TAKING THE ORANGE PILL

What the Average Person Should Know about Bitcoin

BY

MARIO CANTIN

 TAKING THE ORANGE PILL First edition. December 12, 2021. ISBN: 979-8201046002 Written by Mario Cantin.

Preface

The purpose of this book is one-fold: it is to try and place a single thought at the forefront of your mind.

It's a public service, which is why the book is free, except on platforms which do not allow for free books. Where that is the case, it is available for the lowest possible price allowed.

I'm not writing about new concepts. I'm not even trying to prove what I'm saying. I'm placing this single thought in your plain view for you to consider. All the information related to it is freely available on Crypto Twitter, YouTube, podcasts and blogs, ad infinitum. The rabbit hole for you to jump into, should you choose to, is deep.

Of course, I'll expand on that single concept, otherwise, the writing would not constitute a book. It would be the equivalent of a single tweet. The reason why I'll fill the pages herein is for your convenience, to help contextualize that single thought, which is:

BITCOIN MAY BE MORE IMPORTANT TO YOUR PERSONAL FUTURE THAN YOU HAD ASSUMED.

It needs to be mentioned that, while crafting this book, my aim has been to keep my writing to the point, even at the expense of style.

Chapter 1

You keep hearing about Bitcoin. You're pretty sure you know what it is: it's a digital currency used as a form of payment or a way to store value. And you even grasp that it's sort of important. You're open to owning some, but you haven't yet acquired any.

However, if we are to uncover what is so imperative about owning this emerging asset, we'll need to delve deeper into Bitcoin's anatomy. If I do a good job of peeling the onion for you in the following pages, you may notice that your sense of urgency about buying BTC -- as we commonly refer to it -- grows exponentially.

First of all, have you recognized that when you discuss Bitcoin with some individuals, they are skeptical about it and are willing to go to great lengths to convince you to stay away?

Their reaction is typically human and it is not so much directed at Bitcoin per se, but rather, at change in general.

You can run an experiment. Dream up a bold daring move that would introduce a big departure into your regular life, and go tell friends and family members about it. Then pay attention to how many of them are quick to talk you out of your new endeavor. Perhaps even, if you'd be willing to dig into your own psyche, you'd discover that you also have a similar inclination, whether you'd go as far as let it manifest or not.

Now, imagine you are in Detroit, near Bagley Avenue. The year is 1896. Henry Ford is riding his newly-built horseless carriage -- the first automobile. For centuries, societies have been using horses for transportation. Horses are deeply ingrained in the culture. Your father has one, and so do all your uncles, neighbors, and so forth. You've just fed and cleaned the horse this morning, as a matter of fact. You dream about owning your first horse and you can't wait to be old enough to finally get one. And now, Henry Ford is testing his Quadricycle in plain

daylight, in your neighborhood. He's being laughed at and derided. Freddy, your uncle, just shouted out loud, "Go get a horse!" At the dinner table this evening, the subject is going to come up, and the adults are going to have a good laugh about it as they gobble their malt liquor.

Well, as we all now know, Henry Ford was right. He changed the world, and he had the last laugh. But he introduced a paradigm shift into culture that exceeded the human tolerance threshold for change.

We could argue the same thing is currently happening with Bitcoin.

It's a breakthrough in computer science which, for the first time in history, makes certain fundamental socio-economic changes possible. Understanding what that shift is, however, requires you to take the time to learn more deeply about Bitcoin and to revisit some of your assumptions about money. Hopefully, I'll be making this part easier for you in this short book.

Chapter 2

Foresight. What does it take to develop this elusive skill?

In the example I gave in the previous chapter, what would it have taken for you -- or me -- to be so sharp with our wits that we would have grasped what was going to take place in the future? And would we have had sufficient conviction in our belief to invest at least a modest sum of money in the emerging technology -- in this case Bitcoin – just as an insurance policy in case the car eventually did indeed replace the horse?

Let's face it, we would probably have failed to see it. It's always much easier to appreciate the situation in hindsight. And we wouldn't have been alone either in our lack of clairvoyance. Many businesses have failed to have foresight. You may be old enough to remember Blockbuster Video. They were a giant in the 1990's. Reid Hastings, co-founder of the then nascent Netflix company, offered Blockbuster the opportunity to acquire his budding enterprise, which he suggested would likely become the format of the future for movie consumption. They laughed him out of the room, so of course they didn't take the offer. They weren't open to the possibility that he'd be right. Well, Netflix incinerated Blockbuster Video to the ground in the years that followed. On the other hand, Jeff Bezos, Elon Musk and Zuck -- to name but three -- have demonstrated foresight. The empires they have respectively built bear witness to this fact.

It's difficult to see what's coming our way. However, understanding important distinctions about a particular topic can help you predict certain outcomes.

If you decided to learn how to play hockey, what skills would you need to eventually excel at it? Ok, you'd need to learn to skate really well. You'd need some physical strenght. You'd need some teamwork savvy -- you get the idea. So you spend a few years working on acquiring and honing those skills and soft assets. But even then, you still perhaps haven't excelled yet. Your skillset is matched by your opponents and you can't surpass their effort by an adequate margin… that is until the day when you finally understand the game and your

opponents enough that you stop following the puck around and, instead, *you start skating ahead to where you think the puck will be in a few seconds from now*. And, should you turn out to be right more often than not, then you'd at last become the high-level player that you had wanted to be. The other players would have no idea how you were doing it.

Well, in the Henry Ford example given earlier, the dollar is the horse. Bitcoin is the automobile. To the degree that you can -- and are willing to -- exhibit the foresight necessary to skate to wherever the Bitcoin puck will materialize, you and your descendants could end up in a better position to fare well, in the event that Bitcoin does become the monetary way of the future.

Chapter 3

What's wrong with the current financial system?

Did you know that for the entire economy to "function" it needs to run on debt as its primary engine? In other words, the building block of how humans have engineered their economies is based around the idea that many, many people, businesses, and countries must continually be in debt in order to avoid the entire house of cards from falling down on itself.

Let that sink in for a moment.

Before we dive into it any deeper though, let's first make sure we understand what money is at its most basic essence.

To put it in the simplest way possible, money stands for things. You have something that I want. I'm not going to carry livestock with me to pay you, right? I need a token that symbolizes my purchasing power. Nothing more, nothing less. Currencies were created by communities for communities in the beginning. *Government intervention is not a prerequisite of money*. In Africa, for example, glass beads were used as money. At one point, Roman soldiers were paid in salt. Russians used squirrel pelts as currency during the Middle Ages. Today, only gold and silver largely remain of these commodity-based monies.

At its purest essence, a currency represents produced goods or rendered services. Let's say people lived in a large village centuries ago, and sea shells happened to be rare in that locale. So they could have chosen the latter as their denominated currency. It would have worked just fine as the basis of their monetary system if everyone in the village had agreed that seashells were a suitable medium of exchange. Price discovery would have occurred naturally within the community. For example, a dozen eggs costs 1 shell. A live lamb costs 20 shells, etc. Money, as described here, is nothing more than an intermediary of exchange. This is another way of saying that I don't need to bring my lamb to your egg store. It would be a

pain to have to carry the animal, plus you may not want lamb in the first place. But I want your eggs, so I bring along 2 shells and I buy 24 of your eggs with them. And you now have some purchasing power in your pocket to be spent or conserved, at your discretion.

If nothing extraneous is added to the above explanation, we have what we call "sound money". However, over the centuries, money has transformed to become "unsound money." Goldsmiths used to store people's gold in exchange for a fee. They essentially turned themselves into bankers when they caught on to the idea that they could issue more gold-denominated paper notes than they actually had gold in reserves, since most people would leave their gold permanently in their custody. It was much easier to simply exchange the gold-denominated notes from one person to another within the society than transferring actual gold between parties. By issuing more paper notes than there was gold and offering them as loans, they created debt money that they could collect interest on, thereby introducing the precursor to today's debt economy. Another contributor to currency debasement has been when governments gradually began to contrive in monopolizing money. In the process, they destroyed free markets through banking intervention and meddling with the principles of sound money creation.

