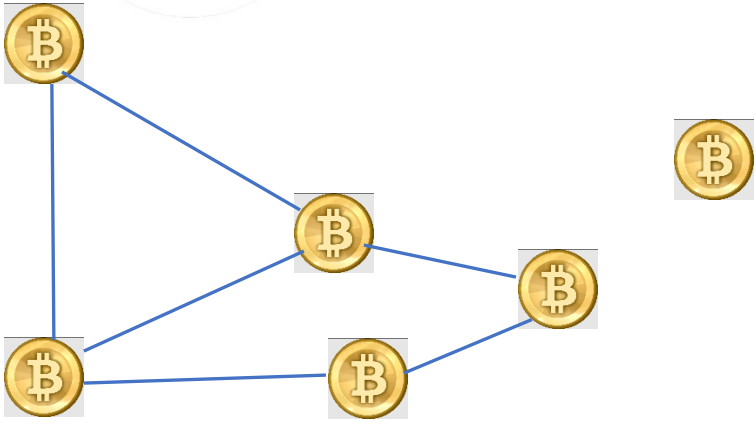
FOUND

SATOSHI NAKAMOTO

The Visionary Behind Bitcoin

bitcoin

Part 1 – Chapters 1 through 9



WRITTEN BY: E.J.H.

FORWARD

Mysterious unknowns left unresolved, can turn curiosity to obsession -and inspire us, with strong resolute, to solve a seemingly unsolvable puzzle. The pieces of this puzzle, found and assembled over time, determine with certainty the identity of Satoshi Nakamoto. That is a bold statement, I know, given Satoshi Nakamoto has remained anonymous for well over a decade and is the visionary behind the world's first cryptocurrency, Bitcoin. Bitcoin has changed many lives, some for the better and others to their detriment. Whether Bitcoin continues and evolves into a dominant world currency or ceases to exist at a future time, cannot be known now. But, make no mistake, the use case for blockchain, the structure fundamentally behind the digital currency Bitcoin is based on, is here to stay.

Debate will continue as to whether Bitcoin, or other alternative cryptocurrencies will appreciate or depreciate over time. This book's author does not claim to be an authority on the digital currency that is Bitcoin. Not its use, nor the likelihood of global adoption or its future value. Bitcoin and other cryptocurrencies fluctuate on any given day and are expected to have wide swings in value for the foreseeable future as they have in the past. It's not particularly pertinent to the puzzle or enigma that is Satoshi Nakamoto. Having said this, it is important to understand that at its creation, Bitcoin had no value whatsoever and thereafter for a time, very little value. The expected increase in value for bitcoin is but one reason for anonymity. There are other reasons that will be discussed in this book. However, as the value of Bitcoin increased in a relatively short period of time, the desire to remain anonymous would only deepen, logically.

The release of the Bitcoin White Paper made public on October 31, 2008, by Satoshi Nakamoto has now become a very momentous event. Although at the time, it came in more like a cool summer breeze –some interest but not anything to write home about. Without the description for the protocols and the vision set forth by the White Paper who knows how it would have developed. The White Paper provided the guiding rules for this new digital currency, how it would work and the fundamentals of its security. Releasing such a document and developing the protocols or rules for bitcoin while maintaining anonymity are achievements in themselves.

The ability for the person that is Satoshi Nakamoto to remain anonymous all these years later is nothing short of a 21st century miracle given all the events, communications, and information in the modern world now associated with Bitcoin. With so many means of tracking communications, and the blockchain itself providing a public record of transactions, it only provides resolute proof of the vision Satoshi Nakamoto had for such a currency. That it could be independent, publicly viewable and verified, yet anonymous at its core. The idea that someone, anyone, could transact across the blockchain, independent of any government, any place on the planet, was envisioned to be life changing for humankind. I believe the creator Satoshi Nakamoto intended Bitcoin to be of benefit to humanity and not a means for greed or astronomical increases in one's wealth.

It remains debatable as to the vision having a net positive upon humanity. There certainly are those who have had realized astronomical wealth from Bitcoin. One could make the case, at least for now, Bitcoin has become greed based and not need based. However, we are really just in the early stages of this transformation to digital currency and if it is to take hold

universally across the globe it does stand the ability to have incredible wealth for those early in the acquisitions of Bitcoin. Additionally, bitcoin has potential for incredible utility of use for all.

Bitcoin's protocols were set up to never have any more than 21,000,000 coins. Most of which to date have been mined and will be explained further in this book. Due to the publicly viewable transaction history and Bitcoin ledger, it can be seen that of the total mined coins to date, an estimated 1,000,000 bitcoins roughly, were mined by Satoshi Nakamoto and placed into his controllable ownership. With no monetary conversion or realization of the Bitcoin under this single apparent ownership stake, Satoshi Nakamoto would have an equivalence value in excess of $65 Billion U.S. dollars at the time of this writing. This would make Satoshi Nakamoto one of the world's wealthiest individuals. As the value of each Bitcoin continues to fluctuate considerably up or down this value will most certainly change in time and is unknown now whether it will be worth more in the future. Arguments on all sides can be made for where Bitcoin value will be in the near and long term.

One thing is clear, Satoshi Nakamoto, wanted to remain anonymous. To date, there are no legitimate evidence revealed publicly that identifies the person behind the pseudonym that is Satoshi Nakamoto. The identity of Satoshi Nakamoto will continue to remain anonymous even with the extensive information contained in this book. In today's world, and with the value of bitcoin, there is no safe means to reveal the person, nor is there desire by this author to do so out of respecting the wishes of someone that clearly wants to remain anonymous. However, the pieces of the puzzle as revealed by this book will shed light on the individual and character of Satoshi Nakamoto

and the original intent to make this world a better place. Satoshi Nakamoto shared a number of correspondence early on and wrote about anonymity.

Satoshi Nakamoto Quote (circa 2009):

> *"If you post your bitcoin address on the web, then you're associating that address and any transactions with it with the name you posted under.*
>
> *If you posted under a handle that you haven't associated with your real identity, then you're still pseudonymous. "*

In honor of Satoshi Nakamoto, this publication will be made available on October 31, 2024. This book release and its posting to its associated domain, are being done precisely 16 years after the Bitcoin White Paper was first published. Anyone following the four-year halving cycle and release of the White Paper would be aware of the significance of this incremental time frame. Regardless of how bitcoin ultimately ends up and is used, the vision is quite remarkable and has already affected many people across the globe in too many ways to fully describe.

Dedication

This book is dedicated to my daughter which always loved a good puzzle. From early childhood through adulthood, solving puzzles has provided her with a great deal of joy and self-fulfillment. Solving this puzzle, has been fulfilling for me as well in one sense, yet not being able to share the true identity of Satoshi Nakamoto with her or anyone else nor self-identify as the author of this book does leave one with a bit of a hole, much like forever losing one piece of a 1000-piece puzzle. Perhaps one day, that one missing piece will be found and complete the puzzle for my daughter to know her father solved one of the great mysteries of our time.

Author's Quote:

"Trust should always include the context of risk/reward. Consider any degree of trust, from minimal to extraordinary, keeping it proportional and illuminated to the potential risks and rewards." --EJH

Chapter 1
Introduction

Where to start? To be clear, the author here is no expert on Bitcoin. The point of this book is more about the person behind the curtain that is Bitcoin. And to have an understanding of the character that is Satoshi Nakamoto it's important to understand the basics of what Bitcoin is and how it was intended to work going forward from its inception. Thus, this introduction and subsequent chapters attempt to provide some basics on Bitcoin. Written from the perspective of a novice and not one in any way claiming to be an expert in the formulation of Bitcoin or what has transpired in the intervening years since being made available.

Additionally, this book is not intended to be one about Bitcoin value, where it has been or where it will end up. Nor is this book intended to cover its protocols, its security, or whether a person should purchase, sell or hold bitcoin. It is a book about Satoshi Nakamoto, the pseudo name for the person that created bitcoin. To that end, it is important to understand certain basic principles about bitcoin so one can better understand the person behind its creation.

Fundamentally, bitcoin is about decentralization of a currency in its most basic sense. The original vision was all of humanity at some point having the ability to transact and/or store value in a digital world without relying on the trust of a third party such as a bank or other financial institution. In other words, creating a means through secure "blockchain" and transacting directly between two parties, one sending and one receiving. More on blockchain later, but apart from banks, financial institutions, governments, or other third-party entities one would control how

and when it was used securely, quickly and efficiently at minimal transacting cost or impediment. This has been a mixed bag to this end thus far. Some governments downright outlaw it, while others control its use to a high extent and others are just beginning to regulate the who, what, how and when of it.

Bitcoin is essentially built off of coding and a network across the internet that allows for checks and verification of what's termed a "blockchain". In its most basic form, blockchains are essentially a grouping of numbers that complete a block and then is verified across many nodes throughout the decentralized network. This verification of the blockchain creates a bitcoin transaction or mined bitcoin which then can be parsed or further transacted by persons having whole or partial ownership of the bitcoin.

There would be much to explain here in how bitcoin works in detail, how one can purchase it or use it and there are numerous books, movies and internet writings describing all these aspects. How someone or companies can mine bitcoin by way of hard drives and computing power have all been covered well by others. These aspects will be touched on but again are not the focus of this writing. For now, the essential part of this is knowing that the blockchain for bitcoin is on ledgers with many people having access to the same ledger showing confirmed blocks and thus cannot be altered by any one individual or even many individuals. This provides a level of security and integrity in its use and public transparency that is simply not afforded in typical FIAT (traditional currencies) or financial institutions.

The focus herein is this vision for a new world of decentralized currency and the person behind it referred to as Satoshi Nakamoto. How successful Bitcoin ultimately becomes is yet to be written. Although, it has to be acknowledged Bitcoin already has exceeded well over $1 Trillion market cap in a relatively short

period of time (about 15 years). Beyond pure market value, Bitcoin has brought upon much change in many areas including other potential uses of the blockchain.

Lastly, in introducing this writing, please understand it has been written, edited, compiled and posted all by one person. Unfortunately, in the effort to remain anonymous, there inevitably will be compromises in quality due to this limitation and lack of other eyes on the material prior to publishing. I've done the best I can to accurately reflect my experiences and knowledge on the subject matter.

Chapter 2
The Journey is Greater than the Destination

Once in a blue moon, as they say, everything lines up just right. And with the stars aligned just right, one can see remarkable things. This story is just that. An alignment so unlikely, even I wouldn't believe it, if I hadn't lived it myself. Just as the earth being the right distance from the sun at just the right time to sustain life, by some happenstance or destiny perhaps, I too was "in the sphere" at just the right time and distance. Any closer and I wouldn't have likely been entrusted with certain information and any more distant I wouldn't have known certain information. It's that sweet spot alignment that enabled me to assemble and place the pieces to the puzzle together.

Like the story of any great treasure hunt, how the treasure got there is often of greater interest than the treasure itself. The person behind the curtain that is Satoshi Nakamoto, is one of great interest to many including myself. How did this person come to utilize the fundamentals of blockchain... was anyone else really thinking about it? From what we know, the idea of a digital currency was not really new at the time and probably lots of people were mulling over the idea given credit cards and their limited security and other challenges. One could certainly make purchases from many places in the world without having the physical currency in their hands.

However, in general terms, there are security concerns and a whole host of other problems with methods, particularly when viewed on an international and global basis. Having the ability to exchange at a rate agreeable to both parties and do it independent of another third party certainly would be favorable if widely used and done globally. No fees, in a secure way

anywhere. But how to achieve this? This is a great question and worthy of someone's pure devotion to solving this problem. How to remove the typical bank which would only add fees and other interference and with more areas where security could be breached. It needed to be done in a way where those two parties exchanging at an agreeable means would do so in a trusted manner. It needed outside and independent verification of the transaction but not the interference. Hence the concept of using a blockchain was born to aid in these currency transactions. It would be this verification or "proof-of-work" as it would come to be known.

Proof-of-work would provide undeniable verification of each transaction by having enough independent outside points of confirmation that could not be altered. Hence, solving many problems of security, transaction ease, minimal if any transactional costs, and universal acceptance across a very diverse and varied globe of nations. Yes, the blockchain and proof-of-work solved many of life's concerns with regards to currency and transacting. The only question that remained is would it be accepted and adopted as the sole means of currency across the globe and in what time period would such an adoption occur? Given this would be many years in the making, the journey certainly would be of interest to anyone initiating this and that would include the person that is Satoshi Nakamoto. More to come on this.

