# 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 <u>not</u> 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.