the reason I see people who have gotten into bitcoin and cryptocurrency lose their money. If you at almost any point in the history of bitcoin (earlier than say, this month of June), merely bought bitcoin and held it to the present day, you would have made money. However, countless people have actually lost money in bitcoin, and this is because they ended up trading their bitcoin somewhere along the way.

I would venture to say that most people have far more confidence in their ability to predict short term market movements than is actually the case. I've seen plenty of instances of people who have thought that they could capitalize on short term volatility on the way up, and essentially 'buy the dips and sell the tips', and in every single instance I can recall, this strategy eventually fails, and often in a big way. At face value, this seems to make sense. If you think you can time when the dips will occur and when they will end, and similarly when the peaks will occur and when those will end, you can definitely make more profit along the way by selling high and buying low.

However, as I've mentioned before, this is far more difficult, if not impossible, to do with cryptocurrency, more than even normal investment vehicles like stocks. I've seen people who think that bitcoin has hit a peak and must

necessarily stop going up sell, intending to wait until bitcoin falls again to buy in again and make maybe a 20% extra profit, miss out entirely because bitcoin kept going up and never came back down. There are numerous stories of those who bought into bitcoin at $1 or less, but sold well before it ever reached even $10, much less $2500.

Real friends getting real screwed with real money

With something as speculative as cryptocurrency in the first place, it makes no sense to invest in this space to begin with if your only goal is to make 20% profit. It almost certainly isn't worth the risk at that level of gain. Hence,

risking losing out on the long term upside of 10X+ that you've calculated and come to the conclusion does exist for a gain of less than 1X or .5X in most cases makes little to no sense at all. It only makes sense if it's essentially a guaranteed gain with no risk, and that, again, is almost certainly not the case.

Indeed, some market movements are fundamentally unpredictable in their short term timing. Two very vivid examples of this were the collapse of Mt Gox for bitcoin, and the hacking of the DAO for ethereum. Both of these events absolutely cratered the price of bitcoin and ethereum respectively, and both of them were fundamentally unpredictable in their exact timing. These are examples of the black swan events I mentioned that are certain to continue playing a large role in short term price developments for bitcoin and all other cryptocurrencies at large, that make it doubly dangerous for those who day trade.

I've also seen plenty of people who intend to hold long term, but lose faith when they see their investment crater 30%, 50%, or even 70%. At this point, they lose faith, and decide to sell their investment to at least recoup some of their initial capital, and not lose everything outright. Thus, they end up buying high and selling low, and then having double regret when bitcoin eventually ended up rebounding even higher than the 'high' they bought at.

This illustrates even more vividly why it's incredibly dangerous to invest in anything you don't actually believe in, and aren't willing to hold, long term. If you aren't going to hold something long term, then generally you must believe that while the price will rise in the short term, it will not continue to rise in the long term. If you hold this belief, it generally means that there's some reason that you believe what you are investing in won't hold true value long term, but that there is enough speculative mania in the short term to make the price go up anyway. The thinking goes that if this is going to be true, you might as well profit from this speculative mania and buy in now, wait for a little bit for the price to rise, and then sell it for short term profit.

The problem with this is that just about everyone else investing in these things is thinking the same thing, and everyone involved is effectively playing the greater fool theory, expecting that they will be smarter than everyone else and be able to time the market better than everyone else, and get out before everyone else does, and before the price eventually collapses. By mere inviolable fact, most people who engage in this form of speculation are guaranteed to lose in a big way. Over enough iterations, the eventual likelihood of loss generally grows to become

one, in my opinion, as one must continue to time a market correctly time and time again for this to work. While it may seem like the market will continue being bullish for you to get in and get out before things go south, this is true of every moment in time right up until things go south all at once. Inevitably, at some point, the gravy train will have to derail and explode in a rolling ball of fire.

