

Wences Casares  
wences@gmail.com

### The case for a small allocation to Bitcoin

What Bitcoin is today, what it may become and why it could make sense for you

#### 1- Preface

This essay is focused on the potential financial gain to be had from responsibly investing in Bitcoin. But if Bitcoin does for money what the Internet did for information the prospect of unprecedented economic freedom is much more exciting than any possible financial gain.

I grew up in Patagonia, Argentina, where my parents are sheep ranchers. Growing up I saw my family lose their entire savings three times: the first time because of an enormous devaluation, the second time because of hyperinflation and the last time because the government confiscated all bank deposits. It seemed like every time we were recovering, a new and different economic storm would wipe us out again. My memory of these events is not economic or financial but very emotional. I remember my parents fighting about money, I remember being scared, I remember everybody around us being scared and returning to desperate, almost animal-like behavior. I also remember thinking how unfair it was that these crises hit the poor the hardest. People who had enough money to get some US dollars or to have a bank account abroad were able to protect their life savings. But the poor could not do any of those things and simply got wiped out every time.

When the Internet emerged I thought, in a very naive and idealistic way, that it was going to solve many of the world's problems and that it was going to democratize money and fix money quickly and forever. Now 30 years have passed and the Internet has fixed many problems but increasing economic freedom is not one of them. I was about to give up hope for the Internet to fix this problem when I ran into Bitcoin by accident. At first I was very cynical but the more I learned about it the more curious I became, after six months of studying and using Bitcoin I decided to dedicate the rest of my career to help Bitcoin succeed.

If I am lucky enough to one day have grandkids nothing would make me prouder than to be able to tell them that I was part of a very large community who helped Bitcoin succeed, to tell them that because Bitcoin succeeded now billions of people can freely and safely send, receive and store any form of money they want as easily as they can send or store a picture. And that what I saw happen to my parents and countless others can never happen again.

#### 2- Summary

Bitcoin is a fascinating experiment but it is still just that: an experiment. As such it still has a chance of failing and becoming worthless. In my subjective opinion the chances of Bitcoin failing are at least 20%. After 10 years of working well without interruption, with close to 100 million holders, adding more than 1 million new holders per month and moving more than \$1 billion per day worldwide, it has a good chance of succeeding. In my subjective opinion the chances of Bitcoin succeeding are at least 50%. If Bitcoin does succeed, 1 Bitcoin may be worth more than \$1 million in 5 to 7 years. That is 100 times what it is worth today (at the time of writing the price of Bitcoin is ~ \$11,000).

I suggest that a \$100,000 portfolio should invest at most \$1,000 in Bitcoin (up to 1% but not more as the risk of losing this investment is high). If Bitcoin fails, this portfolio will lose at most \$1,000 or 1% of its value over 3 to 5 years, which most portfolios can bear. But if Bitcoin succeeds, in 5 to 7 years those \$1,000 may be worth more than \$100,000, more than the value of the entire initial portfolio.

In today's world it is hard, if not impossible, to find an asset that is possibly so mispriced and where the possible outcomes are so asymmetrical. Bitcoin offers a unique opportunity for a non-material exposure to produce a material outcome.

I recommend that you open an account at any reputable Bitcoin wallet ([Coinbase](#), [Square's Cash App](#), [RobinHood](#), [Revolut](#), [Paxos](#), [BitGo](#), [Abra](#), [UpHold](#), [Luno](#), [Kraken](#) or many others) buy a small amount of Bitcoin you can afford to lose and keep it there for at least 5 years. If you don't want to open a Bitcoin wallet and want to use your existing brokerage account instead you can buy Greyscale's Bitcoin Trust ([Ticker GBTC](#)).

It would be irresponsible to have an exposure to Bitcoin that one cannot afford to lose because the risk of losing the principal is very real. But at this point not owning any Bitcoin is also irresponsible and lazy.

### 3-Definitions

**Bitcoin Blockchain:** Bitcoin the platform. When I say "Bitcoin Blockchain" I am referring to the Bitcoin platform as a whole, including the Bitcoin Blockchain and the Bitcoin currency. Many different systems for different use cases may one day run on top of the Bitcoin Blockchain.