Chapter 3
Pseudonymous and Privacy

It should be clear to anyone following bitcoin, the creator Satoshi Nakamoto wished to remain anonymous when unleashing a new form of currency into the world. There are numerous steps this person took to begin with an alias and continue for a time as a private person. From early communications to the published White Paper, great care was taken not to reveal himself or too much behind his character, including his whereabouts, origin of communications, professional background, or birthplace amongst other characteristics and identifying information.

Having said this, there are a number of correspondences we know originated from accounts with the pseudonym, Satoshi Nakamoto. This has led to much speculation but no proven connection with any of the past communications, publications, or otherwise as to who this individual might actually be. Very little has been gleaned by others as to the person behind the curtain. In fact, some speculate it's more than one person or potentially a government entity which speaks to how well he was able to hide the details of his identity. I can definitively say it is not a group of people nor a government entity and will be described later in this release.

There is substantial merit as to why so much thought and effort went into this anonymity. Satoshi Nakamoto knew that if bitcoin, a new form of digital currency, were to take off as a global asset there would be many that would have in interest in the mined coins initially, or worse yet, take issue with it from a government standpoint. It has the potential to threaten government's control over its own currency if universally accepted by a global population. And as discussed later, the banking industry would be fearful potentially of such an application for a variety of reasons

we won't go into here. That was the initial thought and as time will have it, has actually materialized much along these ways with some governments and banking industries threatened by its existence. Some are slowly coming around with increased regulations and oversight while others are continuing their resistance to adopting or allowing it. It's likely governments are getting more and more involved with it as one of those, "if you can't beat them, join them" conditions. Motivated by wanting to maintain order over it and be involved in the potential it offers as well as limit any risks associated with its widespread use in the future. Additionally, bitcoin could ultimately lead to an alternative store of value and replace gold as some believe it will eventually.

As governments and financial institutions become more threatened by this new form of currency it would have undesirable implications on the person that created it, potentially. As time passes, the reasons for anonymity only become more plentiful and this author believes there is substantial reason for it not just initially but for it to continue in some respects. Not all that has transpired I'm sure was as predicted by Satoshi Nakamoto but perhaps much of it as expected. For similar reasons, this author finds the need to remain anonymous and has taken steps for that to occur. However, in today's world it is much more difficult to do much of anything anonymously.

Anonymity is becoming increasingly difficult. In the mid-2000s around the time of the White Paper release for instance, one could with little knowledge simply have any number of emails, web sites, and communications in online forums that were cloaked in secrecy. Today, this has largely changed, and most people are not even aware of the interconnectivity and identifying information being used.

Large and small corporations as well as governments are making it increasingly difficult, if not impossible, to remain anonymous even for very mundane activities. For instance, email accounts are no longer just logged in with a single password. They are inevitably linked to phone numbers or addresses or real identification without option. And for those with multiple emails they tend to require being linked to one another now. This has only within the past several years been the norm and not the exception.

There are likely many books and writings on the increasing intrusion into privacy but suffice to say it's probably a combination of government driven and corporations having an increased interest on knowing what people are doing more and more. Soon it will be unavoidable. There are work arounds I'm sure as some people will argue and use, but they probably delve into dark areas I'd rather not be familiar with or have knowledge of. All I know is it was once very easy for anyone to be anonymous and now it is very difficult. The author only describes this at the 30,000-foot level because it is very relevant to the person that is Satoshi Nakamoto. In today's world I wonder if it would have been possible to create such a thing as bitcoin, anonymously. The timing seemed to be just right for Satoshi Nakamoto.

Often, these intrusive privacy concerns are occurring in very insidious ways. Cloaked in ways that seem innocent at first glance such as "cookies" being required to be accepted. Even the term "cookie" implies something warm and nice. But, to look at a web site, any web site running the gambit from sports to gambling to government sites, they all have cookie acceptance requirements before proceeding on through the online site. Grabbing information about the user and in many cases sharing that information with others and between multiple parties. This sharing of information sometimes occurring in broad ways with large data batches, but sometimes not. It really is quite insidious

when you lift the cloak and see what is behind all the information gathering, we are not even aware of, at times.

With the recent advent of artificial intelligence this intrusive collection of information is becoming increasingly expansive as well as incentivized in value. Combine this evolution with data breaches and it all becomes ever more concerning. So how does this play into the discussion that is the person that is Satoshi Nakamoto? Because this is part of the need for personal security. As we lose this privacy, whether it's with one entity or many, or it is shared across governments or private industry, we are losing a piece of ourselves. It all is very disconcerting and affects our safety. It affects all those around us. Satoshi Nakamoto was aware of all this and logically would take whatever measures necessary to assure the anonymity would stay in place indefinitely.

The blockchain underpinning bitcoin and how the network of nodes function are set up to work anonymously. Of course, with the way bitcoin has developed much of that anonymity has dissolved, largely with the introduction of cryptocurrency exchanges. These exchanges will generally collect every aspect of personal information that your typical banking institution would. This is contrary, I believe, to the intent that Satoshi Nakamoto originally desired and envisioned. The idea was to have it decentralized and apart from corporate exchanges, governments, or other entities. However, even very smart people way down the rabbit hole have found their transactions traced and identity revealed, not all, but most. The vision has clearly diverged from its onset intent. I sometimes wonder what Satoshi Nakamoto thinks about the current outcome of that initial vision and where it is headed.

There's no question in my mind, governments and corporations and everyone in between are able to glean information from users of their web sites, email accounts, social media platforms, gaming or other applications. It's presented as something fairly innocuous. However, there is much more to be seen and discovered by the public on what and how this information is being used and to what extent. Even as I type this, I've signed away rights for cell phone corporations to glean information off it. Your audio and mine on our phones are extracting background sounds. Applications from large and small corporations are hearing and using collected audio as well as video. Your camera on your cell phone is being used routinely. Some will argue its being compiled into large data sets, but through A.I. or other searches, functionalities have the ability to glean all sorts of information. You've already accepted that in some form or another by accepting the legal agreements on the use of any of your electronic devices. They are all collecting and sharing information within and with external partners, often for financial gain. It's no accident after talking about something random or taking a photo of something, you will begin seeing a related advertisement on various platforms you visit. All directed at you and based off information gathered from your daily, hourly and by minute real time activities.

In short, it was critically important that Satoshi Nakamoto create a pseudonym and remain anonymous to this day. Similarly, the author wishes to remain anonymous and have taken steps to this end. However, there is only so much one can do.

Some might argue if the author has such a desire to remain anonymous with this sort of knowledge why write a book when one can just be silent? Well, that is much easier said than done. When you have knowledge of something very significant it weighs heavily on your soul, your thoughts, your body, your mind. It's

hard to escape it and really needs a release. This is why people sometimes disclose traumatic events that happened to them many years earlier. It's hard to hold onto over time. All I can say is I've done my best with this regard, and I don't wish to reveal either Satoshi Nakamoto's true identity or my own.

For America, the public is not fully aware just how interconnected and intertwined our lives and our information has become -all within a few short years. It's becoming increasingly invasive with the advent of artificial intelligence always listening, always viewing our moments in real time and preserving that information in cloud-based data banks. This is no longer future dystopian type hypothetical stuff or some far out conspiracy theorist ideas. Any person can verify it for themselves. Simply try to create something online in private now. Virtually everything is now linked to your identity. Your emails are all linked to your identity, your visits to web sites, anything done online all traceable to who you are. Your government identification all linked to the various forms. Even your facial recognition is linked to many aspects of other things. Try taking a trip anymore without having your face scanned. In the background it is all being collected and stored in data farms or the "cloud".

Just as we should have the right to free speech and say things within certain limitations, we should have the right to privacy if we choose also within certain limitations. In both cases, some might argue the pendulum has already swung too far having widespread implications. With irreversible adverse impacts on each and every one of us and our freedoms. Where does this trend go from here? In the opinion of this author, we as a society have surely gone beyond the intent of our forefathers when they drafted the U.S. Constitution. All this discussion of privacy is in fact relevant to Satoshi Nakamoto and the purpose behind the vision that is bitcoin. These commentaries on free speech and

privacy are not intended to be political statements or advocacy for certain policies, but rather provide some foundation to what Satoshi Nakamoto was thinking as his vision was being developed and ultimately released for global consumption.

Privacy is as needed as free speech in maintaining personal freedoms. There is much talk these days about the need for free speech. I would suggest these rights are being threatened in both free speech and privacy. There is bias in media and whether that includes intentional censorship or incidental screening of information it is happening in America and many places around the world. Free speech goes to the heart of personal freedoms and maintaining a free world. And like free speech , being able to maintain one's privacy also goes to the heart of a free world. When the government wants to invade every aspect of our lives with no limitations that becomes a threat to democracy. Of course, there is a need for balance and limitation. Going to extremes on anything including free speech and privacy does not serve humanity or the prospect of societal transformation for the better. A global digital currency and its transformational possibilities can have similar impact on our freedoms as free speech and privacy rights.

As it relates, Satoshi Nakamoto introduced bitcoin at a time where it was possible to do so in a private and anonymous way. Today, I would argue this would be much less likely to have occurred in this way. Governments and corporations alike are ever increasing their attachment to what each of us are doing at any moment in time. There is largely no avoiding now, and it has eroded our freedoms. Free speech and privacy are two areas that will continue to be debated by peoples of all nations with varying degrees of freedom and limitations. I believe these freedoms, and not the financial gain, was the impetus behind bitcoin for Satoshi Nakamoto.

Chapter 4
What's in a Name?

Why the name "Satoshi Nakamoto" ? Well, there are lots of theories out there certainly. Some believe that "Satoshi" is a word in Japanese referring to having intelligence or great wisdom. While "Nakamoto" in Japanese can have meaning associated with origin. These would presumably have some connection to a new and original digital currency. Or the person that would introduce such a vision.

Everything that is associated with bitcoin that we know is well thought through as a visionary would do. So, do we think the name would be random or of a real person? No, that wouldn't fit the character or mode of operation of this visionary. The name is not that of a real person. It would make much more sense the name used has significance to the individual creating a currency with the expectation of its use by the world and the hope to change people's lives for the better. People that have been oppressed or people that perhaps have a history of their currency being dissolved or becoming worthless after a lifetime of hard work, sacrifice and savings. No, the name Satoshi Nakamoto is deliberate and not lightly created. It has deep meaning. It would be in line with the introduction of blockchain. The creation of a new architecture that is the framework for bitcoin.

Nobody to date really knows the connection other than Satoshi Nakamoto himself. But I do believe it would have great meaning and cultural reference and perhaps even a nod to a great architect. There have been many guesses across the internet with various people assembling the used letters in Satoshi Nakamoto to reference acronyms or businesses or what not. But these are too simplified. The pseudonym is undoubtedly a nod to something greater.

It is interesting early on, Satoshi Nakamoto did not want others to be falsely labeled as the person behind bitcoin. It is obvious why that is given all the troubles that have followed and ensued around people that have either voluntarily claimed to be Satoshi Nakamoto, or it was put upon them by others. Satoshi Nakamoto knew from the start that using a pseudonym was of utmost importance and doing everything possible to not come out from behind the curtain would be necessary.

The following quote is known to have come from Satoshi Nakamoto;

March 7, 2014 01:17:00 AM
"I am not Dorian Nakamoto."

Just one example of Satoshi Nakamoto's interest to not having a burden of identity placed upon someone else falsely.

Due to the sensitive nature of privacy concerns and maintaining respect to those which wish to remain private, the association with the person that possibly could be the inspiration for the name will also be held by the author. However, there are certain aspects that can be inferred such as it being inspirational to the person that is Satoshi Nakamoto. The author does not know of any actual relationship to another person or this person the author believes could have influenced the name, but there are many elements which line up properly as the inspiration.

Including:

- Inspirational person
- Ethnolinguistically similar
- Same letter count

- Majority of letters in the correct order and overlapping
- Visionary and builder of new things from grand ideas

Satoshi Nakamoto
[ ]

Put yourself into the mind of the person that is Satoshi Nakamoto during the early to mid-2000s. Your experiences cultivate and influence your life. It is likely that there is meaning behind this which I don't fully know, however, the pieces do all line up as this being a nod to a visionary and builder of grand things. Architect, perhaps? After all, at least the great ones, are visionaries at their core and reaching for new limits and innovation. Architects build upon and rebuild upon past visions and create new visions. There are many parallels between great architects and the vision for bitcoin. To build a new world through financial stability and security. The overlap of seeming influence is too striking to ignore.