I know for a fact that I'm certainly not remotely smart or knowledgeable enough to pull off this kind of short term investment that aims to profit from market sentiment alone, especially not in the turbulent, mercurial waters of cryptocurrency, and that's all I can say about this here. On top of this, the existence of black swan events that can crater an entire market unpredictably short term introduces a variable that inherently is just about impossible to predict, and makes short term bets like this even more dangerous.

The most dangerous game of all, then, in my opinion, is day trading in altcoins that one doesn't believe in long term. This is basically combining every 'mistake' I mention above: trading in something because of short term price movements, not holding it long term, day trading, and speculating in highly risky small cap altcoins. If you manage to survive doing this over any long period of time (5 years+, let's say) and end up net profitable (particularly if you end up more profitable than just buying and holding over that same period of time), please do let me know, as I'd be extremely curious to hear just how you pulled it off.

Going back to my personal story, ultimately the crash from $1200 to $200 for bitcoin was the best thing that could have ever possibly happened to me. At the time, of course, it certainly didn't feel that way. It felt like I had made an absolutely stupid, foolish decision, and had lost all my money. In fact, I *did* make a stupid, foolish decision, but not for the reason I thought at the time. I didn't make a stupid, foolish decision because the price had cratered to $200. I made a stupid, foolish decision in deciding to invest in bitcoin and altcoins without actually having done my research and without really knowing anything about them.

Had I actually done my research and believed that it was a fair bet to make that one day bitcoins would be worth far more than even the height of the local maximum bubble at the time, it absolutely could have been the right decision to buy in then, even if it crashed later temporarily to $200. What wasn't right was buying in simply because the price was going up and I had a fear of missing out.

The crash proved to be the best thing that could have happened, however, because it gave me time to actually do my research and learn about bitcoin, and have real reasons for believing in it long term, at a point in time where the price was unusually deflated. As a consequence, I was able to buy *more* bitcoin at the very bottom of the market, around $230 or so, when I became truly convinced of bitcoin's long term potential. I was also lucky enough to decide not to sell the bitcoins I had originally purchased for $1000 or so, and ultimately saw even those return 250%+ in profit.

It was at this time, incidentally, that Coinbase, became worried about stagnant growth of their user base, and decided to offer a truly astounding proposition. They offered to pay anyone who referred a new customer to Coinbase $75 if the new customer purchased just $100 in bitcoin. Coinbase took a 1% transaction fee at the time, meaning that for every $100 in bitcoin a person purchased, Coinbase charged $1. In short, Coinbase would pay out $75 for every $1 a new customer paid them.

It didn't take a genius to see a clear arbitrage opportunity here, and I wrote up a quick blog post detailing this opportunity and fired out a single Facebook post telling my friends about it. From that post and just a few hours of work, I ended up earning almost 17 bitcoins entirely for free — worth over $45,000 today. I had plans to scale this strategy en masse, but singlehandedly ended up killing the program almost as soon as it started, when Coinbase finally came to its senses and realized just how much money it was hemorrhaging here with no hope for eventual recoupment (at the time, the lifetime value of the average customer was only something like $25 to Coinbase — a far cry from the $75 they were offering).

Digression aside, that sums up most of the thoughts I have about the primary things to be cautious about when it comes to bitcoin investment. There are a few more practical matters to be extremely cautious about (namely, how you store your cryptocurrency), but I'll address those in the next part, which will be an actual how-to guide showing actually actionable steps for those interested in getting into bitcoin investment.

The final point to make, then, are a few thoughts on how to *correctly* invest in bitcoin and other cryptocurrencies. I have no truly great pieces of wisdom to offer here, but do have a few ideas that primarily aid in being psychologically being resilient to the short term vicissitudes of cryptocurrency investment.

Once you've decided that you truly believe in a cryptocurrency long term, and are willing to commit to it for the long term and hold it no matter what the short term price movements might be, the next step is to decide how much to invest, and when to invest. One might be hesitant, with not bad reason, to invest at an all time high, even if one believes that that all time high will one day be exceeded.