The ensuing "innovations" have had detrimental effects, for example:

- Fractional-reserve banking

This term describes a way for banks to artificially inflate the money supply by retaining only a percentage of deposits in their "vaults" -- often 10% -- and then lending out the rest.

You've read correctly: when you bring your $1,000 to the bank for safekeep, there's only typically $100 that will be put aside for you as reserves in case you come and claim it back. To explain it in simplistic terms, when too many people come to get their money out all at once, the bank becomes insolvent and that's

referred to as a bank run. Because a sufficient number of people leave enough of their money in the banking system at all times, the system (typically) does not collapse.

The side effects of fractional-reserve banking inflict damage to an otherwise healthy economy. Let's create an exaggerated fictitious scenario to illustrate the point. After making your $1,000 deposit to your bank of choice, $900 may be lent to Suzy to pay for her college tuition. When the learning institution deposits the $900 at their bank, $810 of it is lent to Steve as a deposit on a truck lease. When the vehicle dealership deposits the $810 at their bank, $729 is lent to Marissa to replace her broken baby stroller. When the baby supply store deposits the $729… you get the idea. It takes a staggering 113 transactions in this theoretical and over-simplified case study to run the cycle to its full course. At the end of it, your initial $1,000 became $10,028.60. In other words, the banking system manufactured over $9,000 of debt inventory that they collect interest on. The fictitious money that they've created out of nothing got added to the economy's total money supply in excess of the money that represents actual production of goods and services. Prices inflate as a result and the currency's purchasing power decreases for everyone throughout the entire society. Ever wondered why so many people finish their under-grad or graduate degree, get a job, but still can't afford a home? That is wealth redistribution at work. Through something called the Cantillon Effect, a form of regressive tax takes place. I invite you to look up any terms presented herein, but essentially the rich are getting richer, and the middle class poorer. Inflation is legalized theft, *and it is you who is being robbed*.

The benefits of stimulating economic growth that come with fractional-reserve banking could also be had with the implementation of full-reserve banking. However, it will take external disruptive factors to force the banking system to make such a transition. In the meanwhile, this is how we got to a money supply that is largely debt-based, and only marginally currency-based. It's a form of money "engineering" that requires that the population mostly remain in debt for the entire house of cards not to cave in. Ask yourself, "If I don't benefit from that, then who does?" *And that's who's controlling you*.

- Central banking

Now get this: the United States of America does not issue its own currency. "Wut!?" you exclaim. That's right. The Federal Reserve Bank is the sole issuer of the US Dollar. That is why it says "Federal Reserve Note" at the top of a US dollar bill. The Fed's existence was planned in great secrecy in 1910 on Jekyll Island -- a private club for the ultra-wealthy, at the time. The seven men who conducted the meeting all carried duck hunting gear to mislead potentially curious reporters into believing the event was nothing more than a hunting expedition. They subsequently denied having had the meeting until the 1930's, when they no longer could hide the fact. It was a deception of the American public they resolutely wanted to keep under wraps. They set their agenda into motion on Jekyll Island, and their plan eventually came to fruition when Congress quietly enacted the Federal Reserves Act in 1913. The name was chosen after careful deliberation to make it appear as though the Federal Reserve Bank was part of the government. It is not. Just like everyone grasps that Federal Express has nothing to do whatsoever with the government, it should be understood that the Federal Reserve is not in any way a branch of the U.S. Government. *It's nothing more than a bank cartel which has empowered itself with the ability to enslave the U.S. Government with debt.* Instead of directly issuing currency, the U.S. Government must issue U.S. Treasury bonds, which it trades for Federal Reserve Notes from the Fed. *And every year, the U.S. Government must pay hundreds of billions of dollars in interest for a debt that need not exist in the first place*.

The Federal Reserve Bank is an opaque organization. It operates in secrecy. It has never been subjected to a comprehensive audit since its inception -- so in over a century! It accounts to no one. But it has given itself an air of legitimacy. It creates money out of thin air. The Fed has been allowed to have such powers as the ability to manipulate the US economy by means of adjusting the national interest rates as they see fit. And they also control the money supply by pumping into, or removing, trillions of dollars from the economy. They have been responsible for huge societal problems, one of them -- as per many analysts -- being nothing less than the Great Depression itself, when they unwisely continued to contract the money supply for years after the 1929 U.S. Stock market crash.

The Fed's existence has been normalized. In other words, it seems "normal" to many people. But if we look at the situation from a first principles approach -- starting with an absolutely fresh, logical viewpoint -- it begs many questions. Another way of saying it would be, let us say, you are an alien landing on Earth, trying to grasp our world's socio-economic architecture. The first thing you might say to yourself is, "Wow, who set up this scam?"

Now, over a century later, there are undoubtedly individuals who work at the Federal Reserve Bank who believe they are on the right side of history and are helping the economy through the policies they help put in place and enforce. This doesn't mean the Fed as an institution isn't built on quicksand, though.

- Fiat paper money

Over the centuries societies have been made painfully aware that excessive currency issuance will inevitably lead to inflation -- an undesirable outcome. For this reason, simple guardrails were installed at some point in time as a preventive measure. This mechanism was called the Gold Standard. It meant that an actual physical quantity of gold constituted a limit as to how much paper money was allowed to be in circulation at any given moment. In other words, the currency of a gold-standard-operating country was backed by gold. Putting such an elementary rule into effect would remove the temptation of issuing money without restraint. It was successful in keeping inflation or deflation -- another unwanted situation -- in check. A convoluted series of events resulted over time in all countries eventually transitioning to what is called a fiat monetary system. This is a form or currency that is not backed by a commodity such as gold or silver. It has no inherent value other than having been established as legal tender by the government (or more accurately, the central bank) that issues it. It cannot be presented in exchange for its corresponding value in gold, as was the case under the gold standard. It has value within society as long as people retain their faith in it. Fiat currency allows governments to more easily meddle in the economy. Instead of letting business cycles run their course -- much like forest fires are natural factors that play an important ecological function -- governments collude with central banks to alter the money supply, aiming to manage financial crises in

hopes of minimizing their impact. That might be a noble cause, were it not for the simple fact that it's all too easy to make matters much worse.

Fiat currencies lose their purchasing power through inflation, and can even become absolutely worthless when subjected to hyperinflation -- in other words, when they are worth even less than the paper they're printed on!

- The World Bank / IMF

The World Bank and the International Monetary Funds are joint-at-the-hip institutions that share a stated goal of reducing global poverty. Their individual mandates are different and yet complementary to one another. They provide loans to underdeveloped countries on which certains "restructuring" conditions are imposed. The risk is that such macroeconomic interventions can all-too-easily occasion worsening conditions. For example, say the IMF has lent money to a country that now experiences a minor economic slowdown. In this illustration, the IMF demands that the country in question be increasing their interest rates and exerting fiscal restraint with the aim of reducing the budget deficit. But it backfires and the country now plunges into a severe recession. Again, we have to ask ourselves, if the IMF or World Bank demands of a country -- in yet another example -- that large-scale privatisation of its public assets occurs and the outcome does not benefit that country, then who does it benefit? Find the real answer to that question and you'll know who controls that country's circumstances.