From what I have come to learn and know about bitcoin, there is an association of ideals with architecture. I'm not aware of any personal or professional relationship or even if the two sharing so much in name, knew each other then or now. It may be purely coincidental and speculation on my part. I can say with certainty, however, Satoshi Nakamoto is not the person having another name referenced herein. That would surely be too close in reference for a pseudonym. Whether this other person's name is an influence upon the pseudonym Satoshi Nakamoto is something else entirely. It is even possible the two had some shared experience, unknowingly. There may be other underlying reasons why this referenced person had been possibly chosen for the basis of a pseudonym used by Satoshi Nakamoto. Having chosen

pseudonyms myself in the past, I can say there is usually some connection to the name, not unlike a nickname.

Lastly, and this is probably a stretch of speculation, but potentially one more piece of the puzzle. The person I knew to be Satoshi Nakamoto was using a name I knew them by which had inference to “expertise” or “guide”. This may be purely coincidental as well, but I do find it interesting given all the other pieces of the puzzle as they fit. The name, I knew him by, was likely not his birth name and indeed potentially an alias in itself.

The author does have other thoughts on this aspect, but in the interest of minimizing speculation and not risking other privacy concerns, will limit to what has been said here. Take it for what it’s worth, it may or may not have a connection but from what I know, the odds are pretty good.

Chapter 5
The Timeline and White Paper "draft"

The author came to know the person that would become Satoshi Nakamoto, not as Satoshi Nakamoto, but as another individual with an entirely unrelated name. It was only later, much later, that the realization set in as to who Satoshi Nakamoto was and how we crossed paths. It took some connecting of the dots and assemblance of puzzle pieces over time as described in this book. At my initial knowing of this person, I had never heard of the reference for Satoshi Nakamoto, and it wasn't until many years later that I would first hear the reference. However, the name I knew this person by was entirely different and may not have been his true birth name and quite possibly a self-given name in itself. If so, this would seem consistent with what else I know of him but at the same time erases information of one's past and limits traceability.

The author's first encounter with the person that became known as Satoshi Nakamoto occurred back in the Fall of 2005. With encounters continuing through the Fall of 2006. The final encounter extending into November 2006. So, for a little over a year, the author came to know the person that would become Satoshi Nakamoto. It's not clear then or now looking back that this person was using or planning to use the pseudonym Satoshi Nakamoto since it was a good two years prior to the release of the Bitcoin White Paper on October 31, 2008.

As noted in the known correspondence of Satoshi Nakamoto dated "2008-10-31 18:10 UTC", Satoshi Nakamoto messages the online, Peer-to-Peer Professional Forum, referred to as the P2P

forum; “I’ve been working on a new electronic cash system that’s fully peer-to-peer, with no trusted third party.”

Satoshi Nakamoto also writes in another known correspondence with Hal Finney dated “2008-11-09 01:58:46 UTC”, the following:

> *“I appreciate your questions. I actually did this kind of backwards. I had to write all the code before I could convince myself that I could solve every problem, then I wrote the paper. I think I will be able to release the code sooner than I could write a detailed spec. You're already right about most of your assumptions where you filled in the blanks.*
> *Satoshi Nakamoto”*

In thinking about the timeline and the release of the White Paper on October 31st, 2008, my experience with the person that would become Satoshi Nakamoto is consistent. One might imagine the time in thinking through all the parts that is bitcoin. Satoshi Nakamoto did not invent a new math solution, or a new formula, or any one real new piece. It’s the sum of the parts, and the vision in putting all these pieces together in a manner that solves a particular problem around transactions/currency relying upon other third parties. This is the driving force behind bitcoin and in my view behind Satoshi Nakamoto. It was the removal of that third party that was at the heart of this creation.

Relying on other third-party sources for administering currency as we generally have to date can have a considerable effect on the security of that currency. Bitcoin brings uniformity across the globe to transacting and storing currency value in a secure means free of the need for third parties. Of course, this was the vision and since has morphed into many transactions today having that third party through cryptocurrency exchanges. This is in direct

conflict with the original vision. Bitcoin was intended to remove the need to trust a third party in any transaction. Although, current exchange traded funds (ETFs), crypto exchanges, and other regulatory means from certain governments of transactions are overriding this onset goal. Having said all this, thinking through the potential pitfalls of attacker methods, proof of work concepts, the 21,000,000 limit to bitcoin, the halving of it every 4 years, and other innovative and ingenious methods would take some time.

One of the most ingenious aspects of Bitcoin is the reduction or halving of its supply and limiting it to the 21,000,000 coins. At first thought one might simply have a trend line that gets to this limit over a certain time period. The genius concept here, however, is that the difficulty in achieving a bitcoin through mining it in a blockchain increases or decreases based on a set time frame for achieving the coin. This method takes into account the ever-increasing computing power or capacity of chips going forward. If this had not been set up this way, it's very likely all the coins would have been mined by now. Or if it was set up very difficult in the beginning it would not have gotten off to a rolling start. The variation in difficulty across a set timeframe of 10 minutes allows for a certain number of bitcoins to be mined in a relatively predictable manner.

Back to the timeline for my encounters. With the above in mind, it would take some time to work through those pieces of the puzzle. As noted by Satoshi Nakamoto himself, he had to write all the code before he could convince himself every problem could be solved. No easy task. Then he wrote the White Paper which was released on October 31, 2008. As anyone who's written anything of significance knows, a final release version always goes

through draft versions first with the timeframe for those drafts varying depending on many factors.

It is very likely the person known as Satoshi Nakamoto had been thinking about this for quite some time while diligently working through the problems, the code, and the vision. Likely for at least two to three years prior to the release of the White Paper. This places the interaction of the author with Satoshi Nakamoto into the plausible timeframe consistent with my experiences.

The author again states to not have any influence or input into the creation of Bitcoin. Only that there was peripheral interaction and conversation about similar concepts– in person, and in very broad terms. I'm sure it's easy for some to view this as perhaps a grab for attention or credit. But it is not. It's simply a conveyance by this author of experiences to shed a bit of light on the person that has come to be known as Satoshi Nakamoto.

Some of the conversations this author had with the person that is Satoshi Nakamoto were entirely on other subjects. Again, this was at a time before release of any public information related to cryptocurrencies. The author certainly was not following or aware of any progress that had been made in the area of blockchain technologies or any of the foundational processes described in the White Paper.

For this author, the following was the most critical piece of the puzzle that would prompt the assembly of all the pieces to arrive at the completed puzzle.

The author has a distinct memory of one particular interaction with the person who became Satoshi Nakamoto. One day in late 2006, while talking with the person I believe to have come to be known as Satoshi Nakamoto, he handed me a few sheets of paper stapled together and asked that I read it and what my thoughts

were. At the time it was only a few sheets, perhaps 5 or 6 in total. I do recall it was a fairly slow read given its formulas and technical subject matter and new topic area I was not familiar with. As I stood there reading, I remember pausing momentarily part way through not fully understanding things then made some comment I don't quite remember now and continued on with the rest of the read. To this day, I can still remember certain details of the surroundings and circumstances of that situation, but not all the details of the information being read.

For the record, digital currency or fundamentally proof-of-work concept, is not this author's specific area of training or background. So, reading a technical paper overviewing it , even in concept and casual conversation to an extent how it works was not something I could fully put my head around. However, as an engineer, college educated and experienced, I do have training broadly in certain technical areas and from this was an innocent ask of opinion. My opinion at the time after reading, what I now know was an early draft version of the White Paper, before it was published, was fairly non-descript and not very thoughtful.

As it were more than a decade ago, the concept of digital currency would have been foreign to me and as much of interest to me as nuclear fusion. Something maybe fun to talk about to a limited extent but seemingly so far out in the future for application that it wouldn't seem to materialize in my lifetime. Because of this, the significance of what I was reading did not sink in. Some of this with respect to the White Paper and a draft version might come across as repetitive but it is a very important part of my interactions with the person that is Satoshi Nakamoto and the impetus for me in solving this puzzle.

I do remember as I read having a certain curiosity and trying my best to follow along and grasp the concept of "proof of work" tied

to the transactions occurring. The part that intrigued me was the idea that completed blocks would have a time stamp and therefore verifiable and not changeable as it sequenced along. That "timestamp" verifying each connection was the proof of work element that is so critical to blockchain. That's as much of it that I could really grasp. And truthfully, much of it did not make sense to me given the formulas and newness of such an idea. I still struggle with certain aspects of the operation and proof of work chronology.

At the time, I just didn't have the vision for a world that would accept a new common singular currency out of this. For one thing, currency wasn't the emphasis of this draft version of the White Paper I was reading. It was more about the verification process (or completing a block in today's terms). I also stated at the time of my read through that I didn't think this was something that would materialize in my lifetime. Cleary wrong on that front. But it is interesting that the person who became Satoshi Nakamoto made reference to a certain timeframe for fruition of bitcoin. We hadn't talked specifically about the timeline for global adoption, only that I felt it would be at least a few decades out given all the competition for transacting at the time and widespread use of those alternatives.

Satoshi Nakamoto would later write; Quote (pre-2010):

> "I'm sure that in 20 years there will either be very large transaction volume or no volume. "

Well, all this to say this was my single point of confirmation for myself that I once knew the person that would become Satoshi Nakamoto. I have certainty of dates as I look back at my recorded past. I know I read a draft version of the paper which would later become the published Bitcoin White Paper well before October of

2008. I do not have a copy of the draft as it was never given to me to take away. I know how this sounds, that there is no proof of my reading an early draft of the White Paper. When you work so hard on something whether it is a patent idea or a new currency or a business proposition there are elements that you are willing to talk about and other elements you would never share. It is a balance and to a certain extent necessitates an aspect of trust. I fully understand and can appreciate now the position this person would have been in at the time.

Handing over written material of a grand vision you believe will change the world would simply be going too far when in the end, you want to remain anonymous. And yes, one might say why share anything related to this with anyone. Well, it does happen all the time and human nature is such that it is very difficult to keep everything, 100% of something, bottled up in oneself. It is a very heavy burden. The fact that I was close enough to have a very early broad discussion of concepts while far enough away from things to feel safe in sharing certain things by Satoshi Nakamoto was that sweet spot. Any closer I don't think he would have shared, and any further away I wouldn't have been available in this way. It was an alignment of stars. It wasn't so much about trusting his secret as I never knew of Satoshi Nakamoto at the time. I was not on those online forums or even in any of those circles of conversation. It was to a certain extent by happenstance that I was presented with a concept or idea in which who could have ever imagined would develop in the manner it has.

I'm sure it's easy for some looking back at this with today's knowledge to think, wow, I would have been all over Bitcoin had I read an early version of what it was going to become. But this is not the case I can assure you. It was nothing being talked about in

any circles of society whether engineering, computer science, cryptography, finance or otherwise. To me at the time, I had to ask, well what problem is this solving? As an engineer, that is what we do -solve problems. I went on to say in our conversation, we have credit cards, we have banks, we have electronic forms of payment already that allow processing online, and other means for transacting in finance. And I remember distinctly saying to him, "I could see a need for one day having a purely digital means of transacting securely between two parties, but I could not see it occurring in my lifetime. In my view, as I conveyed to him, this is something that if it occurred, would occur over decades and not in a short few years or even the near foreseeable future. This is the part, looking back, I clearly missed. Not that it couldn't be useful one day. But the aspect that it would not develop and have widespread utility as speedily as it has. Essentially, taking a foothold globally over a single decade rather than many decades. This aspect of a rather rapidly and widely accepted currency actually materializing in this manner goes back to the earlier discussion about the genius of the vision. That is, the mining of bitcoin occurs with relative ease and minimal resistance at first but becomes ever more difficult and limited as time passes and computing power increases. This puts an urgency or more immediate outcome of digital currency that is Bitcoin and allows it to take a foothold early on.

As I think back on my interactions with the person that would become Satoshi Nakamoto, and the casual conversations in person, few as they were, I know now the connection to what has become a worldwide phenomenon. I understand how all the pieces of the puzzle fit. How and why the vision for bitcoin was so important to this person. And how I missed the vision myself even though it was right there before me. A closed mind will never see the potential in something with such huge implications. In

hindsight for me personally, my regret is more about the loss of opportunity with what could have been a friend with incredible vision and the narrowness of my trust. It's hard for some people to trust because we have experiences where trusting can lead to bad outcomes. However, as discussed later in this book, trust should be proportional to risk and benefit for many, if not all decision making, in one's life.