The mere fact that the future potential is still huge doesn't necessarily preclude the fact that cryptocurrency may be in a short term bubble, and that prices might crater any day by 30%, 50%, 80%, or even more.

Generally, the strategy suggested to average out such short term volatility for something that one is investing in long term is to practice dollar cost averaging. This preaches that one should set an exact time at regular time intervals to buy an exact amount in fiat currency of the investment one is looking to purchase — e.g., $1,000 worth of bitcoin on the 1st of every week, or every month. This means that over time, you'll be able to take advantage of bitcoin's general trajectory upwards, but balance out the relative short term volatile price movements both high and low, such that you experience a more linear growth trajectory over time of your principal.

I think that this is a great strategy, and personally practice it with a few modifications. While I'll never sell at any price essentially (unlike other investments, bitcoin and cryptocurrencies are unique in that they *are* currencies, and consequently if they succeed, you won't have to sell them to gain value from them. You can just use them directly, just as you might US dollars or any other form of currency. In the manner that I use the word sell here however, I mean that I likely won't sell at any price under $100,000, as that's where I personally see the moonshot value of bitcoin going towards, in the slight chance that it does succeed), no matter how high the price rises in the short term, if and when the price becomes particularly low as a result of a cratering market, I will look to buy more than I normally would, to double down on my investment here — all the while keeping in mind never to invest more than I'm perfectly willing to lose entirely.

Psychologically, if it's helpful, I think it may be fine to sell off some small portion of your upside if you do realize upside over time, in order to recoup your initially invested principal. I don't think that this is necessarily the most optimal actual move to make, but do think it likely makes a huge difference psychologically, such that it makes it

far easier for you to hold your remaining investment with sangfroid in the case that it ends up cratering sometime in the future.

As for investing an initial lump sum to begin getting exposure in this space, my personal strategy would be to do a semi-timed dollar cost average, if one is particularly concerned that they might be investing just before a local minimum market crash, but also particularly concerned that the price may keep rapidly appreciating ad infinitum, and would like to get in before that happens. That is, I'd decide the total lump sum I'd be willing to set aside to invest here, say, $10,000, and invest 33% or 50% of it immediately. Then, if the market did crash, I'd be psychologically very happy, and be super excited to invest another 33% or 50%. On the flip side, if the market continued to rise indefinitely and never fell again, I'd also be happy that at least I was able to get exposure to the market and didn't miss out entirely. A 33–33–33 split would allow me to invest 3 times when I felt the market was at a particularly good time for investment, and a 50–50 split twice. Just random arbitrary examples of divisions I might do here, depending on how exactly wary I feel about the market at the present moment in time.

That about sums up my thoughts on cryptocurrency investment at large. There are some nuances, but I figure 8000+ words worth of a brain dump is a good enough place to start. If you're still here, please feel free to read on to Part III if your constitution allows for further word consumption.

Part III: How to Buy and Store Your Cryptocurrency

The shortest section by far. If you made it this far, you deserve to just be able to buy your crypto and be done with it all. I'll try to make that as easy as possible. There are still quite a few bases to cover, however.

Note: The following bit about exchanges to use holds true for those in the United States. For those based elsewhere, you'll need to do your own research on the best exchanges to use in your country. The rest of this post should hold the same for everyone in the world, however.

The easiest way to invest is to sign up at Coinbase.com. If you sign up with a referral code, you get $10 when you purchase $100 in bitcoin or ether. I've linked my mom's referral code here if anyone is interested. Straight to her

retirement fund! (*In the interest of having zero monetary gain from my fiduciary advice, however, just email me if you use this link and buy over $100 of bitcoin, and I'll send you the whole $10 my mom receives on her end as a referrer — so you get $20 for investing $100. Not bad! →SORRY NEVER MIND I'VE BEEN OVERWHELMED WITH THESE MESSAGES AND CAN'T KEEP MANUALLY DOING THIS, but you're still welcome to use the code and get a free $10 and give my mom a free $10 too!*)

However, this is not the cheapest way to invest. That's GDAX.com (no referral bonus with this, though). Thankfully, GDAX.com is the same company as Coinbase, and utilizes the same login. Once you make your Coinbase account, you can just login with it to GDAX.com.