- The dollar hegemony

The United States leveraged the advantages it had gained during WW2 over Britain to make its dollar the world's currency. Even when it fell off the Gold Standard for good in 1971, it had gained enough trust globally to see its value-less fiat currency remain the international default. [Note: I'm glossing over details

here for the sake of conciseness.] And should poorer nations have challenged the US dollar's global hegemony -- also referred to as "The Exorbitant Privilege" -- they would have likely been the target of economic sanctions, CIA-backed operations, or even downright bombing campaigns. But we live in a new era now, and global sentiment toward the US has been on the decline. Countries have begun to enter into bilateral agreements with one another to move away from the US dollar. And with the recent advent of digital currencies and their imminent decreed implementation by China, reportedly even Russia (and who knows who would be next), a likely chain of events could be triggered in which the US, having greatly diminished its production capabilities in the last 80 years, will lose its currency dominance, along with all the perks that came with it. As much as an end to the United states' dollar hegemony could be something to be celebrated, it would have devastating effects on, not only America, but on many parts of the world. So that's now a situation of being stuck between a rock and a hard place.

- Quantitative easing

QE is a recent form of financial engineering in which the central banks create money out of thin air as yet another monetary tool to stimulate economic growth when more "conventional" avenues are no longer workable, such as lowering interest rates. It's a highly dangerous hard drug. And like heroin, the end result is eventual overdose and death of -- in this case -- the economy, ultimately through hyperinflation. Former Federal Reserve Chair Ben Bernanke was quoted saying in 2014, "The problem with QE is that it works in practice, but it doesn't work in theory." It might be more correct to say that even though it may first appear to work, it clearly doesn't in the long term. The leading global central banks have reportedly injected over $25 trillion in their respective economies since 2008, with over $9 trillion as a result of Covid-19. In the U.S. alone, the money supply has expanded a staggering 250% since 2001! And it's not over, as when other crises inevitably manifest in the coming decade, the endless cycle that has been set into motion will require more and more money printing to produce an equivalent outcome -- just like the heroin junkie needs a bigger and bigger hit to achieve the same high. As per Finbold.com, the October 2021 consumer price index (CPI) for the U.S. came in at 0.9 percent, representing a 6.2 percent year-over-year increase -- the highest it's been in over 30 years. And if the index was

still measured the way it used to back in 1980 with its original formula, it would more accurately be reported as 14 percent!

Another one of the by-products of manufacturing trillions of dollars out of nothing is that this capital becomes an enabler for many possible outcomes, at the sole discretion of those who have issued it. For example, will that money be used to buy back bad mortgages from U.S. banks? Or will it be deployed to acquire certain corporations, but not others? Will it be deployed to purchase corporate bonds or stocks? In other words, someone is adjudicating who should be helped and who should not be, as they see fit. That is the very definition of intervention and one of the catalysts of inequality. For example, while you are getting essentially zero interest on your deposits, banks are getting cheap money with which they buy back their own stock. They've concurrently been allowed to artificially boost their performance for which their executive teams have received fat bonuses.

***

In summary, governments and central banks have turned sound money into its unsound counterpart. Ideologically, their inclination of meddling with fiscal and monetary affairs are a reflection of the now prevalent school of economic thought, called "Keynesian Economics". It espouses the idea that business cycles are best managed with active government intervention. It was thought out as an explanation and solution as to how the Great Depression could have been prevented. It's a road that leads to socialism. The latter is being promoted heavily these days — while capitalism is being targeted as the cause of society's economic ills. It's the red herring of all red herrings. The real culprit is unsound money, not capitalism. Socialism's end goal is the taking away of your freedoms. It's akin to being agreeable — eager even — to be put under the care of a "babysitter" (for lack of a better word), so he or she can provide for your every need, but to soon realize that you are being controlled within an inch of your life. You can slowly become indoctrinated over many years into this type of thinking — hence the expression "boiling the frog."

There is a contrasting school of economic thought, called "Austrian Economics". It believes that the free markets left to their own devices will resolve business cycle

problems naturally. What the average person is most often not familiar with is that Bitcoin and Austrian economics share a similar ideology. That is why simply viewing Bitcoin as a digital currency misses the point as to why it provides humanity, for the first time, with incorruptible money that's impervious to manipulation by those who would otherwise be incentivized to distort the monetary supply, trigger recessions through intervention, and wage wars that they can only afford to sustain by means of unrestrained money printing.

Chapter 4

Here is a way to think about Bitcoin that does not require a computer science degree:

BITCOIN IS BASICALLY TRANSPARENT ACCOUNTING AT ITS CORE, PAIRED WITH MONATERY CAPABILITIES.

What does that mean?

Imagine that you have some extra money and are willing to invest it in the second location of a restaurant, the first location being a cool concept and always busy. The owner of the establishment assures you of its profitability. You ask to see the business' books, but can you really trust that the accounting ledger has not been manipulated?

Bitcoin is an accounting ledger that is hosted on thousands of computers around the world in such a way that the content cannot be corrupted. It's what we refer to as BTC's "immutable" property. Thus in this light, Bitcoin has been referred to as a "truth machine".

Miners -- individuals who make use of specialized computers that turn electricity into Bitcoin -- keep the network secure. Because of the careful way the incentives have been built around Bitcoin, it is in their best interest to do so. If they tried to harm the network, all value would disappear for everyone -- including themselves. They work in tandem with node operators. A node is essentially a computer that holds a full copy of the Bitcoin blockchain and verifies new transactions so they can be added to the next block by the miners. There are thousands of active node operators at any given moment. In order to erase the Bitcoin blockchain, every single one of them would need to be destroyed. This makes the Bitcoin network extremely resilient.

Because the network is not controlled by a single entity, one or few individuals seeking to game the system to gain an unfair advantage could not change how Bitcoin operates. It's pretty much set in stone.

On top of this tamper-free ledger lies the money rail. Bitcoin is a blockchain, meaning an accounting ledger -- as I've just described above. (It updates at intervals of roughly ten minutes that we call blocks, which form a chain in time, hence the term "blockchain".) But it is also a digital currency.

So there are TWO separate definitions FOR THE SAME WORD.

There will only ever be 21 million Bitcoins (the currency) issued in total. That adjudication has been built into the protocol, and good luck changing that. It's in the same magnitude of risk as fearing that Bitcoin will go to zero -- not ultimately impossible, but oh so unlikely.

Chapter 5

The power of Bitcoin is its decentralized nature. When all you have known is centralized systems -- in other words, trust in a central authority or intermediary -- it may be initially difficult to wrap your head around the fact that the Bitcoin network is independently distributed across thousands of computers worldwide. This might seem even riskier to you in some way. How safe is it to have vital information stored on regular people's machines around the world? Why would I possibly want that?

But this is the key concept to be grasped. What Bitcoin's decentralized system does is *it enables you to transact with anyone without the requirement to have to first trust them*. This is why Bitcoin is referred to as a trustless system.

Because Bitcoin's ledger becomes immutable as each block gets propagated through the network, *intermediaries are no longer required to secure currency movements*. This enables a peer-to-peer network in which you can financially transact with anyone in the world at the speed of light without the need of banks, governments, or anyone else to stand between you and the recipient or sender — as the case may be.

But more importantly, having a monetary system which operates outside the reach of central banks and governments means that the principles of sound money can be restored. The takeaway is not to debate whether these institutions ought to be reformed, but rather, to point out that some of our freedoms can be restored (as long as we can collectively seize the opportunity). Sure it is convenient to put a transaction on a credit card, having the assurance that the bank that offers the card will cancel a bad transaction and refund your money. But you are paying an enormous price for that privilege, as you suffer the effects that unsound money is having on your life. The truer question remains whether you are aware of this fact or not…

Bitcoin's decentralization offers a radically new and incorruptible architecture with which to build a more sustainable economy. It offers a window of opportunity to democratize wealth.

There is currently a democratization of power that is occurring with the advent of social media. At the push of a few keystrokes, a single voice can ignite mass protest and effect a globally-felt change. Gen Z is currently being acknowledged for claiming that power.

Much in the same way, a bottom-up (rather than top-down) social movement can occur to force a restructuring of the financial system. While such a notion undoubtedly would have seemed like an impossible dream in the past, Bitcoin is the closest thing humanity has ever had to get there with.