As our paths crossed during this time period mentioned, October 31st was a very significant date for both Satoshi Nakamoto and this author. Not in the sense that those reading this will likely make of it but significant, nonetheless. And I believe it is not by happenstance that the White Paper was published on October 31st, 2008. I no longer was interacting with the person that is Satoshi Nakamoto at that time of publication as our paths crossed before that and we now had each continued down our distinct paths in life never to cross again.

Chapter 6
Behind the curtain

Before the White Paper was published and available publicly on October 31, 2008, I had been to the residence of the person that would become Satoshi Nakamoto. Of course, at the time, before anyone knew what bitcoin was or its potential, I had no idea the significance of my encounters until much later. Looking back, and knowing what I know now, I can share aspects of the person behind the curtain.

The person that's come to be known as Satoshi Nakamoto lived a relatively simple existence. No furniture. Nothing. Not even a bed to speak of, just a mattress. This was observed over a period of time. At the time I found it odd, to not have any personal items to speak of. Only empty space in the residence. This was not due to affordability. I can say that much and at the time I knew it was by choice. But I didn't view it as something for me to spend a lot of time thinking about why that was the case. Looking back, I now see the significance of living such a simple uncluttered life in the context of the vision. It firmly fits with the character and mode of operation for Satoshi Nakamoto.

It is an odd thing to think someone would live with no tv. No radio or stereo. Just a computer. Satoshi Nakamoto would order pizza as evidenced by the pizza boxes I would see when visiting. I remember just thinking this person is working on their computer 24/7 and did not have a great deal of exposure to outside activities beyond what appeared as all work. I thought at the time it was exclusively on their day job and was just bringing work home to continue progress. However, I know differently now, and Satoshi Nakamoto was a visionary working on many other areas

beyond the narrow band of work from their quote, day job. And as described in later chapters, blockchain and bitcoin as important as it has become to the world, was not a singular mission of existence. There would be other very important endeavors that have the potential to change the world.

The person that is Satoshi Nakamoto was cordial and respectful. Not overly outgoing or overly friendly but not unfriendly either. If I had to characterize, I would say Introverted. Some of the people claiming to be Satoshi Nakamoto now in social media are quite laughable as they are seeking attention or tend to be extraverted in nature. This is not Satoshi Nakamoto by any stretch of the imagination. Satoshi Nakamoto living alone, in a very simple existence, yet clearly driven by unimaginable vision and desire to create something better. Something that had not existed before in the form Satoshi Nakamoto had envisioned. Something that could and would change people's lives. No matter what is thought of the value of Bitcoin, it has certainly changed many people's lives all around the world. It is not just a one country change but reaching and extending into all realms of livelihood for many people across the income spectrum with positive opportunities in some cases or faltering in other cases.

I believe Satoshi Nakamoto had an idealistic vision for Bitcoin and a desire for it to have a net positive for humanity. Unfortunately, as time passes, it is becoming increasingly evident the scale may be weighted more heavily on the negative impact for society and this in turn I'm sure is weighing heavily on Satoshi Nakamoto. After all, in creating bitcoin who could have thought of all the extreme negative case uses, from illicit hiding of income and tax evasion to alternative criminal payment and transfer uses amongst many other uses now occurring. The United States and some other governments have only scratched the surface in

retrieving misappropriated funds and prosecuting illicit criminal activities. This is in the context of so many other countries with minimal resources in some cases to regulate, oversee, or counter criminal activities.

These negative outcomes have to weigh heavily on Satoshi Nakamoto and give pause to the creation. We are hearing similar commentary now with Elon Musk and his role in helping to create OpenAI. Where does artificial intelligence and advanced machine learning take us in the future? There inevitably will be negative consequences in creating this and if not Elon Musk then who? Was OpenAI inevitable much the same as a decentralized digital currency? It's likely it would have occurred without the initiation of Satoshi Nakamoto. It's just Bitcoin got rolling in a significant manner first, established, and in many ways is the "gold standard" for a digital currency. This has to be rewarding on one hand, but on the other hand drive one to correct or develop a better tool that achieves the original vision while addressing the negative role Bitcoin in particular has had on society. I do believe Satoshi Nakamoto is not done in this regard. Given the role artificial intelligence is now having in society and people's lives, it is very likely this is where Satoshi Nakamoto can be found. To endeavor even further with a new and greater vision for humanity: a vision and outcome now that will be secure, safe, and prosperous for all of humanity and to work to that end.

Chapter 7
Satoshi Nakamoto's Age

Earlier it was stated that we were not going to get into the weeds of bitcoin itself including its value in the past or future potential. However, it is helpful in knowing or inferring more on Satoshi Nakamoto by understanding what bitcoin is fundamentally. How it was created, when it was created, and what's transpired since then. For instance, the ledger held by each of the network nodes, many thousands, all work to validate bitcoin and keep its integrity intact. This validation across independent nodes is considered decentralized and not owned by any one individual or organization or nation state. In general terms, no single entity controls bitcoin. This was always the intent from the start. This could be inferred to have benefit of currency across nations and humanity of all status.

At the onset, bitcoin was set up to increase the available or awarded supply of coins nominally with the ultimate constraint of 21,000,000. It would never exceed this amount and is pertinent to assessing age for Satoshi Nakamoto. Rewarding those that mine new bitcoin with diminishing return on investment would encourage, in theory anyway, the price value to increase. It is set to reduce the reward by one half generally every four years. This 4-year span has some variability but is rather close to the schedule. At the time of writing here, the most recent halving occurred on April 19, 2024. This is the last real significant value add as future 4-year halving rewards have very low reward relative to the input energy and effort for outcome.

The concept of bitcoin halving plays a key role in assessing Satoshi Nakamoto's age. When bitcoin was created it was inherent to

reward those mining new bitcoin with a predetermined number of new bitcoins. Keeping in mind these new bitcoins in cumulative would never exceed 21,000,000. The initial mining of bitcoins in 2009 rewarded those mining new bitcoins with 50 bitcoins. At today's valuation of bitcoin that 50-bitcoin reward would be valued at $3,250,000 (approximately $65,000/bitcoin x 50) . Of course, when bitcoin first started out the valuation was essentially zero and in fact a negative number given it requires electricity and one's time and effort to achieve that first reward. At the time, few people were aware of the endeavor or its potential. Thus, accumulating rewards and not doing anything more with it would be expected and not out of the norm of what anyone would do in that position. Sending or receiving bitcoin early on with no value would have been an exercise in fun or test and not financial reward.

It is now known, those early mined bitcoins are likely connected to Satoshi Nakamoto and held in upwards of 20,000 wallet addresses. Each wallet having a varied number of bitcoins and many having at least 50 bitcoin. Those early onset rewards at times grouped and although anonymous in nature, all points to a single individual and likely the originator of bitcoin. That 50-bitcoin multiplied by 20,000 wallet addresses would amount to about 1,000,000 bitcoins. The math on this is not entirely certain but most people agree the person that is Satoshi Nakamoto would hold over 1 million bitcoins at one point in time. At today's valuation of bitcoin being around $65,000, that puts the value in today's dollars at approximately $65 billion. Again, in 2009 when this all began, it would have been at zero or even in terms of negative valuation in holdings.

An interesting side note is that many other individuals in the cryptocurrency realm have since "donated" or transferred

portions in whole or part to some of the bitcoin wallet addresses supposedly held by Satoshi Nakamoto. Likely these are from persons not connected with Satoshi Nakamoto that simply want to pay homage to the creator of bitcoin.

The first Bitcoin transaction started in 2009 with Satoshi Nakamoto. That first transaction appears to be 10 bitcoin, although subsequently rewards began at 50 bitcoin that year. With rewards at the time being 50 bitcoins and then each subsequent 4 years the reward protocol would provide for a halving in the amount of bitcoin rewarded. Thus, in 2012 the reward became 25 and in 2016 the reward became 12.5 and in 2020 the reward became 6.25 and in 2024 the reward became 3.125. This halving will continue until the total limit for bitcoin is reached (21 million allocated in cumulative). As one can see there is considerable diminishing return with each halving and after 2024 the next halving will be only 1.5625 bitcoin with fractional bitcoin rewards subsequent to that amount.

How does all this halving relate to Satoshi Nakamoto's age? Well, as one can see from the year 2009 to the year 2024 or perhaps into the next halving in 2028 the timeline is about 20 years. This 20 years is also referenced in emails known to have originated by the person that is under the pseudo name of Satoshi Nakamoto early at the onset of bitcoin.

This 16-year to 20-year timeline to get to very limited dispersion of bitcoin to date is not repeatable. One must think this is a reasonable timeline for a creator to see just how far their creation would go. For example, 40 years would potentially not be a timeline to see the outcome given its likely starting age. Beginning with the likely age at start of bitcoin given the educational needs of the person and the desire to see the outcome of such a creation the likely age range today would be

between 40 and 55 years old. Any younger of a range and the person would not likely have the education necessary to formulate and exercise such an intricate creation. Any older would run the risk of not seeing the outcome of the creation. Some might argue the upper end of that range could be older but, when viewed in the context of the language used in email correspondence, and the uncertainty of how long it might take for bitcoin to actually take off and make a difference in the world a person beyond their 30s at the time of creation would be running great risk in not seeing their creation materialize. They would potentially be in their 60s or older and with later age would come greater risks to seeing that outcome.

In summary, we would expect Satoshi Nakamoto to be between the ages of 22 and 40 at time of creation in 2006, 2007 and 2008 (again, the vision for bitcoin was arguably being created long before its public release). The most likely age being 25 to 35 given education and timeline to think about it. Adding the 15 to 20 years we are at in the development of bitcoin to have it largely materialized onto the likely age of Satoshi Nakamoto at the time says they would be between 40 and 55 today, give or take a couple years on that range. Any older or younger is not supportive of what we know about bitcoin. I will add for what it's worth, this range is consistent with my own observations at the time of knowing the person I believe came to use the pseudonym Satoshi Nakamoto.

Chapter 8
Satoshi Nakamoto's Education

Much of this chapter includes some speculation on the part of the author. Although, it is an educated speculation based on a number of relatable factors. Much like a weather model can speculate about the upcoming pathway for a particular hurricane, there are factors that lead one to believe in a certain likely pathway and conclusion. It should be made clear; the author does not know with certainty the exact pathway and historical aspects of Satoshi Nakamoto's education. However, with some limited interactions together with what is known publicly one can infer certain things from the known correspondence on the P2P forum and "reading between the lines" of the published White Paper by Satoshi Nakamoto.

Thinking about the aspects of Satoshi Nakamoto's age described earlier, it places Satoshi Nakamoto's age at between 25 and 35 at the time of the published paper in October 2008. This also coincides with observations of the age of the individual the author knew prior to the release of all the public information on Bitcoin. It is highly unlikely that Satoshi Nakamoto could have developed such a visionary and concise solution to such a complex problem without both specific technical skillsets and specialized knowledge in various computer related fields. It is known through the communications following the release of Bitcoin, there were questions people had and there is a dialogue of question/answer to get to the heart of many of the issues. One can certainly tell much thought had gone into the development of the vision, resolving certain peripheral issues and concerns but also a detailed coding element that some would know in computer sciences, but not all.

Thus, the education encompasses, not just the computer sciences, but an understanding of cryptography, and broadly the finance and banking system, as well as a firm handle on the English language as the written word of Satoshi Nakamoto is very concise, well spoken, and responsive to the particular question at hand. This is not a person that embellishes or flavors any given response to a question. One might say "he did not colour his responses 😊 " (this sentence is a not-so-subtle nod to Satoshi Nakamoto for those familiar with his writings).

Given the required training, skillset and other clues contained in the public known universe on Satoshi Nakamoto, there are only a handful of University Institutions that would be ranked very high and be on the cutting edge in the subject areas involved with a digital currency or proof-of-work technologies useful for Bitcoin. Not considering today's rankings in schools, but the likely outstanding candidate schools from the timeframe of 2000 to 2005 this author has arrived at one potential candidate institution. Keeping in mind, this author knew the person that would become Satoshi Nakamoto over a period of time circa 2006 when he was not enrolled in college. One likely candidate institution is Carnegie Mellon University. It is a private research university in Pittsburgh Pennsylvania. This institution is located in the same region as Sovereign Bank which comes into play in the banking discussion later in this book.

