Perfect Money

How Your Enslavement Ends
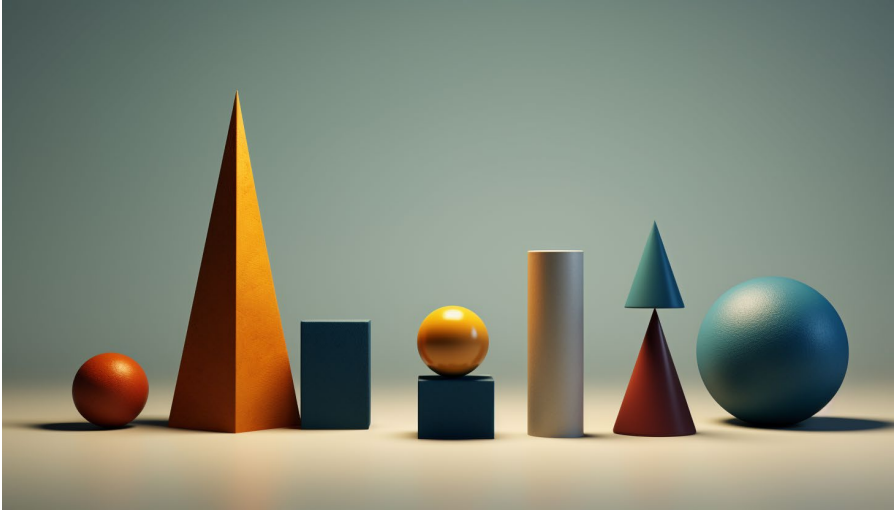
SEAN H. WORTHINGTON

For thousands of years, we have been blinded by governments. Now let us see.

CONTENTS

ACKNOWLEDGMENTS

1. CORRUPT MONEY IS USED TO ENSLAVE YOU

Nearly everything you do is guided by money. Money, as we shall see, is an information system in which you depend on to make decision so that you can receive goods and services that use deserve based on the work you have done for others. Corrupt money is the most powerful tool that can be used to steal from you, and without you even being aware of it. Corrupt money allows others to rob you, your family and your future generations. Corrupt money reduces your life expectancy. It delays childbirth, which leads to unintended childlessness, which is the main cause of low-fertility rates. Corrupt money causes divorce. It causes people to work to madness. It causes stress. It causes mental illness. It causes children to be neglected. It causes unnecessary scarcity. Because of corrupt money, you work like a slave for other people and miss out on the wonderful life you deserve.

Putting You in your Cage

Your enslavers know how to hack the money so that they can gain at your expense. At first, they just wanted you to pay them more for their assets than they were worth. But today, they want you to

pay them rent and give them money for their entire lives. Today, in the United States of America, young people can no longer buy a home unless they have received a gift or inheritance from their parents or are they the rare ones with high incomes.[1] Corrupters were able to highjack the monetary system so that they would receive freshly counterfeited money allowing them to buy all the homes and farms that they could manage. According to the Theory of Perfect Money, such asymmetric monetary inflation is counterfeiting that taxes without representation. But these taxes don't go to government. They go to hackers that will use that power to enslave you for your entire life without you even knowing.

The Young Are Cheated the Most
If you bought your home before 2021, you will have a very low interest rate and an average mortgage of $1,500. If you bought your home after 2021, you will have a very high interest rate and an average mortgage of $3,000. Now it is possible to have two families living in identical houses right next to each other with one needing to make $20,000 more than the other just to survive. And, if we look at people who bought homes 25 years ago, the discrepancy is much greater. What has been normal for all human history is for

adults to retire, downsize and depend on their children. Today it is normal for children to live with their parents until adulthood.

This is not a short-term situation. The situation will become worse and rents will continue to rise. Today, 27% of all homes have one person living in them.[2] These people are able to live alone because the monetary system is corrupt and allows money to be counterfeited and given to them at the expensive of those that work. Without this counterfeited money, they would have to find roommates, freeing homes for younger generations. 46% of people today are single and the amount rises every month. You are more likely to be single because you cannot afford to establish a household. The American dream of home ownership is dead to the young because of our monetary system.

Men On Couches Watching TV While Stoned
What do you do when you are young and all the money you make is secretly taken from you? In America, there are over seven million unemployed men who are not looking for work. They are not developing any skills beyond watching TV for 2,000 hours per year. They are for the most part, unmarried, living with their parents, and getting money from a variety of social programs, especially disability programs. They make up 4.5% of the workforce and are growing. Why should they participate in the monetary system? It's their parents that have all the money. Working would just cost them more that they would receive causing a net loss to them in value.

Born to Pay Someone Else's Debt
The national debt means that everyone born in America owes $200K to the older generations on the day they are born.[4] The U.S. government brought in $4 trillion in 2021 but spent nearly $7 trillion. The government needed to print $3 trillion to make these expenditures. This new money was directly transferred to people over the age of 65 who got to spend this money at its full value while the young had the value of their money stolen without them even being aware of it.

Your children will cost you dearly. $233,000 each.[3] You will pay an average $10,000 per year for childcare and thousands for their college. However, their college may be too expensive for you to pay

and instead they may borrow tens of thousands to pay for it. When they are adults, they may not be able to afford to help you when you need it. Instead, the production they create will be taken and given to help people who didn't even have children.

Enslaved By Academia

Kids today were told that they would make more money if they attended college, but they were not told that college is very expensive, will delay their earnings, that they are unlikely to graduate and that they may actually earn less because of their degree. Only 40% of blacks who enter college will graduate college within six years. For whites, only 65% will graduate within six years. These kids will owe huge debts but will have no income to pay for it. And, in a rather new and insulting phenomena, they may earn less than if they had just stuck with your common sense instead of the pretend-education and indoctrination they received from their Marxist educators. According to research presented by economist Douglas Weber, the odds of college paying off today are the same as flipping a coin.

Anti-White Racism is Here.

People sense there is something wrong. But they do not think to blame the monetary system. Instead, they blame the people who seem to being doing well: old white men. It is now claimed that old

white men do not deserve to have money and that they got their money from standing on the necks of minorities, women and having "privilege". It follows that they must be removed from the workforce, their history must be re-written, their monuments torn down. The Diversity, Equity and Inclusion movement is anti-white racism and corrupt money is the fuel the fires it. Corrupt money is the same fuel that could drive the European race to be marched into gas chambers.

New Evil Money Threatens You
The story is becoming even more dark and disturbing. With the invention of new digital currencies, artificial intelligence, quantum computers and the corruption of the Federal Reserve Bank, your enslavement will become even more terrible as oppressors gain new tools of control.

How to Enslave with Information
Let's look at so-called "Slaver Ants" to understand how information can enslave. Ants have their own information system that they use to coordinate the activities of millions of ants within their colonies. They use pheromones. Pheromones can be thought of as words written with chemicals and read using antennae. Ant antennae are specially designed to detect pheromones but ants can also create pheromones. With these pheromones they can tell each other things like: We need more food. There is food over there. Someone needs to clean the nest. With some exceptions, ants are generalists who can do any job within the colony. Dig, carry, feed, scavenge, fight, etc. A cruel prank to play on ants would be to spray random pheromones from helicopters. They would no longer be able to decide the best behavior to help their colonies and the colonies would collapse.

Slaver Ants AKA Kidnapper Ants
The "slaver ants" send out scouts to locate the colonies of other ant species which they can enslave. When a slaver ant scout discovers another colony, it will return to its nest and communicate the finding by using pheromones. The slaver ant colony will then organize a massive coordinated raid on the victim colony. Once

enough slavers are gathered, they will storm their victims' ant hill in a surprise attack that overwhelms the victims' guard ants. The slavers rush in and snatch the larvae of their victims and carry them back to their lair as fast as they can. They kidnap and run, doing just enough fighting to keep the guards distracted.

Then, the slaver ants smother the victim's larva in their own pheromones. This imprints the larva so when they become mature, they will think they are the same species as their kidnappers and will unwittingly serve them as slaves. This saves the slaver ants from needing to invest the huge number of resources that are required to create and care for new workers. The slavers corrupt the information systems of their victims. You too are a victim of a corrupted information system. You were born smothered in someone else's lies. Your children are unlikely to share your values because they are indoctrinated in Marxist philosophy at public schools.

[1] https://www.msn.com/en-us/money/realestate/how-are-young-homebuyers-affording-homes-these-days-help-from-mom-and-dad/ar-AA1izVfc
[2] https://www.census.gov/library/stories/2023/06/more-than-a-quarter-all-households-have-one-person.html
[3] Cost of having a child: https://www.usda.gov/media/blog/2017/01/13/cost-raising-child
[4] https://www.statista.com/statistics/203064/national-debt-of-the-united-states-per-capita

2. PERFECT MONEY – BRILLIANT FUTURE

Perfect Money: Ending our Enslavement

Imagine if you will, a future where there are no national currencies. Instead, there are *natural currencies* that are distributed among Earth and Space in a way that make them incorruptible by even the greatest powers on Earth. People trade by verbally passing symbols that they store in their minds where they cannot be detected or seized. These symbols are authenticated by a distributed global counterfeit detection system called the *Redundant Array of Independent Detection Agents*.

Because people refuse to use national currencies, governments and central banks have become powerless to use their national currencies to tax, cheat and manipulate. Tax systems have all but disappeared. Only taxes on land and homes (wealth) are possible. Governments went into decline as their income was limited to fees, bonds and donations. Because of this, they lack the money to fund wars, wealth redistribution schemes and wasteful programs.

There has been a massive population collapse due to the present-day monetary systems. With few people, cities, with all their roads, sewers, gas lines and other infrastructure have fallen apart and have gone back to a wild state. This is similar to today's Detroit. Now everyone lives in either gated communities or in the so-called "hills". With off-grid technologies, flying cars and shopping via drowns, people now live far away from each other.

State schools cannot be funded. What little taxes are collected go to paying for police and the judicial system. Nearly everyone's children are home schooled and receive an amazing education. Kids learn real knowledge and how to think critically, argue logically and treat others with respect and kindness. They have also learned so much more facts than any other generation in history. They are part of a new generation called "off-grid kids" and they have no citizen ID number and governments don't know they even exist. Still, the kids will get in the self-driving heli-drone to meet other kids for sports, play, church and even scouting.

Banks
In the future you are paid in digital cash that arrives to you electronically. You will receive your income by email, text message, or website downloads and it will go directly into the bank on your desktop. You will never be forced to use a bank except for the banks on your cell phone and computer. These desktop banks will pay your bills automatically on the dates you specify by sending emails with money attached. Your banking software will also automatically send any unused money (via email) directly to investment banks where you can withdraw it in seconds should the need arise.

Private banks will completely change. There will be no physical tellers, vaults, loan officers or buildings to house them. These investment banks will give you a respectable interest on your savings, and will fund the great inventions of the future.

Commerce

You will be able to buy anything from anyone in the world using your computer. All laws dealing with customs and tariffs will be ignored and useless. Virtual global organizations made up of people unhindered by bureaucracy will flourish. Drones secretly carry goods across borders at a rate that governments cannot afford to police.

It is possible to get medical advice from any doctor in the world. There is no point for a government to try to enforce medical licensure. In fact, so many laws and regulations that the government created long ago are forgotten as enforcement is impossible. Labor laws will be futile too. But who will make sure things are done fairly and without fraud? It won't be governments. Free market institutions will form to fill this niche.

Because you use digital money, you are very efficient and productive. You can search the whole world to find the most efficient products, services and employees for you. The whole world is also able to search for you and hire you to work for them. This means you are able to be paid much more than you could with fiat money and you pay much less for all your expenses too.

With perfect money, you are richer. No one is taking your money

from you through taxes. Your money does not lose its value from dilution. You are able to make better decisions because you are not being tricked by the fake prices created by fiat's boom and bust cycles. People are not at each other's throats because of inequality caused by corrupt money so there is social peace. You can actually afford to own a home and have plenty of money left over to have a successful marriage, happy children, spare time for vacations and leisure. Most importantly, you are getting what you deserve, you are happy, free and control of your own life.

Putting Things Together

According to the laws of thermodynamics, everything falls apart, everything entropies. Things go from a state of organization to a state of ruin. However, there is an exception and I am going to call this the Fourth Law of Thermodynamics: It's Life. Living things have senses, they bring in information through those senses and put that information into biological circuits. These circuits are infused with knowledge and this knowledge is processed with the incoming information in a phenomenon we can call intelligence. Intelligence is comparing options and choosing actions. Actions are executed in the physical world by a lifeforms' use of its physical faculties. I call these physical faculties "Rights" or "Natural Rights". For us people, our natural rights include our thumbs that allow us to use tools, tongues we use to communicate, and our big brains

that allow us to create the monetary systems we use to organize our civilizations.

When life forms act, let's call that action work because a common definition of work is: "Physical or mental effort or activity directed towards the production or accomplishment of something". Work requires information. Bad information confuses us. Good information helps us to act productively and efficiently. Monetary systems are information systems. Without them we have no civilization. With good monetary systems, we can have good civilizations. With perfect money, we can have the most prosperous civilization possible assuming we have freedom.

Information is not enough. We need to be free to use our faculties (our "Natural Rights"). Perfect money allows us to achieve a much higher degree of freedom than would otherwise be possible. Now, for the first time, we possess the technological capability to establish a nearly perfect monetary system. The potential benefits of this are Utopian; With such a system, people who are able to exploit the shortcoming of the current system will be bucked off like a rider from a horse.

A Perfect Monetary System Starts with a Theory
With a Theory of Perfect Money, we can answer important questions like:
• What is money and what does it represent?
• What came first: Money or Governments?
• What are the desirable characteristics and features of money?
• How much money should there be?
• Who should create money? Governments? Banks? Companies?
• How should new money be added to the system?
• What are flaws in monetary systems that should be fixed?

Creating a perfect monetary system will give us some major advantages
• Flaws in current economic theories will be apparent and we can more closely agree on a just monetary policy.

- Inequality caused by a defective monetary system will be reduced.
- People will be able to make better decisions, leading to greater productivity and greater efficiency.
- There will no longer be false boom cycles that lead to true bust cycles.
- There will be fewer government regulations that are needed.
- We will be accurately rewarded for the value we produce.
- Charity will increase because of greater surpluses in income.
- There will be less war and military expenditures.
- There will be no so-called "inflation."
- There will be steady economic growth.
- We will have the most efficient economy possible, in relation to current circumstances.
- We will have stronger families and will experience a general increase in global happiness.

Finally, Money that will unite Jesus, Darwin and Tech

Rudyard Lynch runs a YouTube channel called @WhatIfAltHist. He argues that there are four religions fighting for control. Darwinists (10%), Machine Worship (15%), Marxists (25%) and Christians (50%). Lynch says the Marxists have already seized all institutions public and private and have corrupted everything. I say that Perfect Money is the most effective way for the rest of us to unite and squash Marxism for good.

3. THE TRUE ORIGINS OF MONEY: MESSOPOTAMIA 8000 BC

Tokens from Tepe Gawra, present day Iraq, ca. 4000 BC. Courtesy the University Museum, the University of Pennsylvania, Philadelphia.

Before we get into the Theory of Perfect Money. Let's talk about how money began so the theory will be easier to understand. I can assure you that unless you are reading this book for the second time, you know nothing about how money truly came to be.

Archeology interpreted through the discipline of Computer Information Systems Management
What follows are my own original ideas supported by the physical evidence. No one else has ever interpreted the physical evidence in this way, so what you are about to read should blow away any other theories about how money started. Money did not just start one day. It evolved over tens of thousands of years. If you are like me, you will be very skeptical of my claims here. This is why I will back up my claims with citations immediately following.

Mesopotamia 8000 BC
Ten thousand years ago, the last ice age was just ending. The ocean had just risen by 400 meters, swallowing up any coastal dwellings

that may have existed. Areas that were dry before, such as Mesopotamia, suddenly became wet with rain. The people were still in the stone age and just learning how to farm. They hadn't invented irrigation yet and scythes made out of copper would need to wait another three thousand years. There were no kings, governments, armies, numbers, or writing. However, they had just invented ceramics. Amazingly, there new ceramic technology was not at first used to make pots or vessels. Instead, ceramic technology was used to create geometric solid shapes. Keep in mind that pottery and ceramics are different. When thinking about ceramics, think about toilet bowls. The Mesopotamians fired clay geometrical shaped objects in their recently invented kilns at thousands of degrees Fahrenheit to convert them into a hard insoluble ceramic. What they created was data.

"When tokens were invented, they were great novelties. They were the first clay objects of the Near East and the first to be fired into ceramic. Their shapes also were revolutionary since, as Cyril Smith has pointed out, they first exploited, systematically, all the basic geometric forms." ~Schmandt-Besserat pp 17

The Invention of Data

Archaeologists have called these objects "tokens", "counters" or simply "clay objects". These solid shapes include spheres, cubes, cones, disks, pyramids and more. To archaeologists, these shapes seemed to be symbols. Symbols that represented something else. Perhaps the cubes represented the number 5 while the spheres represented the number 9. Maybe one cone was one bushel of

wheat while a pyramid was a goat. Or maybe they were just game tokens used in a game that didn't use a game board. Keep in mind that the wheel and thus the pottery wheel wouldn't be invented for another 4,000 years and writing would be in 5,000 years.

"Plain Token: Token typical of the periods between 8000 and 4300 BC and after 3100 BC. The shapes are mostly restricted to cones, spheres, disks, cylinders, and tetrahedrons." ~Schmandt-Besserat pp 13
Photo: Ziyaret Tepe Archaeological Project

As a person with a PhD (ABD) in Computer Information Systems, I understood these tokens to be data. Data are symbols with meaning. However, this data was significant because the data is "self-symbolizing". Self-symbolizing means that a sphere symbolized a sphere, the cube symbolized a cube and a disk symbolized a disk. These symbols were quite beautiful and extremely advanced for stone-age people. How would they even know about these solid shapes?

This data was the most primitive that data could be because it didn't mean anything besides itself. However, the use of ceramics to make the tokens gives us a clue to what they were used for. These tokens were high-tech items at the time. They would have been extremely difficult to counterfeit. Earthenware files at 1800 degrees while the tokens were probably fired at 2100 degree. Hotter than lava! That takes knowhow and resources that were not possessed by the

typical person.

> *"It is not at present possible to establish the meaning associated with each token type"*
> ~Artifacts of Cognition: The Use of Clay Tokens in a Neo-Assyrian Provincial Administration, John MacGinnis et al.

These solid shapes were not counters or symbols that represented sheep or bushels of grain. They were "authenticity tokens" and were used to stop the counterfeiting of "rights" to resources.

There Were Large Numbers of Tokens Found in Hundreds of Locations in Mesopotamia.

> *"The catalog of seven thousand tokens has been compiled by studying the collections in the museums where they were stored"*
> ~ Schmandt-Besserat pp 31

The Invention of Locks and Keys

Looking at the context of where these authenticity tokens were found, it is clear to me that these geometric shapes were used to create the first locks and keys which would later evolve into the first money.

Back then, the first farmers had a real problem. They needed a place to store their grain where it was safe from barbarians, theft, fire, pests, and floods and other catastrophes that could ruin them. The answer was to store the grain in "banks." These were buildings managed by priests and constructed from their newest technology: bricks. The problem was that the priests could not remember which farmer owned which grain. There was no writing at that time and they didn't even know how to make scratch marks to represent numbers. They did not have symbols, let alone symbols for farmers and store rooms. If the priest forgot (or never learned) the relationship between the farmer and the storeroom, the farmer could lose access to his grain. And what if the priest died taking all the information with him? What they needed was authentication. They needed a way to authenticate the farmers without the use of writing.

"The data available on the structures associated with tokens indicate that the 'counters' were often located in storage facilities and warehouses." ~ Schmandt-Besserat pp 97

Authentication can be achieved by having a shared secret between the farmers and the priests. If we think about modern day locks and keys, the key and the lock share a secret. The shape of the key is the same as the shape of the lock. The Mesopotamian were successful in creating the first locks and keys. These locks and keys were extremely primitive by today's standards but very clever for people whose greatest technology was bricks.

To make their locks and keys, they would first need two containers (Data-stores). One to hold their key data (authenticity tokens) and the other to store the lock data. The lock data was probably contained in a bowl made from clay. This bowl would have been filled with sand and the tokens hidden under the sand. This bowl would have been located near the door or the storeroom. Most were found just inside the doorway.

The container for the key was probably a leather sack. To create a

shared secret, the data in both the lock and key containers had to be the same. The priests would put the exact number and type of tokens in each container. The shapes they used were picked by random to thwart guessers.

"Their distribution through the palace does not allow for any further conclusion as to their use or significance. All contexts in fact appear to be random, the tokens chance-finds"
- Artifacts of Cognition: The Use of Clay Tokens in a Neo-Assyrian Provincial Administration. John MacGinnis, M. Willis Monroe, Dirk Wicke, and Timothy Matney.

Again, the bowl would become the lock. These "locks" would be placed just inside of the doorways of storage rooms. The leather-bags with the matching tokens would be given to the farmer as the key. Now the problem of authenticating the owner of the grain has been solved. We assume that when the farmer (or anyone else with the key) shows up to access his grain, he gives his key (the sack of authenticity tokens) to the priest and shows the priest which storage room he owns. The priest then compares the contents of the farmer's leather sack to the contents of the bowl inside the storage room. If they match, the priest lets the farmer in. With this system, no one has to remember anything and there is no need to have writing technology.

"No impression of textiles has ever been recorded, either on tokens or on the floor where they were recovered. It is more likely, therefore, that leather was preferred to cloth for storing the clay counters."
~ Schmandt-Besserat pp 97.

The system was also used at the gate houses of cities. People may have had to show keys in order to gain access to the city.

"Eight buildings of Habuba Kaira, including one of the city gates, produced sixty clay 'counters,'" providing a unique insight into the distribution of tokens in the fourth-millennium Syrian city."
~ Schmandt-Besserat pp 97.

Permissions

The Mesopotamians may have also created a system that allowed the keys to include permissions. This would allow a key to be broken into parts and each part would give the user a different permission. Suppose you wanted to let your assistant go and count how much grain you have but you did not want to allow him to remove any. Or suppose you want your son to be able to remove grain but not change the key so that you would be locked out.

Permissions could have been implemented by making different shapes mean different permissions. The cylinders, for example, could represent the ability to see the grain. So, if a person wanted to just look at how much grain there was, they would only need to know the number of cylinders in the lock but would not need to know the correct number of cubes or other shapes.

The cones may have represented the "remove" permission that allowed the user to remove grain. If a person wanted to remove grain, they would not only need to know the number of cylinders but also the number of cones. The spheres may have allowed the user to change the lock. Changing the lock would require the user to have all the key parts including the spheres, cylinders and cones.

The permissions could have included: Inspect grain, Transfer to another room, remove a small amount, remove a large amount, add new grain, Change key, or Full control. There may have been special permissions like "rearrange room" and "seal door." Actually, this is unlikely but it could have been done.

With this kind of permission system, there would be more keys that had full control as all keys would need to have that permission. Some people may have no interest in giving their key permissions so other tokens would be used less. So, we may see more spheres that are needed to grant full control than cylinders that are required for just read permissions because anyone with the spheres automatically gets read permissions.

Keys To Heaven

"Tokens, together with other status symbols, are sometimes included in the burials of prestigious individuals, suggesting that they were used by members of the elite." ~Schmandt-Besserat pp 107.

Soon after, I think something interesting happened. Tokens began to be made out of highly polished stone instead of relatively inexpensive ceramics. I believe that the priests of the time figured out a way for them to get some extra grain from their followers. Like the indulgences of the Catholic church, the priest sold "Keys to Heaven." If you can create a key to a storage room, then why not create keys to other resources much more valuable, like to the doors of Paradise? The priest could sell these "heaven keys" at a high cost so that only the wealthiest could afford them. At these prices, priests would make them out of stone instead of clay to make them more valuable.

"The manufacture of the plain clay token was simple. It required neither skill in craftsmanship nor complex technology. In fact, tokens could be shaped by anyone without the help of any tool."
~Schmandt-Besserat pp pp 30.

I can imagine that the priest would attend the funeral of the person

who died and pull out a jar (the lock) where he had long ago hidden random tokens in. He would take the key from the corpse. He would then break the jar open to reveal its contents. If there was a match, between the tokens in the jar and the tokens in the dead's sack, he would declare that the person had entered heaven! If a jar was already broken, it was automatically labeled a fake - which probably never happened.

This system would allow a single family to buy a key and use it for the first family member who died. They could also sell the keys to others to creating a nonfungible token.

Keys To Hell

The next evolution of the Mesopotamian monetary system was the creation of spells designed to either summon demons or banish them. People would purchase sacks full of random tokens from the priests and then burn the sacks in their hearths. Burning would activate the key so that a portal could be opened. Humans made of water, demons made of fire, the demons would be expected to dwell in their element.

These keys to "demon gates" would be placed in special data-stores that were impossible to open without destroying the container. These containers were flammable and probably made out of basket

material or pulp that was sealed by some kind of pitch, glue, or paint. The priests would want a pyrotechnic display when they were burnt.

"It is puzzling that counters were located in fireplaces…One of these houses was still filled with long spouted jars that held a black, powdery substance." - Schmandt-Besserat pp 97.

Forgotten Technology
The reason I recognize this lock and key technology as the beginning of an ancient monetary system is because I, myself, have a patent on a modern version of this technology: USPTO #10,650,375 Method of Authenticating and Exchanging Virtual Currencies. I implemented this technology in a digital currency called CloudCoin. It is the World's first digital cash.

From Keys to Money: The World's First Fungible Money
Back then, if you didn't work as a farmer then you probably worked as a priest. Priests would have been able to do all the work that farmers did not do, including being a doctor, therapist, magician, advisor, artist etc. There was not much to know about any of these subjects so it would have been easy to learn them all. The priests were able to create temples by rallying followers. They took on the role of being bankers by storing grain in the temple warehouses. There were over 3,000 gods back then so it was easy for priests to specialize and gain adherents. However, it is clear that there was no centralized religion and no governments. Kings would not arrive for another 3,000 years.