You hear various attacks on Bitcoin, such as accusations to the effect that it is used for criminal activities, or that it consumes too much energy. Aside from the fact that the dollar is used orders of magnitudes more for crime, and the banking system requires manyfold Bitcoin's energy output to operate, these criticisms are coming from those who have the most to lose from the advent of sound money. It's the straw man fallacy in full display.

When you encounter comments along similar lines, ask yourself whether, 1) the person has spent over 100 hours researching Bitcoin to really understand it, or 2) could the original source of the information be someone who has a vested interest in keeping the status quo?

So we once again see that Bitcoin is not merely a digital currency. For the first time in the history of humanity, its bona fide decentralized property enables a global monetary system to be established by and for the populace itself. This puts it in the league of our greatest collective advancements, along with the printing press, electricity, Penicillin, the internet, etc.

Chapter 6

The principles of sound money emerged with Aristotle over 2,300 years ago. He was a philosopher who thought deeply across multiple disciplines. He defined the characteristics of what he called “good money”:

1. Durability
2. Portability
3. Divisibility
4. Intrinsic value

In 1517, Nicolaus Copernicus, a scholar -- famous amongst other things for his writings about predicting that the planets revolve around the sun, rather than the prevalent belief at the time that Earth was at the center of the universe -- formulated what came to be known as The Quantity Theory of Money, which makes understood the relationship between the supply of money and inflation. He added “Scarcity” as a fifth characteristic of sound money and proposed gold as a sound currency.

BITCOIN IS SOUND MONEY FOR THE DIGITAL AGE.

- *Durability*. One can easily understand that a silver coin will be more durable than wheat as a medium of exchange. But it should be understood that Bitcoin is extremely durable as a digital asset. While a credit card company can be hacked and its data compromised, Bitcoin cannot be destroyed, provided that you do not lose the password connected to it (which we call the “private key”), and that out of the well-over ten thousand nodes currently in existence, at least one of them remains uncompromised -- in other words, as long as at least one instance of the Bitcoin public ledger remains unscathed. You would have to literally blow up the entire internet, and as some nodes are circulating in outer space, that would be even more problematic to execute.

- *Portability.* As you can imagine, it is not so easy to transport gold bars in great numbers. But Bitcoin is made of digital bytes, which allows you to move BTC anywhere around the world. This greatly facilitates transactions and makes Bitcoin impervious to capital controls imposed by some countries. For example China, Russia, Argentina and others prevent their citizens from taking money beyond a certain threshold amount out of their respective countries. Even in developed or non-communist nations, you'd tend to believe that you exert full control over your money, but you do not. Leave or enter your country with over 10,000 undeclared dollars, pounds or Euros -- as the case may be in your jurisdiction -- and it will get seized if you are caught.

- *Divisibility*. Bitcoin is highly divisible, which by the way addresses a common misconception. You may think that Bitcoin is "too expensive already". Well, think again as one Bitcoin is divisible into 100 million smaller units called "Satoshis" -- "Sats" for short. When the "Sats Mindset" occurs, you will no longer think in Bitcoin, but rather, in Satoshis. You don't go to a coffee shop and offer to pay in fractions of a billion dollars, do you? You pay in multiples of a dollar, correct? While you may or may not be able to afford a whole Bitcoin, what will ultimately matter is how many Sats you've accumulated.

- *Scarcity.* As a unit of currency, Bitcoin cannot illicitly be duplicated and double-spent. This technological and cryptographic innovation has made a breakthrough of paramount importance possible, which is Bitcoin's deflationary property: the amount of Bitcoin that can be produced has been capped at 21 million units in total. Bitcoins are currently being issued with every block, but in ever diminishing quantities at a ratio that cuts into half, roughly every four years. The last halving took place on May 11, 2020. As a result, the current block reward is 6.25 BTC per block, which means 900 bitcoins are currently being produced every day. Before that date, 1,800 bitcoins were being mined per day. The next halving event shall occur around 2024, after which the block reward will be 3.125 BTC per block. At that point, only 450 bitcoins will be created daily. And the halving will repeat every four years. It is referred to as the Bitcoin halving cycle. It means that newly minted

BTC will be harder and harder to come by over time. The bulk of Bitcoin's total supply is already in circulation, as 7,200 bitcoins per day were mined for the first four years of Bitcoin's existence, for a total of ten and a half million bitcoins. The remainder of the supply that is yet to be issued will taper off into a thin long tail that will finally end in approximately 2,140. An estimated 3.7 million bitcoins have been lost due to mismanaged custody of various forms. This means that each person on the planet could only expect to own about .002 of one Bitcoin, if it were evenly distributed (which is not going to happen, but that's beside the point). The real point is that Bitcoin is very scarce as a commodity — much more so than gold. There are over 50 thousand tons of gold that can easily be estimated to exist in the ground, and likely much, much more than that (not to mention the gold that we'll eventually extract from comets in outer space). The actual quantity is unknown. As for Bitcoin, there will unequivocally only be 21 million individual bitcoins, less the ones that have been lost. For a planet of 8 billion inhabitants, that is the very definition of scarcity indeed.

- *Intrinsic value.* I've kept the fifth characteric of sound money for last, as it is the most misunderstood when it comes to Bitcoin. There are many pundits who believe that Bitcoin has no intrinsic value. What should be understood is that *the intrinsic value of an asset is tied to those qualities it possesses that make people want it*. Just like gold, silver, real estate, etc, Bitcoin has properties that people want. The fact that these properties differ from other assets in some respects, does not signify that BTC has no intrinsic value. Satoshi Nakamoto -- the pseudonymous creator of Bitcoin -- has touched on this point in a bitcointalk.org post on August 27, 2010. The forum thread was titled "*Bitcoin does NOT violate Mises's Regression Theorem*". It states:

"As a thought experiment, imagine there was a base metal as scarce as gold but with the following properties:
- boring grey in colour
- not a good conductor of electricity
- not particularly strong, but not ductile or easily malleable either
- not useful for any practical or ornamental purpose

and one special, magical property:
- can be transported over a communications channel"

Such a metal would nonetheless have intrinsic value then, would it not?

Bitcoin's properties constitute something as a whole that enough people want, for it to possess intrinsic value.

INTRINSIC VALUE IS RELATIVE TO THE FRAMEWORK WITHIN WHICH IT IS BEING APPLIED.

The intrinsic value of a physical asset will not apply in a digital environment, and vice-versa.

In a physical-property framework, gold has intrinsic value because of the ***wanted*** qualities it possesses, in addition to its understood scarcity: it is beautiful and shiny; it is hard enough and yet malleable; it does not corrode; it is a great electrical conductor that can be used in electronics manufacturing; and it is highly regarded for ornamental uses, etc.

In a digital-property framework, Bitcoin has intrinsic value because of the ***wanted*** qualities it possesses in addition to its built-in scarcity: it is tamper-proof and can be transferred across distances or geographies with a keystroke to any party without the prerequisite of trust needing to be a factor.

The key word is "wanted".

By the way, the reason why fiat currency has no intrinsic value is because no one inherently wants it. Its value has been assigned by decree. You are coerced into using it to pay your taxes with. And as legal tender, it must be accepted for payment by law. Gold was outlawed on April 5, 1933 by President Roosevelt. Anyone caught with a quantity of it after that date would have had to pay a fine

representative of twice the amount of gold that they were hoarding, and its possession could as well have carried a ten-year jail sentence. The gold had to be turned and exchanged for Federal Reserve Notes at the price of $20.67 per troy ounce. This was legalized grand theft on a massive scale. Physical gold never made a comeback in earnest after that. You can buy some now and take physical possession, but that rarely happens in the general populace in any meaningful volume. Most times, only “paper gold” is being traded.

In a pre-internet world, Bitcoin would have made no sense whatsoever. But gold did make a lot of sense then, although lack of transportability was its main impairment.

Let’s take the metaverse as an example. Gold would make no sense whatsoever in that scenario, but Bitcoin would make a lot of sense there, due to its irrevocable assignment of ownership and instant transferability.