Carnegie Mellon includes a number of colleges within its campus including the College of Engineering, School of Computer Science, and School of Business to name a few. All of which at the top of the rankings. Carnegie Mellon is known for its advances in research and new fields of study and has many firsts in computer science. In today's terms, it is the first for computer science machine learning robotics. The school includes both Computer

Science Systems and Computer Science Theory amongst other relatable learning that would have been integral to the foundation for developing the concepts in what became Bitcoin. The author cannot say with certainty the level at which Carnegie Mellon had such programs available in the early 2000's, but it is likely there was some form of these trainings that could have very much trained, educated and influenced a person such as Satoshi Nakamoto.

It should be noted, Carnegie Mellon as a private school is very difficult to gain entry. It's not entirely certain as to the difficulty in the early 2000s but it is likely to be similar in challenging entry to today demanding excellence from its applicants. Only a small percentage of applicants today are admitted. For example, in the year 2022 from published sources, of more than 30,000 applicants less than 4000 were admitted with less than 2000 actually enrolled. This provides some indication of just how difficult it is and perhaps was to gain entry. It is likely the person that is Satoshi Nakamoto had he gone to Carnegie Mellon or perhaps a similar school with restrictive high standards would have a very high intelligence and quick study of information. I mention this because, as discussed in subsequent chapters, it leads one to infer what this person could be doing today. This author believes the story that is Satoshi Nakamoto is not limited to only a new digital currency with global reach. Much greater transformative work and broader ambitions are likely being worked on by this person.

Chapter 9
Patents and their association to Cryptocurrencies

It is well known that the specific bitcoin protocols are free of patents and people around the globe routinely utilize the network and its blockchain in transactions freely without restriction. It was always intended for this to be the case with bitcoin, with the exception that at some point it might have nominal transactional fees. That at least was the initial thought, and in the years that followed transaction fees have actually come to be very steep at times.

The author does not know the full extent of any related patents that might be associated with variations of either alternative coins, or aspects that exchanges have created to manage bitcoin. Likely there are relatable patents, especially as much of this topic area has evolved into other digital forms such as NFTs , phone aps, or alternative variations of cryptocurrencies, referred to as altcoins. This is an area the author does not assert to be knowledgeable in the least. Again, this book is not about the protocols or structure of current digital currencies.

However, the curiosity of patents as it pertains to blockchain technology was of interest to the author as it potentially would shed light into the character of Satoshi Nakamoto and is a curiosity with my own background as an engineer. With a thought experiment it led to a path down a very deep rabbit hole of research. The author did find patent ownerships that related, not specifically to bitcoin, but rather to the fundamentals of proof-of-work and relatable protocols. And this is an area, I really cannot discuss in too much detail as it would potentially disclose too much information around bitcoin and contributors. Suffice it to

say, my deep dive into the rabbit hole provided further confirmation that the person I believed to be Satoshi Nakamoto was in fact the person I had thought. As the pieces began to fall in place, the patent awards were sufficiently relatable and gave me pause to say, yes, this is entirely consistent with the person I believe to be Satoshi Nakamoto. It is interesting what one can discover in the wee hours of the early morning.

There is more to this account I wish I could tell. But any more said, would be potentially too revealing and I may have already provided too much by mere reference. I tried my best to let go of this in as minimalist way as possible while still maintaining the anonymity of both he and I.

This concludes Part 1 of introducing the person, this author believes to be Satoshi Nakamoto. Hopefully, a balance has been struck with shedding some light on the person behind bitcoin while not revealing too much to unravel his identity. Part 2 follows and will continue to dive deeper into the person that is Satoshi Nakamoto.

FOUND

SATOSHI NAKAMOTO

[The Visionary Behind Bitcoin]

Part 2 – Chapters 10 through 20

Chapter 10
What we know of Satoshi Nakamoto, publicly

As described in Part 1 of this book, there is fairly limited information with respect to the person that is Satoshi Nakamoto. From social media speculations to falsehoods of people claiming to be Satoshi Nakamoto, it is difficult to know what are the facts or basis for claims to the person that is Satoshi Nakamoto.

Believe what you may about the claims made in this written format. I have tried to provide an accounting to the best of my recollection. Is this author, yet one more voice claiming something that is unproven or without evidence? Is this book merely a fictitious novel? Well, I suppose there would be skepticism along these lines. I've already stated that I do not intend to reveal the person behind Satoshi Nakamoto for reasons elaborated upon in this book. However, there will be information revealed that for some may be flavored commentary or make sense in the context of what is publicly available through early correspondence by the person that is Satoshi Nakamoto. I'll leave it to the reader after taking in all the information to make their own assessment.

As mentioned, it does not serve the author nor Satoshi Nakamoto to come forward – no good can come of that. Hence the anonymity of this writing. What we all know from early available correspondence on public forums can be helpful in better understanding the person that is cloaked by the pseudonym of Satoshi Nakamoto. The following is not by any means an exhaustive description of publicly available information. It really only scratches the surface. Perhaps future updates of this book

will explore correspondences we know attributable to Satoshi Nakamoto in greater detail.

Satoshi Nakamoto corresponded in the early set up of Bitcoin with others from behind a digital curtain. A curtain that is not traceable to the user. Hidden behind a curtain, identity undoubtably would have been leaked by now if there was any association whatsoever to a government agency. From behind this curtain there has been a bread crumb trail of messages written by Satoshi Nakamoto before, during and shortly after the launch of bitcoin. Then, radio silence. Why complete silence, one might ask after a certain period? It would be far too risky as technology advanced to keep the digital curtain intact.

There is quite an extensive library of messages early on when bitcoin was first introduced and publicly known to be attributable to Satoshi Nakamoto. These messages shed light to an extent on the person that is Satoshi Nakamoto. For instance, a message by Satoshi Nakamoto reads:

> *"How Does everyone feel about the B symbol with the two lines through the outside? Can we live with that as our logo?"*

Clearly not someone with a huge ego. This is someone that wants collaboration and feedback from the community in aspects of bitcoin to a certain extent. To learn from others and incorporate their feedback. It is not just limited to something that might seem relatively trivial as the symbol for bitcoin but does extend into other more practical aspects. Although, the vast majority of bitcoin was developed without extensive feedback from the community. Satoshi Nakamoto seemed to use this forum more as a sounding board for confirmation in areas than anything for

substantial changes in direction that say a committee or tech group would serve purpose wise.

Another quote from Satoshi Nakamoto correspondence reads:

> *"There are legitimate places where it's free. Generation is basically free anywhere that has electric heat, since your computer's heat is offsetting your baseboard electric heating. Many small flats have electric heat out of convenience."*

We shouldn't overlook this seemingly innocuous commentary on the energy use associated with Bitcoin - it is very significant. Given the high energy use of mining bitcoin, it is notable that Satoshi Nakamoto would make a point of the energy use. First, baseboard heat is not widely used everywhere. There are many alternatives to baseboard electric heat from natural gas and oil to boilers, radiated heat and furnace/duct systems to name a few. The fact that Satoshi Nakamoto references baseboard electric heating together with the term "flats" are key indicators of influences in language as well living situation. The term "flats" is not commonly used in America as "studio" or "small 1 bedroom" would be used more commonly. The word "flats" together with the term use of "bloody" (elsewhere) begin to paint a picture of the language influence of Satoshi Nakamoto. This use of unusual terms not commonly found in America, yet , used together with most of the language being American English are entirely consistent with my observations of Satoshi Nakamoto being in a "flat" and having baseboard electrical heat. The reference related to energy also speaks, I believe, to Satoshi Nakamoto's interest in the broader societal costs and recognizing that energy plays a role in people's freedom and ability to further themselves. Energy is a critical component in the living standard of whole

communities and nations for that matter and I believe this was recognized by Satoshi Nakamoto.

Another Satoshi Nakamoto correspondence reads:

> *I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party. The paper is available at:*
>
> http://www.bitcoin.org/bitcoin.pdf
>
> *The main properties:*
> *Double-spending is prevented with a peer-to-peer network.*
> *No Mint or other trusted parties.*
> *Participants can be anonymous.*
> *New coins are made from Hashcash style proof-0f-work.*
> *The proof-of-work for new coin generation also powers the network to prevent double-spending.*
> *Bitcoin: A Peer-to-Peer Electronic Cash System*
> *Abstract. [refer to link]*

One of the key takeaways with the provided highlights list from Satoshi Nakamoto is "No Mint or other trusted parties". It is clearly of critical importance to Satoshi Nakamoto that Bitcoin be decentralized and not something that is dependent upon any single government, person, or entity. The "Mint" in this case is in reference to currency production. The idea is that bitcoin would not rely on currency production by any single source. It would come from many sources and be checked and double checked by the fundamental and underlying basis for Bitcoin. Also, of note is this production would be by participants that can remain anonymous, or at least that was the intent upon creation of the Bitcoin electronic system.

Another interesting correspondence by Satoshi Nakamoto reads:

> *"Before strong encryption, users had to rely on password protection to secure their files, placing trust in the system administrator to keep their information private."*

This is an initial important goal of the use case for Bitcoin with having it decentralized. Bitcoin in theory would not be reliant on any government, entity or other person to entrust one's own Bitcoin holdings or trusting of passcodes. Although some of the initial and early adopters of Bitcoin have this independence, most new transactions do involve other parties and rely on the trust of those other parties are acting in the holders best interest. However, in recent years with most Bitcoin exchange transactions involving third parties that may or may not be sacred and trusted some have lost much, if not all, of their holdings to unscrupulous parties. This is evidenced by some businesses not properly holding in trust or transacting in valid and responsible ways. There has been limited regulatory oversight in some countries while other countries have no oversight.

The lack of regulatory oversight in some countries have inevitably created opportunities for unscrupulous and nefarious activities. This reliance on other parties, contrary to the vision, has materialized as the main means for transactions. This requires the placement of trust in a system administrator as well as the bitcoin custodian. This aspect of strong encryption is only as secure as the trust in humans overseeing the companies, entities and governments involved in the holding and transacting of Bitcoin on behalf of others.

Many of these quips by Satoshi Nakamoto were made as quick responses to other's inquiry on some topic. Sort of an off the cuff casual means of communication. It is fun to the author of this

book to explore these as they really get inside the mind of the person that is Satoshi Nakamoto. Frankly, I could go on for many pages along these lines. However, will leave the reader with this final message more relatable to the protocol that is bitcoin. It is fundamental to the integrity of bitcoin and at the heart of what makes bitcoin unique and relatively secure at its core.

> *"Blocks can only contain transactions that depend on valid transactions in previous blocks or the same block."*

Unless you're able to time travel, this makes bitcoin extraordinarily difficult to break. The blockchain is a forward processing mechanism that is irreversible and provides confirmation along the way. This is the part that grabbed my attention early on and will be discussed later in this book. It also provided a key piece of the puzzle for me that I had only realized in later years. That I had actually crossed paths with the person that came to be known as Satoshi Nakamoto given my conversations prior to the release of the published Bitcoin White Paper.

Chapter 11
Who is not Satoshi Nakamoto

There has been much speculation over the years as to who is the person known as Satoshi Nakamoto. The interest is varied from those that would like to meet the person that created the phenomenon to those that have monetary interest and many other facets that spark one's curiosity. Some have claimed to be Satoshi Nakamoto and have gone as far as taking the issue to court in an attempt to gain access to the sizable holdings of bitcoin thought to be associated with Satoshi Nakamoto. Some believe more than a million bitcoin can be connected to Satoshi Nakamoto so claiming to be that person and being awarded that somehow by courts would have potential financial gain. Well, I can say with certainty that no one thus far has come out as the person I believe to be the true Satoshi Nakamoto.

For those that make a case for mathematics as a basis for the identity of Satoshi Nakamoto they are far too vested and with self-interest selling a false outcome. That character of self-serving interest does not fit the building blocks of information for the individual that is Satoshi Nakamoto.

Some have speculated that Satoshi Nakamoto represents a group of individuals, or a government agency and I can say with certainty this is not the case. Others have speculated on various individuals having seemingly some connected facets to the timeframe, or other attributable provision. They have been discussed and largely debunked by the online community including those that have made documentaries on cable/streaming services, or gone to court, or otherwise. Its tempting to list the names of these individuals but they are easily

found online and could have unintended consequences by doing so.