Priests would each create their own "blessings" to pay the workers who created their temples. These blessings were just keys that could be traded to others. They were pretty much exactly like locks only they were not backed by grain and did not open magical portals.

But the system still had a problem to overcome in order to be real money. The money that the priests made had to be counterfeit proof, otherwise it would lose its value. The Mesopotamians then faced the same problem that I faced when creating CloudCoin.

How can we make money that is file-based/clay-based? Anyone can counterfeit by simply making thousands of copies of the file/clay. After much thought, I realized that it does not matter how many copies of a coin there are. What really matters is that the owner of the coin can only spend it once.

Here is How I Stopped Double Spending with CloudCoin:

Suppose that I have a data-store (file). In that file are 25 passwords composed of sixteen random tokens (hexadecimal numbers similar to clay shapes). Because I have the file, I know the passwords. Whoever knows the passwords is the owner. If I give the file to you, then you know the passwords too. Whoever knows the passwords can take the file to the server nodes and authenticate them and then change the passwords. Now you have become the new owner because you are now the only one who knows the passwords.

How Mesopotamians Stopped Double Spending with ClayCoin:

Suppose that I have a data-store (leather pouch). In that pouch are up to 9 clay random tokens (data). Because I have the pouch, I know what the random tokens are. Whoever knows what the tokens are is the owner. If I give the pouch to you, then you know the tokens too. Whoever knows the tokens can take the pouch to the priests and authenticate it. The priest has a record of what is in the pouch. These are called impressed tables and he created them when he created the pouch. The priest will smash open the clay ball and compare it's contents to his impressed table. If they match, the coin is authentic. The priest will then issue the new owner a new coin to replace the old.

First Money: Sacks of Solid Shapes

Now these sacks of solid shapes were real money with integrity. There was another epochal invention here: impressed tablets. These tablets that priests used to record what symbols were associated with which money required a new technology: A very primitive writing system.

"The more than 650 tablets were stored in10 jars in a room of the outer courtyard of the Assur Temple. Four of the jars were fairly well-preserved, and three carried an inscription naming the owners - or rather responsible officials - of those archives."
~Artifacts of Cognition: The Use of Clay Tokens in a Neo-Assyrian Provincial Administration, John MacGinnis, et all 2014, Cambridge Archaeological Journal 24.

Impressed Tablets

A writing system uses a set of symbols and rules to encode meaning. The priests came up with a way to encode their authenticity tokens (solid shapes). They could simply take a lump of wet clay and press the authenticity tokens into it so that the impressions of the tokens would be understood as the contents of the pouch. Although it is very primitive, this is technically writing because the symbols are no longer self-representing. While the solid shapes in the pouch were pure data, these impressions in clay could be understood to mean the solid shapes in the pouch. The impressed tablets were abstract symbols that meant real tokens.

If these assumptions are true, this would be the first form of writing. Since they had not invented a pencil or any other writing utensil, the information was written by pressing the key's solid shapes into clay.

Note that the word "signs" used in the quote below is used to describe the impressions made by tokens:

"The techniques for impressing signs on tablets were the same as those used for envelopes. For example, signs were still made by pressing tokens against the surface of the tablets. This is the case for Sb2313 of Susa, which bears three large wedges showing distinctly the entire outline of the cone used for impressing them. Furthermore, the signs corresponding to pinched spheres, ovoids, and triangles had to be impressed with tokens since no stylus could have assumed such shapes. "- Schmandt-Besserat pp 136.

These impressive tablets were probably created for security reasons. Tokens in bowls could be switched by corrupt guards so that counterfeiting was possible due to inside jobs. However, this problem could be solved if tokens could not be switched around and the tablets stored in jars whose lids could be sealed with clay in rooms whose doors could also be sealed with clay. These seals allowed the priests to detect tampering of the data.

"It is remarkable that each of the 17 impressed signs can be traced to a token prototype."
- Schmandt-Besserat pp 133

Additional Protection from Counterfeiting

The next step in the evolution of Mesopotamian money was the invention of additional counterfeit prevention measures. This invention took another 5000 years to develop. To reduce counterfeiting, increase the people's confidence in the currency, and reduce the number of counterfeit detections that the priests were required to do, they developed cryptography.

Instead of putting the authenticity tokens in leather pouches, they decided to hide authenticity tokens in 2-inch clay balls. They then rolled a cylinder seal on the outside of the clay ball before it dried.

This seal would have been very difficult to counterfeit. Then they included the equivalent of a serial number to the outside so that the priests could find the matching tablet where the matching data was recorded. The purpose of the seal was also to show the user who the administrator was so they knew where to get it authenticated. The clay ball above was probably made by a priest who worshiped the god of the horses and lions. The ball is only two inches wide.

Cryptography

Cryptography is the process of hiding information so that only the person that it is intended for can see it. To achieve authentication, there needed to be a shared secret between the priests and the money (clay balls). The shared secret was the authenticity tokens inside. To keep the secret, priests hid the authenticity tokens by simply covering them in clay. This must have been one of the first cryptography methods known to.

Counterfeit Detection

To repeat, if a person was offered a mud ball as payment but suspected that the mud ball was counterfeit, both the buyer and the seller could go to the counterfeit detector (priest) and have the mud ball broken open to see if the tokens matched what was recorded on the administrator's tablet. If the mud ball was good, the administrator would then issue a new mud ball to the new owner.
This new mud ball would have a new and different combination of tokens hidden inside. This was very efficient because mud was cheap and the priests had the time. Because of the counterfeit protection measures already in effect, it was probably rare for the administrators to need to inspect the balls.

The Results

Thanks to this first money, humans for the first time came together to form a "collaborative specialized workforce" where jobs and professions existed for the first time. The first economy. The first civilization. The first free market and the first Capitalism. The money that was made out of simple clay. All this in a time when mammoths were still believed to walk the earth and three thousand

years before the great pyramids were constructed.

FIRST MONEY

Clay envelopes concealing covert cryptographic self-symbolizing data using ceramic solid Shapes

10K to 3K Years Ago

What Came First? Money or Government?

The answer is Money. Money is required to enable more than one hundred people to organize a proper economy where people are dividing labor efficiently and productively without a dictator that owns everything. Civilization in Mesopotamia developed at the same time as their money which was created out of ceramic authenticity tokens. That was six thousand years before governments.

8500 BC	Money Created From
8000 BC	Authenticity Tokens
7500 BC	
7000 BC	
6500 BC	
6000 BC	Impressions
5500 BC	
5000 BC	Clay Envelopes
4500 BC	Pottery Wheel
4000 BC	
3500 BC	Transportation Wheel
3000 BC	
2500 BC	Writing
2000 BC	Government
1500 BC	
1000 BC	
500 BC	First Metal Coins
0000 AD	
1000 AD	
1500 AD	
2000 AD	Today
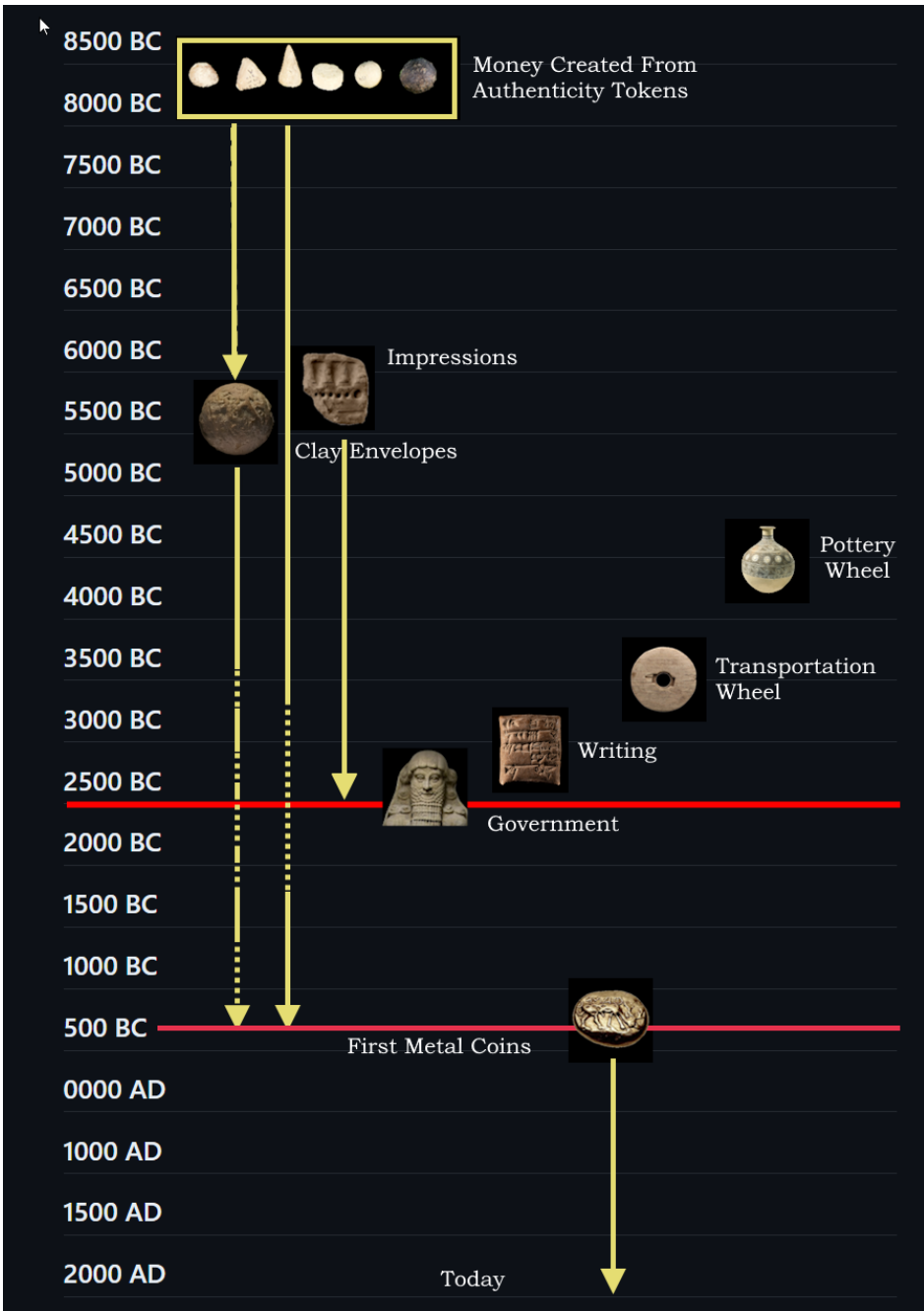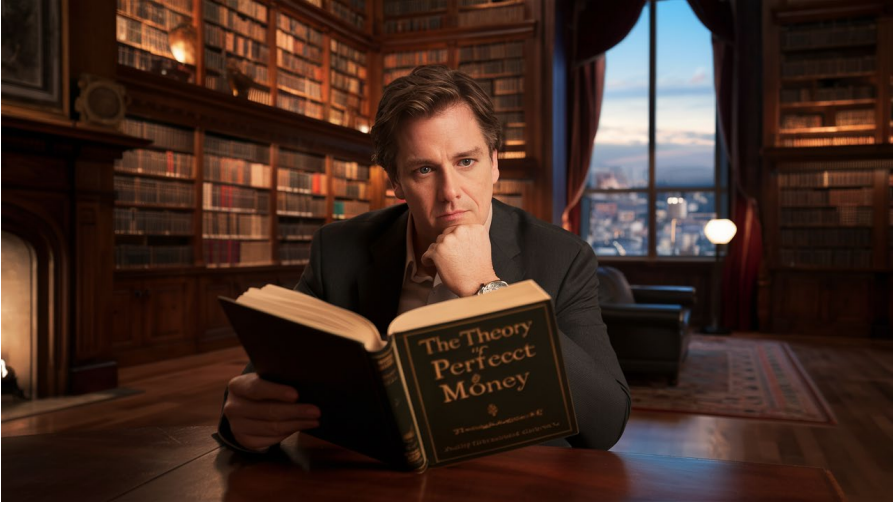
4. HERE IS THE FIRST THEORY OF PERFECT MONEY

What is the Theory of Perfect Money?

TPM (Theory of Perfect Money) is an idea of how money should be in order to create a just civilization that is able to maximize its productivity and its efficiency. TPM answers questions such as how much money should there be? How should money be created? Who gets the money that has been created? What is monetary inflation? And other things such as denominations. Included in this are some very new ideas including what it should be in terms of its confidentiality, availability and integrity.

TPM is a "Normative Philosophy" and a moral philosophy that prescribes what actions we people should take to be good and moral. As a moral philosophy, it is extremely important we understand that this is only a theory and has yet to be shown to work in practice. No one should think about forcing everyone to obey rules set out here and I can guarantee that some of my thinking here will change with new information. There have been many instances throughout history where moral philosophies have led to great death and destruction including the philosophies of

Marxism, Nazism, and many religious moral philosophies. The modern-day philosopher, Stefan Molyneux, has warned in his book, "Universally Preferable Behavior," something to the effect that those who would create moral philosophy should be very careful because it might end up killing people. I am certain that the TPM will provide the roadmap to great freedom and prosperity, still...do not close your mind to other possibilities.

Universally Preferable Money?

How do you like your money? Do you like to lose it? Do you like to have it stolen? Do you like it only to be usable Monday through Friday between the hours of 9am and 5pm at the General Store and only to buy certain products? Do you like it to be heavy? Do you like it when it goes down in value? Do you like it when your purchases are posted on Facebook so that everyone knows how much money you spent at the medical clinic? Do you like it when everyone knows how much money others gave you, who those others are, why they gave it to you and when?

Do you want everyone to know how much welfare you receive, taxes you paid and how much taxes you did not pay? Do you like it when someone else says that they are you and buys things for themselves using your money? I have yet to do a survey, but I would bet that most everyone in the world who uses money would have the same answer: NO! That's why these preferences are universal.
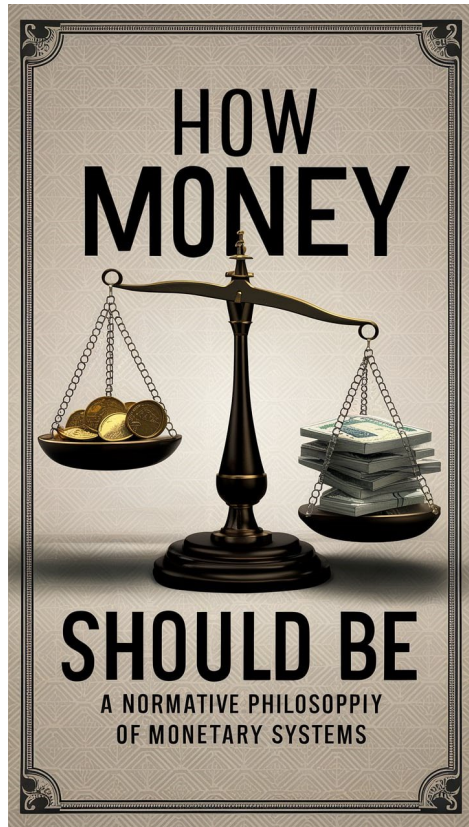
But there are more questions:

- Do you like it when people are able to steal from you without you being able to detect it?
- Do you like it when the government taxes you without you even knowing about it? (Taxation without representation)
- Do you like working so hard only to find that you cannot purchase the things that you were working for because the price has gone up so much that now you can't afford it?
- Do you like it where there is tension between races, sexes, rich and poor because the monetary system creates injustice and inequality by favoring people who get newly printed money?
- Do you like it that people who should not be able to buy anything can live in mansions while those who should be able to live the good life struggle to feed themselves?
- Do you like it that the well-being of generations is being wiped-out?
- Do you like war in which everyone is worse off at the end or dead?
- Do you like it when the government gives trillions of dollars to rich bankers so that the government doesn't go broke because of their own stupid decisions?

If you answered 'No' to all these questions, then congratulations, you are a human and now you have been introduced to the theory of "Universally Preferred Behavior." The TPM explains why these are all big "Nos" and what we can do about them.

Do We Even Need Money?
I hear it all the time: The future will be like Star Trek and they don't use money. Or, we will have a "Post Scarcity" economy. Or a "Resource Based Economy" and we will not need money.

At minimum, we need to feed ourselves and our children. Essentially, we need an information system that will allow us to collectively figure out what job each of us needs to do to collaboratively put food on the table. But this seems like an easy enough task. Why don't we just take the food that is grown and

divide it among us and we can all eat? Ok, but our population is so large that it requires nearly every acre of arable land to feed the millions in our cities and that requires fertilizer, tractors, trucks, and farmers. Okay, then we will assign someone to make the fertilizer and some other people to make the tractors. Yes, but fertilizer needs to be created in chemical plants and those plants need metals and materials that must be mined. So, we need mines and mines require mining equipment and people who know how to operate it. So, we need schools for farmers and miners and that means we need a college and that needs to have light bulbs to light the rooms and … dang, a million other things.

Our food system is based on technologies that are based on other technologies that create a pyramidal-web of dependent variables.

If we are to have more than a few million people on the planet, we need a way to organize ourselves so that everyone is productively and efficiently creating something that will contribute to putting food on the table and so that everyone is conserving what they have and that the food is distributed to everyone and not left to rot.

All that work just to feed ourselves. But we would also like to live in houses, have some fun and go on trips. Okay, now we have a huge number of other jobs that are needed.

We tried coordinating all these activities with a central government (Communism) but it didn't work! Forty-seven million people starved in Communist Soviet Union's Holodomor Famine. Communist China lost 50 million to starvation and these are just the worst. With command economies, you can forget about quality housing, entertainment, or vacations in Florida. You will be lucky if you are treated better than a pig who is never let out of its pen.

But, what about the Spartans of Ancient Greece? One of them came up with the idea that they could all be equal. But then the question was asked "Who will do all the work?" The answer: The slaves of course! The Spartans enslaved tens of thousands of Helots who did all the work needed to keep the Spartans fed. Soon, we can

do the same thing, except replace slaves with robots. With robots, there is no moral downside. There are potential job losses that we will talk about later in this book. Still, there is no decision support system better than money.

Capitalism: Decisions Based on Information, Numbers and Math

Monetary systems are information systems and they give us information that we need to become productive and efficient to make a living and have a family. Money does this by giving us actionable information. What should you do when you wake up in the morning? Money tells us to get a job so we can buy food and eat. But what job should we get? Money tells us to take the job that pays the most because that is most likely the job where we can produce the most value.

What food should we buy when these gallons of milk and cartons of eggs look identical in the store? Money tells us through the price of the products which one was made the most efficiently, and we buy the cheapest. This is an oversimplification but it makes the point that money is our system of mass coordination.

Without monetary systems, our nations would implode because no one would know what to do. If some great force, such as a government, was to meddle with this system, they could cause people to do a lot of incorrect behaviors as has been shown historically.

Progressives have tried other systems like Communism. The Soviets had hordes of economists who would figure out how much of each product their economy should make and how much of a price those things should sell for. They decided who did what job. We have "been there and done that". Communism performs much worse than a free market economy with a good monetary system. A major problem for authoritarian systems is that everyone has their sense of "value" and not even authoritarian systems are able to know what people want at any given instant. Thus, Communism can never give people what they value, only what the authority

thinks they value or what the authority thinks they should value.

But can't we just have a quantum AI computer tell us all what jobs we should do? We could just check our computers in the morning and be told what is the best action for us to undertake. It would tell us where to work and what to buy. Maybe this system would be so efficient that we would all have awesome lives?

Myself and many others have concluded that General Intelligence AI is dangerous and should never be created let alone allowed to run our economy. It is fine if each of us has an AI program that helps us make specific decisions. But there is no theoretical way that we can create a Super Intelligent AI without it threatening our existence. And, according to some science fiction, such as the Terminator movies, AI may make the decision to destroy us within seconds of becoming self-aware. This means we should not create AI that is conscious and any AI that would run our economy would certainly be conscious.

With super intelligent AI, we will have the problem that AI will not know what you want every second of the day and what you value at any given time. Instead, it will have you do what it wants so it can achieve what it values. Besides the danger of AI, it is still unlikely that a quantum computer would be able to match the computational power of seven billion human brains working in parallel, especially if each has their own quantum computer.

Money forces us to economize. We only have a certain amount of money so it limits what we buy and encourages us to produce more. Authoritarian systems have found other ways to limit what we can buy and encourage us to produce. They can put us in gulags, feed us the bare minimum rations and threaten us with death if we don't work. Not only do they make our lives hell, they also do a poor job at creating an economy that can even feed us.

We need Perfect Money

TPM will help civilization reach its full potential. Everyone's' lives will be better with the exception of those who are currently living at the expense of everyone else. More people will be rich and there will be more charity. This will help everyone, especially the poor. When people are efficient and productive, we can afford cleaner air, better health and longer lives. This will even help wild animals and vegetation as we can afford to respect their needs. Perfect money allows us to "pursue happiness" based on what we value as individuals.
.

Overview of TPM

There are general principles of TPM and each of which can be broken down into several subcategories.

The major categories are:
     1. Confidentiality
     2. Availability
     3. Integrity
     4. Preferences
     5. Principles

Overview of Confidentiality

When Facebook said it would join a Consortium to create a new currency, everyone was so alarmed because it was seen as a threat to privacy. Privacy is something we may not think we need, but in fact it is crucial. Also, we may think that we need privacy but others do not. The Philosopher Ayn Rand once said that "Privacy is the movement towards Civilization." I agree.

With total privacy, we would achieve the highest form of civilization and we might not even need governments. In order to evaluate the "perfection" of a monetary system, the following criteria can be evaluated. Note that I will go into much greater depth in these criteria in later chapters.

Evaluation Criteria for Perfect Confidentiality:

• A monetary system should not reveal a money's owner.

- A monetary system should not reveal a money's location.
- A monetary system should not reveal a money's change of ownership.
- Users should not have to authenticate themselves to use money.
- A monetary system should not record money use.
- Must be impossible to know if a person owns money without their cooperation.
- No person should be able to force another person to become the owner of money.

Overview of Availability

Ever go to use a debit card and even though you have huge amounts of money in your bank, your card is declined? There are a million reasons why your money can become unavailable. Meteor strikes, hackers, government intervention, or bad computer code. Our money needs to be able to survive all these and keep working.

Evaluation Criteria for Perfect Availability

- Money should be able to be exchanged at any time.
- Money should be able to be exchanged over any distance including to other planets.
- Money should be able to be exchanged with no measurable expense or fees.
- The time it takes to willfully spend money (change ownership) should be faster than perceptible.
- A monetary system should be able to serve all the users of the system in parallel without slowdown.
- A monetary system should have no systemic risk of failure.
- A monetary system should be easy to use so that it is available to low-tech people.

Overview of Integrity

Imagine that your bank balance dropped from $100,000 to $10,000 because of a computer glitch. Or, your kid was able to withdraw $90,000 without your permission. Or, your bank thought your money belonged to someone else and gave it away. This can happen if our money does not have integrity.

Evaluation Criteria for Perfect Integrity
- All Money must have an owner and no money can be lost.
- Money should be impossible to steal.
- All Money should be storable on any media including the human mind.
- Money should not reference some other thing of value (like a silver certificate).
- No one except the owner of money should be able to change the owner of the money.
- Low IQ people should be able to understand how the money works and make decisions based on the information.
- Money should be made of the same stuff and be completely fungible so that every equal unit is worth the exact same as another equal unit

Overview of Preferential Integrity
What denominations should a cash system have? 1s, 2s, 5s, 10s, 20s, 50s and 100s like the US dollar or, 1s, 10s, 100s, 1000s, and 10,000s like CloudCoin digital cash? Should our money have fractions or just use whole numbers? What level of precision should we have? Should a gallon of gas cost $.345, $3.45, $34.5 or $345 in nominal terms? There may not be a perfect answer to these questions.

Evaluation Criteria for Perfect Preference

Take up very little space and require very little bandwidth to transfer.	Separate data from logic.	Cross over from virtual reality to reality.
Be "Turing Complete" usable by any programming language.	Able to work within customary legal frameworks.	Able to work within current merchant and payment systems.
Be able to be deposited into banks.	Be able to be used to fund investments.	

The TPM Model - Components of Money

Another thing to introduce here is the concept of "components" within a monetary system. It is common for information systems to be modeled in components to facilitate development.

Here are the TPM components:

Physical Media	**System Administrative** Minting, ownership, denominations, encoding, anti-counterfeiting, destroying.	**Data** Inks, embossment, writing, magnetic fluxes.
Paper, precious metals, plastic, nickel, copper, hard drives, USB drives.		
User User interface, user preferences, usability.	**Transportation** Armored trucks, email, Internet, satellites.	**Application** Banks, credit cards, checks, payment systems, investments.

Banking systems may seem to be part of the monetary system but they are really a layer that floats on top of it. The TPM only deals with the first three layers, the Physical, Administrative and Data. The other components fall outside of this theory.

.

5. ECONOMISTS ARE WRONG ABOUT MONEY

Symbols of How People Have Valued Our Work

TPM is a moral philosophy. The first rule of morality is that we should do unto others as we would have them do unto us. It seems to be part of our human nature and we recognize this as justice. If we contribute value to civilization then we should receive a matching value from civilization. This is fair and good.

When we receive money, it is from people who value what we are providing. This assumes we are not robbing them. Our giving to others is symbolized by data: Money. These symbols prove to others that we are worthy of receiving goods and services that they have created. It is of paramount importance that no people are able to fake that they provided value when they didn't. Otherwise, those who contribute to the system will be swindled of the value that they created.

Monetary systems are information system and can be hacked. I know because I have done it myself (legally). Perfect Money will

stop the hack (unauthorized access).

A Model of Money

In the field of information systems, we typically use the words entities, schema, and fields when we are working with databases. We typically use the words objects, classes, and attributes when we are working with programming. These terms are handy when creating a model of anything in the universe including money. The universe, it seems, is just a big database. Let's create a logical model of money.

The Universe

The universe is made up of information, has information and is information all at the same time. The universe is an entity whose attributes and schema create its form. But the form of the universe is made up of other entities that have their own forms. These entities are also made up of other entities and on and on until at some point we reach the bedrock of reality which is information.