It’s a case of different “wanted” properties for different environments with respectively varying intrinsic value for each.

The digital use case is particularly hard to grasp for boomers in general -- not all of them, just most. Try to explain the appeal of e-sports to one. So it shouldn’t be surprising that boomer economists, investors, professors and politicians don’t get that a digital property can have intrinsic value. They’re unable to comprehend the context.

And while there are academics and others who flat-out reject the theory of sound money and what Bitcoin stands for, you can examine the notion for yourself. How hard is it for you to imagine a world in which the architecting of money is out of the hands of central banks and governments? In this new reality, a given government has to be a participant of the financial system to the same degree that you and I are, if they want to survive. In other words, by disrupting how the government works, a new paradigm could take place around the financial system that would go a long way to restore equality and stability. Now, if this seems like a pipedream, take a few minutes to visualize hundreds of thousands of people, at

first, then millions, and finally hundreds of millions of individuals worldwide transacting on a peer-to-peer basis with a currency that never was issued by a single government, but that yet sits alongside any fiat money for as long as fiat is around. With whom would the power be situated then?

Of course, governments and central banks will fight tooth and nail to prevent this from taking place. Many nations will seek to organize together in this objective. It is likely to affect Bitcoin for a time, possibly gravely so. But Bitcoin was most cleverly designed around a robust set of incentives. Should these incentives hold up as intended, *the governments and central banks will be forced to also buy Bitcoin to mitigate the risk of being left behind, if and when Bitcoin prevails and becomes the world's default value system -- a phenomenon which we call "hyperbitcoinization".*

Chapter 7

As much as this book may have so far been somewhat of an eye-opener, can the situation really be that bad, though? You're thinking that as long as things stay "pretty much the same" for a "long-enough" time to come, it should all be fine, right?

Well, it's too late for that. Things have irrevocably changed and will no longer go on as they have been: *Bitcoin has already happened to the world and the financial centralized planners know it*. The genie is not going back into the bottle.

I have virtually cited no sources up to this point in this work for the simple reason that I wanted to convey the message as succinctly as possible. The writing strategy was to avoid a TL;DR situation at all costs. This meant I had to place the burden of proof on you. It is up to you — and I urge you — to search every concept I have thus far presented so you can assess the matter for yourself. (I should also stress that, should you decide to go deep to understand how Bitcoin can disrupt modern finance, it wouldn't be far-fetched in my opinion to expect to spend in the ballpark of 100 hours doing so.)

But I shall make one exception in this chapter in citing a source and going deep on it. Central banks and governments worldwide have begun thinking in earnest about making use of blockchain technology to further their own agendas. A perfect way to illustrate what their intentions are is to bring up a recently published Vanderbilt Law Review paper. On October 26, 2021, the publication "Wall Street On Parade" covered the following news:

"**Biden's Nominee Omarova Has a Published Plan to Move All Bank Deposits to the Fed and Let the New York Fed Short Stocks**

This month, the Vanderbilt Law Review published a 69-page paper by Saule Omarova, President Biden's nominee to head the Office of the Comptroller of the Currency (OCC), the Federal regulator of the largest banks in the country

that operate across state lines. The paper is titled "The People's Ledger: How to Democratize Money and Finance the Economy."

You can find the full, 69-page PDF file by searching the title online. It was published on October 19, 2021, as best as I could tell. It is also referenced as "Cornell Law School research paper No. 20-45".

Before I start dissecting it for your pleasure, let me first opine that the financial central planners are looking directly at their own demise. They're contemplating losing their stranglehold over the population. Don't you think they're scared? What would you do if you were in their predicament? I'd say you would be scrambling. You'd be plotting. And you quite likely might also publish a paper in which, in all likelihood...

1. you would use Covid-19 as a cover for your master plan
2. you would demonize Bitcoin
3. you would steal the Bitcoin concept and try to pass it as your own idea
4. You would misinterpret the definition of "democratization" to mislead
5. You would deceive with lies and half-truths
6. You would paint what you are doing in the best light to appear legitimate.

Obviously, I cannot comment as to Saule Omarova's true motives and ethical compass, but let's take a look at some of the perhaps more alarming sentences or paragraphs from her paper (italicized and in quotation marks), along with my perception of their potential impact for you and your descendants (in regular font), if ultimately implemented .

"The COVID-19 crisis underscored the urgency of digitizing sovereign money and ensuring universal access to banking services."

"[This article] offers a blueprint for a comprehensive restructuring of the central bank balance sheet as the basis for redesigning the core architecture of modern finance."

"Focusing on the U.S. Federal Reserve System ("the Fed"), the Article outlines a series of structural reforms that would radically redefine the role of a central bank as the ultimate public platform for generating, modulating, and allocating financial resources in a democratic economy—the People's Ledger."

"The Article shows how the proposed reforms would make the financial system less complex, more stable, and more efficient in serving the long-term needs of the American people."

What is being said so far is the absolutely incredible statement that the Federal Reserve Bank should have absolute power to create, influence and dish out money at their sole discretion, by becoming the "blockchain for the people".

Please note that throughout my commentary, I'll ignore any questionable claims she makes -- for example, that Covid brought about the need for her proposed reforms, or that her recommendations are aimed at the long-term needs of the American People. I'll let you weigh such assertions of hers against points 1 to 6 above and decide for yourself.

"…the Article envisions the ultimate 'endstate' whereby central bank accounts fully replace—rather than compete with—private bank deposits."

This is saying that your deposits will no longer reside in a "regular" bank the way you've always done it. You will deposit your money directly with the Federal Reserve Bank. This will give incredible powers to this central entity over you. Initially, you will be able to keep banking at your existing financial institution, alongside your Fed account. By extrapolation, the next step will be to make it mandatory for you to do your banking only with the Fed. By that time, you will live in a cashless society in which all your transactions will go through your Fed account. You will have no leverage over the Fed and they will wield this power over you. They'll know all your transactions. Any shred of privacy, you shall have lost.

“Issuing a new form of digitized central bank money, or CBDC, became an increasingly hot topic of policy discussion as a result of the rapid rise in the volume and popularity of privately issued cryptocurrencies. The success of Bitcoin paved the road for the subsequent emergence of numerous crypto-assets purporting to challenge the supremacy of sovereign money.”

“Not surprisingly, Facebook’s plans to launch its own stablecoin, Libra (later renamed Diem), immediately heightened the salience of CBDC on central banks’ agendas.”

In essence, she is not even trying to conceal the fact that Bitcoin is threatening the legacy fiat currency system. Furthermore, Facebook was seriously entertaining the idea of issuing their own digital currency, and this fact has added to the Fed’s sense of urgency. The financial central planners feel compelled to react to retain their control over the issuance of money by creating their own version of Bitcoin, called Central Bank Digital Currency (CBDC).

This is why you cannot run away from Bitcoin. You’ll either have to be using the central banks’ version of it, which will enslave you more than you already are to the financial system. Or, you will be using the real Bitcoin, which they can’t tamper with, control or confiscate. It’s your individual choice. And it’s our collective choice.

“...the Chinese government began pilot runs of its official digital yuan, widely seen as the potential challenger to the U.S. dollar in international trade.”

They are also facing the risk of losing the dollar hegemony. It’s a double risk now. So you can bet that they will not rest on their laurels until they feel they have re-secured their dominance.

"Focusing on the ultimate "end-state" whereby central bank accounts fully replace— rather than uneasily coexist with—private bank deposits, the Article explores the full range of new monetary policy options the proposed structural shift would enable."

"For U.S. citizens, Individual FedAccounts would be opened automatically upon birth or naturalization."

Just like today's bank… accounts, all FedAccounts would earn interest. The interest rate on these accounts would serve as an important tool of the Fed's monetary policy, setting an effective floor in the overall interest rate structure."