At GDAX.com, which is Coinbase's exchange, you're able to get trades in for either 0% as a market maker (meaning you limit buy or sell and set your own price and 'make' the market), or 0.25% as a market taker (meaning you just buy or sell at whatever price the market is currently at with a market buy).

You can trade immediately as much as you want by sending a wire (only applicable for US customers) to your account following their deposit instructions. There's a $10 fee for this that GDAX charges, on top of whatever your bank charges to send wire transactions. This is the fastest method to deposit any amount of money you want and trade immediately with no limits, but not the cheapest.

You can alternatively conduct ACH withdrawals from your bank as well by going to the Coinbase accounts page, clicking on your "USD Wallet", and clicking the Deposit button in the top right hand corner. These are completely free, but take anywhere from four business days to a week to complete.

You can even use a credit card to buy straight from Coinbase.com, but fees here are very hefty. Use as a last resort.

Keep in mind that while you can put however much money you want into GDAX at any point in time, you are generally limited to withdrawing $10,000 per 24 hour period. Thus, if you are buying a large amount of say, Ethereum to send to a token sale address, keep in mind that if you want to send over $10,000, you'll need to purchase that amount and withdraw it well in advance of the token sale.

For instance, if you wanted to send $100,000 of ethereum somewhere, you'd need to buy all that ethereum and withdraw over the course of 10 days (assuming you withdrew perfectly each day every 24 hours — realistically more like 11–14 days) back to Coinbase or your personal ethereum wallet before you could then send that ethereum on to somewhere else all at one time, like you would need to do in a token sale.

On GDAX, you can buy bitcoin, ethereum, or litecoin.

From there, if you'd like to buy any alternative currencies, you can use your bitcoin or ethereum on Shapeshift.io without any account to instantly transfer your bitcoin or ethereum to any other cryptocurrency under the sun, essentially.

To buy/sell on Coinbase or GDAX, you need no wallet, as Coinbase/GDAX will keep your coins for you. You'll want to enable Google Authenticator for two factor authentication and keep your passwords and your phone incredibly secure, however, as if someone hacks your account, all your money is gone for good with no recourse. This happens a lot. Use a super strong password that you have not used elsewhere and that no one knows and that you won't forget.

Ideally, you'll keep the coins yourself on your own hardware device, which is ultra secure. I recommend Trezor.io (as of this writing, they've just run out of stock, but are only backordered a few days if you're willing to pay a premium) for this purpose. Ledger Nano S is also good and cheaper to boot, but I personally haven't used it and it's very backordered in sales. I can recommend Trezor 100% wholeheartedly, however.

Trezor will keep your coins safe because the device itself is immune to hacking by design, and never exposes your private keys (the passwords to your accounts, essentially), even if your computer is infected by malware and is logging all your typing/passwords, or is specifically scanning for private keys, or is engaging in any other form of sneaky bad behavior.

It does this by signing all transactions on the device itself using your private key, and only transmitting the signature to your computer, and never your private key. As a general rule, this is very good, because a good rule of

thumb is to never expose your private keys to the internet, under the assumption that the internet is inherently insecure, and if you ever have your private keys interact in any direct way with a computer that has been connected to the internet, you should consider the addresses those private keys correspond to to be compromised and vulnerable to being hacked.

A Trezor also allows you to set multiple passwords that open secret vaults to different wallets on your device, such that even if in some crazy scenario someone just kidnaps you and threatens to beat you with a wrench until you give them your coins (not *too* crazy actually — I've been abducted before and had to ransom myself for thousands of dollars in Africa), you can just give them a second password to another wallet that holds say $500 in cryptocurrency instead of $10 million, and there's no way for them to know that that's not all the money you had on your Trezor.