Self-Representing Symbols

Data are symbols that have meaning. The universe is made up of data but unlike the symbols that are man-made, these data are symbols that are self-representing. Self-representing means that the entity represents itself and not another thing or concept. A simple

example of this is when we draw a triangle. The drawing of a triangle represents a triangle so the triangle that has been drawn is a self-representing symbol.

The significance is that since symbols with meaning are data and entities are self-describing symbols, then entities are also data. And in fact, as we will learn later, most monetary systems use people to symbolize themselves. Money, on the other hand, symbolizes a person's just claim to goods and services. This "just claim" is the person's purchase rights or simply the person's credit. We will expand on this later.

Schema
Entities have a schema. For those of you who study philosophy, schema can be thought of as a modern take on Plato's forms. Schemata are used to describe the attributes of the entity that define its overall shape, size, proportions, and profile [4]. Schemas also constrain the values of an entity's attributes. If we look at the schemata of oranges, lemons, and limes we would see that their schemas are different in part due to their allowable colors. Oranges must be orange; lemons must be yellow and limes must be green.

The color is their attribute, the schema constrains the attribute. Purple oranges do not fit the schema and we will reject calling them oranges. Schemata are also called classes. If we were to classify fruit, we would be looking at its schema to see how it is similar to other entities.

Entities
Again, objects are the same as entities. Classes are the same as schema and forms. Attributes are the same as fields.

The sum of all the self-representing symbols in the universe can be called reality.[2] Entities are related to other entities and entities are often made up of other sub-entities. Let's take a look at a lemon.

We can model lemons by creating a table with columns and rows. The schema defines what the column fields are: color, mass,

volume, flavor and location. The schema will also define the constraints of each field like: Yellow is the default color, mass must be between 20 and 30, flavor must be sour. If the values of these columns go outside the constraints, then the lemon may become a lime. If the value for weight was ten pounds and the value of color was orange, then it's not a lemon. These constraints taken together create the idea of a lemon object and form the lemon class.

Arrays of Entities Within Arrays of Entities
Some of the properties of the lemon are discrete entities or arrays of entities. The lemon is going to have a property we can call cells. However, cells are entities to themselves and a lemon is made of billions of them. We could also create a table to show each cell. And the cell table may have a column for molecules. And then we can have a molecule table that contains quarks.

Physical Space
Every lemon in reality is going to need its own row within the lemon table because every lemon has different values of its attributes. In reality, each instance of a lemon will have a "Unique Identifier" that will allow us to tell one lemon from another even if they are identical. The unique identifier is the space that the lemon takes up at the time of now. No two lemons can take up the same space at the same time.

Modeling Reality
In the field of computer information systems, we use ERDs (Entity Relationship Diagrams) or UML (Universal Modeling Language) Class Diagrams to model reality.

"An ERD is a graphical representation of the data entities, fields, and relationships in a system or domain. It helps to visualize the structure, logic, and constraints of the data, and to communicate them to different stakeholders".[3]

Domains and Systems
Every entity in the Universe is related to every other entity in some manner. We could create an ERD (Entity Relationship Diagram)

to model the whole Universe. Here we are not interested in the whole Universe but just the domain of money. We can place entities into groups called domains or systems. There is a domain for fruit and a domain for money. If we are studying money then we do not need to worry about the fruit domain. We may also group entities into systems.

Entity Relationship Diagrams of Money

Common Cash Money like the US Dollar can be modeled very simply like the diagram on the next page.

One user may have many media. The media is a container of data and may consist of metal coins or paper cash. The media contains currency symbols ($), authentication symbols (like watermarks), a denomination, date created, serial number, and the name of the system administrator who is the Treasurer of the United States in the case of US dollars. The denomination specifies how many units of credit the user gets from possessing the money. While this model is true for the US dollar, it is not true for ledger-based currencies such as Bitcoin. Much of the data attached to the media is not needed and is left out in other cash systems like CloudCoin.

Entity Relationship Diagram for Banks

Later we will be talking about the difference between money and banks. Here is the ERD for banks so you can contrast it with the ERD of cash money.

Typical Cash ERD
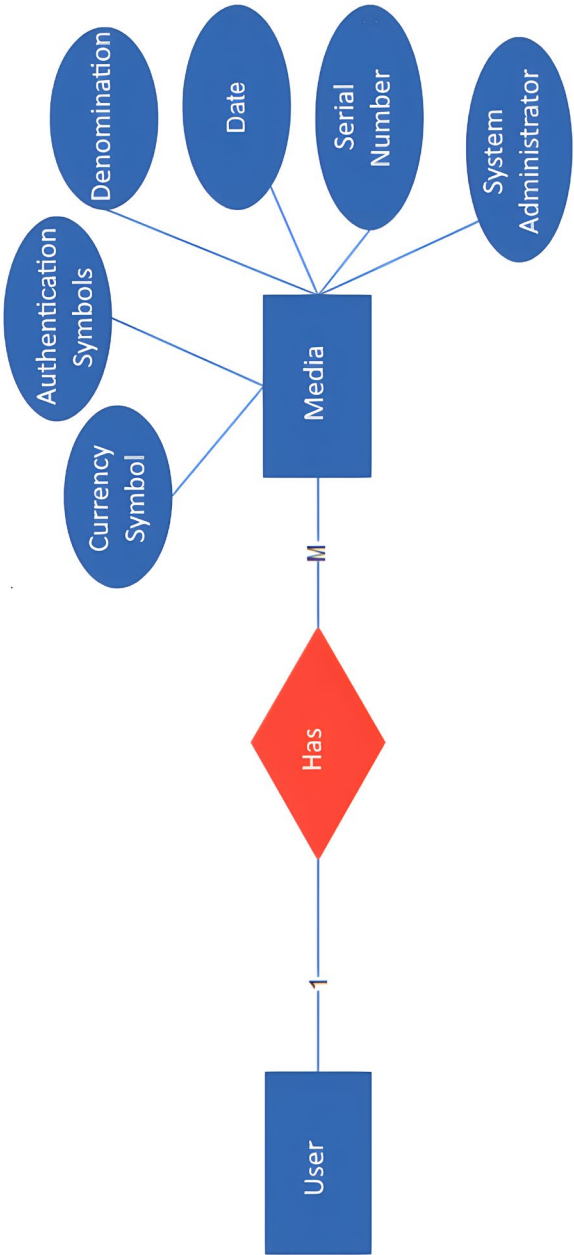
PERFECT MONEY

Online Banking System ERD

49
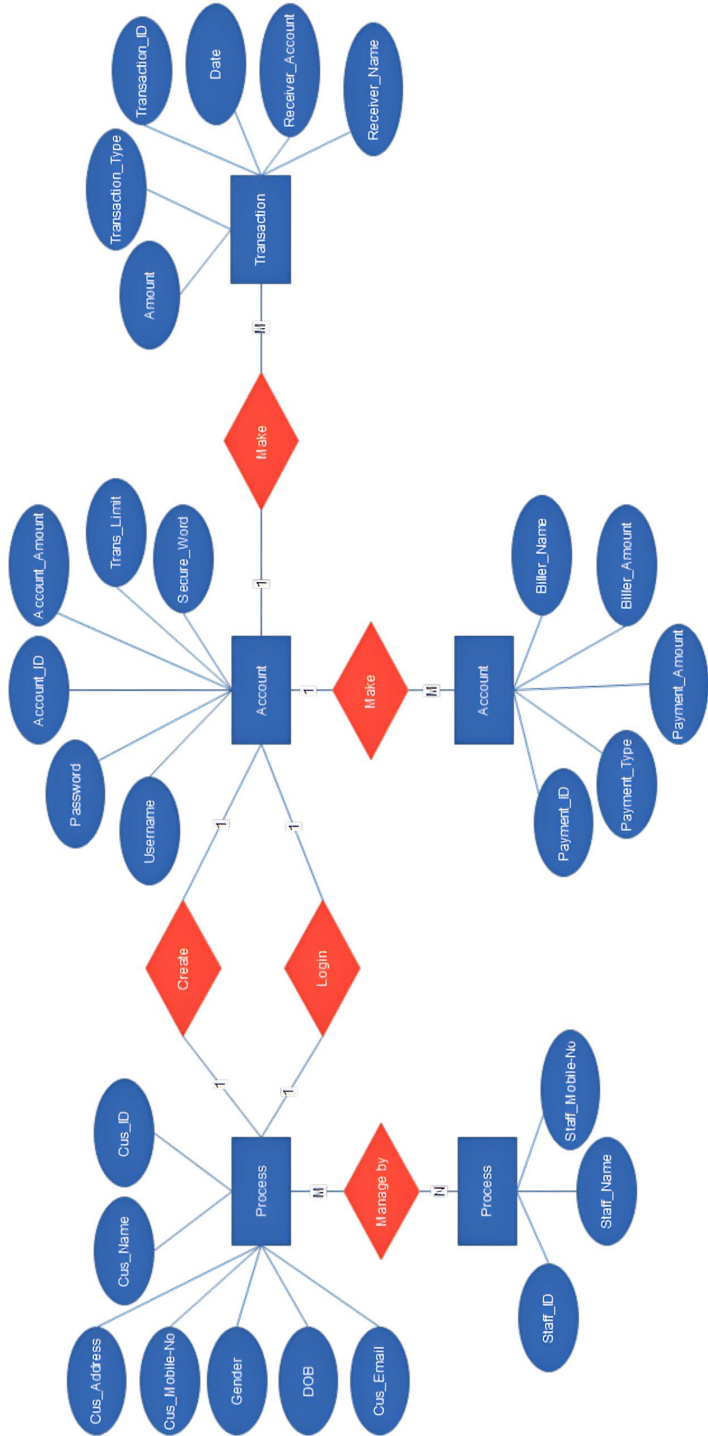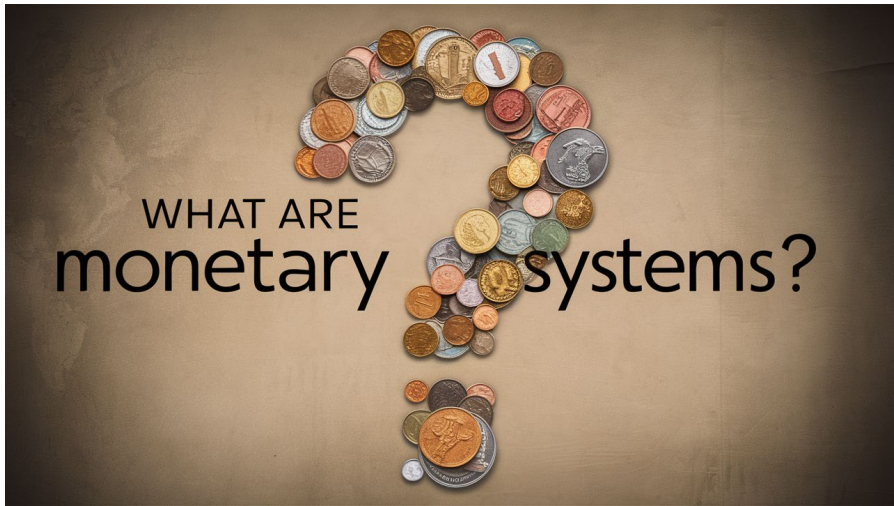
6. ECONOMISTS ARE WRONG ABOUT MONETARY SYSTEMS

Monetary systems are information systems that make it possible for us to be rewarded for pleasing others. We could easily call monetary systems "reward systems" or "incentive systems." Monies are "units of rewards." This system inadvertently has the effect of making all of us arrange ourselves so that we act productively and efficiently. In order for someone to get a reward, there must be a person who is willing to give up one of theirs. People naturally have a goal to increase their rewards either by getting more money or getting more stuff for their money. In other words, by being efficient and productive.

The search for rewards

Monetary systems give us information about how much resources and human effort (cost) were put into creating a good or service. Knowing the cost allows us to economize by reducing the resources we use to a level that is appropriate. Monetary systems also provide information to us about work and actions that we can take to be the most productive. High paying jobs, for example, pay a lot because they produce resources that are needed by people the most. Monetary systems allow us to achieve a Division of Labor so that

we can each specialize without worrying that we may not get our fair share of the economic output.

This can all be achieved by us voluntarily participating in the system. However, most governments create fiat money and use it as a form of taxation and perhaps wealth distribution. They will often demand that we use it to pay our taxes which forces us to use it.

Good money creates good civilization
When we are all looking at our little piece of the economy, our collective effort organizes everything in parallel. Everyone (for the most part) wakes up with an intention to earn money and they execute actions to get it. If money gives us actionable information, we have a good civilization. If our monetary system gives us fake information (most likely government inflation and regulation) we will make bad decisions and the whole civilization will suffer entropy.

Freedom is Needed
Not only do we need good, true money but we also need to have the freedom to act on what money is telling us to do. Good monetary systems will not be able to deliver their potential benefits if we are not free to use them.

Monetary Containers
Let's take a deep dive and look at the data containers of a monetary system. We will look at the monetary database, ownership table, price table, monetary data, cash, and some other key words.

Monetary Database
Monetary systems are a logical database which can be composed of just one table that I will call the Rewards Table.

Money Table
This table has two columns implemented differently for cash and ledger systems. The first column is for an entity and the second is for that entity's attribute. The entity is a person or group of people.

The attribute is how much value they created and thus value that they are due. Credits are received when the purchaser sells their resources.

Person	Money
Jerry Jenkins	$35
Sue More	$55

Money is Data

I write your name on a paper ledger with a pencil. The letters are symbols that represent you. However, if I took some chalk into the parking lot and drew a large table with rows and columns on the blacktop, I could actually have you stand in one of the cells in the Purchaser column instead of writing your name. In this case, you would be a "Self-Representing Symbol." We saw early that the Mesopotamians used clay spheres, pyramids, disks, and cubes as self-representing symbols to stop counterfeiting.

Cash

Cash is a monetary system whereby the individual in physical possession of the money is considered its rightful owner. Cash uses people as self-symbolizing data. Credit is symbolized by placing numerical values on physical media, commonly coins made of metal, notes made of paper, fabric or plastic, and today - files stored on cell phones and USB drives. These symbols of credit written in physical form are money and whoever has the money, owns it. Note the coins are cash just as notes made from paper, cloth and plastic are cash.

Ledger

A system in which the possession of money is recorded on a table and this table is maintained by a different entity. Legers symbolize people using numbers or letters. Credit is also symbolized by numbers or letters. Here there is no self-symbolizing data as everything is abstract. There may be symbols that represent sounds (words). There may be symbols that represent quantities (numerals). Also, the credit symbols are all located on the same physical media (like a paper ledger or a hard drive).

Ledgers will delete symbols and replace them with new ones based on calculations. If the ledger uses Blockchain, then the symbols will

be based on prior symbols and will not write over the old ones. The old symbols will be needed to be stored indefinitely to ensure the new symbols follow the rules and do not reflect double spending.

Human Mind

The most important part of a monetary system is the human mind. The system will not work unless we are able to receive, process, and act on monetary information. Ideally, we want "perfect information," although that is something different than perfect money. Perfect information is when we know all the products, pricing, and utility from the products. We also want to know the job market and have all employers know about us and know which job pays the most given our utility for the job.

A monetary information system is a system that provides us actionable information in a timely manner. Money certainly does this when we look at prices in a store. But there are other systems that bring this information together, such as Amazon, that may do a better job at giving us this information. Employment sites may bring together jobs in one easy to find place.

If we do not value the rewards that money brings us, then money is worthless. So, what we value is also of utmost importance to the successful workings of a monetary system. For example: Our dog does not value money but does value a milk-bones. Fido will not take the money and buy milk-bones but will instead beg for you to give him one. Today, executives at the Disney Corporation value so-called "Diversity, Equity and Inclusion" but not profits. The company will bankrupt itself because its only goal is to meet its diversity hiring goals. It directly antagonizes people based on sex and race prohibiting white males from employment and upward mobility. I will talk about this Supervirus later in the book

7. THE BIG MYTHS OF MONEY

Economists are not trained in information systems and are not able to recognize them or build their theories around them. That is why I, as a person with a degree in Information System Management, feel compelled to write this book. Here are some of the issues that I find particularly incorrect starting with some of the definitions of money. Many sound more like what money does than what money is. Here are some of them:

The Problem of a "Medium of Exchange"

One claim about money made by economists is that money is a medium of exchange. I consider Bitcoin to be money. But it is difficult to call Bitcoin a media of exchange because we don't exchange any media when we exchange Bitcoin. Medium is a physical thing. "Medium of exchange" could only be applied to physical cash and that means it is not universal. Thus it cannot be said that, "Money is a medium of exchange", nor does it serve the function of a medium of exchange. We do exchange money but money is separate from the medium. Money is the data written on the medium.

The Error in "Store of Value"

Economists also say that money is a store of value. This is incorrect for a few reasons. First, value is all in the minds of people and thus value cannot be stored. That is unless we define the word "value" to mean numerical values. In this case we can store symbols that represent numerical values. But if this is true then "store of value" is too confusing to be useful.

If all people were to suddenly die tomorrow then there would be no value anywhere. There would still be money, however. So, money is not a store of value. You could say that money is a "store of symbols" but in my mind, symbols are data so it is just better to say, "money is data."

Also, money goes up and down in value so if it is a store, it leaks sometimes and sometimes value sneaks in and pumps it up. That does not make sense.

So instead, we should say that money is a "symbol of value," or better yet, "symbols of the value we have created for other people," or "symbols of how people have valued our work."

Unit of Account

Economists say money is a unit of account. I agree that money is used as an accounting unit but money is not an accounting unit. When I am defining accounting, I am talking about the activity of recording economic activity. But money does not require any accounting to be money. There certainly are many people who never take account of their money and that proves that the unit of account is not universal and therefore not true to money. Still, it is a unit of something. I think it would be better to say that money is a "unit of purchasing rights."

Myth: Money has Value Because we all Agree it has Value

The world is filled with our symbols. When we play a dice game and a six is rolled, we understand that two lines of three dots means the value of six. If I want to write a book and you want to read it, we must both know and agree on the meanings of these symbols

that are called letters and words. Money, just like any other symbol, needs to be understood by all participants. We all need to understand what they mean to make the economy work. I remember in kindergarten when students would be willing to trade their dimes for nickels because they believed that nickels were worth more because nickels are larger than dimes. Kids were quick to learn that it was the symbols (the numerals) which gave the coins their value and not the size.

Money does not have value because we believe it has value. As we will see in later chapters, there is a lot involved in determining the value of money. Monetary systems are information systems. It is very difficult to calculate how much value an information system provides. Perhaps the most important factor for the value of money is when it effectively allows us to obtain the goods and services we value from others in proportion to the value of the goods and services we provide to others. If a monetary system does not do a good job at giving us what we put into it then it will stop being valuable.

We cannot all imagine inflation and counterfeiting away and agree that money has value in spite of real factors such as availability, confidentiality and integrity. Also, the monetary system can work regardless of what people believe. There is much more to this and we will cover value later.

Myth: Gold and Silver are Money
Gold and silver can be money, but they are not always money. Gold can be made into coins but the coins need to have "domain integrity" and be the same purity and weight. If I have a bunch of gold coins of different diameters, thicknesses and silver/gold ratios then there is no domain integrity. To achieve this domain integrity, some trusted authority is needed to create the coins identically. A symbol of the mint is usually included on the coin along with the date and often the king who is the trusted authority who ensures the coins' integrity. This is money as the coin is a self-representing symbol. One gold coin is one gold coin. One silver coin is one silver coin. It is okay if they have names such as doubloon or piece but

they cannot be part of a monetary system and given a name like a peso, dollar or pound.

Once a numeral is placed on the coin and symbol of a monetary

unit like a $ (dollar sign) or pound sign, the gold and silver are no longer money. Instead, the gold and silver disks become the media upon which money is written.

I know this is confusing but it is key to understanding the nature of money and the design of monetary systems. The symbol of the numeral is the money and metal are just the media that holds it and gives the data its physical integrity. Once we start writing numerals on metal disks, we can say that copper coins are worth $.01 or we could say that copper coins are worth $1 or $10 even if they are all the same size. This is fiat money. It's not based on the weight in silver. Note that it may be roughly related but it does not have to be. Think about the difference between paper $100 bills and $1 bills. Same thing, different numerals.

But just because we put symbols on a precious metal does not mean that the metal is worth that amount. It could be worth more or less. The value of the metal may be far greater or far less than the face

value. The "face value" is its unit of credit within the monetary system. Of course, the big problem here is that there is no domain integrity because the values of the metals can fluctuate so greatly that the money does not compute.

It should be noted that if a coin made of precious metal has symbols that describe its weight like "1 oz" but does not contain units of accounts such as "$1" then that coin is also money because the metal is still self-symbolizing even though it also contains symbols that do the same.

Myth: Fiat Money is not Money

While it is true that money can and should exist outside of the realm of politics, money that governments force people to use is still money. Fiat money can provide the same function of allowing us to produce and receive production. However, governments often print out their own money causing it to lose integrity resulting in people trying to buy things that don't exist. The users of the monetary system suffer because while there is more money in the system, there are not more goods and services. This means that everyone who uses the money must fight harder to get production. The existing production is transferred to the people who received the freshly minted money. This is a good reason to separate money from the government.

Myth: The Other Party is to Blame for Bad Economies

Americans are deeply divided about many issues and the sum of these decisions can be described as "Red" or "Blue." The Red being the Republicans who generally want more economic freedom and the Blue Democrats who want the government to take an active role in promoting equality (at least here in America).

There is a contentious fight between these groups and the contention grows as the rich become richer and the poor become poorer. Which group's thinking is true? Like most philosophical problems that I have studied, there is a false dichotomy in choosing the correct one because the arguments that both make are wrong. Some are more wrong than others. The major problem here is not

the Republicans or the Democrats, but the monetary system. I cannot blame the bankers because they have created the best system with the technology that they have. The fact that the US dollar has succeeded this far without going the way of the Continental (early American money during the revolutionary war that went to zero in value) is a major achievement.

Myth: Economic Inequality is Caused by Free Markets

Capitalism is purely a mathematical system, that allows us to make decisions based on prices, costs, salaries, return on investments, insurance rates etc. Who causes capitalism to flounder? The number one culprit are Socialists who have caused the deaths of many hundreds of millions of people in the past hundred years trying to achieve equality. Most socialists have absolutely no idea what the importance of money is. When the soviets took over Russia, they were so ignorant, they tried to eliminate money altogether. Their plan was to print up so much money that the money would be worthless and undermine the upper-class society. The government would then be in charge of distributing all goods and money could be eliminated. Because of this lack of money with integrity, the people didn't know what to do so their civilization collapsed. Industrial production fell to one third of what it was before the takeover. Five million people starved to death. Finally, Lenin realized that in order to make communism work, they would need to build it on capitalism. The Soviets gather all the nation's precious metals and mint valuable coins of gold, silver and platinum to regain the people's confidence that their money had integrity.

Our current American monetary system has proven far superior to all the hundreds, if not thousands of socialistic schemes that have been tried. I do agree that imperfect monetary systems contribute to unfair inequality. However, we will see these imperfections disappear with Perfect Money so long as people have the freedom to exercise their freewill.

The only people who will be antagonized by Perfect Money are those who are now exploiting the vulnerabilities of our current monetary system to gain undue resources. Perfect Money squashes

the kleptocrats who are now on top and lifts up the people who mind their business, even those people whose minds lack intelligence. In fact, it is Perfect Money that will create a fair playing field, lift all boats and create the most financial equity among people.

References:

[1] Quantum Gravity Research said that Reality is Information

[2] It was the philosopher Plato who conceived of the notion of forms although he did not think of the Universe as a form (as far as I know).

[3] ERDs https://www.linkedin.com/advice/0/what-purpose-entity-relationship-diagram-skills-system-development-vsjaf

[4] Bank ERD https://images.edrawsoft.com/articles/er-diagram-for-banking-system/example1.png

[5] Borrowed from https://www.archisoup.com/architectural-form
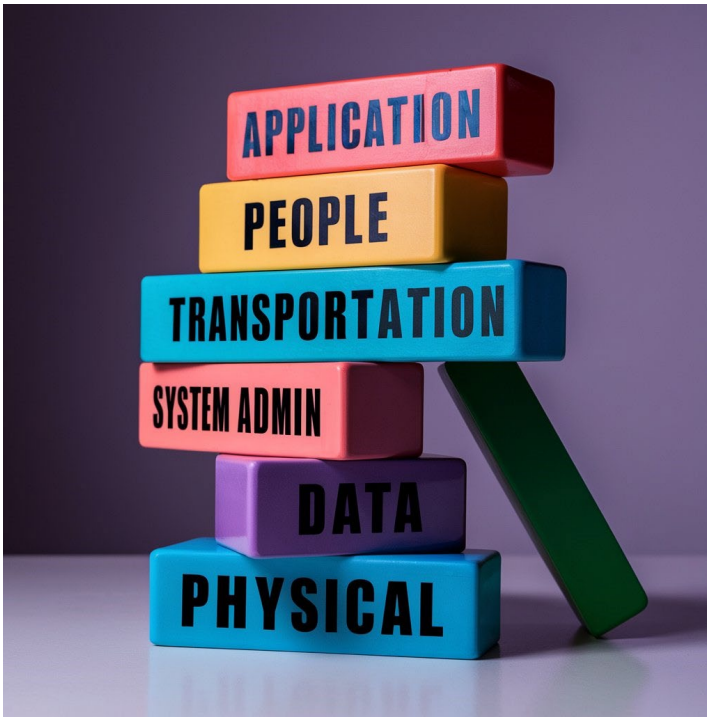
8. THE FIRST MONETARY REFERENCE MODEL

When talking about monetary systems, there is a lot of confusion about the differences between cash, ledgers, banks, PayPal, money transmitters, tokens, utility tokens, NFTs and "DeFi". The confusion often affects the legal framework that a technology may operate under. What follows is a model of monetary systems to help evaluate the technical, ethical and legal properties of a monetary system. With this model we can understand how to separate the data from the logic. This is important because money is data and when logic is incorporated into it, the money becomes something else.

I call this the "Monetary Reference Model" or MRM for short to serve as a common basis for standard development and coordination of laws. It is common within the field of computer science to create such models to describe information systems.