"Far more importantly, offering deposit accounts to individuals and entities will enable the Fed to modulate the aggregate supply of money and credit by directly crediting and debiting the accounts of all participants in economic activity, without interposing intermediary-banks."

In basic terms, the Fed will credit all eligible FedAccounts when it determines that it is necessary to expand the money supply… this form of unconventional (by present standards) monetary policy is commonly known as 'helicopter drop' or 'QE for the people.'"

"Implementing a contractionary monetary policy by debiting FedAccounts… [while] aiming to minimize the economic and political fallout from what is likely to be perceived as the government 'taking away' people's money."

"In essence, banks will become non-depository lenders."

"Banks, in other words, will not be 'special' anymore. By separating their lending function from their monetary function, the proposed reform will effectively 'end banking,' as we know it."

"Thus, both federal deposit insurance and deposit-based bank reserve requirements will become unnecessary."

The claim is that the money you keep in your Fed account will yield interest "just like today's bank accounts" (which by the way, is close to zero). But by that time, you will be at the mercy of your Fed account. What will stop the central planners to implement negative interest rates by then? This would mean that you'd need to pay interest to the Fed for them to hold your money. The answer is: nothing will stop them.

Another thing that is likely to happen is they'll adjust interest rates around money velocity. The latter refers to how much money is moving through the economy. If most people simply "hoard" their money and keep it in their bank account, we say the velocity (the speed) of money is low. If money is moving around a lot (you eat out and tip the server, who then takes a cab home, then the cab driver stops at the convenience store and buys milk with their earned profits, etc.), then we say that the velocity of the money is high. Central banks will be able to penalize the interest rate yield to increase the velocity of money. Doing so would let them control exactly how much inflation to inflict onto the economy. In other words, if you don't spend a certain portion of your money by such and such a date, you will have to pay more negative interest on those funds.

To help them micromanage the economy even more, the Fed will be able to drop money into your account or REMOVE MONEY, at their discretion. They'll do this with the stated goal in mind of expanding or contracting the money supply, as they see fit. Remember her words: banking as you know it will end. There will no longer be a need for federal deposit insurance, as you will be at the sole mercy of the Fed.

All this raises the question, do you really want to live in that world?

"The creation of FedAccounts, discussed above, would give the Fed an entirely new set of tools for achieving its monetary policy goals in a more direct and finely tuned manner."

"This Article offers a blueprint for reshaping the basic architecture and dynamics of modern finance. Using the creation of digital-dollar FedAccounts as its starting point, the Article constructs a coherent set of structural reforms aiming to make the financial system more inclusive, efficient, and stable. It contemplates a comprehensive update of the Federal Reserve's balance sheet—the nation's core economic ledger—to maximize its structural capacity to support productive economic enterprise, in the long-term interests of the American people. In effect, it reimagines the role of a central bank as the ultimate public platform for generating, modulating, and allocating financial resources in a modern economy—the People's Ledger."

The People's Ledger framework embodies precisely this type of a cohesive reform agenda. Putting it in action would profoundly change the organization and essential dynamics of the financial system.

"Doing so is especially urgent in light of the ongoing digitization of finance, which includes rapid proliferation of privately issued digital money and privately run digital payments systems. Notwithstanding their rhetoric of democratization, these technologies threaten to undermine the fundamental balance of the sovereign public's and private actors' relative powers and roles in the financial system. As decades-old institutional arrangements come under increasing pressure, what replaces them becomes a matter of utmost public policy importance. This Article offers a unified set of structural solutions to this all-important structural challenge."

And of course, she lets the cat out of the bag at the very end. The central banks are under increasing pressure, and that is what this is about.

And the dystopia will be even worse in communist countries. There, your social score will be linked to your CBDC account. Fail to be an exemplary devotee to the dictator, and see your freedom of movement — as but just one example — restricted. For instance, you try to buy a train ticket to visit your loved ones for

the upcoming holidays, but you are no longer allowed to for the next 18 months, as a form of punishment.

To reiterate, you will not be able to run away from digital currencies. Your future and your descendants' future depends in no small measure on whether or not the power to issue currency can revert back to the people, so that governments can go on existing by selling their services honestly and transparently to the people they have been entrusted to serve — and without the malfeasance (whether intended or not) of central banking cartels.

Chapter 8

To invest means to put resources – oftentimes money – into something with the expectation of making a return.

There are many investment strategies.

You could be into real estate.

Perhaps you prefer investing in commodities via ETFs.

Trading stocks or various cryptocurrencies may be your thing. Or, maybe holding these for the long term better suits your risk profile.

It's also quite possible you've chosen not to – or haven't yet been able to – invest at all.

All of it is irrelevant to this book.

This book is not about convincing you to buy Bitcoin as an investment.

Instead, I prefer to convey the metaphor that *Bitcoin is an insurance policy against dangerous monetary and fiscal policies*.

It is a display of sheer arrogance on the part of central banks and governments to assume that they can endlessly pull economic levers up and down (i.e., interest rates and money supply expansion/contraction) with unprecedented abandon without there ever being the real possibility in their view of a massive, total, widespread collapse. But why should they care? When crashes do occur, those directly responsible are rarely personally affected. Being close to, or at a point of

power, they can simply push the repercussions away from themselves and their cronies. I would even suspect that they don't lose too much sleep over what happens to you.

THERE IS FRAGILITY INHERENT WITH EVERY SYSTEM, PARTICULARLY IN THE PRESENCE OF A MISALIGNMENT OF INCENTIVES, AS IS THE CASE IN THE CURRENT SOCIO-ECONOMIC CONTEXT.

Living on this planet carries a set of risks in its own right. You spend your life navigating those dangers, such as trying to ensure you and your loved ones don't starve, get sick, get exposed to excessive heat or cold, get victimized, etc. And you do it all while you seek to achieve as much success, rewards and satisfaction out of living as you possibly can.

But living in our modern society now carries this additional, unnecessary risk, which is that you could suffer untold hardships merely because what was supposed to be sound money has been made unsound.

Well, what are proven risk mitigation strategies in this day and age?

There are several: hedging, insurance policies and antifragility. (The latter means that your circumstances are such that adverse events actually benefit you. For example, if you owned a hand sanitizer manufacturing company during the pandemic, you did pretty well, while travel agents didn't perhaps have it as good as you.)

Let's focus on insurance for a second. Would you be a landlord without liability insurance for your properties? Would you drive an automobile without vehicle insurance? Would you manage a public corporation without B & O (board and director) insurance? The likelihood is you wouldn't dare taking on such unnecessary risk in each respective scenario.

So what about central bank policy-related risks? Is apathy really the best response we've got?

If history is to be considered as a guide, the way the showdown is likely to take place is as follows:

1) Money printing gets out of control
2) Runaway inflation occurs
3) Politicians and other desk jockeys blame price increases on businesses
4) The financial central planners put price controls in place
5) The ensuing collapse makes the Great Depression look like a holiday.

In the past, there was little you could have done to not find yourself at the mercy of the financial central planners. But now there is an option to help you hedge against this risk.

TO OWN BITCOIN IN A TIME OF SOCIO-ECONOMIC COLLAPSE COULD POSSIBLY MAKE YOU ANTIFRAGILE.

Any perceived risk associated with Bicoin, such as the regulatory environment or its price volatility pale in comparison to the greatest risk related to it:

BY FAR THE BIGGEST RISK ABOUT BITCOIN IS NOT OWNING ANY.

When you see cash's purchasing power eroding away — as is already occurring at the time of writing — where do you put your money?

When inflation grows higher than the appreciation of any real estate you own, what will you do?

If gold's price remains as flat as it's been for the last decade (in no small measure due to Bitcoin being a better version of gold in the digital age) what will happen to any plan you may have had to use gold as a hedge?

During times of monetary expansion — such as we are currently experiencing — the stock market gets artificially propped up. Will you wait for the bubble to burst to reconsider? Look into what happened to Venezuela in 2016. Do you think placing your money on the stock market is any less risky than putting it in Bitcoin?