Potential candidates are numerous having been called out by all sorts of publications and online listings. If the person that is Satoshi Nakamoto does ever come out from behind the curtain, I will not hesitate at that point in time to affirm it. But, until then, I'm sure there will continue to be false characters presented.

Chapter 12
Trust

Trust is difficult for many people. Many of us have been figuratively burned in so many ways it is sometimes difficult to put faith in the unknown. Nobody can predict the future, and trust is part of that unknown with lack of predictability in the future. When we infuse our past failings or events that involved trusting whether that be people, systems, machinery or other aspects one must put a certain level of trust in accepting what is before you in order to move forward. This does not mean one should trust everything with unlimited bounds, nor should it mean having no trust in things or people that have potential to create great reward with little risk.

There are many examples that could be used to describe the degree of trust being proportional to the potential risk and reward. The author brings this into play here because as we age, we learn from lessons of the past and the most important lesson of all in this author's opinion is to keep an open mind and consider the level of trust relative to risk and reward. At times, trust will be zero or nearly zero, but it shouldn't be done in hast and without consideration for what the risks and rewards are.

In earlier days, it was a measure of arrogance that prevented me from better considering the relationship between trust, risk and reward. I say this due to its relevance in the context of Bitcoin and the person that is Satoshi Nakamoto. When someone presents an idea that is far reaching and seemingly implausible, e.g. Elon Musk's goal of human colonization on another planet, one shouldn't be so hastened to disregard that vision. Much has been accomplished by visionaries across humanity and time. In hindsight, this author really should have taken more care to listen,

to consider, and trust to a degree that is proportional to the risks and rewards at the time.

As the forementioned relates to the appeal of Bitcoin most, is its integrity and security. By way of the proof of work protocols, the bitcoin blockchain establishes a nearly unbreakable storing mechanism. I say nearly, because even Satoshi Nakamoto himself in the White Paper acknowledges nothing is absolute, but it is certainly improbable. Now that improbability was in the early days in the context of self-custody and maintaining one's own secure wallets and private keys. With the advent of exchanges and other holders of bitcoin, there are additional means of potential intrusion and security loss which in turn requires additional trust.

There are varying forms of securing cryptocurrency from keeping it on the network exposed to other computers to keeping it offline and off the internet in what's called cold storage much the same as thumb drives or floppy disks back in the day. And even yet, there are methods of paper security that allow for keeping both the wallet where the currency is held and the written code or key along with it that only the holder would have custody. There have even been embedding bitcoin into gold coins as a means of storage. At this point in time, there is no shortage of variations to not just securing bitcoin but many other cryptocurrencies as well.

As one becomes more educated with the integrity of Bitcoin and the different means to secure it, the degree of trust increases as risks diminish proportionally. The same could be said inversely with the trust decreasing as risks appear to advance. Not having the informed basis for this trust would inevitably result in very low trust for most people and likely in the end result in no action or involvement in Bitcoin.

Trust should always be in the context of risk reward. Consider the risk or fall out of trust relative to the reward. This applies to every decision and every action, not just in the context of bitcoin or cryptocurrencies. Something with very little risk and tremendously high reward, one can afford a great deal of trust and move forward easily. Conversely, something with a high degree of risk and little upside or reward should have minimal, if any trust. There will be a near infinite sliding scale of degree in trust based on the extent of risk and reward.

They say trust is earned. Well, this would imply zero trust until earned with having no consideration for the risk or reward. Or having limitless trust with no consideration as to the risks or rewards. Everything, every action, every decision has a risk and a reward, either quantitative or qualitative. My regret, as it pertains to bitcoin, is not better understanding this relationship between trust, risk and reward earlier in time. Apologies if much of this is repetitive or obvious but it is an extremely important life lesson, I believe everyone should consider.

In this end, my regret as it pertains to the person that would become Satoshi Nakamoto, is not better assessing this trust, risk and reward and the potential of a long-standing friend.

Chapter 13
If so close to Bitcoin, why not buy into it?

A lot of people have pointed out that Satoshi Nakamoto likely holds in excess of 1,000,000 bitcoin which in today's dollars would be well over $65 billion US dollars (this figure is changing all the time due to the volatility in price action of bitcoin). Some might say, why hasn't Satoshi Nakamoto cashed in some of those funds or transferred at least some of it into other forms of currency or stores of value. I believe there are many reasons for this, some of which will be touched on in this writing. But the short of it is, I'm convinced, bitcoin for Satoshi Nakamoto was never about greed or making a lot of money. It was always about a societal impact for the better and providing a means for greater financial stability outside of financial institutions and government instability around the world. There are many places on this planet where hyperinflation exists and the local currency has little value, if any. Bitcoin would offer a stable alternative, relatively speaking, to the people of many areas around the world.

I believe as Satoshi Nakamoto mined those early coins at 50 coins a block and accumulating mass numbers of coins, it was as much about testing the system and the methods as it was about any possible alternative motivation. In those early days bitcoins had essentially no value and as time went on it took years before really any value to speak of. Satoshi Nakamoto likely had faith it would take off and be accepted across the globe and have significant value at a certain time, but it was not certain exactly when. In fact, Satoshi Nakamoto makes reference to this in one of his communications that essentially it would either be broadly accepted in 20 years or not at all (from the time of his launch).

One might also ask, if the author knew so much about this all along why not invest in it as well in those early days. Frankly, it was very much on the peripheral of things out there akin to Ponzi discussions or other farfetched ideas in the early days. It was also very difficult for the average person to figure out the means for accumulating bitcoins. How does one acquire bitcoin before exchanges? Not that straight forward, particularly given all the security risks which have actually materialized in many cases. Yes, some figured it out but most not so much. It wasn't until only recently in the last few years that bitcoin became mainstream available for purchasing options through online exchanges. It has become as easily purchasable as any stock or other investment at this point in time. And like stocks having the potential to lose all of their value, so does bitcoin. Bitcoin is not FDIC insured like a Certificate of Deposit and many of the regulations around bitcoin and other cryptocurrencies continue to evolve and not have clear guidance as to their security as evidenced by the corruption and failing of the FTX Bankruptcy. Significant amounts of bitcoin value in that exchange were allegedly misused and many people entrusting their purchases would have their funds lost. This crypto exchange continues to go through various legal actions of recovery. Whether these investors of bitcoin ever recover their full funds is still not entirely clear.

Given all that has materialized with intrusive thefts of bitcoin, difficulty of acquisition in early years, ongoing trust issues around stability of bitcoin, and other risk factors, is it really any surprise someone with conservative tendencies and skepticism to new things would not purchase or acquire bitcoin?

I do believe this aspect of having a higher purpose beyond money is something that Satoshi Nakamoto and I had in common at the

time our paths crossed. Greed and financial gain were not foremost or even at the least a motivating factor in much of our life's interests. Our paths crossed and my conversations with him were more out of common interests. Beyond it having potential unfavorable consequences to his identity, "cashing in " some or all of the held bitcoin in the various wallets potentially linked to Satoshi Nakamoto would not be motivated by an interest in receiving the funds. Unless, that is, it served a greater purpose originally associated with the mission of bitcoin to better serve humanity.

Chapter 14
Running a Node?

Running a node? As mentioned, this book is not about explaining bitcoin or its operations and protocols. But it is important to understand the basics of nodes as they relate to bitcoin to understand the person that is Satoshi Nakamoto and why in those early moments, I did not explore more or have an open mind about bitcoin.

Nodes in the context of Bitcoin are simply computers interconnected to share information about Bitcoin. Nodes or other computers are needed to maintain the decentralized nature of the network and its integrity. When Bitcoin first started, simple desktop computers could be used to run nodes and had enough computing power to also "mine" bitcoin as they ran. More about mining bitcoin later, but the aspect of two then three then many nodes interconnected allows the network to grow and strengthen over time assuring its integrity. Nodes are intended to follow a certain set of rules or bitcoin protocols which ultimately result in the independent verification of transactions and the most recent block before its accepted into the blockchain. This is then added upon the public ledger and all those nodes assure the ledger is common to all and cannot be altered.

To put it simply, and as best as my novice mind can describe blockchain and proof-of-work is this search for the correct numbers that complete the next block which is completed with the verification by the network of nodes. Each having a time stamp that couldn't be altered due to the totality of the node network ultimately validating the assembly of the block.

All that said, nodes were just your "average joe" computer back in the day and ran on most any computer you could purchase at

your local computer store. Today, giant buildings and complete server farms with incredible computing power can be nodes and are generally needed for mining new bitcoin. Many bitcoin miners today are quite large enterprises with multimillion-dollar investments expecting returns in mined bitcoin to be profitable.

Before bitcoin went public however, I had a brief conversation about the prospect of running a test of sorts with the person that would become Satoshi Nakamoto. The application or code for running a node had not yet been released (as had the White Paper not been released) and it was not presented to me in any connection to bitcoin or as a quote “node”. It was simply use of my computer that would run an executable file (.EXE) and be able to provide some back-and-forth testing with the person that would become Satoshi Nakamoto. I had run executable files prior to this and in fact had written code and familiar with the capabilities of executable files. However, I was extremely uncomfortable to say the least about the concept of running an executable file on my computer from a source I was not familiar with nor anyone else was.

At the time, running a file of this nature (.exe) was not so straightforward or well understood by me as this was not my specialty area of engineering. I was incredibly sensitive to the prospect of someone else giving me a program or sending me something that could potentially be a virus or worse yet something that would be a backdoor into accessing information on my computer. Of course, I knew just enough about security breaches to be hesitant but not enough to know it would be okay. So, I did not offer up my computer at the time. I was doing website design and other engineering computer activities and had basic knowledge of what could go wrong if I was not careful. I didn't need intrusion into my computer including data or personal information at risk.

Looking back at all this now, I still think the reservation I had was merited. I just should have pried deeper and learned more is all. So many intrusions have occurred not just related to bitcoin but other data and information with people's personal or professional computers that to this day the reservation is still merited. This being the case even for those working in the field and very knowledgeable in security. Take any number of examples from major corporations with computer patch breaches to crypto owners having their crypto stolen from one wrong turn or assumption. Nope. This was not an activity for the weak stomached. To be a trial on something that was not developed by a reputable company is not something most conservative engineer's would trust doing without extraordinary care. Again, at the time nobody knew anything about all this. It was entirely new and an unknown that would make most people reluctant even today.

It's no surprise to anyone that's ever operated a computer that there are numerous viruses and methods of intrusion into data on one's computer. And at the time in the 2000s software to guard against these intrusions was fairly limited. They are still limited today, but there are many more companies and methods for protection. Having said that, the "bad guys" are becoming ever more innovative and keeping up with the "good guys". So, for a very long time we have had both an offense and a defense as it relates to security and data and personal information. The fundamental aspect of bitcoin is its security protocols. This is where its strength lies. And at the time, before anyone really knew much of anything about bitcoin, it had to start with a node and then another node and another and another. So, two nodes first started bitcoin. From what I know, most people believe the person that is Satoshi Nakamoto was one of those first two nodes running off his personal computer. Now, sure, Satoshi Nakamoto could have had a second computer and run the other node from that and started it that way in a trial capacity to test for operating

bugs and work out details. It's not fully known to my understanding how those early nodes were run. However, I will say, I had a discussion about it with Satoshi Nakamoto in very broad and brief circumstances but not characterized as nodes. The discussion was in the context of me not fully understanding where this vision was headed. They say hindsight is 20/20 and well in this case it certainly is. It's hard, I'm sure for people knowing what they know today to follow along with the thought that you wouldn't just run the node if asked by the creator of this vision for something today that has taken such a foothold. However, you really have to step back in time and put yourself in those shoes.

As an engineer, I would have a natural hesitancy to run anything that sounded as intrusive as it did at the time. Running a computer program from an unknown source on my computer that then is connected to someone else's computer? Not a good idea. In hindsight and knowing more about it today, I can see more of what it was about. However, I really can't fault myself for not wanting to run something of that nature or be a connecting host (a node in today's terms) at the time.