**Bitcoin:** Bitcoin the system. When I say "Bitcoin" I am referring to Bitcoin the currency that can be bought, sold, sent, received, held, etc. You can think of the Bitcoin currency as the first system to run on top of the Bitcoin Blockchain.

**Sovereign:** One possessing supreme and ultimate authority and power. A sovereign only obeys its own rules, no one can impose rules on a sovereign. Kings and Queens used to be sovereign and then nation states became the sovereigns of our time.

#### 4- Introduction

The current state of the Bitcoin Blockchain is similar to the state of the Internet in 1992. Back then the Internet was nascent and experimental.

Just like in the early days of the Internet there are many bold claims about how the Bitcoin Blockchain will revolutionize the world and solve so many problems. Many of these claims are exaggerated or wrong.

You do not need to know the technical underbelly of the Internet to understand the Internet and, similarly, you do not need to know the technical intricacies of the Bitcoin Blockchain to understand it. Even though right now most of us feel like we do not fully understand the Bitcoin Blockchain, over time we will all understand it as well and as intuitively as we understand the Internet today.

Understanding the Bitcoin Blockchain first principles will allow you to form your own judgment about its potential applications without you having to trust any expert. If the Bitcoin Blockchain succeeds, the investors who develop this understanding and the accompanying intuitions earlier will have an advantage over the investors that take longer to do so.

#### 5- What is interesting about the Bitcoin Blockchain?

To understand the Bitcoin Blockchain first principles let's understand what changed when the Bitcoin Blockchain first started running in January 2009. All of the Bitcoin Blockchain separate components (Public-key cryptography, distributed databases, open databases, tokens and proof of work) existed many years before Bitcoin went live. What changed when Bitcoin went live? What was new and potentially revolutionary? What changed, that may potentially be revolutionary, is that all of those components were combined in a new intelligent and innovative way to create the first potentially sovereign computer platform. Up until that moment, all computer platforms belonged to a person, to a company or to a government and those platforms were subject to the will of their owners and the rules of the jurisdiction where they resided.

In the world of crypto we use the word "decentralized" a lot, often hailed as an end in itself as in "Bitcoin is a truly decentralized system". When you read that, if you don't understand why does that matter or if it or it seems confusing to you simply replace the word "decentralized" by the word "sovereign". Decentralization is the current means by which the Bitcoin Blockchain achieves the end goal of sovereignty. In the future we may be able to achieve the same level of sovereignty, or even stronger level of sovereignty, with other means that we cannot imagine today. It truly does not matter how the system achieves it as long as the result is a sovereign system.

The Bitcoin Blockchain is sovereign in that no one can change the number of bitcoins that exist or will exist, no one can change the transactions that already exist in its database and nobody can keep the system from accepting new transactions.

Today there are 18.5 million bitcoins in circulation . The system will reach the maximum possible number of bitcoins in circulation, 21 million, in the year 2140. The issuance schedule is fixed and it does not change if there are more or less miners.

Today the Bitcoin Blockchain issues 900 new bitcoins pay day to reward the miners who are protecting it. This reward gets cut in half every 4 years, in May 2024 it will be cut to 450 bitcoins per day, in May 2028 it will be cut to 225 bitcoins per day and so on until May 2140 when there will be no new bitcoins mined.

The miners earn both the mining reward, which today is 900 bitcoins per day, and the transaction fees, which today is 5 bitcoins per day on average. As the mining reward has been going down over time the transaction fees have been going up over time because more people use Bitcoin and there are more transactions. By the year 2140, when there are no more bitcoin rewards, the miners will only earn the transaction fees.

The main resources securing the Bitcoin Blockchain sovereignty are the Bitcoin miners and the Bitcoin nodes. If my laptop was the only computer mining Bitcoin in the world and it was also the only Bitcoin node in the world, the Bitcoin Blockchain would not be a sovereign platform, anyone who used it would simply be using my platform and trusting me. The Bitcoin miners and the Bitcoin nodes make sure that new bitcoins are not being created out of thin air, that each transaction is valid, that the platform keeps accepting all new transactions and treats each transaction equally, etc. The more miners and the more nodes that join the Bitcoin network, the more sovereign the Bitcoin Blockchain is.