When CBDCs happen, will you trust the central banks with the leverage they will undoubtedly hold over you? Do you believe the financial central planners would only "in theory" have the power to: a) withdraw funds from your account, b) freeze it, and c) control your spending, without ever going so far as to exercise those powers in practice?

Now, let's test how convinced you are at this point that Bitcoin is indeed the best "insurance policy" against financial collapse risks — as well as offering a better alternative to the current Keynesian Economics craze that's all too prevalent.

Let's say we were already 90 days into a 10% monthly inflation scenario. At this rate, every $100 you were holding three months ago will only be worth $10 in another six months (as compared to its former purchasing power). The clock is ticking hard for you. Every day you delay taking action, you are witnessing more of your purchasing power erode away. It took you whatever long to save the stash you had been able to put aside, and you intend to salvage as much of what's left of it as possible. Below are your choices. Where will you, actually, truthfully, at a snap of the fingers — this month! — put your money:

a. Leave in cash?

b. Stocks?
c. Bonds?
d. Mutual Funds and ETFs
e. Real Estate?
f. Startups?
g. Gold or silver?
h. Art?
i. Other cryptocurrencies such as Ethereum, XRP, Polkadot or Solona?
j. NFT's (non-fungible tokens)?
k. Bitcoin?

On the spur of the moment, which one are you picking?

If you've picked Bitcoin, congratulations, you have been successfully orange-pilled. (To *"take the orange pill"* is a reference to the movie *"The Matrix'' in* which Neo is asked to choose between the blue and the red pill — the former representing blissful ignorance and the latter leading to the complete, unvarnished truth. In the case of Bitcoin, the "pill" is orange, and it means you went down the Bitcoin rabbit hole deep enough to understand its philosophical import.

Chapter 9

How does one even begin to own Bitcoin?

THE FIRST STEP IS TO GET OFF OF ZERO BITCOIN OWNERSHIP

As with any condition of inertia, the first thing to do is to *start* moving.

"Getting off of zero" means that you acquire your first *tiny* amount of Bitcoin, so you get to experience BTC ownership for yourself. Once you've begun the journey, the experience will seem much less daunting, if at all.

Furthermore, even if you appreciate the points made earlier, you are nonetheless in a race against time. As more and more people take the orange pill, they will also want to get off of zero, which will create a competitive environment. The earlier you are in the game, the better it will be for you in the long run, should hyperbitcoinization occur.

First, here are some caveats:

1. Do your own thinking and act on your own counsel.
2. Anything I say is not financial advice.
3. It is advised to NEVER purchase more BTC than you can *easily* afford. For some people, it could mean as little as $10 a week.

In terms of how much Bitcoin would you need to own to secure a good standard of living in a hyperbitcoinized world, no one knows for sure, but there's a widespread "agreement" that owning as little as 1 million Satoshis (0.01 Bitcoin) could do it. It's also anticipated that owning 28 million Satoshis (0.28 Bitcoin would put you in the most wealthy 1% bracket. Even owning as little as 250,000 Sats (0.0025 Bitcoin) would be very helpful, others believe.

Again, this book's aim is not to pitch Bitcoin as an investment to satisfy your greed, but rather, as an insurance policy that could make you antifragile in the event that the financial central planners' overzealous monetary policies blow up majestically in our collective faces.

It's as if you and I were racing this expensive car together, and I continually maneuvered the vehicle dangerously. And since I'm the driver, you're at the mercy of my actions, except that at the very least, you took out a race car insurance policy to protect yourself against losing your portion of the investment.

In order to understand how to proceed purchasing BTC, the concept of custody should be understood.

Anything valuable requires safekeeping, whether that is done by its owner or someone else. Custody of an asset means that someone or a legal entity safekeeps the asset on the behalf of its legal owner. Non-custody of an asset means that the owner safekeeps the asset themselves.

You keep your money at a bank so that, by placing custody of your money with a financial institution, they are the ones responsible for not losing it. It protects you, as long as the bank remains trustworthy and solvent — and as long as the government doesn't overreach and confiscate your funds.

Non-custodial Bitcoin cannot be confiscated, as long as you don't lose your private key. But with that freedom comes the burden of responsibility for not losing your funds. *It's the price that must be paid to opt for that freedom.*

I'll first cover the pros and cons of the various ways to store Bitcoin, and then I'll explain how you can (in much of the world, at least) get *very easily* started and progressively sort out which combination of options best suits your circumstances over time.

Bitcoin uses a cryptographic mechanism by which a piece of software is used to generate a private key. From this private key, a public key is also generated, but the latter cannot be used to reverse-engineer the process and reveal the former. (Your public key is an address of some sort that you make known, as required, to receive Bitcoin. Your private key is the password that unlocks the funds.) In practical terms, what this means is that you can use an offline computer to generate a set of private and public keys and print them out using a printer that has never been (and will never again be) on a WI-FI network. This will generate a printout that will show both the private and the public keys, along with a QR code for each. Then, you can scan the public key's QR code — or type it manually — and share it publicly, so you can receive Bitcoin. Those who see the public key are unable to decode it and derive the private key from it. This is because the encryption Bitcoin uses only goes one way (the private key is created first and it generates the public key — and never the other way around). The transaction's originator can only send Bitcoin to the public address. When you decide to spend or transfer your Bitcoin, you use your private key to do so. If you lose your private key, your Bitcoin is lost along with it.

This is an example of a private key:

B3EC7FM8B03667180E01FB4251G546C2B9F2JE33507K68B7V9D4E1WA5714195201

And here is an example of a public key:
1DfcjkvUUG3gTdNMtZ4zQ59kegA4Mfrb3TW

The process I have described above is referred to as a paper wallet. It is one of the offline methods to store Bitcoin we call "cold storage". It is now considered antiquated. From 2011 to 2016, it was considered the most secure way to keep your Bitcoin. *"Being secure"* means no one can confiscate your BTC as long as you keep the private key secret and away from any form of electronic storage that can be accessed by a hacker. With this method, the reason why you would generate the set of private and public keys offline — using a computer that is never

connected to the internet — is to keep your Bitcoin safe from hackers. The reason why the printer needs to never have been on a WI-FI network (and needs to have been purchased new), is to ensure it does not contain malware in its memory. And it should NEVER thereafter be on a WI-FI network *because it holds your private keys in its memory.* (Some sources even advise destroying the printer afterwards!) The computer doesn't have to be new, but it should have the operating system freshly installed and never again be connected to the internet. Taking a screenshot of the paper wallet should be avoided, as hackers can access a smartphone, *even if it's an old one that's permanently turned off.* Lastly, it is advisable not to keep your paper wallet in your home, but rather, in two separate deposit boxes, in different banks, in tamper proof envelopes. There are also risks connected to how you go about choosing and transferring the software that generates the private and public keys to the offline computer. For me personally — and I go against the grain on this one — I consider a paper wallet still to be the most secure way to store large amounts of Bitcoin in a non-custodial way – say 1 full bitcoin and more. But it is very much for advanced users, *as you really have to know what you are doing*. And one needs to start small and test, test, and retest their approach before committing substantial amounts of Bitcoin to a paper wallet. Cold storage means that the private keys are not exposed to the internet.

The cold storage non-custodial method which is most widely accepted is a hardware wallet, which is a small hardware plug-in device that allows you to transact while never releasing your private keys. Even if you lose the device, you can recover your funds by replacing the hardware wallet, as long as you have saved a copy of the recovery code generated during the initial setup. While they are highly secure, hardware wallets can nonetheless be hacked and can carry malware, so they are not, in my opinion, an "ultimate" option.

Examples of hardware wallets are the Nano S, Nano X, and the Trezor Model T. There are other brands and models too. This is not an endorsement. These simply seem to be the better-known ones. Personally, my view differs once again here from the general consensus, keeping over 1 BTC on a hardware wallet would make me nervous – just my opinion though.