Examples of this include the "5 Layers in Software Architecture" [1] and the Open Systems Interconnection Reference Model [2]

For example, using this model may help us determine if there are laws preventing the US Treasury from minting virtual US Dollar coins using digital cash technology.

There may be a common belief that money originates from banks and or governments. However, while it may be controversial, systems such as Bitcoin, Ethereum and CloudCoin show that money may exist without banks or governments and thus banks and governments are not specifically included in the model
.

Components of The Monetary Reference Model:
>   1. Physical
>   2. System and System Administrators
>   3. Data
>   4. Communication and Transportation
>   5. People
>   6. Applications

All of these components have cultural and technological aspects.

1. The Physical Components
The physical media that is able to contain data. Money is a marriage of physical media and symbols (data). All data takes up physical space and must be stored somewhere. This somewhere is called the media. Media can be categorized as either Static and Dynamic. Static media allows data to be "Read Only" while dynamic media can be both written on and read from.

Static Media include:
>   * Paper
>   * Cloth
>   * Plastic
>   * Metals such as gold, silver, copper, nickel, zink
>   * Stone

Dynamic Media:
* Erasable paper whose data can be updated.
* USB drives
* Magnetic storage such as hard drives
* Non-volatile memory such as solid-state drives

2. System and System Administrators

What is the system and who is going to administer it? Money has to answer these questions. These are all the business rules that apply. They include:

- Who has the right to manufacture the money?
- Who gets to use newly created money first?
- How much money is there?
- How do we know who owns the money?
- How is the money destroyed?
- How is the creation of the money paid for?
- Who is going to police the money and stop counterfeiting?

These are all things that do not require banks, governments, financial departments. They do require policies and administrators. They may require "governance" but other times not.

The Clock Tower

In medieval times, there was the development of the clock towers. These great towers allowed people to see and hear what time it was from all over the city. This was an information system that allowed people to be more productive and efficient. People could coordinate their activities such as meeting at the same time.

The people who designed and built the clocks were not the same people who kept the clocks working. The clock keepers were Administrators of the time information system and all they had to do was keep the clock wound up. This would seem to be easy work that did not require any special skills. At least by today's standards. Besides for a few exceptions (like how loud the bell was, how high the tower was and perhaps what sound it made) there was no need

for any kind of governance or government oversight. There may have been some gray areas like who would pay to build the clock tower and the administrators who kept it wound up. But this could have been done without government involvement. There was however one thing that needed to be governed, who would be the administrators? What if they died? What if they did a terrible job? Would these people get paid? If yes, how much and by whom? How would the money used to pay for it be collected?

Legally, the administrators of the clock were not responsible for any defects in the clock mechanisms that may have caused it to be inaccurate. There was a separation between the developers and the administrators. The same holds true for money. The people who make the money do not have to be the ones who arrest counterfeiters. The people like myself who design cryptocurrencies do not have to be the people who run the server nodes.

The people who run the Bitcoin nodes are called "miners". But they are not miners, they are administrators. They just need to keep the nodes going and they don't have to know anything about the code, protocols or governance.

Do We Want Governance?

Whenever a cryptocurrency has decisions that need to be made, that's governance. You don't want any governance. Governance brings in all kinds of things like voting, representatives, republics, emperors and dictators.

In the past, the King would decide if the money supply would increase and sometimes the emperors would add more junk metal to the silver coins and try to make more coins. This would have an unintended effect of devaluing the money. Certainly, governments of the 20th century have been able to print up huge amounts of money. Today they print up all the money that they want. This is an example of bad governance and it would be preferable to have money growth follow some algorithm instead of being a political issue.

The political nature of existing monetary systems is what really contributes to the corruption that can cause the ruin of a civilization and enslave those people who work hard and deserve to get what they have earned from the monetary system.

3. Data Component

- Symbols with meaning are data. Important symbols that we use in money are: A number or numeral that represents the money's denomination.
- The symbols that represent the brand of the money such as $, ¥ and £.
- A serial number that serves as a unique identifier.
- Date or version of the money.
- Information on who is the administrator (such as the Treasure of the USA).

The symbols may be generated in many different techniques depending on the physical media including stamping, writing, dying, engraving, and applying magnetic flux in the case of magnetic storage devices such as hard drives.

The Data that is stored will need to be "secure." In information systems, we say that a system is secure if it has the characteristics of confidentiality, integrity, and availability.

What is the difference between Monopoly money and the US Dollar? Integrity. We will talk about data integrity extensively in the next chapters that include:

>Physical Integrity
>Entity Integrity
>Domain Integrity
>Referential Integrity
>Preferential Integrity

4. Communication and Transport Component

One of the hallmarks of cash money is that possession is ownership. This means that where the money physically exists is extremely important for establishing ownership. Moving money from person to person adds some complexity as the amount of money changing hands must be verified by both parties and so must the authenticity of the money.

Money Handling includes:
* Counting and double-checking cash
* Making change (breaking large notes into smaller ones)
* Authenticating money (detecting counterfeits)
* Grouping and organizing
* Storing (such as putting in a safe)
* "Changing hands" - Moving from buyer to seller
* Moving money from merchant to bank for safe keeping.
* Paying cash for things.
* Moving money by train, plane and automobile for remote transactions.

As stated before, money takes up space and therefore must be stored and moved. This applies to virtual money just as much as physical money.

US Dollars are kept in:
* Wallets
* Purses

* Vaults
* Safes
* Under mattresses

Virtual Currency is kept on:
* USB drives,
* Smart phones
* Desktop computers
* So-called "Clouds"
* QR Codes
* Remembered in one's mind

There are whole industries that are involved with money handling. Part of the money handling layers include:
* Counting machines and counting software
* Authentication machines and authentication software.
* Brinks trucks
* Payroll transportation
* ATMs
* Bank tellers

All of this is expensive and needs to be paid for. Efforts and technologies that reduce costs of money handling are highly valuable.

We also need to be able to communicate with each other by sharing prices, costs, profits, salaries, taxes and other information measured in terms of money units (like dollars, pounds, Euros etc.). Elements of communication include:
1. Employment websites
2. Signage
3. Bills (like utility, insurance, mortgage, etc.)
4. Paychecks
5. Advertisements
6. Media (like newspapers, catalogs, the Internet)

All of these cost money and any increases in efficiency are also greatly valued.

5. People Component

The most important component in a monetary system is the human mind. Examples of what falls within the people part of a system are:

1. Usability
2. Presentation
3. Values
4. Understanding

Usability refers to how easy the money is to use. Cash seems to be very easy to understand, while Bitcoin wallets require much more learning. For digital currencies that require software applications, there's a whole science about making Apps easy for people to use.

Presentation is how the money looks. The color, font, style, and artwork. It may also be how the program looks that allows one to use the money. People are suckers for a good presentation. I've learned this the hard way by watching cryptocurrencies that are clearly a scam but run by expert marketers with beautifully designed websites but no technological acumen, make billions. Think Sam Bankman Fried with his commercial starring famous celebrities conned into pitching dirty wares.

6. The Application Component

The application layer describes the processes created to use money to achieve goals. The application layer often has money represented not as itself but as other data and information.

Money is data and we can use it without needing any other symbols. For example, suppose a bank wanted to track how much money each client has. One method they could use is to create a physical box, file, or envelope that the client's name was written on and then the physical money was put into. Then, to know how much money a client has, the bank could simply count how much money is in the container. However, banks do not do this because they plan on using the client's money to make loans with the goal of making more money in the form of interest. Instead, they use a logical system to create a ledger to record the amount of money that each

client has by writing the results of a calculation in the ledger.

The use of the logical layer causes potential problems because the numbers and calculations could be incorrect because of human or machine error. This requires more administrative effort and costs more to prevent errors. When errors do occur, it can be very expensive.

 Examples:
    * Recording transactions
    * Creating receipts
    * Accounting systems and software
    * Online banking
    * Debit cards
    * Credit cards.
    * Financial services

As previously noted, cash requires that the data and application layers be separate. RAIDA Tech's cash coin solution also allows the data and application layers to be separated and that gives it much more flexibility. Systems that use the Blockchain force the data and application logic to be combined in such a way as they cannot be separated.

Benefits of the application layer that are performed by banks to enhance physical money include:

* The ability to move dollars logically, thus massively reducing handling costs
* The ability to make digital change (break bills) automatically
* The ability to handle dollar denominations that do not exist such as fractions down to .00000001
* The ability to create larger denominations including $1 Million dollar coins
* The ability to store dollars in digital form to reduce storage cost.
* The ability to handle transactions faster and to handle more transactions in parallel

Thomas Jefferson quotes:

"The system of banking [is] a blot left in all our Constitutions, which, if not covered, will end in their destruction... I sincerely believe that banking institutions are more dangerous than standing armies; and that the principle of spending money to be paid by posterity... is but swindling futurity on a large scale."

The Application Layer is the component in the monetary system where a lot of innovation can occur and cause both success and failure. For example, many financial services such as Apple Pay, PayPal, CashApp, are stacked on top of other application systems such as banking. The Logical layer encapsulates the money to create systems that use the money.

References:

[1]   https://www.indeed.com/career-advice/career-development/what-are-the-layers-in-software-architecture

[2] https://en.wikipedia.org/wiki/OSI_model

9. CONFIDENTIALITY: THE OPPOSITE OF SURVEILLANCE

Civilization emerges from our behaviors. Money guides our behaviors. When our monetary activities lack privacy, our economic behaviors change. Most of the changes will lead to behaviors that are less productive, less efficient, and cause our civilization to decay.

Confidentiality is one of the three necessities for security. Security means knowing. As the age of AI begins, security and thus confidentiality becomes of critical importance.

Of all things, we must keep our money secure. Everyone wants our money. Criminals, corporations, governments, banks, stock brokers, (and AI?). They will use every bit of information they have to get it. They will spare no expense. We must be secure by not letting them know our vulnerabilities, otherwise, we will suffer the consequences.

Privacy Features of Perfect Money
When it comes to confidentiality, the United States Dollar (paper)

is nearly perfect. Its only drawback is that it takes up so much physical space that it is difficult to hide on our person. Perhaps if dollars were smaller, they would be easier to send via FedEx or carry with us through the airport. A digital cash dollar would solve this privacy issue. Instead of trying to bring briefcases full of money through the airport, we can store the money in our minds.

General rules about confidentiality and perfect money:
A monetary system should not reveal the identity of a money's owner. Users should not have to authenticate themselves to use the money.

When we send someone money, we should be able to send it without them or anyone else being able to prove that it was us who sent it. When we receive money, we should be able to receive it from anonymous people. Not only does this save us from needing to log in, but it removes the risk of us being denied the permissions and rights on the system because of our identity. As soon as people have to show their identities, they can be "de-platformed" from a system by having their rights and permissions removed.

There are times when we will want people to know that it is us who sent them money and times when we will want to know who sent money to us. However, this knowledge can be achieved on the Application layer and does not need to be on the Data layer. In perfect money, data must be separate from logic. On the Application layer, we can use third parties to act as a witness or escrow to ensure that the sender sent authentic money and the receiver received authentic money. These escrows can be automated by using servers to check the currency.

A monetary system should not reveal a money's location
For digital currencies, spies can get a very good idea of the location of a person based on their IP address. A person must include their IP address to receive a response from system nodes. There are a few potential solutions to this problem. One is to use the UDP transport protocol (a connectionless transport) instead of the TCP protocol (a communications standard delivering via networks). The

UDP can be given a return address that is spoofed. The client fires and forgets a request assuming that the request will work. Or, the client could spoof the address of a confederate server that receives the response and will tell the client about the results. This way money servers are able to communicate with the client by going through a proxy. Any proxy server including VPNs would work assuming the proxies are trusted. Ideally the system would have location protection built-in, perhaps by some kind of Tor Network (short for The Onion Router for enabling anonymous communication).

A monetary system should not reveal a money's change of ownership or record use.
When money changes owners, there should be no way for anyone to know about that. There certainly should be no public ledgers where everyone can see transaction information and there should be no recording of transactions.

It should be impossible to know if a person owns money without them telling you.
When we go to make a transaction, we prove we have the money by actually giving it to the other person. We could also show people the money to prove that we are a viable purchaser. However, no one must know how much money we have unless we want them to know. Therefore, there must not be any account balances and that means money must not use accounts.

No person should be able to force another person to become the owner of money.
People need to take ownership of money after being offered it. If I can force you to own money, I first have to know who you are. Also, bad actors may try to give others money in an attempt to defraud them or frame them for a crime.

The system should use quantum-safe encryption
Assuming the system depends on encryption for its security, that encryption must be safe from the quantum computers of the future which theoretically can decrypt PKE (public key encryption). This

should be built into the monetary system now and not put into place when quantum computers prove that they can decrypt PKE.

Questions to ask when evaluating the confidentiality of a digital currency:

☐ Can the activities of your token be analyzed to infer what individuals are doing?

☐ Do users need to sign up or become a member to use your token?

☐ What personal information must a user provide to use your token?

☐ Under what circumstances could administrators of your token know what individuals are doing (like knowing Sam bought something from Dave)?

☐ Under what circumstances could administrators of your token know how much money an individual has? Like knowing the Governor has $1000?

☐ Under what circumstances could administrators of your token know how much fees a user paid?

☐ If quantum computers were to crack the public-key encryption used by RSA, TSL, SSH, what information could the cracker know about the use of your token?

☐ If quantum computers were to crack the public-key encryption used by Elliptic Curve Cryptography, what information could the cracker know about your token's activities?

☐ What measures have you taken to protect your token against attacks by quantum computers?

☐ Please provide a statement about the confidentiality of your token.

☐ Do users of your token have privacy, pseudo privacy, no privacy, or something else?

☐ Is user identifiable information such as biometrics required to obtain or spend your token?

☐ How do users of your token send tokens to other users?

☐ Must all users be placed in a directory to be found for tokens to be transferred?

☐ Are there "memos" associated with transactions and if yes, what is the level of privacy of these memos? Are they encrypted?

☐ Can users force other users to own tokens? Like if one user was trying to "frame" another user for a crime. Are users able to have plausible deniability?

☐ If a user was to commit a crime using your token, like buying illegal fireworks, could the crime be proven?

☐ Does your token save information about activities - such as a blockchain saving records of transactions - that could be used to surveil users?

☐ Under what circumstances could your software engineers update all the

server code to include surveillance measures without changing the network protocols?

☐ How can we know that your server/node software is not spying on its users on behalf of an organization such as the NSA, IRS, CIA, KGB, CCP?

☐ How can we know if client code cannot surveil our activities?

☐ How do clients find the IP addresses of the servers/nodes?

☐ Are there single points of failure for your name-resolution system assuming you have one?

☐ Does your client software have logs that could be used to know what the client has been doing?

☐ Under what circumstances would you install secret surveillance software within your token's client and server software?

☐ Can a user with your token prove that he or she has tokens without actually sending money?

☐ Can the physical location of a user of your token be inferred?

Quantum Computers are Real and They are Here

Quantum computers have worked like magic to decrypt simple public keys. It is estimated that a quantum computer with 1,500 quantum-bits would be necessary to crack the SSL that we all rely on to keep our internet conversations private. Do you need privacy? Yes, unless you want everyone in the world to be able to see the username and password you use to log into your bank and other websites.

As CoinTelegraph discusses, quantum computers could (theoretically) break through the SHA-256 hashing algorithm that Bitcoin and many other blockchains rely on for producing blocks and signing transactions. If this happened, then a quantum computer could forge transaction signatures, recover private keys from public keys, change data in the blockchain's history, outpace all the miners/validators in the network and completely hijack the blockchain.[1]

"In the United States, the White House has released guidance in National Security Memo eight as well as National Security Memo ten to jumpstart the government to action. And the House has passed H.R. 7535, the Quantum Computing Cybersecurity Preparedness Act on July 12th. And there is a complimentary bill in the Senate that we expect to be approved favorably," explained moderator Jennifer Sovada, president of public sector at SandboxAQ.

But how do we achieve quantum-safety?

Use stronger encryption?

The solution may seem easy, just use stronger encryption. However, because of how public-key encryption works, adding more bits of encryption will not solve the problem. Shor's Algorithm is able to factor prime numbers. It is the inability to factor prime numbers that allow public-key encryption to protect us. However, Shor's Algorithm is able to infer what the encryption key is and start refining guesses. Adding more bits does little to strengthen the algorithm. "The problem is that the increase in key size doesn't boost security proportionally. For starters, RSA 2048 is four billion times stronger than its predecessor. But, RSA 3072 is only around 65k times stronger. Effectively, we'll reach RSA encryption limits at 4,096".

Use Quantum Computers to Create the Keys?

If Quantum Computers can crack codes, then why not have quantum computers write the codes? It sounds good but there are some problems. The first is the enormous amount of energy that is requiredd. With this scheme, everyone would need to own a quantum computer. That may seem plausible until you understand that quantum computers require their core temperatures to be next to zero kelvin. According toTroyer of IEEE Spectrum, "The new 1,000-qubit machine installed at Google's Quantum AI Lab spends most of its power on keeping cool." "While the 'flat power requirement' is a good statement to make for marketing, it is unclear at the moment what the true power needs are once the

device is optimized and scaled up," Troyer says. "Right now they need orders of magnitude more power than competing classical technology." It certainly will not work on cell phones that lack processor power.

Use RAIDA Technology and the RAIDA Key Exchange Protocol?

We can solve this problem by using CloudCoin which does not use public key encryption. With RAIDA-based money, the coin holder and the RAIDA server share a common secret. This common secret is the 16-byte authenticity number. This is a highly random number and can be used as an encryption key. This allows us to use "Synchronistic Key Encryption" rather than the "public key" Asynchronous Encryption. The RAIDA used in CloudCoin uses AES-128 which is believed to be quantum-safe meaning quantum computers cannot crack it. Furthermore, AES encryption uses less energy than SSL/TSL

Keys can be exchanged by using RKE (RAIDA Key Exchange). This is a newly patented protocol whose workings I will not go into here. However the plan is to make it an open standard. At the time of this writing RAIDA Tech is looking for a $2 Million VC investment so any help would be appreciated.

References:
https://www.msn.com/en-us/news/technology/are-quantum-computers-a-threat-to-cryptocurrency/ar-AA11YjBv.

In Cryptography, Experts Urge Organizations to Take Immediate Action in Protecting Against Quantum Attacks.
https://spectrum.ieee.org/how-much-power-will-quantum-computing-need

https://www.govconwire.com/2022/09/cryptography-experts-urge-immediate-action-in-protecting-against-quantum-attacks/

https://www.makeuseof.com/what-is-post-quantum-cryptography/

10. CBDC: TO SURVEILLE OR NOT TO SURVEILLE

CBDCs are seen as a threat to liberty. Let's talk about the issues.

The Big Question: Privacy vs Policing
Today there is a burning question among makers of government and bank controlled digital currencies: How can we keep bad guys off of the platforms while at the same time providing privacy for the good people?

There are three major reasons why money must be 100% private and any attempts to stop "bad guys" is a waste of effort. Some major reasons we can go into detail about are:

1. It is technically and logically impossible to require people to provide identifiable information and guarantee them their security and privacy at the same time.
2. Achieving the goal of policing would require a "platform" which is not money and is in practice a virtual bank or virtual

financial system and this could put all other banks out of business.

3. Deciding what is "good" and what is "bad" requires the application of a moral philosophy and sooner or later, a moral philosophy will be applied that destroys civilization and perhaps billions of people with it.

The Logical Problem

A currency cannot be private and NOT private at the same time. An information system cannot identify people and not know who they are based on if the people are "good" or "bad".

Even if only one person can see user activities, there is still a risk of a breach.

A monetary system cannot treat people differently based on who they are (bad guys or good guys) unless the system has a way of knowing who they are. Thus, if a currency is to have accountability, it must have authentication or identification. This means that you cannot have anonymous access and accountability at the same time. Note that "accountability" is defined as "A property that ensures that the actions of an entity may be traced uniquely to that entity" https://csrc.nist.gov/glossary/term/accountability

A currency that authenticates or identifies a person can surveil that person and exercise complete control of their rights and permissions within the system. If a person must log into a payment system (such as PayPal) the system can take away their confidentiality by monitoring their activities, availability by shutting down their account and integrity by changing how much money they have. Just because a system may not have these features, does not mean it cannot have these features added at a later date. And, these features will most likely be added secretly to avoid user resistance. Once you require users to create accounts that are linked to their identities, there is no security for the user. Security is "knowing". The user cannot be guaranteed confidentiality, availability and integrity of their data. This makes the currency risky for users and greatly reduces its ability to perform its function to

promote efficiency and productivity.

The Technical Problem
In terms of confidentiality, there are a few types of systems that I can categorize: Truly private, Pseudo Private, Private to the Public, and Public.

Truly Private
The US Dollar is completely private because no one knows where a dollar is in the system or who owns it. It is impossible to know when it trades unless you are one of the two people in the transaction and you reveal your identity to the other person. CloudCoin, which is true digital cash and uses the RAIDA data structure, is also 100% private. There are many blockchains that report to be private. However, these blockchains require accounts and record activities. And they also use public key encryption that could be vulnerable to attacks from the quantum computers of the future. This means that in theory, someone could start their own node that has some extra software to record user activity. There could be techniques to discover the owner of wallets and techniques for deciphering records. These records may provide hundreds of gigabytes of past transactions that AI and quantum computers could use to know all transactions and users.

Pseudo Private
Most blockchain based digital currencies are not truly private but instead are "pseudo private". This means that all the people have accounts but the accounts are not linked to user identifiable information. However, when you trade with someone, that person will know your account number and will be able to know how much money you have and know all your prior transactions with that account. There are very sophisticated tools that can allow anyone to snoop on everyone. Although we do not know what secretive organizations (such as CIA, FBI, NSA, and countless foreign agencies) are doing. It is likely that they have rooms full of super computers that analyze everything that is happening on blockchains and record and understand everything users are doing. This makes it risky and gives its users a false sense of security.

Private to the Public

Private to the Public is where the system is not private but there are safeguards in place to keep the data within the knowledge of a few people. Systems like PayPal, Western Union and proposed CBDC are like this. These systems have the problems of not being money because they have a logic layer. They are more like a virtual bank or financial institution. Systems that are Private to the Public always have an owner and that owner can shut the system down and lock people out.

These systems must employ a moral theory to decide which users are good and bad so that they can lock out who they think are bad. That can be an expensive thing to do so in actuality, the decision will be made by AI. That is absolutely dangerous because no matter what bad users are doing, it is probably not as bad as what AI can do on a mass scale without any sense of morality.

Guarded systems like this must authenticate people. This means that all the users need to have an account on the system and be granted permissions to use it. Systems like these can cause people to have "life quakes" that greatly disturb their wellbeing by locking them out of their money that they need to acquire food and shelter. These systems are extremely risky for anyone who may do things out of the ordinary or things that are unpopular with the system owner.

Platform or Money?

If a government is going to create a CBDC (Central Bank Digital Currency) that provides the same services as a bank (accounts, transfers, AML (Anti-Money Laundering), KYC (Know Your Customer), then all of the banks that are members of that central bank will be destroyed by the CBDC thus negating the need for a CBDC in the first place. Banks need deposits to make loans so they collect interest. People need banks to give them productive and efficient loans. If the deposits are sitting in some ledger, then it will not be a deposit. CBDCs will not just destroy the banks, they will

also destroy other financial institutions like PayPal and Western Union and have other unintended consequences. However, this will not happen with true digital cash like CloudCoin. If nations adopted truly private currencies like CloudCoin, that currency will be extremely valuable and make that nation wealthy. People will flock to the currency as the people are able to use the money to become more efficient and productive and they obviously prefer security over risk.

AML and KYC

A question we may ask ourselves is how can we create a digital monetary system that follows existing laws dealing with "Anti-Money Laundering" and "Know Your Customer"? The answer is pretty simple: Create cash systems and not virtual banks. AML and KYC are things that monetary systems do but are left to banks and financial institutions. Money needs to be just data with no logic applied.

We have been dealing with cash for thousands of years and all the laws in the world are written for cash. If we stick with digital cash then we simply must follow the existing laws. For example, suppose there is a law that says that any deposit of cash (into a bank) over $10,000 must be reported to the government. This law is easy to follow with digital cash. However, if we create some system that has accounts that functions like a bank then it would seem logical that laws pertaining to banks must be followed.

Let's compare digital cash with physical cash (like the US Dollar):

1. They both use a person as a self-representing symbol within the system. This is a fancy way of saying that we don't need accounts because we use actual people as account identities and not user IDs like in ledgers or payment systems.
2. They both use data that is written on discrete media that takes up physical space. Dollars use ink on paper, CloudCoins use magnetic fluxes written on hard drives.
3. The relationship between the owner of the money and the money are based on physical possession and not a logical

representation within a ledger or database. Possession is nine-tenths of the law meaning that it is assumed that whoever has the money is the owner unless there is compelling evidence showing otherwise.

What are the differences between digital and physical cash?

1. Physical cash must be authenticated by people while digital cash must be authenticated by software. When people accept physical money, it is up to them to make sure it is not counterfeit. With digital currency people need the help of software to ensure authenticity. In truth, we don't actually need to authenticate physical or digital cash but this is very risky not too.
2. Physical cash is much more expensive to make, transport, and handle than digital cash and that makes digital cash more efficient.
3. Digital cash can be stored within programs and that makes it much more productive than real cash.

The big difference, and the one that really counts when it comes to AML and KYC laws is that digital money can be transported over network media (such as wires) while physical cash cannot. Some states within the USA have money transmission laws that at first may seem to apply to digital currency. However, I would argue that when an individual sends their own money, that is a lot different than when a company sends money on another person's account. Also, these laws vary from state to state so anyone living in a state such as Wyoming will not be affected by such laws.

How Can We Keep the Bad Guys Out and Give the Good Guys Privacy?

The question might as well be, "How can we keep the good guys off the system while at the same time providing privacy to the bad guys?" This is because different people may define good and bad differently. But wait, you may ask, "Clearly people who torture children are bad!" Yes, but the sicko might disagree. And what if that sicko ends up in charge of the system? Then it will be the police that are locked out because police are bad for sickos.