Today the Bitcoin mining network consumes more than 60 TWh of electricity a year which is significantly more than the total electricity production of the largest hydroelectric dam in the United States. Often this exorbitant electricity consumption is cited as a criticism of the Bitcoin Blockchain because of its environmental impact. I believe those criticisms are misplaced: the Bitcoin Blockchain's value to society is proportional to its electricity consumption. If the Bitcoin Blockchain did not consume any electricity it would not be sovereign and it would be worthless. Only if you believe that society does not get any value from having a sovereign platform can you be correct to assume that the Bitcoin Blockchain electricity consumption is an enormous waste.

The Bitcoin Blockchain is secured, to an important degree, by the bitcoins that the miners earn. If you were to remove the bitcoins, most miners would stop mining and, therefore, the Bitcoin Blockchain would not be robust and not sovereign. In corporate circles, especially in financial institutions, it has become fashionable to say "I am interested in the Blockchain but not in Bitcoin", which is the same as saying "I am interested in the web but not interested in the Internet" (remember Intranets?), not understanding that the web could not exist without the Internet. The only innovation of the Blockchain is it's sovereignty, the only sovereign Blockchain so far is the Bitcoin Blockchain and the fuel that keeps it sovereign is the Bitcoin currency. Saying "I am interested in Blockchain but not Bitcoin" is an oxymoron.

If a group of people wanted to take away the Bitcoin Blockchain sovereignty today they would not only need an extraordinary amount of capital and the capacity to develop specialized mining hardware in very large quantities, but they would also need access to the equivalent of the United States largest hydroelectric dam for an extended period of time. That would be hard to do but not impossible. Every day that goes by it gets even harder to “break” the Bitcoin Blockchain sovereignty. The Bitcoin Blockchain sovereignty has been attacked in the past (in fact, one of those attacks found me on the wrong side of history and that is how I painfully learned many of these lessons, but that’s another story...) and so far it has always survived intact. We can expect the Bitcoin Blockchain sovereignty to come under attack from more and more resourceful bad actors, coalitions of bad actors or even from nation states eventually. Only time will tell if Bitcoin is truly sovereign or not.

#### 6- Where can a sovereign platform add value?

It is a lot easier to see where the Bitcoin Blockchain will not add any value. For any Blockchain to add value it has to take advantage of its sovereignty and be the ultimate arbiter of truth: nothing has to be able to contest it or change it. For any use case in which the Blockchain information can be contested or changed by a government, by a registrar of deeds, by a court, by the police, any other entity or group of entities it does not make sense to use a Blockchain. In each one of those cases it would be easier, better and faster for each one of those entities to simply run their own system, letting other parties access them with an open protocol, maybe making the databases public too and perhaps using tokens that can go to other systems if needed. Running a sovereign Blockchain is expensive, not only in terms of electricity, a sovereign system pays a high price in terms of transaction throughput, data storage capacity and flexibility in order to remain sovereign. Any user of a Blockchain who is not taking advantage of its sovereignty is wasting resources and running a very sub-optimal system for no reason.

Claims that the Blockchain can solve property titles, securities settlement, supply chain management, the authenticity of works of art and many other similar cases are misplaced. It is true that the systems that we are using today in all of those cases are old, antiquated and inefficient. And it is true that all of those cases involve many stakeholders that use different data formats and transaction protocols that are often proprietary, but all of those problems would be better solved if those stakeholders agreed to use open standards and if they used better technology. Most often the word “Blockchain” is being used by consultants who want to scare their corporate customers into buying new technology projects, or by executives at those corporations who do not yet understand the Blockchain but understand that they may get the budget they want if they say their project is using “Blockchain”, or by entrepreneurs who think they are more likely to get the funding or press coverage they want if they add the word “Blockchain” to whatever they are doing.