Third in the non-custodial category of Bitcoin storage options are hot wallets, which are apps that reside on desktops or mobile devices. There are many flavors of them for your discovery and exploration. They offer convenience in the form of ease of use over cold storage solutions. However, since they typically keep your private keys online, they are recommended only for day-to-day transactions with low balances kept in them.

When it comes to custodial methods to store Bitcoin, there is a "rule" which is generally understood. It states: "*Not your keys, not your Bitcoin".* In other words, when you give custody of your BTC to someone or a legal entity, they don't provide you with the private key. *They* control the asset *on your behalf.* And that is a risk you should consider seriously.

Within this category, there are three main options.

At the top, there is the institutional-grade third-party professional custodian. These companies specialize in safeguarding Bitcoin and other crypto currencies for institutional investors and wealthy individuals. They insure deposits and have extremely robust security. If you have multiple millions of dollars worth of Bitcoin, this is likely how you are storing it.

Next, we have custodial wallets. They are similar to hot non-custodial wallets in their function, except that you do not control your Bitcoin's private key, which is kept online on the service provider's servers. The way you access your account is most often with a username and password. It is highly recommended that you maintain only a small balance on a custodial wallet — an amount that you wouldn't stress over too much, if lost.

Lastly, you can (initially) leave your Bitcoin on the exchange where you bought it, as long as it is not a large amount. I mentioned earlier that I would explain how to get started very easily. This is it.

ALL YOU HAVE TO DO TO GET OFF ZERO IS TO CREATE AN ACCOUNT WITH A CRYPTO EXCHANGE SUCH AS COINBASE OR KRAKEN, FOLLOW THE INSTRUCTIONS, AND MAKE YOUR FIRST SMALL PURCHASE OF BITCOIN.

You can do an online search for the safest crypto exchanges and go from there. I've mentioned Coinbase and Kraken only because I've personally used both with success. (Disclaimer: I have no affiliation with both of them. This is just my opinion. Please do your own research.)

Once you have more experience and have done your homework in determining what your strategy for holding Bitcoin needs to be, then you can act accordingly. The choice is yours and only yours to make. There is no one-size-fits-all approach. It all depends on multiple factors, such as the size of your portfolio, your risk tolerance, your investment horizon, and your personal preferences.

If you subsequently decide to keep accumulating Bitcoin, one way to do it is by dollar cost averaging. This essentially means you simply keep buying the asset at regular intervals, regardless of the current price. You can set this up automatically on the exchange so that, let's say, once a week, your bank account is debited for an amount of your choosing. That amount is converted into BTC and held in your account on the exchange until you decide to transfer it to one of your own wallets, if that's what you chose to do.

There are even more variations of wallet types available in the above-mentioned categories, but I limited the list to provide you with a foundational understanding that you could choose to expand on, at your discretion.

In summary, if you haven't started yet, but intend to, the most important step is to "get off zero".

Chapter 10

Bitcoin is a multi-layer system

Layer 1 is the underlying blockchain with its key functionality as described thus far in this book.

Layer 2 refers to solutions that have been added to greatly improve the speed and reduce the cost of Bitcoin transactions, as compared to Layer 1. The Lightning Network is a Layer 2 solution that allows for transactions to occur off the blockchain and get later on grouped in batches that are recorded as one transaction. The advent of Layer 2 solutions have made possible the adoption of Bitcoin by entire countries, such as has occurred in El Salvador in 2021. It has allowed that nation to raise financing in the form of Bitcoin tokenized bonds, directly leading to the disintermediation of the IMF and the World Bank, who can no longer hold El Salvador hostage with onerous loan terms. It has also opened the door for Bitcoin to become legal tender in that country. This means that if you live in El Salvador, you can pay for your lunch at McDonalds with Bitcoin.

As the Lighting Network gains widespread adoption, Bitcoin will get a foothold as a peer-to-peer network. Regulatory risk only exists with Bitcoin at the fiat currency onramps. Let me explain. The only way the governments can stop Bitcoin is by preventing you from buying some via the current banking system. If they make it illegal to buy Bitcoin through banks and exchanges, they would make it difficult for you to get your hands on some.

Now, let's imagine a scenario in which the Bitcoin whales (those individuals who hold very large positions) begin in earnest to spend some of their BTC stash to pay various service providers directly in Bitcoin. Then, as mom and pop shops proceed to widely accept Bitcoin, the service providers who have been paid through the lightning network start to pay for goods and services in Bitcoin at the mom and pop stores, and thus the flywheel eventually reaches critical mass.

In other words, short of shutting down the entire internet, there is no way to fully stop Bitcoin, because citizens can ultimately decide to simply trade it directly with one another and, given sufficient organizing, bypass much of the legacy system.

A lot of humanity's magic has been captured and recorded throughout history. Someone can be born today and in a few years discover a great live jazz recording dating back to 1961 and experience much of the enchantment.

A lot of humanity's magic has undoubtedly also not been committed to our collective memory. And the innumerable accompanying acts of heroism can not be reminisced over and be fully appreciated today. But they can be imagined.

There is a lot of positivity about humanity to be focused on.

The failures of the past do not have to be repeated by default. Ingenuity and some luck can do much to save the day. It does not mean they will, but they could.

Imagine a world in which the incentives are such that it is no longer financially beneficial for a government to engage in warfare. In this vision of the future, wealth redistribution from the poor to the rich through currency manipulation is no longer possible. It is a world in which abundance is made possible because money is stable.

Are you sure you're not going to own at least a little tiny bit of Bitcoin by the end of today?

-- THE END --
[*Or is it the beginning?]*

Afterword

In February 2014, my wife and I went on a ten-day tour of San Francisco and the Valley, during which we attended the Launch Festival — an entrepreneurship-centric conference. I was working on my startup at the time, PreAcquaint.com. I had heard about Bitcoin in late 2013, but had not yet gotten involved. It was at that event that I cemented my belief in BTC in a very material way. While going around and socializing, I stopped at the booth of one of the early startups in the field. The founder had a degree in finance and was highly intelligent to boot. I'm thankful to this day that he was very generous with his time in giving me a crash course in Austrian vs Keynesian economics, sound vs unsound money, and how Bitcoin mattered from a macroeconomic viewpoint — all of it as opposed to merely being a speculative vehicle. In addition, I attended the formal Bitcoin talks that were on the conference's schedule. Looking back at them, they were remarkably prescient.

I subsequently wrote up a post on PreAcquaint about my experience at the Launch Festival, as well some of my thoughts about Bitcoin at the time. Even though I finally deemed my startup to be unsuccessful by late 2014, you can still see that write-up here:

http://preacquaint.com/story/attend-the-2014-launch-festival

In the following few years, my conviction about Bitcoin never wavered, even as it seemingly went sideways for on and on and on and on and on and on and on.

But then, in 2017, it started to go up, up, up. BTC surging at last was *incredibly* rewarding on so many levels.

I went on to other things for a while. For example, I self-published my science-fiction book, *Awakened in the Future*, which is a semi-satire, semi-philosophical reflection on the Silicon Valley "wanting-to-change-the-world" sentiment.

I also composed, recorded, performed, arranged, mixed and produced a ten-year-in-the-making album for my socially-conscious musical project, "*Veer Van de Valk*".

My wife and I also traveled, pre-pandemic.

For months now, I've been enjoying a "retirement mode" state in which I take extended walks, go on bicycle rides, read, and reflect a lot, then rinse and repeat — all of it punctuated with spending quality time with my other half.

It was as a result of one of those moments of reflection that I made the observation to myself that, while many people "knew" about Bitcoin, they never had been presented with the opportunity to understand how Bitcoin may be more important to their personal future than they had assumed. And the thought concurrently occurred to me to write this book.

Let's engage on Twitter and let me know your thoughts. My handle is @mariocantin.