If someone steals your Trezor, they won't be able to find your coins either, as they're protected by a PIN that only you know (plus a password if you want to use that feature I mentioned above). You can also recover the coins yourself with the recovery seed the Trezor will give you the first time you use it, which you should store in a super safe location like a safe deposit box somewhere. If you don't use utilize the password feature, however, keep in mind that anyone who discovers this recovery seed instantly has access to all your coins, and all your other forms of security are for naught. If you enable the password feature, however, they will need your password as well as the recovery seed in able to access your cryptocurrency, which makes it significantly more secure.

A Trezor will give you your own personal wallets for bitcoin, ethereum, dash, zcash, and litecoin, as well as any ERC20 token built on top of ethereum.

Another benefit of holding coins yourself, in a hardware wallet or elsewhere, is that you know that you 100% own all of your money. Exchanges are just like banks, in the sense that you trust them to hold your money for you. If they end up losing that money to hackers or stealing it themselves, you're out of luck. This isn't just a scary bedtime story — countless cryptocurrency exchanges have been embezzled or hacked (an enormous percentage, actually), and hundreds of millions of dollars have been lost.

Moreover, in the event of a hard fork, whereby two blockchains are created, and consequently, two sets of coins that you technically should own, only some exchanges will actually give you access to both sets of coins. Most notably, Coinbase has explicitly stated that they will only give you access to the dominant blockchain that emerges from a hard fork, no matter how much value the market assigns the non-dominant chain. They may or may not give you access to the other coins in the future, but there is no guarantee either way. In any event, with any exchange you are fundamentally agreeing to trust them to give you access to both sets of your coins, even if they say they will. If you own your coins yourself in your own wallet, however, you need to trust no one. You will automatically own both sets of coins by default in the event of any fork.

This, too, is not merely a theoretical matter. Ethereum did indeed hard fork after the DAO hack, and split off into ETH (the current dominant blockchain for ethereum) and ETC (the 'classic', or original blockchain for ethereum). As of this time, ETC is worth over $20 a coin — more, in fact, than all of ethereum was worth before the hack. Had I kept my ethereum on Coinbase or another exchange like it at the time of the hard fork, I personally would have lost 5 figures in ETC (at present values) merely because the exchanges wouldn't give me access to these coins that I rightfully owned.

Finally, my personal preference is to avoid keeping all my eggs in one basket. Despite the fact that a hardware wallet like Trezor is technically one of the most secure options for keeping your coins safe with a fair amount of redundancy in recovery options, the fact remains that one day I might somehow lose access to my coins held within Trezor. I might suffer a concussion, for instance, that causes me to forget the password or the PIN required to access the Trezor, or perhaps I lose my Trezor and am unable to locate or decipher my recovery seed.

Because of this, I actually personally keep my cryptocurrency distributed in *several* reasonably safe baskets. For instance, despite Coinbase being an exchange that fundamentally requires some trust, they are more trustworthy than almost any other exchange on a technical level (their customer service, however, leaves something to be desired), and it is virtually impossible for their coins to be hacked to any significant degree, and all those at risk of being hacked are fully insured. As a consequence, I leave some of my coins with them, merely because in many ways, I trust their technical security measures more than I trust my own. Before GBTC started trading at such an absurd premium, I also kept some of my funds with them, both in part to diversify across multiple platforms to

reduce the risk of losing all my coins with one bad black swan event, and also because it was the only immediately easy way to put some of my retirement funds into bitcoin, short of creating a self directed IRA.

Okay — so that's about it for investing in the dominant cryptocurrencies available today. If you want to invest in other more speculative altcoins, you'll have to create your own wallets for them, and investigate the best and most secure solution for doing so yourself. This should generally be a good exercise in any case to determine if you meet the bare minimum requirements for responsible investment in a given altcoin.

Congratulations, you've made it to the end. That's it. Good luck!