So, where does a sovereign platform add value? In use cases where the Blockchain database can be used as the uncontested ultimate arbiter of truth. As an example, an identity system may benefit from a sovereign platform. All of us as consumers would rather not keep all of our identity information (full name, social security #, date of birth, contact information, name of our parents, name of our spouses and kids, our address, passport information, payment information, etc.) on our phones which can be easily hacked, but we also do not want to give all that information to a single company or to our government. A sovereign system that no one can corrupt or control that will keep our information safe and will ask us every time someone wants a piece of our information may make sense. With this example I am simply trying to be creative and guess one possible use case, I am sure we will be surprised by creative and revolutionary entrepreneurs coming up with use cases that take full advantage of a sovereign platform and that we cannot imagine right now.

There is a use case that makes a lot of sense and that it is already working quite well. That is to use this sovereign platform to run a global system of value and settlement. Bitcoin, the currency, is taking advantage of the Bitcoin Blockchain to create a system in which:

- 1) There will never be more than 21 million bitcoins. This seems simple but, until the Bitcoin Blockchain platform came along, it was not possible to have a system in which you could be certain more units could not be created without trusting someone else. Now you can be certain that there will never be more than 21 million bitcoins.
- 2) Bitcoin is uncensorable. No one can change a transaction in the Bitcoin Blockchain and no one can keep the Bitcoin Blockchain from accepting new transactions. This also seems simple but, until the Bitcoin Blockchain platform came along, it was not possible to have a system in which you could be certain that you were always going to be allowed to transact without trusting someone else. Now you can be certain that you will always be allowed to transact in this system.

### 7- What does a global system of value and settlement mean?

Civilization has had different systems of value and settlement.

Today the closest we have to a global system of value and settlement is the US dollar and the SWIFT payment network, in the past other world power currencies have been the global system of value and, before that, gold was the system of value and settlement for two thousand years..

Bitcoin is potentially superior to gold and to the US dollar as a global non-political standard of value and settlement because there will never be more than 21 million bitcoins and because Bitcoin is open and uncensorable. There will never be more than 21 million bitcoins because it runs on a sovereign platform so no one can change or inflate that number. Additionally, Bitcoin is uncensorable because it runs on a sovereign platform so no one can change the transactions that already exist in the system and no one can keep the system from accepting new transactions. This allows for unprecedented economic freedom in the same way the internet

allowed for unprecedented freedom of information. Gold has the advantage that it is tangible and many people (especially older people) strongly prefer something that they can touch. Gold also has in its favor that it has been around for over 2,000 years, and it may be impossible for Bitcoin to match that history and reputation. The dollar has the advantage that it is already easily understood and accepted globally and it is a platform with remarkable network effects. These qualities may be too much for Bitcoin to overcome. Or it may be that we collectively come to appreciate the advantages of a digital unit that cannot be inflated or censored. Only time will tell.

Bitcoin is not an asset. It does not produce earnings or dividends and it does not generate interest. And Bitcoin has no intrinsic value. Bitcoin is simply money and most forms of good money have no intrinsic value. Gold, the US dollar and national currencies do not have any intrinsic value either but because they have had a monetary value for a long time most people perceive them as being intrinsically valuable, which is a big advantage. The main hurdle Bitcoin has to clear to become successful is to develop a similar widespread social perception of value and achieving that is quite an ambitious goal.

#### 8- What does a world in which Bitcoin succeeded look like?

If Bitcoin succeeds it will most likely not replace any national currency. It may be a supranational currency that exists on top of all national currencies. If Bitcoin succeeds it may be a global non-political standard of value and settlement.

The world already has a global non-political standard of length in the meter, and a global non-political standard of weight in the kilo. Could you imagine a world in which we changed the length of the meter or the weight of the kilo regularly according to political considerations? Yet that is what we are doing with our standard of value. Today we use the US dollar as a global standard of value which is much better than nothing but quite imperfect: it has lost significant value since inception, it is hard to know how many dollars will be outstanding in the future and, increasingly, the ability or inability to use it as a platform depends on political considerations. The world would be much better off with a global non-political standard of value.