If a CBDC plans on evaluating good and bad behaviors then they must have a moral philosophy on what is good and evil and apply that to the monetary system. Here we must be extremely careful. Nothing has been more deadly to the human species than bad moral philosophies that are forced on people. I am talking about socialism, communism, racism and fascism that have caused the deaths of hundreds of millions of people. AI is a threat we will discuss later in the book.

If these moral philosophies are incorporated into your monetary system, there will be great suffering. The newest moral philosophy is Wokism, also known as DEI (Diversity, Equity, and Inclusion). If a CBDC is hijacked by Wokists who are trying to forward DEI using the monetary system, there will be mass entropy of our civilization undoubtedly leading to death and destruction. Wokists "wake up" to learn that the differences in outcomes (such as monthly salaries) of races, sexes and other classes are caused by white people. They seem to be ignorant of the fact that in science, diversity and inequality are the same thing. Logically, it is impossible for people to be the same and different at once. The reason that people have different economic outcomes is because people are different.

Wokism is Marxism, Racism, Sexism and other dumb ideas mixed together. If the US Dollar goes Woke, the USA will go broke on a global scale. The makers of the CBDC of the Federal Reserve Bank of the United States of America are woke and dangerous. I know

because I interviewed for the position of the supreme developer of our nation's CBDC (Note that this was done by the Boston Fed) and their primary concern was DEI.

If you look at the short April 2024 video on the Federal Reserve Boston YouTube channel entitled "What Does the Boston Fed Do", the President and CEO of the FRB Boston can't help but to mention Diversity, Equity and Inclusion. The video ends with her stating that the Fed's overall mission is "an economy and financial system that works for all." That mission doesn't seem to align well with Congress's mandate of low inflation and high employment and signals to me that they are infected with the Supervirus and will do all they can to spread it.

This includes hiring people based on race and not qualification. That results in organizations that pretend to be about the mission they are supposed to do but just spend all their resources trying to eliminate uninfected nodes (people) and spread the infection to others.

We can see that past Directors of CBDC Software Engineering were also extremely woke.

If we allow these people to create a CBDC, I can guarantee you the first thing they will do is manipulate the system so that infected people will get more money and non-infected people will be destroyed. They will lie, cheat, steal and do whatever they can because part of what the Super virus does is destroy any sense of their morality.

Because of this, having a CBDC that can identify its users is a death sentence for the dollar and the United States of America. A CBDC would have to be 100% private and have Data Supremacy against the Federal Reserve and the United States Government itself.

The Theory of Perfect Money is also a moral philosophy and prescribes actions as it pertains to money. However, TPM is greatly influenced by the moral code described in the book titled

"Universally Preferable Behavior: A Rational Proof of Secular Ethics," by philosopher Stefan Molyneux. UPB (Universally Preferable Behavior) rationally proves that torturing children is bad and shows that locking out police would not be good. This philosophy allows us to calculate what behaviors are bad so we don't just have to take God's word for it. We can use the logic in UPB to work out the truth. But the likelihood of this philosophy being applied correctly for all time to a CBDC is almost impossible

In Conclusion

CBDCs must be 100% private because once users are required to login, the system will become more like a payment platform than money and administrators will be able to surveil and regulate every action of all the users thus providing no privacy. Any CBDC that acts like a payment platform will put all other banks and payment systems out of business. Worse, moral principles can be applied to the users that deny them their rights and cause great risk including "life quakes" that destroy their wellbeing.

Money needs to be just dumb data and not have any logic mixed into it. The cash system we have today does not require people to log into a $100 dollar bill to give it to the clerk at the checkout counter. The money of the future should function in the same way. If we require people to login to use money then we are really creating a bank. By creating a bank, we are mixing data and logic together and that greatly reduces what and how money can be used. Logic turns money into a platform and necessitates the administrators to exercise dangerous moral theories that present considerable risks to banks, financial institutions, individuals and civilization itself. It is technically impossible to require people to log into a system and have privacy.

11. AVAILABILITY

Availability means that the monetary system can be used at all times. This is not a problem with physical monetary systems like the USD but it is a major concern for digital systems. Paper dollars are not going to suddenly disappear from our wallets. But servers could go down and take a digital currency offline. Imagine if your family had millions of dollars' worth of digital currency and suddenly you could not even access a cent of it. That currency would be insecure (risky) and you would not want to use it for more than trivial purposes.

For a digital currency to achieve 100% availability, there must be no systemic risk of failure.

Physical Location of Nodes
You will need to have many nodes that provide redundant service so that there is not a single point of failure. The number of nodes needed depends on the threat of attack and the impact they have on scaling. We have a few systems that we can look at to get an idea about the needs here. Here are some of the risks and potential solutions:

Risk	Mitigation
Bug in server software, hardware or operating system.	Write different versions of the software in different programming languages, hardware and O.S.
Node crashes	Have multiple redundant nodes
Government seizes server	Have nodes located in many different legal jurisdictions
Meteor strike knocks out building with node	Have nodes in different physical locations
Node administrator goes rogue or quits	Nodes are run by separate and independent administrators
DNS Domain Name Seized	Many different domain names point to the same servers and use IP addresses for some nodes.
Owner of the system decides to shut it down.	Do not have a system owner.
World government attacks nodes.	Nodes in space and on ships in the ocean.
Large amount of people wants to use the system	Build a system that can be used by everyone in the world at the same time.
System becomes too expensive for node administrators to run.	Build a system that is extremely efficient and requires no fees.
Transactions take too long to complete	Build a system that has extremely fast transaction times.
System government is taken over by hostile actors who vote to shut the system down.	Do not have any decisions that need to be made so no system government is needed.
People cannot afford the transaction fees.	Build a system that is extremely efficient and requires no fees.

The first system is Root DNS servers which I call the RAIDA (Redundant Array of Independent DNS Agents). This is the most impressive system because it has not gone down since the day it was created in 1985. This system is incredibly important to the functioning of the Internet and is a key part of the Internet's infrastructure. If I could control this system, I could control all the traffic on the Internet and even redirect everyone to go to my website. Every hacker, government, and tech giant would love to control this because they could use it for their own means. If North Korea or China could control it they would stop people from visiting websites that they don't like. If a hacker got control of it they could stop people from going to any website and redirect them

to spoofed sites or any other site.

Circled in the above image is of one of the thirteen DNS root servers that keep the entire world's Internet working. These systems are extremely efficient and like the blockchain, they have Data Supremacy.

There is no bigger target for hackers but the DNS RAIDA has

never been hacked in all these years. How does it not get hacked? The DNS RAIDA has 13 independent nodes and each one has many mirrors of itself. Mirrors are servers with identical data on them but located in different physical locations.

All the DNS servers in the world are given a "root hints" file that has the IP address of each of these root DNS RAIDA nodes. If a server tries to reach one of the nodes and it is down, then the server just tries the next one. This means that if a hacker wants to bring the root nodes down, they must bring all 13 down at once. This seems impossible because it has never happened since 1985 and not due to a lack of want or trying.

CloudCoin uses a RAIDA with 25 nodes. With CloudCoin, I wanted to use over twice that of the DNS RAIDA. I figured that should be more than enough to keep it going. The CloudCoin RAIDA has never gone down since it was created in 2016.

Ridiculous Redundancy
Bitcoin uses 16,837 nodes at the time of this writing (https://bitnodes.io/). This is a ridiculously large amount of redundancy that uses a lot of unnecessary resources including storage space, hardware, electricity and bandwidth. The Bitcoin network has become unavailable due to heavy use because it is not scalable. This scalability problem would actually be reduced if there were less nodes because there would need to be less synchronization. There is something to be said about having too many nodes.

Cryptocurrencies that have so-called "master nodes" do not have the same scalability issues as Bitcoin. The currency EOS has 23 Master nodes and it too has never gone down because it did not have enough nodes.

My conclusion is that a system that has nodes placed in different geological as well as jurisdictional locations will work fine if it has between 13 and 23 nodes. CloudCoin has 25 nodes in 22 countries, many of which have no relations with the others. Having nodes in

outer space and on boats on the ocean will also give a monetary system a trump card against any attempts to make it unavailable.

Scalability

In January 2016, Lenny had over $2 Million worth of Bitcoin. An amount that he only paid $1.5 million for. The price of Bitcoin just seemed to rise and rise. Then suddenly, the price began to fall. Lenny sold the coins but he could not complete the transaction. The Bitcoin system seemed to jam up. It no longer took hours to process transactions, it took days! The system became unavailable because it could not handle the number of transactions that people were trying to execute. Bitcoin suddenly had a scalability problem. Like a bridge with too many cars trying to drive over it, people could not use it to get to the other side. This scalability problem would expose the bottlenecks of Blockchain in general and give rise to the "Alt Coins." Alt coins are currencies that do not suffer from the Bitcoin scalability bottleneck.

The blockchain must be confidential, available, and have integrity to be secure. However, the more people that use the blockchain, the slower it gets until at some point of usage, it completely stops working. This can be cured by using fewer nodes. But the fewer nodes that are used, the less fault tolerant the system becomes and the easier it would be for hackers or governments to take over the system.

Decentralization

The cryptocurrency community talks a lot about decentralization but not the reason that decentralization is desirable. Furthermore, they don't seem to be able to define decentralization. Is that decentralization of data, code, or governance or all of the above? If you take a centralized database and make millions of copies of it, is that decentralized? Because of this, they may seek decentralization just for the sake of decentralization and not for the sake of obtaining data supremacy. Data supremacy requires more than just decentralization. Remember that Data Supremacy means a database cannot be brought down or controlled even by governments such as China or the USA.

50% Attacks

Suppose I am the nation of China and I purchase fifteen thousand servers and set them up in different locations around the world. I have military personnel administer the computers and if I want the software to change, I simply give the command. This allows me to take advantage of the 50% vulnerability that allows the owners of over 50% of the computational power of the nodes to specify which transactions are authentic, reverse transactions, and even stop transactions from working.

As of this writing there are approximately 18,000 nodes in the Bitcoin network. That sounds like a lot but actually, it is not much at all when you compare it to the amount of people in the World. China will take Bitcoin and almost all other blockchain-based currencies down anytime it wants and this will happen when we are most vulnerable. Yes, the Blockchain is decentralized but it is not redundant because there is just one system and it all synchronizes.

Redundancy

Suppose we had many Bitcoins. Chinese bitcoin, American Bitcoin, Indian Bitcoin and 22 other Bitcoins located in different nations. These are redundant systems that run the same protocols but do not synchronize with each other. Meaning that the data in all three can be different. We have an account on each of these systems with a different key set for each account. We start out with the same number of coins on each of these systems: 0. When we want to trade with another person, we have them send us the same number of coins using all systems. That's true redundancy.

What we need more than decentralization is redundancy. Blockchain uses the same software written in the same program language, running with the same data (blockchain). Blockchain only needs one server to run. But what if there is a bug in the software? Will all the nodes have that same bug? If the software is the same on all nodes, then all nodes will have the same bug. People who know about the bug may use it to secretly steal from accounts that have had their keys lost. This will be undetectable. Or, the bug

knowers may collect their bugs with the idea of attacking the system all at once at a time that they wish the system to go down.

This is why it is important that currencies use more than one code base for their software so many different languages are used and that many different programmers write them.

If we look at the data that a blockchain uses, we will see the same data on all the other blockchains (more or less) thus the privacy concerns. But, if I look at the data on the CloudCoin RAIDA, each is absolutely unique.

Protected DNS (Domain Name System)

```
128
129        // Note that of those which support the service bits prefix, most only support a subset of
130        // possible options.
131        // This is fine at runtime as we'll fall back to using them as an addrfetch if they don't support the
132        // service bits we want, but we should get them updated to support all service bits wanted by any
133        // release ASAP to avoid it where possible.
134        vSeeds.emplace_back("seed.bitcoin.sipa.be."); // Pieter Wuille, only supports x1, x5, x9, and xd
135        vSeeds.emplace_back("dnsseed.bluematt.me."); // Matt Corallo, only supports x9
136        vSeeds.emplace_back("dnsseed.bitcoin.dashjr-list-of-p2p-nodes.us."); // Luke Dashjr
137        vSeeds.emplace_back("seed.bitcoinstats.com."); // Christian Decker, supports x1 - xf
138        vSeeds.emplace_back("seed.bitcoin.jonasschnelli.ch."); // Jonas Schnelli, only supports x1, x5, x9, and xd
139        vSeeds.emplace_back("seed.btc.petertodd.net."); // Peter Todd, only supports x1, x5, x9, and xd
140        vSeeds.emplace_back("seed.bitcoin.sprovoost.nl."); // Sjors Provoost
141        vSeeds.emplace_back("dnsseed.emzy.de."); // Stephan Oeste
142        vSeeds.emplace_back("seed.bitcoin.wiz.biz."); // Jason Maurice

144        base58Prefixes[PUBKEY_ADDRESS] = std::vector<unsigned char>(1,0);
145        base58Prefixes[SCRIPT_ADDRESS] = std::vector<unsigned char>(1,5);
146        base58Prefixes[SECRET_KEY] =     std::vector<unsigned char>(1,128);
147        base58Prefixes[EXT_PUBLIC_KEY] = {0x04, 0x88, 0xB2, 0x1E};
148        base58Prefixes[EXT_SECRET_KEY] = {0x04, 0x88, 0xAD, 0xE4};

150        bech32_hrp = "bc";

152        vFixedSeeds = std::vector<uint8_t>(std::begin(chainparams_seed_main), std::end(chainparams_seed_main));

154        fDefaultConsistencyChecks = false;
155        m_is_mockable_chain = false;
156
```

One thing that people don't understand about digital currencies, including Bitcoin, is that to work, they require the use of the Internet's DNS infrastructure. The DNS changes domain names into IP addresses. It acts like a telephone book used to work (if you are old enough to remember them). Look at Bitcoin's source code: https://github.com/bitcoin/bitcoin/blob/master/src/kernel/cha inparams.cpp#L133 You will see that there are so-called "seed" nodes that are hard-coded into the blockchain. These seed-node

servers are assumed to be available all the time and their job is to tell everyone how to find blockchain servers. You can also see the names of the people who run those nodes. There are nine of them. If these nodes were to be attacked all at one time and taken over, then Bitcoin would become unavailable. This would not affect the actual data on the Blockchain. CloudCoin uses 30 "Guardian" nodes and has IP addresses hardwired for backup. The above is a screenshot of the code that shows the seeds hard-coded into the Bitcoin server software.

No Governance

In 2017, Dan Larimar, an architect of digital currency, created the EOS token. In order to increase scalability, the EOS token would use 21 Master Nodes called "Block Producers". But a decision needed to be made on who would administer these nodes. Who would be the "clock keepers" that would simply wind them up and keep them available. It seems that Dan decided to implement a system of governance. How would it be decided who would run the nodes? The answer is that it would be voted upon. But instead of registering voters and having a membership list, the votes would be based on how much EOS tokens people were willing to spend or donate. So basically, people would buy the nodes. The end results are that the majority of the nodes are now either in China or controlled by Chinese nationals. This would seem to be a serious threat as Chinese are not well known for being independent of the influence of the Chinese Communist Party.

With CloudCoin, we had a CloudCoin Consortium. When I resigned as president, they decided to have a similar election. Learning from EOS's mistakes, I immediately broke all ties between the RAIDA Administrators (node operators) and the CloudCoin Consortium so that the consortium would have no power or influence over the administration of the network. The CloudCoin Consortium was then "bought" by a guy who later said he was affiliated with the World Economic Forum and who attended their elite conferences annually in Davos Switzerland. That guy went on to ruin the CloudCoin Consortium, closing its bank accounts and returning and taking all the money.

The lesson is that we don't want digital monetary systems to require governance. It is even worse with national governments.

National Governments: A Special Threat to Free Market Currencies

Governments are political and they are subject to whatever crazy ideas politicians have. These ideas are volatile and can change in an instant. Governments will try to stop their enemy's monetary systems from being available to you in an effort to manipulate human behavior. These actions will divide us and increase the likelihood of war. When civilizations use a common currency, they are much more likely to be peaceful as being peaceful adds to their prosperity.

An available currency can pass everywhere, anytime, and importantly, regardless of jurisdictions. Money must have no fees. We shouldn't have to pay money to transact. With fees, the currency may become unavailable to those who cannot afford the fees. Thus, monetary systems must be efficient enough to not need fees.

Energy Efficiency

Cryptocurrencies require the encryption and decryption of large amounts of data. Encryption requires many processor cycles and these use lots of electricity that generates heat that needs to be cooled and cooling requires substantial electricity in itself. Electricity is an expensive form of energy so blockchains can become very expensive especially if there are 18 thousand in the network.

Bitcoin's use of energy is not a good thing. We, like all life forms, must economize to survive. We want everything to cost less and produce more. Therefore, it is always in our best interest to have monetary systems that are more efficient than the alternative. It should be noted that cash currencies require a huge amount of energy to operate as well. It takes energy to create a $100 dollar bill and to physically move it around (circulate it). The further across

the world we circulate it, the more it will cost. So Bitcoin is much more efficient than the US dollar in many circumstances. If I want to move $2.5 million cash dollars from California to Peru, I will need to hire a private airplane with a crew that includes a security guard. Not cheap. Paying a $16 Bitcoin fee is cheap in comparison.

Above is a mobile RAIDA *used for CloudCon*

Bandwidth
Bandwidth is another concern for digital currencies. Bandwidth requirements have a large impact on the speed in which transactions take place. There are several things that can be done technically to speed up transactions.

1. Use UDP protocol instead of the TCP protocol. The UDP protocol uses less bandwidth and electricity. TCP requires about .5 second to perform its handshake. UDP does not require a handshake making it .5 seconds faster. The trick is that you will need to keep your requests less than 1,400 bytes long so they can all fit into just one packet. And you will need to have redundant servers because UDP is unreliable.
2. Use AES instead of SSL/TLS encryption. The encryption used to transport data from the client to the servers is almost always SSL/TLS. AES uses less bandwidth and encryption than because SSL/TLS also needs to have a handshake and key exchange. You can save another .5 seconds by using AES. Computers also can encrypt AES faster than SSL so that is another benefit. Plus, it is quantum safe.

3. Use a binary protocol rather than a text-based protocol. This should reduce the bandwidth by at least 50%.

4. Use higher denominations if it is digital cash. Less notes are needed when you send higher denominations. So have a 1 million dollar note instead of 10,000 one-hundred-dollar notes.

5. Always make your requests larger than your responses. This protects you against DDOS (Distributed Denial of Service) attacks too. When you send a request to authenticate on million coins and include one million serial numbers, respond with one status byte that means "all good" or "all bad" or "error."

6. Use zero knowledge proofs to lower the amount of information needed to pass between client and server.

Unaffordable Fees

Another availability issue is that it requires high fees and these fees automatically block small transactions meaning the system is only available for transactions over a certain size. This size is growing as Bitcoin fees grow. Fees make the system unavailable for poor people. Therefore, perfect money has no fees.

The big problem with these blockchains is that they're so expensive to run that they work when dealing with large purchases. But when

it comes down to regular normal purchases, they're not affordable, which makes them unavailable. So, we have to have a system which has no fees otherwise it automatically has availability problems.

Usability

Another factor that will make a currency unavailable is if it requires much learning and intelligence to use it. Does it require the person to download software? Can it work on a cell phone? Do you have to go to college to understand how to work the thing? The easier a currency is to use, the more available it will be. Availability could include things like: is the dime smaller than the nickel? Two people understand the standard - the nickel is actually worth less even though it's bigger than the dime. That's something that certainly trips up kids and can cause some minor problems. In order for it to be available, we want to make it usable. The worst thing is dealing with small fractions like .0000001: confusing.

Questions we can ask About the Availability of a Currency

☐ Can your company personnel such as software engineers and server administrators make your token unavailable?

☐ Under what circumstances can hackers including hostile foreign governments make your token unavailable?

☐ Under what circumstances can you make your token unavailable?

☐ Under what circumstances can tech companies such as Amazon, Google, Facebook make your token unavailable?

☐ Under what circumstances can the US Federal Government make your token unavailable?

☐ Is there any time that your token will become unavailable? (Day, night, holidays, scheduled maintenance?)

☐ Are there any locations on the planet where your token cannot be used due to insufficient resources such as electricity, bandwidth, administration, and cost of fees?

☐ Are there any locations on the planet where your token cannot be used due to lack of legality?

☐ Please list any Internet infrastructure that your token depends on to

---

work such as DNS, CloudFlare.com, AWS, Visa, Twitter, etc..

☐ Does your token system have any systemic risk of failure? One thing that can go wrong to bring down the entire system?

☐ Is the code running on your servers/nodes all identical and written in the same computer language by the same programmers creating systemic risk of software failure?

☐ Are the server/nodes all using the same hardware and operating systems creating systemic risk of failure?

☐ What happens if a server crashes?

☐ What happens if there is a bug in the server/node software?

☐ Can a single bug in an operating system, hardware configuration, server software, or client software make the whole system unavailable?

☐ Can a rogue employee at your company bring down your token? What measures have you taken to prevent this?

☐ Please provide a statement about the Availability of your token.

☐ How many server/node administrators are needed for your system to work. What is the estimated cost?

☐ How much does it cost to create your token (each new one)?

☐ How much does it cost to change the ownership of your token?

☐Under what circumstances could the costs of administering your token exceed the ability of the administrators to afford it?

12. INTEGRITY: THE OPPOSITE OF CORRUPTION

Integrity is when we know that a monetary system has not been corrupted and is giving us the correct information as it is intended. In cash systems like the USD, money corruption could be caused by:

* Cash being destroyed in a fire
* Cash being lost
* Cash being stolen
* Cash not being worth its face value
* Cash not backed by what it is supposed to be backed by (like silver certificates not backed by enough silver)
* Cash not being fungible (not all worth the same)
* Encryption being hacked (in the case of digital currencies)
* Double Spending
* Counterfeiting

These causes of corruption can be classified in the following categories:

* Physical Integrity
* Entity Integrity
* Domain Integrity
* Referential Integrity

Physical Integrity
Physical Integrity: Protects money during storage, retrieval and management from physical issues.

It should be impossible for someone to gain spending rights that they have not earned or lose spending rights that they have earned.

In 1996, e-gold was created. Everyone would put their gold into a central safe and get electronic money in exchange. The money was very successful and billions were exchanged. However, one day, the system went down because a thief stole the vault containing 85 million dollars' worth of gold. The thief was the State of California. The creator of e-gold was forced to pay a $200 fine and spend 300 hours doing community service. Such a small punishment for the man but a giant body blow to the currency. e-gold did not have data supremacy because it did not have 100% availability. As a result of this, everyone using the system lost their spending rights.

Bitcoin was the first digital currency to solve the Physical Integrity problem of digital currencies. The problem is how can we have digital money when everyone can just copy and paste the data a million times with no costs? Physical money has had the same problem for 10 thousand years. If we make our money out of mud or papyrus, how can we stop people from creating counterfeits? If people are able to make counterfeits, then they are stealing and that hurts everyone that uses the system and makes the system worthless.

Counterfeiting
Merriam Webster definition - made in imitation of something else with intent to deceive.
Counterfeiting is the biggest problem in monetary systems and it must be solved for the system to be fair and to function at any level

better than Monopoly money. The reason that counterfeiting is a problem is because it allows people to get spending rights that they have not earned. Counterfeiting is unjust and violates the rights of all other people who use the monetary system. Governments must spend time and money to stop counterfeiting, otherwise, the whole system will become corrupted. These expenditures are part of the administrative costs of running a cash system.

Counterfeiting is also a problem with public ledgers. There have been instances where people have taken the Bitcoin code and started their own Bitcoin network but claimed it was true Bitcoin. They then sold these fake Bitcoins for a reduced price. This is very simple to do for people like me who have a deep understanding of Bitcoin. This counterfeiting requires some very small changes to the existing server and client software by just changing the DNS names used as seeds.

With traditional cash, counterfeiting is when a person puts the symbol of a monetary system on something that is not money in that system. If I take a piece of paper and write a dollar sign on it ($) then try to buy something with it, I am counterfeiting. If I take a coin that is pure silver and write a '$' on it, then I am still counterfeiting. Even though the coin may be worth more than the currency it represents, the dollar sign is a copyright of the USA and only the Mint may use it.

You can learn more about this by looking up the Liberty Dollar. They made silver coins with dollar signs on them and included the national motto "In God we trust". They were accused of counterfeiting by the US government.

Printing Too Much Money
But what about when governments create more of their own money? Is that counterfeiting? Based on the definition of counterfeiting, the answer is no. But, based on the Theory of Perfect Money, the problem is not making fake money, the problem is giving spending rights to people who don't deserve it. If your neighbor uses his color copy machine to counterfeit dollars,

it is pretty much the same thing as if Governments do it. The only difference is who gets to take unearned assets from the economy.

Bitcoin's administrators, which are called "miners," create Bitcoin when they are able to guess cryptographic keys. In this way they are compensated for running the network including spending money on all the electricity that is needed. In this case, the administrators are compensated for the value that they added. This is an improved method of increasing the money compared to how governments just print money.

With CloudCoin, the money in the system is fixed. Administrators are expected to volunteer but will receive the coins that have been lost (not spent in many years). To create new coins, CloudCoin must split, this is where everyone in the system has their coins double, triple, or multiply by however the administrators decide to do so in order to keep the money from becoming too valuable. I consider this just because there is never anyone who can get value that they do not deserve. However, CloudCoin has never split and is not expected to. This is because there may be some confusion when this splitting occurs and many people may not be aware of the splitting and lose spending power. Instead, we implemented fractions that allow us to have very valuable money.

Gold, Fiat or Information?
The architect of Bitcoin (AKA Satoshi), implemented Bitcoin to be like virtual gold. He seemed to believe that money comes into existence by mining. Mining must take a lot of work and as time goes along it requires a lot more work because the more you mine, the less there is to find.