Chapter 15
Mining for Bitcoin

In the early days of Bitcoin, as it was just rolling out amongst a very small number of people, each could have their own desktop computer be used as a node in the network that achieves the blockchain and arrives at the proof of work for rewarding the bitcoin. In those early days, bitcoin had no real value. The value was always in the potential of what it would become. In fact, some that mined bitcoin actually freely gave back some bitcoin to others, both strangers, and people they knew which if held today would be worth many millions of dollars. Its funny today looking back at people tossing bitcoin back around at one another as perhaps someone throws a rock into a pond to see how many skips one can achieve.

One of the more important correspondences by Satoshi Nakamoto occurred on January 8, 2009, at 19:27:40 UTC. It was the announcement for the release of the EXE program which one could use their PC to mine the bitcoin. Most people, even some unfamiliar with the Open-source C++ code, could operate the Windows based program. Satoshi's email reads:

Announcing the first release of Bitcoin, a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority.

Satoshi Nakamoto provides the link to a downloadable Windows EXE program and writes:

- *Unpack the files into a directory*
- *Run BITCOIN.EXE*

- *It automatically connects to other nodes*

There is more detail in the email sent out by Satoshi Nakamoto as to its functionality and noting he made the difficulty of mining the coin " ridiculously easy to start with, so for a little while in the beginning a typical PC will be able to generate coins in just a few hours. "

As noted elsewhere in this writing, Bitcoin starts off very easy to mine to get people interested in it as well as keep it rolling along in a compounding way much like a snowball on a slope. As momentum in mined Bitcoin would build so would its utility, use and store of value.

Today, mining includes giant farms of computers costing many millions of dollars and cooled by the latest technology with incredibly high energy demands all to achieve the same outcome a personal computer did in 2009.

Those early adopters and people willing to have a node on their personal computer were greatly rewarded. At the initial rewarding, 50 Bitcoins would be rewarded on a node owner for completing the blockchain and proof of work. The rewards have a predetermined halving formula embedded into the code as follows:

2009 = 50 Bitcoins

2012 = 25 Bitcoins

2016 = 12.5 Bitcoins

2020 = 6.25 Bitcoins

2024 = 3.125 Bitcoins(April 19, 2024)

2028 = 1.5635 Bitcoins (expected around Mid-April 2028)

And so on until the 21,000,000 coins dispersed over time is reached.

The dates of future halving can generally be approximated, however, due to the method of mining changing difficulty and allocating out coins is a function of both time duration of the blockchain completion (every 10 minutes) and the computing power and nodes on the network, it's not possible to calculate the exact moment for the halving in advance. As the estimated date and time approaches, refinements in the halving moment can occur and become increasingly more accurate until it is finally determined with precision.

The point of all this, for purposes of this book is that Satoshi Nakamoto made it relatively easy at the onset for people to participate in the mining of bitcoin as well as participate in being a node on the network. He had answered some questions early on in the public forum correspondence to assure people could get rolling with it and mine bitcoin. As well as trouble shoot some aspects of it and assure, he had worked out all the kinks. His early communications are a record of some of this guidance and his sincere desire that this be self-fulfilling with no need for oversight or intervention just like a snowball building upon itself down a slope.

Chapter 16
Bitcoin at negative value

Before Satoshi Nakamoto published his White Paper describing bitcoin and its protocols and long before crypto exchanges, the thought to create a bitcoin or digital currency for widespread universal use was quite the moonshot. One had to have very specific knowledge of the concept of a blockchain across a network of nodes, have dedicated hardware and equipment while steep in unique skillsets for use, and willing partners to process and test the hypothesis and application, just as a starting point. Not an easy task in the years leading up to 2009 being in the early evolution of computers and coding. At a time of computer hacking and intrusions or viruses almost being commonplace and limited means to guard against invading intruders, particularly when you would be inviting them into your computer as an established node in a network of blockchain would inherently come with risks and hence costs. Not just the costs of a computer, or your time in setting up and participating in such an endeavor, but also the potential consequences of taking such actions. The costs become specific to the participant at that time and therefore if one had to put a value on the cost of the bitcoin it would be extraordinarily high for the novice but exceedingly reduced for the more guarded and informed.

The greater preparation and skilled one might be, the more it would have diminishing costs per bitcoin as each new bitcoin does not necessarily create a proportional new risk and cost value. The cost in those early initial days would be dependent on its participant largely and number of bitcoin farmed to help set its prelaunch value/expense. The bitcoin held or then redistributed from the node/computer, would also have risk and cost

associated with just this part of it. So, the net value of bitcoin in those early stages would have considerable negative value given the considerable costs in time, energy consumption/mining, holding, securing, distributing amongst other factors. The following summarizes some of these aspects:

- Participant's degree of computer savvy; including fully knowledgeable of hardware, networks, viruses and anti-virus software, blockchain functionality.
- Participant's time
- Energy consumption
- Hardware, computer, internet connection

Equations could potentially be created to formulate the cost of a bitcoin in those early stages of creation given the variables and sets that make up the mining or realization of a bitcoin. However, it's not particularly relevant to the identity of Satoshi Nakamoto other than to convey the steep hurdle that needed to be overcome by an individual with a vision for creating something from scratch that would be used the world over.

In those early days of creation, there is no question that bitcoin had a value that was less than its cost. In other words, it would cost more to mine an award than what one would have from the award as the value was not even $1 per coin for quite some time. At the start, the incentive for anyone to expend their time, resources in computers and hardware, energy or other costs would not be countered for some time to come, and they would be holding bitcoin essentially at negative value.

Chapter 17
"Sovereign Banking"

One might ask, what does banking have to do with Bitcoin. After all, Bitcoin was always intended to be a decentralized currency and void of a third-party association. Free from the pitfalls of banking and financial institutions. Free from losses of one's funds through the insecurity and potential actions of others. This idealistic vision for bitcoin has already proven to be just that, idealistic, with many having lost funds through a variety of causes. Having said this, it can offer newfound security not seen before.

Of late, even the U.S. Dollar has become devalued more and more with some countries moving further away from it. One might question where the dollar is headed. After all, Russia, China and a few others are looking to completely move away from the U.S. dollar and onto currency forms of their own choosing. With the international trading system in place and even with sanctions between some governments, it is still difficult to completely wean off by some governments the dependence on the U.S. dollar. It is likely the dollar will continue to deteriorate in share of global use in the coming decades. Whether gold, cryptocurrencies such as bitcoin, or other forms of transaction occur and replace the dollar fully is yet to be determined.

Why bring all this up? Well, it speaks to why Bitcoin was created in the first place. What was the motivation behind Bitcoin? If one goes back to 2005, 2006 and 2007, the likely timeline of the material development for the bitcoin vision prior to the release of the White Paper in Fall of 2008, one can recall where banking was at that time. Again, Bitcoin's early vision was to eliminate this need for a third party, such as a bank, being involved in the

transaction. So, it is an important element of why Bitcoin was created.

The following is an example in the banking realm and subsequent failings of banking as it might have influenced the creation of an alternative (bitcoin) which eliminates the need of a third party for transacting.

Going back more than a century and in October 1902, Sovereign Bank was founded as a Savings & Loan in Pennsylvania. This bank expanded rapidly in the 1980s and 1990s acquiring numerous other banks. In 2000, Sovereign bought numerous New England branches from newly merged FleetBoston Financial, becoming the third-largest retail bank in the Boston area. As Sovereign continued to invest, grow, and evolve as many banks do, it was subjected to the turmoil of changing and deteriorating economic conditions. In June 2006, another banking institution outside the U.S. established for many years, Banco Santander, purchased a sizable portion of Sovereign Bank (upwards of 20% for over $2 billion). Through various savvy moves, Banco Santander went on to acquire a majority stake in Sovereign Bank with the intention of merging as Banco Santander. The credit rating system of Moody's had downgraded Sovereign Bank institution making it susceptible to further merger/acquisition.

The downgrade of Sovereign Bank was driven by the United States' absence of an effective policy to systemic fiscal challenges that had been rising over time. The common narrative for the start of the financial crises in 2008 suggests that credit agencies downplayed the riskiness of Residential Mortgage-Backed Security or RMBS, drawing in lenders who did not appreciate the intrinsic risk.

In October 2008, Banco Santander completed its acquisition of Sovereign which now was a larger stake for less money than initially set out. Sovereign Bank was severely affected by losses related to auto loans and stock in Fannie May and Freddie Mac. Banco Santander had seen substantial losses in its investment to date but went on to complete its acquisition of Sovereign Bank at much lower costs now on January 30, 2009.

Banco Santander, a new merged conglomerate, much larger and susceptible to a changing economic environment. In 2011, the bank announced plans to formally relocate its headquarters to the U.S. and in September 2011 the bank announced it would officially change its name to Santander as part of its parent company's goal to create a global brand. The rebranding was completed on October 17, 2013.

So, why is all this important? Because during those few years prior to the release of the Bitcoin White Paper on October 31, 2008 and prior to the release of the executable program for mining bitcoin on January 8, 2009 there was much turmoil in the banking and financial industry. Not just in the United States, but elsewhere.

This turmoil and the overlap with the creation of Bitcoin as a decentralized currency is not by happenstance. If one is living through that turmoil and insecurity of the banking system, we can see how this would be motivation to create an alternative to it. One should also recognize that the banking institutions in America, although some failed completely such as Washington Mutual and many lost enormous sums, generally speaking most in the United States are backed by the FDIC to a certain extent. Not always the case elsewhere around the world. So, to think one could have their entire life savings built up over time and to believe it is secure in a bank only to have it lost in one swoop of turmoil in the economy or political environment is disheartening

to say the least. Anyone that cares about the world and would want better conditions for society would want a more secure means of preserving a person's lifetime of work. Bitcoin would potentially offer this under the right conditions.

To summarize, the turmoil occurring in 2008 and 2009 and soon thereafter overlap with much of what was occurring with Bitcoin, its development, its vision to solve a true problem of trust, and has influence with the subsequent known communications by Satoshi Nakamoto. In one such critical communication known as the "Genesis Block" there is an embedded message by Satoshi Nakamoto. What makes this one unique is it was not within the P2P forum or other emails. It was the sole message embedded into the actual blockchain going forward. That very first Bitcoin blockchain has an embedded message together with all the characters that are part of the proof-of-work that ultimately achieves a mined bitcoin. It reads:

...Ethe Times 03/Jan/2009 Chancellor on brink of second bailout f or banksyyy…

Genesis Block –

This caption coincides with the newspaper, The TIMES with the same headline and a story about the banking failures and insecurity of the system.

Clearly, the stability of the banking system in general in the United States and abroad was on the mind of Satoshi Nakamoto and played a role in motivating the creation of a decentralized currency.

Chapter 18
The future of Bitcoin and more importantly blockchain?

What started as a vision to solve problems around the fundamentals of currency, that is transacting in safe and efficient ways and independently of third-party institutions and governments, has evolved into something much more. With the advent of artificial intelligence, the blockchain has become an important piece of the security puzzle. No longer is blockchain useful just for currency transactions.

Ultimately, security is more important and fundamental to all existence on planet Earth than simply a monetary currency. As conflicts continue around the world, security is not just national defense, but security encompasses all aspects of life. Your personal data, your personal freedom, speech, privacy, government, every aspect of one's existence depends on security. And with the potential for adversaries or "bad actors" to intrude upon not just the security of the individual but the security of governments and what most would consider "good actors" this becomes the critical societal goal. I'm convinced the person that is Satoshi Nakamoto is no longer concerned with just the financial aspects of blockchain. Rather societal security becomes a much more far-reaching aspiration. Security in information and security in personal identity amongst other aspects. Security in defense areas, security in all walks of life for all around the world. The blockchain is supported by a network of nodes that provides a means for secure checks and maintaining needed integrity of whatever circumstance that users wish to use it for. Again, the author does not claim to be an expert in blockchain technology. However, it is known that blockchain technology can be used for other purposes beyond currency transactions. The fundamentals

of blockchain or proof-of-work is a rather secure means of communication and transmission. It can evolve and have other uses beyond currency. And with support from A.I. technology and now running increasingly complex and advanced computer chips the potential is really quite mind-numbing. If you can dream it, we will see it in the not-too-distant future.

Chapter 19
Certainty Attained? A summary…

Achieving certainty as to the identity of someone that has been anonymous for so long is not an easy task. Nor is it something that should be taken lightly as to the implications of such an effort. Particularly, given the measures taken by a person which clearly wishes to remain anonymous. It is an assemblance of puzzle pieces that ultimately achieves that certainty and not one particular piece of information. But once the puzzle is assembled, then what? Is it enough to retain that information and simply go on a path in silence never to divulge it? Or to come out and reveal to the world what one knows subject to any number of game theory type outcomes? The path chosen will vary by individual and all I can say is this book is the summation of that thought exercise.