The same is true for a global non-political standard of settlement. Only banks can participate in most settlement networks (like SWIFT, Fedwire, ACH in the US, CHAPS in the UK, SEPA in Europe, Visa and Mastercard, etc). Individuals, corporations and governments can only access these settlement networks through banks. Using these settlement networks takes time (sometimes days), the process is opaque and costly and, increasingly, the ability to use them is determined by political considerations. Imagine an open platform where any individual, corporation or government could settle with any other individual, corporation or government anywhere in the world, in real time, 24/7 and 365 days of the year. This would do for money what the Internet did for information.

In a world in which Bitcoin succeeds all currencies may be quoted in satoshis (the smallest fraction of a Bitcoin). When your granddaughter asks what the price of the New Zealand dollar is she may receive an answer in satoshis: the New Zealand dollar is 72 satoshis today. And the price of the Turkish Lira? 21 satoshis today. The US dollar? 107 satoshis today. A barrel of oil? 5,600 satoshis today. Global GDP? 97,356,765 bitcoins. The GDP of Indonesia? 1,417,007 bitcoins. The reserves of the South African Reserve Bank? 53,230 bitcoins. You get the idea. Then all of these values would be easily comparable across time and across geographies.

When your granddaughter asks “Grandpa, how did you guys keep track of all these things when you did not have Bitcoin?” your answer will be “We used the US dollar”. Then she may ask “Really? But isn’t that the currency of the United States?” after you say yes she may ask “And how did you keep track of the US dollar?” to which you will say “Well... mostly in Euros, sometimes in Yen, Swiss Francs or other currencies depending on what we were talking about”. She may think we were weird.

### 9- Why not another cryptocurrency instead of Bitcoin?

There are about 1,000 cryptocurrencies that have at least one transaction a day. So why Bitcoin and not any one of those other ones? Close to 100 million people own Bitcoin and over 1 million people become new owners every month. The other 1,000 cryptocurrencies have less than 5 million owners combined, so Bitcoin will add more users in the next 5 months than those 1,000 cryptocurrencies added in their combined history. Bitcoin is moving over \$1 billion a day which is also more than all the other cryptocurrencies combined.

The most important metric of all, though, is how much can we trust these platforms or how sovereign they are. The measure of how sovereign these platforms are is the square of the computing power they have. If we use electricity consumption as a proxy of the computing power each of these platforms have, all of those 1,000 cryptocurrencies combined have less than 1% of the Bitcoin Blockchain processing (mining) power so none of them is (yet) really sovereign and in many cases their code is controlled by a person or a small group of people. New technologies may achieve sovereignty without relying on processing power and that may seriously challenge the Bitcoin Blockchain. But if those technologies do not get developed or it takes too long it may be difficult to unseat the Bitcoin Blockchain.

The Bitcoin Blockchain is an open protocol, not a company. The history of protocols is very different from the history of companies. In the history of companies there is a lot of change, disruption and churn (Microsoft-Apple, eBay-Amazon, Altavista-Google, MySpace-Facebook, etc.). However, the history of protocols is very different. Once a protocol gets established it almost never changes. For example, we are using IP (Internet Protocol, or just “the Internet” colloquially) for almost all transport of data (until the late 90s cisco routers used to route dozens of protocols, today they only route IP). We are using only one web protocol and only one email protocol. The email protocol, for example, is quite simple and limited. At the protocol level there is no way for me to know if you received my email, much less if you read it, there is no way for

you to verify my identity when you receive my email, there is no way to handle spam and many, many other things that could be easily fixed at the protocol level today. I am sure some people have already developed much better email protocols, but we never heard about them and most likely we never will: once a protocol gets established it becomes the only protocol for that use case and it is very hard to displace it with a better protocol. Right now it looks like the standard protocol for a sovereign platform will be the Bitcoin Blockchain.