With CloudCoin, we don't see money as being gold. We see a monetary system as being information systems and we see the data as being money. We can write data on a piece of paper, gold disk (coin) or hard drive. All data takes up space so we need to store it somewhere.
Money can get its physical integrity from gold and silver coins (disks) because it's expensive to counterfeit these. However, it is

possible for me to perfectly counterfeit a gold coin by buying gold and minting it myself. Or I could mine more gold and silver. Either way, obtaining gold and silver is so expensive that it would cost more to mine the metal than to just use the real coins. An important lesson here is that a currency does not have to be counterfeit proof. It just needs to be uneconomical to counterfeit. This is why we usually don't worry about one-dollar bills getting counterfeited. So what if they do? Counterfeiters will spend so much time and effort and receive such a measly reward that they will end up being worse off.

Double Spending

Double spending would allow people to spend their money more than once and ruin the integrity of that currency. A classic example is a person putting a string on a coin and then inserting that coin into a vending machine. Then after the purchase, pulling the coin back out using the string so it can be spent again. This "string attached" hack is a big problem with digital money and there are only two techniques that I know of to stop double spending.

One technique is to use the Blockchain to write down every transaction that has happened and make the process of checking to see if a coin has been spent before a processor intensive slow operation.

The second technique is the method used so that every coin has passwords registered with an "Redundant Array of Independent Detection Agents" so that the purchaser gives the seller the passwords and the seller change them so that the purchaser no longer knows them. The CloudCoin method is obviously superior as it is faster, uses less electricity and is 100% private because it requires no user accounts. There is a mountain of other features that also make CloudCoin superior that I will cover later.

Entity Integrity

In monetary systems, entity integrity means that all money has to have an owner. Perfect money cannot be lost or stolen as loss or theft breaks entity integrity. It should not be possible for a person

to spend the money of someone else by faking their identity either as is the case in identity theft.

Today we are plagued with loss of money, theft of money and theft of identity. This is especially true with crypto currencies where exchanges are regularly robbed of hundreds of millions because more than one person has the keys and there is no way to know which of the people who had the keys were the one who stole the money.

Theft Of Coins

If you are interested in cryptocurrencies, no doubt you have heard about the billions of dollars' worth of crypto that has been stolen from crypto exchanges. The Zaif Exchange had $60 million taken. Bitfinex lost $65 million. Mt.Gox lost $360 million. Coincheck lost an incredible $500 million [1]. And the hacks just keep continuing. I went to list CloudCoin on Bitmart but they were hacked for $90 million and had to spend six months improving their software before we finally could list. Is the amount of money being hacked going down? NO! This year (2022), hacks are up 60% from last year according to Chainalysis [2] and that is over $2 billion.

Theft also happens with credit cards and banks are always getting burned. Thieves trick creditors into giving them the rights to spend someone else's money (identity theft). The problem is so great that when you go to the store to buy something with your debit card, the bank cannot confidently determine that you are not a thief so they declined your transaction. It doesn't matter how much money is in your account. If they don't know that it is you who is spending the money, they will decline. That is a failure of entity integrity.

With Bitcoin and crypto currencies, there is systemic risk of loss and theft because the system relies on a "golden egg": The private key. There is no way to mitigate this risk. This flaw makes it possible for a system administrator or software developer who works for a crypto business to steal all of their employer's money without the employer knowing about it. There is no accountability with cryptos. There are no permissions built in. And, you can't change the private

key. If you give an administrator your key so they can set up a wallet for you, they will always have that key. They can take as much as they like whenever they want to. If you are a system admin, you could be accused of stealing because there is no deniability. There is no way to prove that you are not the one who stole the money.

Loss of Coins

Then we have the problem of loss. The private key situation provides systemic risk of loss and theft. Worse, if you try to mitigate theft, it will increase the risk of loss. And if you try to mitigate the risk of loss, you will increase the risk of theft. To mitigate loss, you can make lots of copies of your private key and store them in different locations. But now you have just multiplied your attack surface and your chances of being hacked and your keys stolen. If you want to reduce your risk of theft you could lock your private key in an encrypted USB drive. But now your chances of losing that drive or forgetting your password to the drive, or having a bug with the USB's encryption software has multiplied!

Is loss a real problem? How many people actually lose crypto coins? According to a study by the Wall Street Journal, 20% of all Bitcoins have been lost and will probably never see circulation.[3] Imagine that you lost 20% of your savings? I know lots of people who became a CloudCoin user because they had lost a huge number of other currencies. How many of us can afford to risk losing all of our savings? It is okay for us to take risks but not risks that will ruin our lives. Even if there is only a small risk of this happening, you cannot afford even the chance that you will be wiped out financially. A civilization cannot afford to have such losses. There must be a way to reduce the risk of loss and theft for digital currencies or they will only be viable for people young enough to recover or rich enough to not have to risk their entire fortune.

Island of Yap Achieved Entity Integrity

The problem of loss and theft has actually been solved, albeit by eliminating privacy. The Island of Yap is one of the last places on earth that European explorers discovered. Yap is a small island in the massive Pacific Ocean. When the Europeans arrived, they were

amazed at the monetary system used by the islanders. Each family on the island had a raised platform where they kept their houses and their money. Their money was in the form of giant stone disks. These disks are so massive that they would be impossible to lose. Any person who would decide to be a thief and steal another family's money, would face some serious challenges. They would have to sneak out in the middle of the night with enough people to help them roll the stone from the victim's platform to their family's platform. This theft would be easily detected and everyone would know about the theft because everyone can walk by and see who has what money.

So why can't we do this with Bitcoin? Actually, this is very close to how Bitcoin works. The only difference is that instead of using raised platforms, Bitcoin uses a ledger that can be read by all (Public Ledger) and you can see how money moves from one account to another. Bitcoin has digital accounts and these accounts are pseudo anonymous. This means you don't know who people are until you do some trading with them and learn their account numbers. With Bitcoin, to stop theft, we could require that everyone we do business with simply publishes their account number with their name. Then if there is theft, we can look for the account that got the money, and have them arrested. There is just one problem, we would lose all privacy and privacy is one of the three foundations of a perfect currency.

Boot Camp Technique of Loss Recovery
There is another way that we can achieve loss reduction. This is by using a system similar to the one used in military boot camps. Everyone in boot camp (at least when I was there in 1986) had to write the serial number of their dollars on a piece of paper and give it to their drill sergeant. That way, if some money ends up missing or found, the owner can be identified by looking at these lists. This works because money is just data and we can copy data. We can do a modern-day equivalent by taking pictures of cash with our cell phones or using a photocopier to record what we won. Again, we have stopped loss and theft, but only at the expense of privacy.

How CloudCoin Deals with Loss

I have done real world experiments with reducing the risk of loss and loss recovery with CloudCoin. Unfortunately, I do not think I have achieved the perfect system. But it's worth talking about. RAIDA-Based digital cash such as CloudCoin do not have a systemic risk of loss or theft. This is because there are no private keys to act as a single point of failure.

For starters, we can mitigate loss and theft in the same way we can with paper dollars. All of our CloudCoins can be offline, stored in a USB drive, or placed in a jar that is buried in the backyard. We can store some here and some there so that if one location is found out, the others may stay hidden. However, I am pretty sure that the best way for people to mitigate loss and theft is to put their cash in a bank where the bankers are in charge of providing security. This is just like banks do with dollars and it has seemed to have work for hundreds of years. Unfortunately, governments are now going after people's cash by attacking banks directly. Banks are not as safe as they used to be due to oppressive governments desperate for cash due to their foolish spending.

Store In Mind

In 2017, I ran a study in Venezuela trying to figure out how to get people to adopt CloudCoin. We immediately had a problem with our testers getting their phones stolen along with the CloudCoins that were on them. To prevent this, we came up with something called "Store in Mind."

CloudCoin was designed so that each Coin had a one-byte "network number" and a three-byte serial number. This allowed us to address every coin with an IP (Internet Protocol) address. These addresses are cool because we can put them into something called a DNS (Domain Name System) server and associate them with a FQDN (Fully Qualified Domain Name). An example of an FQDN is "Coin1.MyDomain.com" You may not know it, but you use FQDNs and DNS every day. When you go to www.google.com your computer asks the DNS server to lookup the IP address and your DNS server will respond with something like 8.54.32.54. With

CloudCoin, this IP address means that the serial number of the coin is 54.32.54.

You can give one FQDN many IP addresses so that one FQDN can hold hundreds of coins. Now imagine you named all your coins something easy to remember like "purse.50.usd". If you want to know the serial numbers of your coins you just need to ask the DNS server, "What is the IP address of purse.50.usd?" and the DNS server will return a list of all the serial numbers of your CloudCoins in that purse. .

In other words, we can give a "purse" of our coins a memorable name and have the DNS server track the serial numbers for us. If someone steals our phone, we can still use any computer in the world to know the serial numbers. We just need to go to a computer command prompt and type "nslookup purse.50.us". That is the Name Server Lookup command. Our software can do this automatically. Our client software once allowed people to upload the serial numbers of their coins to DNS servers to make this possible.

But we need more than the serial numbers. We also need the authenticity numbers (passwords) and CloudCoin has 400 bytes of them. We need to have different numbers on each RAIDA so the

RAIDA admins cannot steal the coins themselves. To make it possible to remember the authenticity numbers, we allowed the user to create a passphrase that could then be mixed with RAIDA ID number and the serial number to create a seed. This seed would be "hashed" and the hash would be used as the authenticity number. In this way, we can remember all 400 bytes of the authenticity numbers by just remembering the passphrase. This allows us to go naked through security checkpoints and bring our money with us. This assumes they will allow you to go naked and that you have a computer at your destination to mind dump your coins.

When we rolled out Store in Mind, it did stop theft. But it increased the loss so much that we got rid of it. The problem was that people needed to remember their passphrase and they just couldn't remember it.

Loss Periods and Lost Coin Reports

Our next attempt to stop loss was to use a system where users could report to the RAIDA the serial numbers of Coins that they lost. Then, the RAIDA was set so that any Coins that had not been authenticated in over five years would be considered lost. The RAIDA admins would mine these lost Coins. They would examine their lost Coin reports to see if there were any lost Coins that needed to be returned to the owner. If yes, the Coins would be returned. Then whatever lost Coins were left, would be distributed as pay for the RAIDA admins. In this way, the RAIDA would be funded by lost Coins.

This was a bummer because some people wanted to keep their Coins sitting around for more than five years and people who lost their Coins did not want to have to wait for five years. There was also an element of loss of privacy because people had to provide their email address in their lost Coin report.

As it turned out, running RAIDA nodes is extremely low-cost and the RAIDA admins seemed to be happy to volunteer. They were not interested in getting Coins that had been lost and to my

surprise, there were very few Coins that were lost. However, I wanted a system that did not have Coins "expire" and did not force people to wait to recover lost Coins.

Email Recovery

Another thing we experimented with required a person to insert a hash of their email address into the first part of every authenticity number they used. If they lost Coins, they could tell the RAIDA their email and the serial numbers they lost and if after performing a hash, the RAIDA found a match, the RAIDA would then send them an email with the full authenticity numbers of the Coins.

This system had some problems because we could not send the person their whole Coin. We had to have each of the 25 RAIDA send one part of the Coins and then the user would need to stitch them all together. This was just very inconvenient. However, I could imagine an improved system. The obvious weakness is that it allows someone to force the RAIDA to send emails. If you know your email, I could tell the RAIDA that I lost every single Coin that there is and it would send the authenticity numbers of whatever it found and if that attacker had access to the email account, then the Coins would be stolen. But, since email is so insecure and usually not encrypted, attackers would really just need to watch the traffic.

Storage Lockers

The solution that we are experimenting with now is a system where Coins can be put into lockers on the RAIDA. This is similar to the lockers you might find in a train station. The user is able to decide the key that will be used. Then they tell the RAIDA to create a locker for them that opens with that key. Once the locker is created, they can add all the Coins they want into it and those Coins will stay there forever. This allows people to put all their money in the locker and walk across the border naked (in theory). Then, when they get to a computer, they can enter in their locker key to download all the Coins. Again, if you lose your locker key (password) you are screwed!

Stopping Identity Theft

Identity theft does not happen unless you are accessing your money through some system that requires you to authenticate yourself. This is the extremely empowering thing about digital cash. You are in control and you don't need permission. There is nothing like cash because you can't fake it. Digital cash like CloudCoin requires that you have the data and that can be in your cell phone, USB drive, written on a paper QR code or stored in your mind as a locker key. Nothing stops identity theft like cash. I suggest people read the book "Cloudmoney" by Brett Scott to understand the superiority of cash over every other payment system.

Domain Integrity: Keeping Money, the Same

Domain integrity is the same as Fungibility: The property of a good or a commodity whereby individual units are capable of mutual substitution. "Fungibility" is a term that economics and crypto enthusiasts use to describe the interchangeability of money. I use the term that is customary in Information Systems: Domain Integrity. It means that data should be stored the same way. Money can come in many forms. It is necessary for money within the same currency to be in the same form.

Today money falls into many different "Domains". We have pennies made from copper, nickels made from nickel, dimes made out of silver, quarters made up of silver and other random metals, paper dollars, gold coins, checks, plastic credit cards, etc.

The ownership of Blockchain coins is traceable. Coins are regularly implicated in theft and crimes and flagged as "dirty." Dirty coins will not be accepted by exchanges and other merchants who monitor the past owners. Now we have two domains of blockchain coins: dirty and clean.

What happens to money when the price of silver and other metals changes or when a Bitcoin becomes dirty? The money loses domain integrity and is no longer perfect in that regard. The effect of this on you is that your money will be of a different value depending on your situation.

Bitcoin's Domain Integrity Problem: Dirty Coins

A Bitcoin is considered dirty if it's been used in money laundering, drug purchases, scams, credit card theft, exchange hacks, and other nefarious activities. This problem is so bad that criminals are often unable to get away with their crimes if they choose to use crypto.

If you do not run an "Anti-Money-Laundering" check on the coins you receive, then it is likely that exchanges won't convert them. You will probably have to sell them at a huge discount. There is tracing software that can stop you from making any transaction, and thus making your coins worthless. Who knows, you may even be investigated by the police. New laws are making this a bigger and bigger concern. [1]

Solving Bitcoin's Domain Integrity Problem

We could have everyone register their crypto accounts with the government so that the government could observe all transactions. Then, if someone does something wrong, they can be arrested immediately. This would add assurances to the system so that people would be protected from accepting dirty money. Does this sound like a good idea? No.

In doing this, the currency effectively becomes a CBDC (Centralized Bank Digital Currency) with no privacy features. Experts in security recognize that this could lead to a type of "crypto-Fascism" where ordinary people can be denied their money.

Edwards Snowden said:

" a CBDC is something closer to being a perversion of cryptocurrency, or at least of the founding principles and protocols of cryptocurrency—a cryptofascist currency, an evil twin entered into the ledgers on an Opposite Day, expressly designed to deny its users the basic ownership of their money and to install the

State at the mediating center of every transaction."

In today's weaponization of government agencies, there is no doubt that whoever has knowledge of the transactions of others will use that knowledge for their own benefit.

The real solution
In order to achieve domain integrity, we need to have money that is 100% private. That means there can be no identifiable information and no transaction records that would allow people to discern one coin from another. And of course, within physical money we cannot use dissimilar metals whose value is subject to change. With digital currencies, that is not a problem.

Referential Integrity
Another type of integrity is called referential integrity. And this only occurs if we have a currency that uses tokens that reference something else like stable tokens. So for example, back in the day, America had the silver certificates. These silver certificates were pieces of paper that looked like dollars and were redeemable for one dollar of silver at the Federal Reserve's bank.

These silver certificates lost their referential integrity because the

amount of silver that was supposed to back the notes was not really there. So while there might have had 100,000 silver certificates in circulation there may have been only 60,000 ounces of silver in the

vaults. We can create a token that references anything. I could say okay, here's Bitcoin and here is a token that represents it. For every time we put a Bitcoin into this Bitcoin account, we're going to issue one of these tokens. And then everybody can trade that around privately. So long as there's the same number of coins in the Bitcoin account as there are token coins that are in circulation then we have referential integrity.

Sometimes there are so -called "Layer 2" coins that are a much better technology but represent the base currency.

Today we have stable coins which are supposed to represent $1 or some other fiat currency. Historically, every currency that represents another currency fails. There have been at least 23 stable coins that represent the US Dollar that have failed just in the past six years. These include Terra Luna that lost $45 Billion market cap in just a week.

Here is a list of the stable tokens that have failed since 2016:

Acala USD (2022)
flexUSD (2021-2022)
Deus Finance (2021 – 2022)
Terra/Luna (2019 – 2022)
DefiDollar (2020 – 2022)
BeanStalk (2021 – 2022)
Wault Finance (2021 – 2022)
OpenDAO (2021 – 2022)
Empty Set Dollar (2020 – 2022)
BondAppetite (2021)
Stand Cash (2021)
Freeliquid (2021)
Midas Dollar (2021)
bDollar (2020 – 2021)
Unified Stable Dollar (2020 – 2021)
Iron Finance (2021)
Dynamic Set Dollar (2020)
One Cash (2020)
bitUSD (2014 – 2019)
QCash (2019)
Basis Cash (2018)
NuBits (2014 – 2016)

Other tokens that represent money are checks, credit cards, debit cards, money orders, gift cards, etc. If those tokens are not actually backed by dollars, then they have lost referential integrity.

No Reference Means 100% Referential Integrity
Bitcoin, the USD, and most national currencies do not reference anything else. And so, you always get 100% referential integrity with Bitcoin, USD and others. Currencies that do not have referential integrity built into them always fail. Perfect Money should not reference anything.

13. PREFERENTIAL INTEGRITY

How much money should there be?

This question has to do with how much precision do you want to have. Precision means how many zeros after the decimal. If we have a system that has money at the rate of .00000001 and another that only goes to .01 then the first is more precise. If we have a lot of money then we can expect things to cost a lot of money. If we have very little money in our monetary system, we can expect things to cost a little money.

Imagine that we had a situation in which we had only gold coins for money and we only had a few of them. We might go to the store and buy an entire truckload full of gasoline with just one coin. Suppose that we had another currency like "Chinese Cash Coins" made of brass. We might need to use hundreds of them just to buy one gallon of gasoline. That would be a bummer. We want to have a precision level that allows us to efficiently use the money. We don't want to have huge amounts of money that we haul around with us. At the same rate, we want to have money precise enough so that we can see the price details and know if a product is efficiently produced or not.

Two Gas Stations

For example, suppose I want to buy some gasoline and there are two gas stations, one on each side of the street. Suppose our monetary system does not have much money in it. The gas stations are each selling a gallon of gasoline for 4 coins. We cannot tell if one of the gas stations is more efficient than the other because the price is the same. But suppose we were to multiply the amount of money in the system tenfold. We may now see that one station is selling gas for 38 coins while the other is selling for 36 coins. Now we can economize by buying our gas from the least expensive station. Having more coins in the information system is literally having more data/information in the system. This information allows us to see finer details.

However, we can go overboard on this. We could have it so that on one side of the street it's a hundred CloudCoins and on the other side of the street it's 99.99999999 CloudCoins - off by 0.00000001. That's less efficient for a couple of reasons. One reason is that we have to have all these zeros and that will increase the cost of signage. We are also possibly dealing with physical coins and if we have to have nine coins for each place then we need hundreds of physical coins for this transaction. We would have to have nine dimes, nine pennies, nine Millicent and nine micocents and nine nanocents. I don't know how far we will go but that is a lot of denominations needed just to save one millicent. We'd need to have all of these different coins and that would be expensive to administer and difficult to manage.

But the most expensive cost of precision is that the human brain has a difficult time telling the difference between .0000001 and .00000001. So costly mistakes can be made. That is why I propose a way of formatting fractions of money such that numbers look like:000,000,001 Here I have put a comma between every three fraction digits. But after using this system I decided it could be done better if I made the prices look like this: .00_000_001 This is because we are used to seeing two digits for cents so we might as well keep them together. Use underscores instead of commas so that the fractions are distinct from the integers. End at eight places because that is the precision that the OG Bitcoin uses. The smallest

units of Bitcoins (.00_000_001) are affectionately called "Satoshi."

Who Should Mint the Money?

One of the inherent problems facing all modern currencies (including cryptocurrencies) is how new money is created and who gets this newly created money.

According to my theory of money, the perfect money cannot be created (minted) or destroyed except at the inception of the whole system. If more precision is needed, then the money must be split. This is similar to a stock split. The split results in all people ending up with the same proportion of money - just more of it. The primary purpose of money is to track who gets what proportion of the total output based on their total input. If we just create new money and give it to someone, it would upset that proportion and make the system unfair.

When money (data) is created and introduced to the monetary system, it may join at the expense of everyone else. This is similar to stock dilution. These types of systems (which now dominate the world more than ever), inadvertently cause logic errors, negative feedback loops and submersion of the economy. In economics this phenomenon is often called "inflation," "price inflation" or "bubbles". Sometimes economists argue about what inflation is. Is it when there is more money? Is it when there are higher prices? They are both wrong and need to turn to Information Systems in order to understand the situation. We can solve this problem by calling monetary inflation "dilution". We can call price inflation "price anomalies" or "price corruption." Every-time a new value-unit (dollar) is added to the money supply, it is dilution.

The government's monetary policy of dilution is price-corrupting everything from oil to soil. Here recently, the government diluted 1.2 trillion dollars. Now we are seeing price anomalies for every product and service.

Remember that money is data. If data just appears somewhere in an information system, we call this an anomaly. This incorrect data

will be processed by our human minds and cause logical errors. We will see opportunities in things that are not opportunities. Likewise, we will avoid true opportunities because we cannot recognize them. This can cause a feedback effect in which errors are compounded in "Doom Loops".

Who Decides When the Money Supply Increases?

Okay, so let's talk about who decides when the supply increases. With CloudCoin, we've come up with a solution. The idea is that CloudCoin should be worth one Pepsi and i'm talking about a 12 ounce can of Pepsi. I am sure you are wondering why that is. That's really weird. There are a few things that we have had around for a long time that we can use to measure price inflation by studying how their prices have changed over time. Pepsi is one of those products. Big Macs at McDonald's are another one that is famously used to examine dilution. There's even something called the Big Mac Index in which we can track how the price of Big Macs has changed over time. We can compare the price of Big Macs in America to the Big Macs in France to calculate price parity. A Pepsi cost five cents in the 1920s, over 100 years ago.

Cash Splitting

So technologically, CloudCoin uses a system called splitting and of course we've never actually had to use this because CloudCoin is a brand-new currency and we haven't gotten to that value yet where we have to split. But this is the plan and the plan is to do something like a stock split. Stock splits are something that are well known throughout the world and people that own stock are familiar with it and generally people love it when their stocks split. This is because it makes their stock more liquid. It is better to have two stocks worth $30K than one stock worth $60K. This is because it is easier to find a buyer who is willing to spend $30k than on that to find a buyer who is willing to spend $60K. Bitcoin does not have this problem because it can be broken down in increments of .00000001. Bitcoin allows fractions and stocks only allow whole numbers. You can have 5 shares of a company or 6 shares of a company but not 5.8 shares of a company.

Denominations

If you are going to have a cash system as opposed to a ledger-based system, (and you should) then you will need to have denominations.

The USD has denominations such as 1s, 2s, 5s, 10s, 20s, 50s and 100s. There are also fraction denominations including cents, nickels, dimes, quarters, fifty cents ($.01, $.05, $.10, $.25, $.50 respectively). That is at least 12 denominations total.

My first version of the Theory of Perfect Money specified that there should be no fractions. This was to keep the currency easier for low IQ people to understand. The denominations I chose for CloudCoin were 1s, 5s, 25s, 100s and 250s. In fact, I wanted one CloudCoin to be worth one Pepsi. But I made too many of them and they ended up being worth more like a cent or a Yen.

We did have several complaints that there were no fractions. People didn't seem to complain about the denominations we choose but having such denominations caused us to have to spend a lot of time making change. This was a frustrating process that added to the cost of the system due to the hours of programming needed to make it work. Because we were dealing with digital currency, we could have the user's program send notes to "change servers" that would return smaller denominations. This took a lot of seconds and that failed to meet my vision of instant transactions.

That is why in CloudCoin Version 2, we got rid of denominations all together and just had ones. Ones didn't need to be broken and that was excellent. But if I wanted to send 10,000 coins it would take ten thousand authentications and that also made things slow and did not meet my expectations either.

With CloudCoin Version 3, we got it right. In technology, the third version is usually where the product becomes usable. We changed it so we had 16 denominations and we also included fractions.

The new denominations are:

1,000,000	One Million
100,000	One Hundred Thousand
10,000	Ten Thousand
1,000	One Thousand
100	One Hundred
10	Ten
1	One
0	Zero (For IDs and Encryption Keys)
Dime	0.10
Cent	0.01
One Hundred Thousand Satoshi	.00_100_000
Ten Thousand Satoshi	.00_010_000
One Thousand Satoshi	.00_001_000
One Hundred Satoshi	.00_000_100
Ten Satoshi	.00_000_010
Satoshi	.00_000_001

With these denominations, we could now handle anything that was likely. We also set up our nodes so that they could break or join coins using a new technique. Instead of having a folder full of coins to make change, we had the RAIDA destroy the big notes and create the smaller ones. We can also do the opposite, destroy small notes and create larger ones. This allows us the ability to authenticate a million Coins in the same time it takes to authenticate one coin. We also developed a new tech that allowed us to run a checksum on many coins together and this means we can authenticate thousands of notes with one number. Finally, CloudCoin Version 3 meets my expectations of speed and it is a triumph!

Keep Denominations Substantially Different

One thing I noticed is that it is important for the distance between denominations to be substantial. I have no idea why the USD has a $1 and a $2 bill because there is not enough difference to make sense. I had 100s and 250s for the first CloudCoin but it was not a big enough difference to reduce the number of Coins that were needed to be authenticated.

The rule about denominations is to keep denominations substantially different in value to reduce costs and increase efficiency but not so far that you have to have lots of notes to make up the difference between them (which in turn increases authentication and reduces efficiency). Multiples of 10 seems to be perfect. It also makes the algorithm of breaking and joining coins easy to implement.

I suggest that the US dollar should do the same thing. Imagine that we only had ones, tens, hundreds and one-thousands and just pennies and dimes for fractions. It may seem strange but I would sure like to try it to see the difference.