Will this author reveal who this person with such a grand vision is? Not under any circumstance, but one. If the person that is known as Satoshi Nakamoto wanted it to be the case. We already know the great lengths that Satoshi Nakamoto took to be anonymous and remain anonymous.

However, this author has laid out a reasonable characterization of the person that is Satoshi Nakamoto while maintaining his anonymity. The following is a summary of some of what has been described in this book:

1. October 31st is an important date to Satoshi Nakamoto and this author. The importance of this date extends beyond the White Paper release and release of this book.
2. The name, Satoshi Nakamoto, is strikingly similar to a great visionary and influential person during the time in question. This possible influence for the pseudonym was

found following a bread crumb trail of information from what the author knows of Satoshi Nakamoto.

3. Patent experience relative to the aspects of bitcoin and the person the author believes to be Satoshi Nakamoto.
4. Publicly attributable and available communications in style, response tone, and technical knowhow that match the person the author believes to be Satoshi Nakamoto.
5. Living circumstance, the author had observed which is consistent with publicly messaged information later (e.g. floorboard electric heating just as one instance)
6. Timeline for our paths to cross and my early communications with this person believed to be Satoshi Nakamoto.
7. Persona: let's just say the person this author knew was not a social butterfly when we crossed paths nor an extrovert and had a very limited circle of contact. Observed behaviors would be consistent with the communications known to be from Satoshi Nakamoto.
8. The author's awareness of this person's technical expertise and exceptional intelligence which could be at a level capable of initiating something of this nature.
9. This person the author knew wanted an early computer test-run of relatable file to the topic.
10. Reading by this author of a draft version of relatable information prior to the public release of the bitcoin White Paper in 2008.
11. This author was close enough to the situation to have limited information shared in a conceptual manner, yet sufficiently distant for it all to occur. A perfect alignment of stars in both time and space.

Broadly speaking, it's the accumulation of all the puzzle pieces assembled that provides certainty of the person known as Satoshi Nakamoto to this author. It would be difficult for this author to affirm with just one piece of information known. Even reading an

early draft unpublished version of the White Paper does not in itself convince oneself this is the case. It's that in combination with my known timeline, together with conversations broadly on related matters, and the many other pieces of this puzzle which in summation is undeniable in my mind. For some, this will not be enough, and I recognize this. However, any more detail or connection of information would jeopardize revealing someone's identity which clearly does not want that to occur. This desired privacy must be respected – and protected. Not just for Satoshi Nakamoto but for people in society who wish a level of privacy and within limitations and appropriate application.

Although it was the accumulated pieces of the puzzle that provided this author the assurance of the final image, singularly speaking the one piece of the puzzle to point to was the read and conversation of what I now know to be a draft version of the Bitcoin White Paper. I have certainty of the timeframe being prior to the public release in 2008. And I know the general scope of the content as well as the conversation I had with this person at the time. There is no doubt in my mind that as I verified certain aspects years later all the pieces of the puzzle came to fit.

Some of this had been discussed earlier in this book, but some aspects is expanded upon here. Back in 2006 as noted earlier in this writing, I had been asked in a rather casual setting, what my thoughts were on what I believed at the time to just be another technical paper, not all that long, In this technical paper it had the concept of proof-of-work which essentially was a verification of numbers to complete a block. At least that was my take on it at the time.

Of course, at the time of this read through, I had no idea the person handing me this was to become the person known as Satoshi Nakamoto. Or that this was some grand vision for a new global currency. At the time, the concept of digital currency would

have been foreign to me and as much of interest to me as nuclear fusion. However, as an engineer , then and now, I am able to follow along with new ideas and technical writings. Even to an extent technically advanced ideas and conduct my own thought processes of “what if” scenarios in my mind. Having always been a problem solver myself, I believe this trait of problem solving is fundamental to every great engineer.

The concept of a digital world currency at the time seemed like something fun to talk about but seemingly so far out in the future for application that it wouldn't be something that would materialize in my lifetime. Of course I was wrong on the timing, but because of that mentality the significance of what i was reading did not sink in. Admittedly, I did have difficulty following the technical aspects of it. Even today the concept of a blockchain and its security by way of time stamp and verification across a network progressing in time only one way is challenging to fully understand, yet very much of interest to me. There was no going back on the time stamp, and hence security, once the proof-of-work occurred. This is the part that stuck with me even after all these years. I’ve always thought about time travel and the feasibility of it all. However, time travel is a topic for another day.

The short of it all was, the read through and my conversation largely was dismissed at the time and subsequently for quite a while after as something that might all happen with currency but certainly not in any time frame that would be impactful to me. After all there were so many competing methods of currency as it was at the time. And even if the world went in the direction of a digital currency in my lifetime the likelihood of Bitcoin being the sole source or even the dominant player, well who would take odds on that one? Certainly not a practical engineer like myself.

Additionally, from what I recall, currency wasn’t the emphasis of the draft document I was reading, nor my conversation with the

person that would become Satoshi Nakamoto. It was more about the verification process using interconnection of computers to establish a completed validation. As mentioned, the proof-of-work aspect was front and center. The aspect of eliminating the third party to the transaction or need for another party outside of the two direct transactors (receiver and sender) , really wasn't foremost on my mind. That aspect I've come to realize was and is likely foremost on the mind of the creator for bitcoin.

As I look back at all this, its plainly obvious now where all that was headed. The concern with security of banking, the need to solve a problem of trust through a secure independent verifiable transaction. So much was being addressed in so little of a package. It's no wonder, I or anyone else, would not have seen the forest for the trees.

There are some other aspects of this read-through and my conversations pre 2008 but saying any more would risk further privacy concerns.

At the end of the day, the reader can believe this accounting or choose not to believe. Either way, I do not currently know where the person known as Satoshi Nakamoto is located. And we know Satoshi Nakamoto wants to remain anonymous given all that has transpired in the time following the release of the White Paper. It's clear Satoshi Nakamoto had anticipated much of it, but certainly not all.

Having said this, I would like to once again meet up with Satoshi Nakamoto. It must weigh heavy on the soul of Satoshi Nakamoto knowing what has been created and further knowing that coming forward or sharing more could be very problematic. I would certainly understand if this is not ever possible.

The problem solved by the person that Satoshi Nakamoto is clear now to me and to many people around the world. Although it has evolved and transformed into something that in my view is largely contrary to that vision. By having dependence on financial institutions, exchanges, bad actor states, governance and other oversight, bitcoin and other cryptocurrencies have ironically materialized into just the opposite of what was originally envisioned. As we see more and more unrest and divide and many of our systems failing or in turmoil, the need for such a peer-to-peer exclusive system independent of all this uncertainty takes on new light.

What separates great visionaries from the rest of us is the actions to actually put things in motion on a grand scale. For example, Elon musk with the breakthrough developments of reusable and self-landing rockets. Truly great visionaries take action to make great things happen even with insurmountable hurdles before them to solve never before solved problems. Great visionaries take the actions to put the pieces together and follow through to the extent necessary to assure their success. This is the credit to be given to the person that is Satoshi Nakamoto. Satoshi Nakamoto put all the pieces together to create a singular transformational digital currency and followed through with it until likely he assured himself it would be successful. His abrupt silence in 2011, may have been some combination of both the need to protect his pseudonym as well as seeing his vision materializing and beginning to take forward its motion and success as he anticipated.

Chapter 20
Final Thoughts

This author fully recognizes people just want to cut to the chase and reveal the true identity of Satoshi Nakamoto. However, as noted earlier there are real concerns with revealing identities as well as respecting ones privacy when they truly want it to be the case. Besides, where would be the fun in that? Life is an exploration and a journey, not a destination to arrive at without effort.

Many, but perhaps not all reading this, will simply regard all that is written here as a colorful story with no real proof of anything. The author understands this opinion. But to those that say this, I would ask your understanding of the consequence of coming forward with detailed information of this nature. I know in my heart of hearts all the pieces fall into place for full confirmation in my mind. Frankly, that is good enough for me. I don't expect anything to come of all this accounting of my experiences. To those that do believe, sometimes it is okay to have faith in humanity and faith in other people. It is alright to take the belief that there are people around the world with integrity and no alternative motive other than to do right and convey the truth.

Even after all this time and recounting my experiences conveyed in this book, I don't feel the need or desire to come forward. It has only downside associated with it. I have no intention of financial gain or notoriety or any other benefit. I've already explained as much as I care to on the reasons for recounting my experience. Moreover, any awareness of my own identity would only risk exposure to the identity of the person that is Satoshi Nakamoto. Although, I will say it is no one close to me in terms of family or friends or anyone I am in contact with today. And will even say further that no one from family or friends or otherwise

are aware of what I know or that I am the author of this book or creator of a related web site. It is difficult to keep something of this nature under wraps and contained to only myself but have done what I can to minimize the chance that the identity of either Satoshi Nakamoto or myself could be determined by others.

Lastly, I will say it has been very interesting to follow the speculation and claims by others with respect to the person known as Satoshi Nakamoto. I am convinced I have crossed paths with this person in the past which by name has developed into an almost mythical character over time. The analogy I would present is perhaps there were actually dragons that breathed fire in the past. Myths often have elements of truth behind them. There certainly is enough historical evidence of creatures resembling dragons, right? And at some point, other creatures encountered those creatures. Who are we to say that we've found every skeleton fossil and dinosaur remain that ever existed? New discoveries are found all the time. Sometimes it's okay to let the mystique and legend rest in time for all eternity. While other times the discovery and reveal is glorious and surprising but not outside the bounds of possibility. Only time will tell how this all turns out. The author would like to conclude with a direct message to the person that is Satoshi Nakamoto in the chance he sees this:

A message to Satoshi Nakamoto:

I contemplated the idea of once again setting a meet up around the next halving of bitcoin. Since it is predetermined, one can plan around it and as the time nears, it becomes ever more exacting to the minute. A meet up time that can clearly be known for two individuals. The location would be set as the public place

we both first met. With this, each of us having a shared interest for anonymity. There would be certainty to come alone and not share the place with anyone. I would like to say hi again. Maybe laugh a little at all that has transpired. All that was missed. Perhaps a friendship is the real loss. For I am in a good place. I hope and trust you are too. It was and is never about the money. People will say, oh you could do so much with that kind of money. True. But when you already have what you desire. You are content and true happiness occurs. Vast sums of money do not buy joy. Therefore, maybe it's best it all progressed as it has. I wouldn't change a thing. I know some will say I am crazy or a loser or any other number of derogatory terms. But when you are surrounded by those that love you and content in your achievements the need to look back and want to have gone down a different path is negated.

My hope is that in the intervening four years between now and the next halving, Satoshi Nakamoto, you will have trust in this author to maintain your anonymity. And that if we do meet, I will be alone. Only you and I know the location I am referring to. Although the time is being stated publicly without the location known, we both can trust it will just be us. The meet up time being at noon local time on the day following the 2028 halving of Bitcoin. Hope to see you there Satoshi Nakamoto.

– EJH

Throughout this book, and to the end, what the author has provided is the backside of a many piece puzzle. The edges of the pieces visible and together, yet the image still cloaked in mystery. It's the author alone that has the proper facing full color version of this puzzle in clear view. In the interest of privacy for the person known as Satoshi Nakamoto and myself, the puzzle will not be turned over, unless that interest changes. Coincidentally, it's a remarkable image that is possibly cloaked in an exact moment in time determined by bitcoin and its creator that will only tell, yet not precisely known, just yet.

Part 3 – Chapters TBD

The author intends to complete Part 3 of this accounting, at a future time. This will hinge, in part, on the author meeting Satoshi Nakamoto as described in Part 2 of this book. If our meeting occurs in 2028 as described, the release of Part 3 may include more revealing information contingent on Satoshi Nakamoto's desire and perhaps what he may want to say to the world.

I don't necessarily expect Satoshi Nakamoto to reveal his true identity after all this time. I would certainly understand if our meeting does not ultimately occur. I do feel as though this effort was needed, however. If nothing else, it's been therapeutic in mind, body and soul. And if nothing comes of all this, that is okay. I can continue onward down my path knowing I've done what I felt was needed for my own consciousness and relief with this weight lifted off my shoulders.