Many interesting technologies and applications that are being tested with other cryptocurrencies and other Blockchains and, if they are successful, they may be implemented on top of the Bitcoin Blockchain. It is not efficient to invest massive amounts of new hardware and electricity to replicate sovereignty when we already have a most solid and robust sovereign Bitcoin Blockchain. It is more efficient to simply build on top of it. For example, the Bitcoin Blockchain is limited in that it can only process approximately 3,000 transactions every 10 minutes, you have to wait 10 minutes for the transaction to be recorded in the Blockchain and up to 1 hour if you want to make sure it is irreversible. And you have to pay anywhere from 5 cents to 50 cents in transaction fees for the miners to process your transaction. The Lightning Network takes advantage of the robustness of the Bitcoin Blockchain and it works as a “Layer 2” solution on top of the Bitcoin Blockchain, enabling thousands of transactions per second of as little as 1 satoshi (\$0.00004), for free and in real time. Similarly, other early examples of Layer 2 solutions that work on top of the Bitcoin Blockchain are RSK which enables the full functionality of Ethereum but on top of the much more robust Bitcoin Blockchain. Liquid is an open source wholesale settlement network developed by Blockstream that operates on top of the Bitcoin Blockchain. There are many more examples of technologies being developed to take advantage of the sovereignty and robustness of the Bitcoin Blockchain and enhance its capabilities by building on top of it.

#### 10- How can Bitcoin fail?

Bitcoin can fail in many different ways. It could be taken over by a bad actor. It could be displaced by a better platform. It could be hacked. And Bitcoin can probably fail in many ways that we cannot imagine yet. Because Bitcoin does not have any intrinsic value, and because its value depends on a social consensus which is a sort of collective delusion, in my opinion, the most likely way in which Bitcoin could fail is a price panic. If we all decide at the same time that Bitcoin is worthless, then it will be worthless. It is a self-fulfilled prophecy. If the price of Bitcoin were to plummet to zero or near zero, even if the platform remained intact, its reputation would suffer immensely and it could take a generation to rebuild that credibility. This could happen if people buy amounts of Bitcoin they cannot afford to lose, for example if people invest their retirement funds or their kids' college funds into Bitcoin, and as the price goes down they are forced to sell, pushing the price further down and forcing others to sell. So, in my opinion, the biggest risk to Bitcoin is people investing amounts they cannot afford to lose.

Most of the capital invested in Bitcoin today seems to be capital that people can afford to lose. That is not because people are wise, or because the regulators have been very effective or that

the industry has been prudent. The only reason why most people today do not have an amount of Bitcoin they cannot afford to lose is because of Bitcoin's price volatility. Ironically Bitcoin's price volatility is the best insurance against Bitcoin's biggest risk. If Bitcoin is perceived to be a safe asset before it has matured and people begin to allocate capital they cannot afford to lose we should be concerned. This happens to some degree during every Bitcoin price rally but, fortunately, so far each rally has corrected without destroying Bitcoin, but one day that could not be the case.

After 10 years of Bitcoin working well without interruption more concerning than a complete failure is a scenario where Bitcoin does not fail but it becomes irrelevant. Something similar to what happened to the BitTorrent protocol, which still exists but is less and less relevant as the real revolution in digital file sharing and entertainment happened through Dropbox, Spotify, Netflix, and many others. Similarly, there is a chance that Bitcoin does not fail but that it never becomes mainstream, that it is only used by a group of believers and fanatics but not much more beyond that. That could happen because financial institutions, governments, and regulators manage to keep Bitcoin separate and ostracized from the rest of the financial world, like a non-convertible currency, but it could also happen even if financial institutions, governments, and regulators keep going on their current path of enabling Bitcoin to be fully connected to the financial world. If Bitcoin never becomes mainstream bitcoins will still have a price but most likely lower than what it is today. In my (subjective) opinion the chance of this happening is 30%.