How Money Should Look

If you inspect the 10,000 Dollar bill above (yes there was a 10,000 Dollar bill), you may not recognize the man pictured. His name was Salmon P. Chase. He was the man in charge of designing the 10,000 Dollar bill. He chose to feature the most important man in the world: Himself! He did not include "In God We Trust" or "E Pluribus unum" either. These mottoes are traditionally added to all

American money. What I find the most surprising is that he did not even bother to include the dollar sign. He did add his name. The moral of the story is that the proper design of money is highly subjective. Be careful who you put in charge of it.

Zero Dollar Bills!

You can also create denominations that are not worth anything. For CloudCoin we use zero denominations for encryption keys and authentication of users, computers and programs.
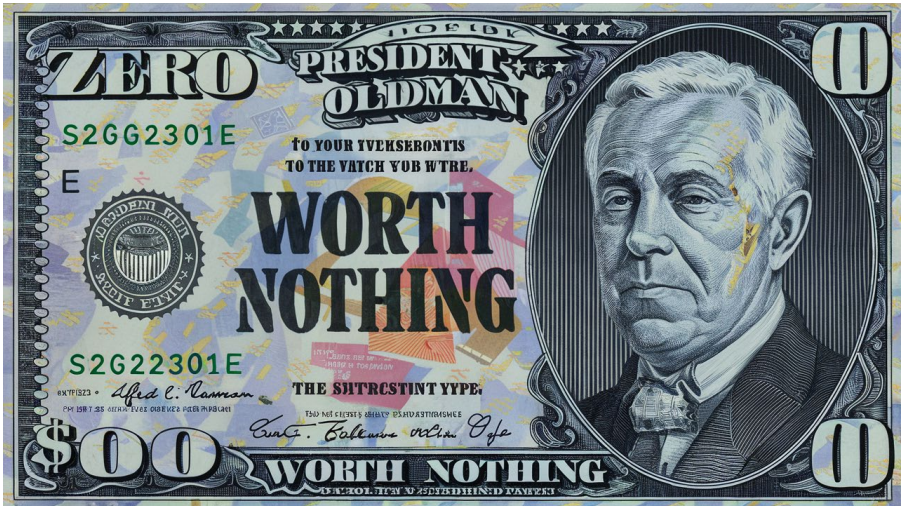
For our Wyoming Stable Coin Proposal, we have denominations for RAIDA servers, system administrators, State Treasurers, KYC officers and common users. There could also be denominations for NFTs, stocks, bonds, real estate deeds and much more.

14. THE REAL REASON MONEY BECOMES VALUABLE

The Network Effect

NOTE: I've adapted most of the ideas here in "The Network Effect" from what I have remembered from the book "The Cold Start Problem: How to Start and Scale Network Effects" written by Andrew Chen. It's a very good book and a must read for startups. I've found that the cold start problem is just as much of a problem for digital currencies as it is for Uber, Facebook or any other software that needs to have a network.

Digital currencies display a characteristic called the "Network Effect." This is when information systems become more valuable as more people use them. A poorly understood reality is that money itself is an information system and has more value than just the numbers it represents. The value of money will increase or decrease according to a lot of factors including confidentiality, availability, integrity and ease of use. But the network effect is a big factor and there is an extreme amount of value that can be created by increasing the network of users who use a currency.

The network effect can be understood by looking at the Uber company. In order for Uber to work, there must be a driver and a

rider at the same place at the same time. If drivers and riders do not come together at once, the network fails. Another example is YouTube. With YouTube, there must be content creators and content consumers, otherwise no network will form. The same is true with currency, there must be a buyer and a seller.

An important concept is an "atomic network". An atomic network is the smallest number of users needed to enable the money to survive. It is within the realm of possibility that a digital currency could survive with only two users. They would need to buy and sell from each other. This would seem unlikely as I know of no money system with only two users. We see atomic network effects in nature. In the 1950s, there were millions of sardine fish off the coast of Monterey California. Sardines need to school together for protection. If the population of sardines drops below a certain level, the entire population collapses. We learned this the hard way when we nearly drove the sardines to extinction by fishing them below their atomic network.

Networks take effort to grow. This may come in the form of marketing or actually paying people to use the network. At some point, networks can hit a "tipping point" or "escape velocity" that allows the networks to add more users without any inputs. If this growth is big enough, we call it "going viral."

Networks have two parts, the "easy side" and the "hard side". For example, it is easy to get content consumers on YouTube but more difficult to get content creators. For a digital currency, it is more difficult to get people to accept the currency as payment than to get people to use it to spend.

One way to solve the hard side is by recruiting "anchor" sellers. This is kind of like when you go to a mall (what's left of them), there are large department stores that bring in the most shoppers. Other smaller retailers in the mall benefit from these huge anchor stores. With currency, anchor sellers accept the digital currency as payment and in some cases (such as the petrodollar) accept the currency exclusively.

Governments create their own massive anchor by requiring everyone in their nations to pay taxes in their currency. Even if the currency is completely inferior, the people must trade for it to pay their taxes. This allows the governments to "cash in" on the network. Once a network is big enough, it is possible to "cash in." In currencies, this is usually done by inflation. The government prints up money for itself and everyone in the network gets taxed by this inflation. But citizens keep using the currency because they are benefiting from the network.

One of the anchor sellers that makes or breaks the value of the US dollar is oil. When President Trump increased America's ability to produce and sell oil to other countries, it increased the value of the dollar. Likewise, when Biden reduced American abilities to create and sell oil on his first days in office, he reduced the value of the dollar. The effect of this "anchor destruction" looks nearly identical to inflation. What makes the dollar really valuable is that people all over the world who need oil must buy it with dollars. The so-called "petrodollar" means that everyone needs dollars to buy oil. This inadvertently boosts the price of dollars regardless of the price of oil. Imagine if everyone in the world switched from buying oil with dollars to buying oil with Russian Rubles. Then the Ruble would go up in value.

Oil is a very "liquid" (easy-to-sell) commodity that everyone needs and everyone is willing to pay for. Other liquid commodities include precious metals and grains. These are all good anchor sellers.

So how can we create a digital currency with a big enough network to be self-sustaining? CloudCoin seems to already be self-sustaining but it has not hit any kind of tipping point or escape velocity that has caused it to go viral and up in value. Coins like Bitcoin, however, have gone up to as high as $72,000 per coin mostly due to their network effect and first mover status.

Scalability

Note that if a currency is not scalable, adding people to the network will slow it down and reduce its value. This is a bottleneck to transaction speed and transaction volume. This is why there are "alt-coins" that compete with Bitcoin. In the past, Bitcoin has come to a screeching halt when people really needed it to work. People don't like it when they cannot spend their money due to too many people using it. You can think of scalability problems like a bridge that will only accept a certain number of cars before traffic comes to a complete halt. For Bitcoin, it is reported that the limit is seven transactions per second.

The Speculation Effect

There is also a "Speculation Effect" caused by investors who believe they will get rich if they buy the currency. This will drive up the price but the same group of people can cause the price to plunge. This is the volatile part of the price of a digital currency. When Bitcoin shoots up from $33,000 to $66,000 and then back to $33,000, we know that $66,000 was caused by speculation and that the $33,000 is the value of the currency's utility. For example, I need to use Bitcoin every month regardless of its price. I use it for its utility. Because people like to use Bitcoin for purposes of payment, the price stabilizes at its utility value.

The Utility Effect

When looking at the price of a digital currency, utility is the non-volatile component of the price. It is created because the digital currency provides a real service. Coins like CloudCoin that are private, always available, free, and easy to use, scalable, etc., will have a high-utility effect.

An example of utility is to use the coin to make purchases that are efficient. Suppose you want to buy some eggs, milk, and a bag of flour. You go to the store and find that there are many brands selling the same things. The eggs, milk, and flour all look identical. How do you choose which one to buy? Price, of course. The price gives us information about products. We choose the lowest price when we are trying to conserve our credits so we can buy other things too. What we don't realize is that by conserving our money, we are also rewarding the most efficient producer and that will mean that the producer will keep on producing. Meanwhile, products that you did not choose may ultimately go out of business if they do not make enough sales. Now multiply this against everything that is sold across our economy including our labor, products, land, and services and you will see that everything becomes more efficient with good money, assuming there are no government subsidies or taxes blocking the signals.

Money that makes us more efficient is very valuable.

Another utility effect of money is to help us become more productive. Why do we like to shop on Amazon.com? Because we can look at hundreds of products and buy them with a single click or maybe two. That's productive! Why do we use Google Search? Because with Google we don't have to go to the library and search through card-catalogs to find books with the knowledge that we need. That's efficient! Why do we value Netflix? Because we can see all the movies in one place and don't have to drive to theaters. What value does LinkedIn provide? We can quickly learn about each other and make contacts. That's a much more productive way to meet people than traveling all over the world.

But what about the United States Dollar, (USD), the monetary system of the United States of America? How does it help us to become more productive? The USD helps us to signal to each other which jobs need to be filled the most. This is done by paying wages and salaries. We may have the opportunity to work at a fast-food restaurant or an engineering firm because we have a degree in engineering. The fast-food restaurant is next to your house, has a nice manager, and is a fun place to work. The engineering firm is none of these things but pays a lot more. Where are you going to work? The place that pays the most because money tells you where to work!

Monetary systems help us to be more efficient and productive. But this is not just true for monetary systems. This is true for all information systems.

Energy Efficiency and Fees

Nearly all digital currencies charge fees. This is partly due to the fact that they often use huge amounts of power and need to offset those costs. Some people think that it is good and necessary for a cryptocurrency to require lots of electricity. However, like almost everything we humans do, it is better to economize and be thrifty. Fees reduce the value of the money. The higher the fees, the more the value is reduced. In public blockchains, these fees are generated by the so-called miners who act as the server administrators. With

the paper dollar, the costs are distributed so widely that no fees are required.

The Bundle Effect

There is another effect called "Bundling". Think about how Microsoft gave away Internet Explorer with its operating system. This gave Internet Explorer an edge against its competition, Netscape. RAIDA Tech has created GPT Anonymous which allows people to use AI without logging in for the sake of privacy. People who try this program like it and RAIDA Tech has now hired a sales company to solicit companies to use it. GPT Anonymous uses CloudCoin and it will not work without CloudCoin. GPT Anonymous may provide a bundle effect with CloudCoin making them both more valuable.

The SEC Effect (Securities and Exchange Commission)

Sometimes, digital stocks and bonds may look like money. Sometimes, digital money may look like stocks and bonds. If you have ever heard of an "ICO" (Initial Coin Offering), there are usually attempts to raise money for a project. It is a type of crowdfunding where instead of selling stocks, digital currencies are sold that represent stocks (but nobody calls them stocks because that would be illegal - at least in America). So, they just call them tokens instead and see if they can get away with it. The marketers of these digital stocks will sell them for US Dollars. This is how you can tell if the digital asset is a stock or a currency. If it is a currency, you don't need to sell it for dollars. Instead, you can just spend it. This is how CloudCoin was developed. The initial system administrators and programmers were paid all the CloudCoin for their part in development. Bitcoin and XRP were the same way.

The SEC does not like ICOs. At least not the ones that are not registered. Furthermore, it seems the SEC thinks it owns the entire world and will go after anyone anywhere so long as there is one American investor involved. This SEC interference can cause massive drops in coin value. Recently, the SEC has been required to pay for the damage it has caused so the SEC effect may be reduced in the future. The SEC is probably the biggest threat to

liberty in the world.

Stability Effect
Lots of people buy digital currencies thinking the price will go up. These purchases indeed cause the price to spike until we run out of "greater fools." Then prices collapse causing the so-called investors to lose their ass-ets. Stable tokens are guaranteed not to go up in value and guaranteed to lose all their value (in my opinion) given enough time. I recommend that stable coins be used to complete quick transactions but never as savings for long periods of time.

The Gift-Card Effect / Lost Coin Effect
There is also a minor "gift-card effect" where some people do not ever use their buying power so that is transferred to the seller. Coin loss makes the coin more valuable by removing some of the supply. But it also makes the coin less valuable because people really cannot afford to lose lots of money.

Determining the Exact Value of A currency
Figuring out the value of information systems is difficult in general. While I have not spent much time trying to understand how to value an entire monetary system, I think the best approach is to use its so-called "market cap." We take how much each unit is worth and multiply it by how many units there are. Since value is a concept in our own heads, we may personally value one currency over another. But the market cap is a good generic way to get the overall value.

Perfectly-Valued Money
Perfect money will have a large user network, be stable enough to make people happy but will appreciate in value enough to be desired by speculators. It will provide all the utility possible by having all the features that make up confidentiality, availability and integrity. It will also have data supremacy so that no government agencies can do anything that would threaten it.

15. INFOOLATION, AKA INFLATION

"A thought is a powerful thing. It's an object that pops out of consciousness and can be very casual in the physical world." [1]

The most important part of a monetary system is the human mind. We need to know what is real so we can think true thoughts. We need to be free to behave appropriately. We need to learn from our mistakes so that we can remember them and make better decisions in the future.

But there are people that want to control what we think so we will help them reach their goals. Governments use propaganda because it works. But there are also viruses of the mind that spread from person to person that do nothing but spread themselves.

No other thing can affect our behavior greater than money. But money can fool us into doing some stupid things. If a person were to counterfeit money efficiently, that person could fool other people into giving them things that they do not deserve: our goods and services.

Dropping Money from Helicopters

Ants use pheromones to make decisions about what actions they should take. Like harvest food, feed the queen, clean the nest and everything they do. If you spray random pheromones around their nest, they will all die because they can't make useful decisions.

When, or if, money is put into the economy in random places, it would cause crazy behavior including people working jobs they should not, not taking jobs that they should, or not working at all. Making bad investments and missing excellent investment opportunities. Making stupid purchases. On a macro scale, this activity can result in booms and busts (bubbles) in markets. Parts of the economy may be unaffected. Other parts could go into hyper mode. This will not last long though. Soon, some parts of the economy will be neglected. Because the economy is built on itself and is dependent on so many seemingly minor technologies, neglected parts are essential in some way and will become bottlenecks that cause the entire system to begin to come to a screeching halt. As often happens, food and energy are neglected first causing starvation and even the deaths of millions of people.

This is what I call infoolation and it causes price anomalies. The word "Anomaly" is a common term used in relational databases to describe when data is inserted incorrectly into a database. So instead of saying that the Federal Reserve/Government is causing inflation, it is better to say that the Federal Reserve is causing infoolation that is "inserting anomalies" into our economy. It is the corruption of our monetary system. But isn't our economy improving? Inserting anomalies may not destroy the economy but will slow its growth.

So called "Modern Monetary Theory"

How about adopting the so-called "Modern Monetary Theory" (MMT) that is being championed these days? Under this theory, the government can simply print up as much money as it needs as long as there are enough real resources such as workers, materials, supplies etc. Why bother with all the expense and trouble of taxing people if the government can just tax by inflation?

Under MMT, should we experience infoolation, we can just raise

taxes to reduce the amount of money in the system. This is the exact policy that the Biden Administration has embraced. This policy has led to massive increases in government spending such as the "American Rescue Plan" ($1.9 trillion), and the "Infrastructure Investment and Jobs Act" ($1.2 Trillion). But as predicted, America now has the greatest infoolation ever. To stop the infoolation, the Biden Administration has passed the "Inflation Reduction Act " which raises taxes and hires 87,000 IRS agents to enforce raising more taxes. This policy fits within the MMT theory.

However, MMT does not recognize that money is an information system and that people need it to make decisions based on this system. Both monetary inflation and taxes distort information and cause people to make bad decisions. Important decisions like where to work, where to invest and what to purchase are made incorrectly. The result is entropy: Our civilization falls apart. But it gets worse. These bad decisions then create a bad decision loop that causes the economy to spiral into ruin.

Note that the people who are part of the Modern Monetary Theory movement claim that Biden did not implement their plan. This may

or may not be true. They remind me of how socialists always say that the hundreds of attempts to implement socialism were not real socialism. It seems Biden's policy is close enough to MMT to get an idea of how it works. Furthermore, I am certain that whatever MMT scheme is implemented under this theory we will see the same failures because good luck changing the behavior of politicians.

MMT believes that the Federal Government cannot go bankrupt because it can print up all the money it likes. It's not correct. If the government prints up too much money, it will drive the value of the dollar to zero. That's bankrupt!

From the American Heritage® Dictionary:

bankrupt /bǎngk'rǔpt", -rəpt/, adjective
  1. Having been legally declared insolvent.
  2. Financially ruined; impoverished.
  3. Depleted of valuable qualities or characteristics.
        a. "a morally and ethically bankrupt politician."
  4. Totally depleted; destitute.
        a. "was bankrupt of new ideas."
  5. Being in a ruined state.
        a. "a bankrupt foreign policy."

Printing up new money causes people to become confused about how they should behave economically. According to FRED (Federal Reserve Economic Data), the real median household income in the United States has been steadily dropping during the Biden Administration.

On the other hand, the real median household income during the Trump years rose abruptly. In fact, it rose at the fastest rate in 40 years. The approach taken by the Trump Administration can be called "Classical." The Classical approach is to lower taxes, reduce regulations, increase economic freedom. This was mixed with better international trade deals and getting foreign governments to

contribute more to their defense. Under Trump, wealth equality went up, carbon footprint went down and the economy became generally more efficient and productive.

By lowering the taxes and reducing the introduction of fake data into the system (printing new money), people received better information and were able to make decisions that were more productive and efficient. MMT's infoolation and taxation fools everyone into thinking that they are making poor decisions and convinces them to make real bad decisions resulting in confusion and ruin. Reducing taxes is the best thing that can be done to give people an accurate understanding of the smartest actions they should take.

The goals of a monetary system should be to provide actionable information in a timely manner to facilitate efficient and productive behavior among all people. One of the biggest moral problems with MMT is that it allows taxation without representation, a rule that has been sacred to Americans for hundreds of years.

No Inflation without Representation
A long-held belief appearing about a decade before the American war of Independence, is that people should not be taxed unless they have some say in it. This idea was formalized in the United States Constitution. According to Article I, Section 7 (also known as the Origination Clause), "All bills for raising Revenue shall originate in the House of Representatives." This means that any legislation pertaining to taxation or public expenditure must be introduced and initially passed in the House before it can proceed to the Senate. This significant power permits the House of Representatives to influence fiscal policy and national budget priorities at their initial legislative stage.

However, the US Constitution has been undermined by the Federal Reserve System that allows for taxation through inflation. Not only can the Federal Government tax American citizens through monetary inflation, but it can also tax any dollar-holding person in the world. This is possible only because of the people's general

ignorance about the true nature of monetary inflation. However, some people aren't so stupid and are taking steps to reduce their inflationary tax burden. This is why there has been a massive push by countries all over the world to move away from using the dollar for trade. Especially in the trade of oil.

Asymmetric Inflation

The problem is "Asymmetric Inflation." This is a term I've coined to explain that the effects of printing new money affect the wage earners more than the asset holders. The wage earners grow poorer as their incomes can purchase less. The asset holders become richer because their assets can be sold for more.

Symmetric Inflation

Symmetric inflation affects everyone the same. To achieve symmetric Inflation, the FRB would need to have a way of increasing everyone's money proportionally. For example, the Federal Reserve could announce that the banks would be doubling everyone's money. Everyone who had a dollar would now have 2 dollars. This inflation would affect everyone the same. CloudCoin can do this and we call it a split.

The problem is that the Federal Reserve System has no technology to create "Symmetric Inflation" and it may not have the desire to do so. They could have everyone turn in old dollars and get two new ones in return. However, this would not enrich the rich at the expense of the poor and that may be their goal.

With the current situation, we could have a housing company that wants to borrow billions to buy houses so they can rent them out for a profit. New dollars would be created and that money would go to the bank who would loan it to the house-purchasing company who would then pay that to the home seller. The banks receive a huge benefit by getting this new money and having a reliable stream of income from the loans. The housing company becomes wealthy with new homes created basically from pieces of paper although backed by houses. And the home owners would make more money because the sales price of their homes would likely be more than

before. The renters however, are screwed. Asset holders become wealthy; wage earners become poorer.

What can be done?
Adopt a monetary system that has a fixed amount of money or uses "symmetric inflation." Or at least reduce the amount of money that can be printed in a given time period.

How the Yapes Were Fooled By In-fool-ation
In the 1800s, an Irish-American captain sailed his ship to an island in the middle of the Pacific Ocean in search of riches.

What he found on the island of Yap was a form of money made of carved stones that were as tall as a person. The stones came from a faraway atoll that had a unique type of stone. The islanders had no metal tools, so once they had traveled months to the atoll and carved them into coins, they had spent massive amounts of the time and resources to make them.

Captain O'Keefe had an idea. With his fast ship he sailed to that far away atoll and used his iron tools to quickly carve the stones to mimic those of Yap. He took the stones back to Yap and asked if he could purchase one of the smaller islands. The islanders happily agree to the trade.

Soon the captain was back with more stones to buy food, servants and the construction of houses for him and the other sailors. The islanders saw this as a boon, so they quit farming and dedicated their time to building the sailor's homes and furniture. The islanders thought they could always buy food later with the new stones they would earn.

STONE MONEY OF UAP, WESTERN CAROLINE ISLANDS.
(From the paper by Dr. W. H. Furness, 3rd, in Transactions, Department of Archæology, University of Pennsylvania, Vol. I., No. 1, p. 51, Fig. 3, 1904.)

But things didn't work out well. With no farmers, the food ran out. The villagers were dismayed at how the price of food skyrocketed. The children were hungry. The women complained to their husbands.
They all suspected that the sailors had something to do with it and they all complained to the chief.

After much thought, the chief called everyone together and said "The sailors have corrupted our money and fooled us into thinking that they deserve all that we have given them. Tonight, we will take back what they stole and then we shall eat them for dinner."

The Smithville City Council: Fooled by In-fool-ation
The city of Smithville received a Federal Grant to build low-income housing. Free money! Yea! That is going to pay contractors who

will then be able to buy things and the economy of Smithville will prosper because of this grant. However, many constituents complained that the low-income housing would bring criminal elements into the city and require more expenditures in public safety.

In the end the Federal Grant was accepted. The Federal Government then printed up the money and gave it to Smithville. The money changed the behavior of many people in the community. Contractors who were going to build houses stopped building the low-income housing. Workers who worked in the surrounding mines, farms and industries quit to become construction workers. This caused less stuff to be mined and less products to be manufactured. Some of these contractors became rich and this caused them to act inefficiently, buying goods and services that normally they could not afford.

Then the tenants started moving in. It turns out that the tenants were all on welfare. The Federal Government printed up money and gave it to the tenants every month so that they could buy things. Suddenly, the prices of everything went up. Food prices increased, energy prices increased, transportation prices increased. The cost of running the schools increased due to more students and many more with special needs. Government costs grew including the dreaded cost of public safety that the people warned the City Council about.

There was more money in the system, but less stuff was being made. Just because more money was printed, did not mean that more goods and services were available to be consumed. In fact, moneyed people stopped making goods and services that were beneficial to them because they were pursuing the new money that had been printed.

The new money helped the so-called "low income" people but hurt everyone else. Many of these low-income people were poor because they were criminals, lazy, drug users, had untreated mental illnesses or worse, they weren't really poor at all and had secret jobs.

And, nearly all these people were from outside of Smithville and moved to Smithville to live in the housing.

Soon people began complaining to the mayor. After much thought, the mayor called everyone together and said "The Federal Government has corrupted our money and fooled us into thinking that they deserve all that we have given them. Tonight, we will take back what they stole and then we shall eat them for dinner."

Monetary Inflation or Price Inflation?
Economists argue about the nature of inflation. There is price inflation and monetary inflation. But which one is the true inflation? Does inflation only happen when more money is created or does inflation only exist if prices go up? I don't think it matters much. We need to look at monetary inflation in terms of an logic bombs thrown into an information system.

16. THE TERRIBLE SECRETS OF THE FEDERAL RESERVE

An allegory of the Federal Reserve

Long ago, ancient tribes near the sea gathered unique blue shells. Both local and far-off tribes loved these shells, using them for accessories, clothes, hair decoration, and crafts like basket-weaving. Since each shell took about an hour to find, they became a currency based on this time value.

The shells being used as money boosted the economy. They let the islanders divide tasks based on their skills, making everyone's work quicker and better.

They occasionally used other shells as currency. The common Red Cowrie, taking 15 minutes to find, was worth a quarter of a Blue Cowrie. The rare Purple Cowrie, which could take days to find, was worth 100 Blue Cowries.

In every tribe, some people came up with new inventions. One person thought of the fishing net. He was sure his idea would work, but knew making it would take much time and hard work.

He shared his idea with a friend, saying it would take a while

because he would have to collect fibers, make them into string, and then form a net. This process would take days, and back then, people needed to use that time to find food to survive.

The inventor's friend thought hard about how to get this task done. While doing so, he ended up creating the concept of a bank. He borrowed shells from his neighbors for the task, promising to return more shells in the future.

Thanks to this early form of a bank, they were able to make a working fishing net. This net made fishing way easier, so more fish came in. Because of this, fish became cheaper, since it was easier to catch them. And people could get more fish with their shells, so their worth went up.

With fish being cheaper, people had spare shells to spend on other items. This enabled other tribe members to come up with new ways to earn these shells, which resulted in more jobs and roles in their economy. Some of the shells people used to spend on fish were now going to those who had invested their shells in creating new things.

Before long, professional investors appeared who were motivated to make investments. They aimed to earn many shells to buy many things. As a result, innovative ideas around the islands received funding from the investors, who only needed to use their intellect to operate.

Despite efforts to prevent it, theft happened. People kept trying to steal others' shells. To protect these shells, new Banks built secure vaults. However, everything shifted when a war-like tribe leader named Brutus wanted to attack other tribes and take their possessions.

War costs a lot. Brutus required soldiers, weapons, and supplies. He needed other tribe members to contribute to his army. The person making fishing spears would need to make combat spears, and the one building fishing boats needed to construct war boats.

Additionally, Brutus needed fighters, whom he could only recruit by offering them many shells in return.