### 11- Bitcoin's price action

Bitcoin launched in January 2009 but it did not have a price until July 2010 when it began to change hands informally at \$0.05 cents per bitcoin. In November 2010 Bitcoin had its first price rally that took the price to a peak of \$0.39 cents to then "crash" to \$0.19 cents. The price was at its peak of \$0.39 cents only very briefly and the volume on prices near \$0.39 cents was negligible, for most casual observers the rally simply took the price of Bitcoin from \$0.05 cents to \$0.19 cents, an increase of 280%, but most of the commentary at the time focused on the Bitcoin "crash" of over 50% from \$0.39 to \$0.19 cents. This exact same story has repeated itself 6 times in Bitcoin's history so far. There have been 6 of these rallies in Bitcoin's 10-year history and in between the rallies the price of Bitcoin has traded sideways or downward for months or years at a time. During most of Bitcoin's 10-year history, the press has been commenting and worrying about Bitcoin's latest "crash". How can something that constantly crashes go from \$0.05 cents to \$11,000 you ask? If you want something to go from \$0.05 cents to \$11,000 and fool everybody into believing that it is failing, do it with as much volatility as possible.

The second Bitcoin price rally happened in February 2011 and it took the price of Bitcoin over \$1.00 for the first time to then "crash" to \$0.68 cents. The third rally happened in August 2011 and it took the price of Bitcoin to \$29 to then "crash" to \$2. The fourth rally happened in April 2013 and it took the price to \$230 to then "crash" to \$66. The fifth rally happened in December 2013 and it took the price to \$1,147 to then "crash" to \$177. The 6th (and currently last) rally

happened in December 2017 and it took the price of Bitcoin to \$19,783 to then “crash” below \$3,200 (and until this bear market is over we don’t know how low it may go).

The Bitcoin price rallies are the most important feature of how Bitcoin propagates, how people spread the word and how more people want to own it. It is a risky mechanism, so far it has worked well but it could lead to a disaster one day. The Bitcoin price rallies are Bitcoin’s best moments but they are also its most dangerous and vulnerable moments.

Every Bitcoin bear market is about working out the excesses of the rally. During the rally too many people buy too many bitcoins thinking that they will be able to sell them for a big gain very soon and that usually does not happen. Imagine a fruit tree that has some good fruit and some rotten fruit. The Bitcoin bear markets resembles periods in which the tree is shaken until all the rotten fruit has fallen to the ground. Every time the tree is shaken some rotten fruit falls to the ground. The Bitcoin tree is shaken by the price going down and by letting time pass by. The more the price goes down and the more time passes without another rally the more people give up their original expectations, they sell, they adjust their exposure and their expectations. Eventually, no matter how much you shake the tree there is no more fruit to fall to the ground and the market may be getting ready for another rally.

I believe that, if Bitcoin succeeds, Its price may do another 6 of these rallies over the next 5 to 7 years. Anyone who tells you that they know what the price of Bitcoin will be next week, much less next year is either ignorant or outright lying to you. It is not possible to know when the price will hit bottom or when the next rally will come and the penalty for trying to time the bottom or the top and getting it wrong can be much higher than the money you were trying to save. If you decide to buy Bitcoin simply decide what is the amount of money you can afford to lose (ideally less than 1% of your net worth), deploy it at market and at once and forget about it for 5 to 7 years. I have been giving this advice for 6 years and, by watching what people do with this advice, I can tell you that “Forget about it for 5 to 7 years” is the most difficult part of the simple recipe I am proposing. This lack of discipline destroys a lot more value than you would anticipate. The price volatility rattles people and makes them trade. If the price goes down a lot they want to buy more to reduce their average cost or they want to sell to stop losing. If they buy more they end up with more than they can afford to lose so they care even more about the price volatility, if they sell they don’t have the exposure when the price goes back up, etc. Even worse: when the price goes up 10 times they decide to sell to rebalance because now Bitcoin represents too much of their net worth and it is too risky but it is not possible to double your portfolio with a 1% exposure if you rebalance it every time it multiplies by 10. If you think this may happen to you, I suggest you invest in two buckets: keep one bucket that you will not trade for 5 to 7 years, and another bucket that you will trade as much as you want (but be responsible and be sure that both buckets combined add to an amount then you can afford to lose).

12- Why do I believe 1 Bitcoin may be worth \$1 million in 5 to 7 years?

How much a Bitcoin may be worth if Bitcoin succeeds is pure speculation. Today Bitcoin is worth a total of ~ \$200 billion (~ 18.5 million bitcoins in circulation x ~ \$11,000 per Bitcoin). If Bitcoin ever becomes the world's standard of value and settlement it may have to be worth more than gold and less than the world's narrow supply of money. All the gold that has ever been mined is worth ~ \$10 trillion and the world's narrow supply of money is ~ \$40 trillion. If Bitcoin is ever worth as much as gold each Bitcoin would be worth ~ \$500,000, and if Bitcoin is ever worth as much as the world's narrow supply of money it would be worth ~ \$1 million.

My preferred way of guessing how the price of Bitcoin may evolve is much more prosaic. I have noticed over time that the price of Bitcoin fluctuates around ~ \$7,000 x how many people own bitcoins. So if that constant maintains and if 3 billion people ever own Bitcoin it would be worth ~ \$21 trillion (~ \$7,000 x 3 billion) or \$1 million per Bitcoin.

### 13- In closing

Bitcoin is a fascinating experiment but it is still just that: an experiment. As such it still has a chance of failing and becoming worthless. In my subjective opinion the chances of Bitcoin failing are at least 20%. After 10 years of working well without interruption, with close to 100 million holders, adding more than 1 million new holders per month and moving more than \$1 billion per day worldwide, it has a good chance of succeeding. In my subjective opinion the chances of Bitcoin succeeding are at least 50%. If Bitcoin does succeed, 1 Bitcoin may be worth more than \$1 million in 5 to 7 years. That is 100 times what it is worth today (at the time of writing the price of Bitcoin is ~ \$11,000).

I suggest that a \$100,000 portfolio should invest at most \$1,000 in Bitcoin (up to 1% but not more as the risk of losing this investment is high). If Bitcoin fails, this portfolio will lose at most \$1,000 or 1% of its value over 3 to 5 years, which most portfolios can bear. But if Bitcoin succeeds, in 5 to 7 years those \$1,000 may be worth more than \$100,000, more than the value of the entire initial portfolio.

In today's world it is hard, if not impossible, to find an asset that is possibly so mispriced and where the possible outcomes are so asymmetrical. Bitcoin offers a unique opportunity for a non-material exposure to produce a material outcome.

I recommend that you open an account at any reputable Bitcoin wallet ([Coinbase](#), [Square's Cash App](#), [RobinHood](#), [Revolut](#), [Paxos](#), [BitGo](#), [Abra](#), [UpHold](#), [Luno](#), [Kraken](#) or many others) buy a small amount of Bitcoin you can afford to lose and keep it there for at least 5 years. If you don't want to open a Bitcoin wallet and want to use your existing brokerage account instead you can buy Greyscale's Bitcoin Trust ([Ticker GBTC](#)).

It would be irresponsible to have an exposure to Bitcoin that one cannot afford to lose because the risk of losing the principal is very real. But at this point not owning any Bitcoin is also irresponsible and lazy.

## Further reading:

- [“Shelling Out: The Origins of Money”](#) Essay by Nick Szabo. Essential background on the nature of money.
- [“An \(Institutional\) Investor’s Take on Cryptoassets”](#) Essay by John Pfeffer. Bitcoin analysis from an investor’s perspective
- [“Bitcoin is Digital Gold - The Ideal Treasury Asset”](#) by Michael J. Saylor
- Square Inc [“Bitcoin Investment Whitepaper”](#)
- Fidelity’s [“Bitcoin Investment Thesis”](#)
- [“The Bitcoin Standard”](#) book by Saifedean Ammous. Non technical explanation of Bitcoin and what it may become.
- [“Mastering Bitcoin”](#) book by Andreas Antonopoulos. Technical explanation of Bitcoin for non-technical people.
- [“Programming Bitcoin”](#) book by Jimmy Song. Technical explanation of Bitcoin for technical people and programming guide.
- [“Bitcoin bites the bullet”](#) Essay by Nic Carter about Bitcoin's design trade-offs.
- [“The Last Word on Bitcoin’s Energy Consumption”](#) by Nick Carter
- [“2020: Reason Enough to Take Another Look at Bitcoin”](#), by Mat Balez