Brutus knew that attacking his neighbors would cost a lot but believed it would also bring profit. So, he asked tribe members for their blue shells. However, they disagreed, recalling their losses from Brutus's past failed attack. Brutus still tried to force them to give him shells for the tribe's sake, but people resisted. Afraid of being attacked himself, Brutus stopped demanding shells.

Brutus decided to set up a reserve bank to always have shells for his military efforts. This bank would let him borrow shells anytime he needed them. But setting up this bank required work and the agreement of other banks.

First, Brutus made paper money, termed as paper shells, with shell images on them. Next, he banned private shell ownership and trade. People had to replace their shells with paper shells. All these shells were stored in a safe place called Fort Shell Nox. Finally, all banks joined a government-supported group called the Federal Shell Reserve.

In return for joining, banks could borrow any amount of money whenever they needed. When banks or Brutus needed a loan, they would print more paper shells, although this would affect everyone else. They were careful to avoid printing too many paper shells too swiftly as they knew it could harm the economy and upset people enough to challenge Brutus and the banks. To suppress insurrections, Brutus first printed money to pay off people who could make sure he stayed in power.

The bow and arrow were invented first. They allowed hunters to hunt more animals in the same time than the spear.

Without the Federal Reserve, top hunters would get new technology first and it would spread gradually. But with the Federal Reserve system and the invention of the bow and arrow, every tribe hunter wanted a loan for this new tool on the same day. Banks

printed more money and gave everyone a loan. This led all hunters to the bow maker at the same time, but he had limited bows. The high demand and low supply forced him to increase his prices significantly, making the bows less cost-efficient for the hunters.

The bow-maker hired many workers to make lots of bows and earned a lot of money. After all hunters got a bow, the demand for bows dropped, leading to many bow makers losing their jobs. At the same time, since so much meat was hunted, its price dropped, which was good for everyone except for the hunters. Soon, many hunters could not repay their bow loans because the bows' value was less than their purchase price.

The Federal Reserve resulted in:
* Bigger market swings and significant price changes.
* Prices of things bought with new loans increased rapidly.
* People made bad decisions causing them to become less efficient and less productive
* As the new money flowed through the system, prices of everything, except the new technology, gradually increased.
* Now there was money available for the government to fund wars that were previously too expensive.
* Now there was money available for the government to transfer to political cronies to stay in power.

The Politicization and Centralization of the Federal Reserve Banking System
The Federal Reserve System is supposed to be separate from the Federal government and be a non-political organization. However, recent developments show that today's Federal Reserve is controlled by Washington DC and has been weaponized politically.[4] It has also been infected with the Anti-White Supervirsus and now will use all of its power to spread the virus instead of achieving its congressional mandates. It is now a threat to the entire global economy, the freedom of people and corporations, and to our very survival.

The Federal Reserve creates a system that allows banks to do what

they could not do before (print money) and allows the governments to do what they could not do before (always have someone to borrow from). But the Federal Reserve System is flawed in such a way that the rich become richer and the poor become poorer. The main problem is that the US Government can order the Federal Reserve to print money for itself.

This causes much trouble in society as the poor understand that something is not fair and the rich simply want to be free and execute their rights as all people should. The poor feel they have been ripped off and "want their money back" so to say. The rich, who are generally savvier understand the work that they have done to become wealthy and for the most part, they think they deserve it. The result of this is that socialists gain ammunition against capitalism when in truth, it is not capitalism that is causing the problems, it is a flawed monetary system.

A lawsuit against the Federal Reserve by Custodia Bank has produced some documents through disclosure that show that the Federal Reserve is secretly doing some really terrible things. Federal Bank Regulators have been pressuring Banks to debank digital asset companies as part of Biden's "all of federal government" attempt to kill the digital asset industry (other than the ETFs run by

Blackrock). Only 3% of banks serve the digital asset community and those 3% have received over 50% of the FDIC's enforcement actions. People who are involved in the cryptocurrency business, and even those politicians that have voted to support cryptocurrencies, have been debanked.

The FRB is acting outside its Authority by granting itself a veto over State Bank chartering decisions for the first time in US history. They allow complete frauds, like the FTX exchange, to operate without investigation, seemly because of the huge donations FTX made to the approved political campaigns.

The Federal Reserve is being used by the President of the United States to "debank" companies and entire industries. The Fed uses the threat of taking away a bank's master account to coerce banks to shut down the accounts of people and companies that they don't like. It is no longer ruled by law but by politicians and their agendas.

"A politicized Fed is a risk to existing banks everywhere, not just to new applicants like speedy banks…No one is immune from a politicized Fed that believes it can close any bank's master account for any reason without judicial review and which ignores congressional oversight over master account and whose own Inspector General won't investigate." ~ Caitlin Long, CEO Custodia Bank

The Fed has a term "Novel Charters" which is a code word for "Shit Bank". Banks that have Novel Charters do not have the same rights as other banks. The law firm Davis Polk warned in its analysis of the District Court Opinion of Custoida's case:

Tomorrow the term novel charters might be expanded to include banks providing traditional banking services to other politically controversial groups such as gun advocacy groups, gun manufacturers, payday lenders, pro-choice or pro-life advocacy groups, LGBTQ plus groups, religious freedom or freedom from religious groups, or even fossil fuel companies.

Today, the Federal Reserve Bank is becoming centralized and

controlled by Washington DC. The Fed is engaging in power struggles with other agencies such as the SEC to see who can control the most of the economy.

The FRB is Anti-White, it Will Go Broke

I was invited to a screening interview for the position of Director of Software Engineer CBDC at the Boston District of the Federal Reserve Bank. This the supreme technical position for a possible Digital Dollar in the United States. Unfortunately, the interviewer brought up the subject of "DEI" which is the code word for "We are infected with the Supervirus" and we antagonize whites, especially white males.

The term "Supervirus" was coined by Simone & Malcolm Collins in their book "The Pragmatist's Guide to Crafting Religion" and describes how the global movement of self-described Wokists is actually an infectious memetic parasitoid. A parasitoid is a type of parasite that lives at its host's expense, eventually resulting in the death of the host. The parasitoid hijacks a person's standard of evidence so that they see feelings as truths. Then the parasitoid hijacks their value system so that traditional values such as family and earning money are replaced with the goal of spreading the virus. Their sense of morality is replaced by the "ends justify the means" way of thinking and they will break every law, such as discriminate against white people, lie, cheat, steal elections. They will no longer seek for the truth.

This parasitoid causes them to not have children and destroy the companies and organizations that they are part of. Just like the HIV Virus, which hides in the cells that are supposed to stop it (T-cells). The Supervirus hides in institutions like universities, churches and government agencies. The Supervirus also acts like harmful bacteria that masquerade as red blood cells to evade the immune system by wearing the skins of dead blood cell. Companies like Disney, are actually completely infected with the Supervirus and no longer care anything about making money. Instead, they will do everything they can to spread the meme, even spending all their billions of dollars on projects with no customers until they are completely bankrupt

and can spend no more.

Back to the Federal Reserve Bank. I looked at a video statement on YouTube from the President of the Boston district entitled "What does the Boston Fed Do" the answer is that it spreads the anti-white virus. The video was only 3 minutes long. Nearly every sentence in the video mentioned diversity, equity or inclusion. Then she ended by saying the overall mission of the Boston Reserve was to "create an economy and financial system that works for all." This is not the Fed. This is a Supervirus wearing the Fed's dead body and pretending to be a bank while in reality just a meme spreader.

While the Fed may certainly be infected with a Supervirus. I call them anti-white racists and I think you should too. When they take over an organization, they fire everyone who is not an anti-white racist and they will only hire those people who are anti-white racists. They are unable to see that discriminating against people on the basis of race is illegal and immoral. When given the option of hiring the best person for the job or an "affirmative action hire". They will always choose the affirmative action hire. Because of this, you cannot tell who in their organization is competent, and who is just there for looks. This means, for all practicality, that the president of the Boston Fed, Susan M. Collins, and everyone else there have

been hired because of the color of their skin and have no economic right to hold their positions.

Because the Federal Reserve is anti-white, it will not make loans based on sound economic principles but instead will discriminate against people they consider "privileged" like white Jews, whites in general and Asians, causing great harm to them. And it will loan money to people based on race alone causing catastrophic bad investments.

They will not be concerned about American Culture, American religion, American traditions, American law or the American economy. They will not care about national employment, national inflation or anything besides discriminating against the "privileged" and spreading their virus. Go woke, go broke. But this time, it is our entire national banking system and the United States of America with it. We cannot allow the Federal Reserve to be weaponized against American Citizens and stay in business.

Perfect money is not political and is certainly not anti-white racist.

17. ARTIFICIAL INTELLIGENCE AND MONEY

"With machine learning on digital computers, nobody knows why it works. The only reason they know it works really well is because they've done experiments on digital computers. And it works." - Peter Shor

The Rise of Androids
The Tesla company is preparing to build millions of Optimus androids every quarter. By 2050 there could be three androids for every human on the planet. It is believed that those robots will be capable of doing 90% of the jobs that currently exist. Meaning, that for 90% of us, our jobs will be done by a robot and we will need some other way to get money. These robots will probably cost less than $25,000 each. They will be able to work all day and all night perhaps on a single charge. Let's look at how jobs maybe done:

Medical
You're sick so you call the doctor. Within a few minutes, an autonomously driven van arrives and an android gets out and knocks on your door. You tell your house android to let the doctor droid in. The doctor droid is equipped with all these medical

sensors. There is a full lab in the van as well as a pharmacy and after a little computing, the doctor droid is able to access hundreds of thousands of cases to determine what ails you and how to treat it. But how do you pay for this? Do you send the company who runs the droid's money or is this part of a government medical program? Is it all for free so no money is necessary? Unfortunately, you have the flu. If it is a company, you called then you will be advised to stay home so as to not infect others. If it is the government, you may be ordered to stay in your home under threat of punishment. People will certainly prefer private companies that they can choose from over true government communism.

Legal

There is a prisoner who is being considered for release. The judge must decide if the criminal has reformed and if he is likely to reoffend. The criminal will tell the judge how he has changed, and learned his lesson and will never do it again. However, studies show that AI can make better decisions than judges. And so, the judge is replaced with an android judge. Now the android judge will make a decision based on cold calculations and not on the criminal's emotional demonstrations. The android judge reduces the money the government must spend and reduces the need for taxes in this area.

Farming

Farming is done almost completely by androids. Androids do an incredible amount of work day and night. They even have androids with little vacuum cleaners that spend all day and night looking for insects on the plants to suck up. This has resulted in almost all food being organic. Gone are all the farm workers. There is a central computer that creates the overall farm-plan and the tractor-bots are deployed at the correct given moment. Is the land owned by the farmer? Or is this a collective thing where all the food is given out to everyone for free. Based on the dislike of communism, the owners will retain the land.

Jobs Left for Us Humans

Even though we may have robots that can do 90% of the work we do today, there will still be scarcity and we still can all move to doing the jobs that robots can't. We may all become athletes in sporting competitions, pole dancers, or comedians. Sure, robots could do this work but who wants to watch robots compete, dance, and tell jokes? How about bartenders, nurses and DJs? There are probably a lot of jobs that customers would be creeped out with if it was done by androids. It also could be that you will still have your job except you will be helped by your androids. This will allow you to charge less and get a lot more done. The owner of the pool-cleaning company may replace all of his workers with androids but he still will have a job. Maybe in the future, we will all have robots. When companies hire us, they will hire us knowing that we will be working with our robots. But clearly there will be a huge number of people thrown out of work creating social instability.

Communism and Universal Basic Income

The communists who took over Russia in 1917 tried to get rid of money but it didn't work. In fact, it was a catastrophe. They had to take every bit of silver, gold, and platinum they could find in the nation and turn it into coins to stave off a complete collapse. It is unlikely that people will want to turn to communism where they

are subjected to authoritarian ways. However, the UBI (Universal Basic Income) movement may become much more popular and soft socialism could be demanded by people put out of work. But there may be a much better way than UBI if people are so inclined to make demands for socialism.

One Person One Robot
We are forbidden by law to marry more than one person (at least in most modern civilizations). Why? To maintain social stability. At least that is what I've been told. If one man was able to marry thousands of women, it would cause social unrest as many men would be deprived of love, caring and respect causing them to want to kill themselves or others.

Perhaps a one-person, one-robot law would provide stability too. There could easily be a law that says all people are only allowed to own one or two robots. This would double or triple the productivity without causing mass displacement. If anyone wanted to have more than one or two robot workers, they would have to hire a person who owns them. If farmers need farm hands, they can hire a farm worker and his two androids. There could be some exceptions to this rule and perhaps companies would be required to have a certain percentage of their workforce to be human or that

the law only applies to certain types of robots. This policy would probably beat socialism at staving off social unrest and actually creating productivity and efficiency.

Beer Barons

AI technology may cause the greatest surge in productivity in the history of mankind (or at least since the invention of beer back in ancient Egypt). Every time there is a new technology, it usually results in the inventor of that technology becoming extremely rich. We can see this throughout American history

* Oil: Rockefeller
* Steel: Carnegie
* Railroads: Vanderbilt
* Automobile: Henry Ford
* Operating System: Gates
* Social Media: Zuckerberg

But what if an invention is so fundamentally economy changing that almost all money goes to that one person who invented it? This was likely the case when beer was invented thousands of years ago. Everyone needed to eat and have their grain crops last through the year. Beer solved their problems. But perhaps there was only one man who knew how to brew beer or who had the capital to create the equipment needed to brew beer economically.

If only one man has the tech, then everyone else must work for that man. And what are their jobs? Building pyramids for the inventor of beer! Paid one gallon of beer per day. The inventor of beer would be so rich that he could hire an army to overthrow whatever other government there was at that time and build the largest building to be constructed for thousands of years.

The Pharaohs of the Future

It seems very clear that AI technology will concentrate money into the hands of a few. More so than we have seen before. A few people will become extremely rich. But what use is it to have money if you have no people to spend it on? The money must come back to the

people otherwise we will have a "gift card" situation where the owner forgets to spend it.

Let's call these inventors the Pharaohs of the Future. Most other people will have their lives disrupted to the point that they are out of work. Who will everyone get a job from? Most of them would have to get their jobs from either the Pharaohs or vendors who cater to the Pharaohs. So, what would the Pharaohs want to buy? It could be something like colonies on Mars. Imagine that you were hired to be a Mars colonist. You could eat on Mars or starve on Earth. If the Pharaohs care about the environment, maybe all the work would center around environmental issues. However, if the Pharaohs desire is to kill off millions of us, then the millions of robots created could suddenly become weaponized and take over the government just like in science fiction movies.


Do Robots Need Money?
If robots are put in charge of buying and selling for people, then they certainly will need to use money. I am pretty sure that any truly intelligent AI will choose CloudCoin. We shall see.

Will We Need Money in the Future?
In Star Trek, they have achieved a "post-scarcity" civilization and there is no money. If you're hungry, just tell the replicator and

bingo, dinner is served. The same thing can be found in our homes when we were kids. We show up at the dinner table at 6:00 PM and bingo, dinner is served. Either way, it requires an authority to make it work and if that authority decides you don't need to eat, you're going to starve to death unless the authority decides to feed you again.
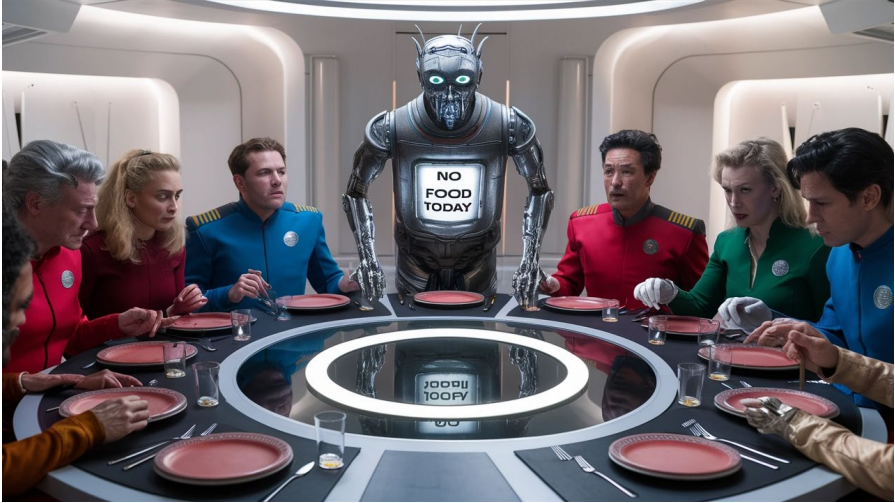
I can imagine a world where food is so inexpensive that it is free. But I doubt that all food will be so cheap that billions of Africans can eat caviar and champagne. And, even if it is possible for us to all eat for free, we are still going to want to purchase palaces, yachts, helicopters, and vacations to the moon. There is no limit to our wants and scarcity will always exist.

Who knows, maybe in the future, everyone will own an acre of land that is farmed by a single robot that is able to produce enough food to feed a family of four and build your house at the same time using naturally-occurring materials.

Money (and specifically cash) will always be needed to help us get what we want and avoid the tyranny of others. I have created CloudCoin and it is the only true digital cash we have at this point and is perfect enough to serve us for the next thousand years. I am very proud of how wonderfully this RAIDA-based currency works

and I believe that the money of the future is CloudCoin.

Guardian Angels

I can also imagine a world in which each of us has an AI "Guardian Angel." These are computers or robots that each day scan the employment ads looking for a better job for us. They figure out what things we should be learning to become more employable. They will be shopping for deals on the things we typically buy. They will be planning our vacations and monitoring our neighborhood police reports for any kind of threats. However, everything will be measured in terms of money. Money will help our Guardian Angels help us.
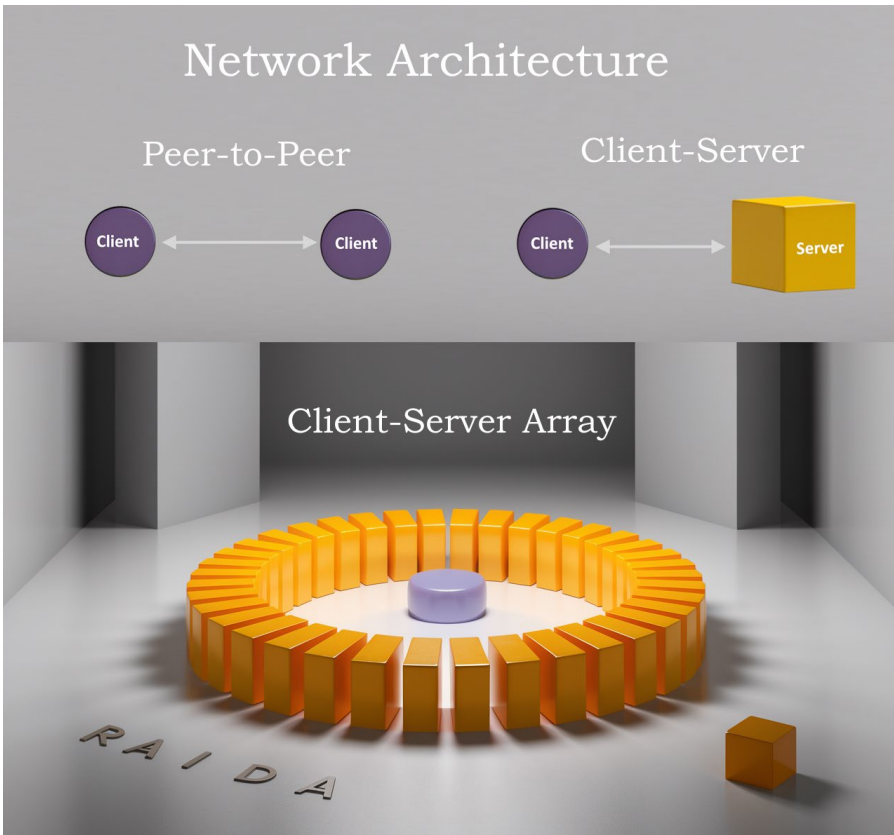
18. CLOUDCOIN: AN EXPERIMENT IN PERFECTION

I coined the term "data supremacy" in order to describe databases that cannot be brought down by the HATERS (hackers, AI, governments, tech giants, quantum computers, system admins, and even the people who created the database). I know of only three database technologies that have achieved data supremacy: The Blockchain, DNS Root servers (which I call the Redundant Array of Independent DNS Agents) and my invention, RAIDA (Redundant Array of Independent Detection Agents).

The DNS Root servers have never gone down globally since the

day in 1985 when the servers were setup. Neither has the Bitcoin Blockchain (2009) or the CloudCoin RAIDA (2016).

The DNS system processes two trillion queries each day, is free to use, extremely quick to respond and easy to include in software.

CloudCoin's RAIDA is based on the DNS Root Servers but is faster, uses less electricity, can handle more transactions, is more secure (and quantum safe) and is easy to develop with.

We call CloudCoin the last digital currency" because it is the last currency that we will ever need. It has obtained near perfection based on the criteria described in this book. CloudCoin can trade 24/7 in any part of the world with no fees. A coin that uses nearly zero electricity and bandwidth. A coin that is 100% private because it requires no usernames, logins, passwords, or public ledgers.

A coin whose loss and theft can be mitigated. A coin with a fixed amount so that there is never any inflation. A coin that is file-based and separates data from logic so that it can be hidden in jpeg files or imported into software and video games. A coin that is patented by the USPTO so that it will not have thousands of copy-coins at least for the next 20 years. CloudCoin has a SkyWallet that allows people to send coins using easy to remember DNS names. A digital currency that is quantum safe and will survive the extinction of cryptocurrencies that could occur in just a few years.

Note that Cryptocurrencies built on Blockchains come with a host of challenges, making it difficult to do simple things like buy a cup of coffee. Transactions take too long, fees are too high, and it is still too difficult to scale. We developed CloudCoin to overcome these challenges and pave the way for mass adoption.

CloudCoin may be the first patented currency. On May 12, 2020, The United States Patent and Trademark Office granted CloudCoin a rare patent for "Method of Authenticating and Exchanging Virtual Currencies" (Patent No 10650375). I don't know of anyone else who has been granted a patent for a unique

virtual currency!

Just as the DNS system allows billions of people to find their web pages, CloudCoin enables millions of users globally to buy, sell, and exchange with superior privacy and zero fees. Each CloudCoin is a file that contains a serial number and 438 bytes of secret authenticity numbers. Using RAIDA, CloudCoin shreds those secret numbers into 25 streams of data and ships them to RAIDA Clouds located around the world in different jurisdictions. The security of CloudCoins is due to shredding, not encryption; and there is also a fixed amount of CloudCoins, so there is no inflation. CloudCoins also feature quantum security and require no consensus mechanism.

Since the complete CloudCoin data is stored directly in the CloudCoin files themselves, they remain secure in the event RAIDA Clouds are taken down. The "Triple Kerberos" fix-protocol allows CloudCoin owners to call on trusted RAIDA Clouds to convince new RAIDA Clouds of a coin's authenticity. Each RAIDA Cloud is administered by an independent agent so there is no centralized control and no recorded transactions, ensuring a fully anonymous, private system. As the value of CloudCoins increases, more RAIDA Clouds can be added to handle the demand.

Over 150 million CloudCoins were traded in the month of June, 2022 alone, demonstrating volume and realized value from the crypto community, With Blockchain, the amount of transactions would have cost millions in electricity and server power; however, CloudCoin offers a fast, secure and energy- efficient alternative eliminating massive server rooms and costly energy consumption.

The Root DNS and Blockchain were not built for storing data. We built CloudCoin using the RAIDA architecture and it can store very large amounts of data. You can get the "CloudCoin Learning Kit" for $11 https://cloudcoin.com to see how it works. Send them by SMS and hide them in png files. It's pretty cool.
 of PNG files. Fun!

Jeff Berwick, George Gilder, Sean Worthington, Ed Moy, Naomi Brockwell, Freedom Fest 2019 talking about going beyond Bitcoin

19. PERFECT MONEY PLATFORM

Core Principles:

1. The voluntary use of money is a natural right.

2. That monetary systems should not be controlled by governments or banks but by system administrators who are not political.

3. We have a natural right to exchange currency. Governments infringe on our natural rights by regulating and surveilling currency exchanges. The right to exchange currency shall not infringed.

4. Monetary systems should be decentralized and have data supremacy even over all nations.

5. We understand that in general, monetary inflation causes economic inequality because it drives up the value of assets and reduces the value of wages. Therefore, we oppose asymmetric monetary inflation.

6. We acknowledge that certain government expenditures can give us false information that is likely to cause us to adopt unproductive and inefficient behaviors.

7. We understand that asymmetric monetary inflation causes hurtful boom-bust cycles by tricking people into thinking they should involve themselves in endeavors that seem productive but are actually wasteful.

We hold the following to be true:

1. That the natural state of civilization, the economy and life in general is to decay, fall apart, become random, and entropy as noted in the Second Law of Thermodynamics.

2. The fourth law of Thermodynamics could easily be that life requires "directed work" initiated by a conscious life form who interpret information collected through their senses and freely executes actions based on its knowledge by using its natural faculties known as "Natural Rights."

3. The Natural Rights of Mankind include the ability to communicate and use communication technology (language, writing, press, Internet); the ability to collaborate (associate, marry, form corporations and/or partnerships); the ability to use tools (guns, press, shovels, computers); and to believe, learn, and teach.

4. That monetary systems are information systems that provide numeric information in the form of prices and payments (salaries) that indicate the most efficient way to consume and the most productive way to produce.

5. That each individual person will have unique values: For example, some may value vacations, others entertainment, and some raising children. That people may create or adopt unique "ideologies" as strategies to obtain what they value.

6. That good monetary systems allow individuals to obtain what they value by following their ideology while civilizations that command people's actions through threat of force, do not.

7. Monetary systems will not create financial equality because equality is not possible when people are diverse, as varying results will occur due to these individual differences.

8. Monetary systems should be blind to who's using them and users should not have to log in, be authenticated, identifiers or have to produce self-identifying information.

9. That monetary systems should follow the generally accepted ideas of what all information systems should do such as provide actionable information in a timely manner and be secure so that it is confidential, available, and possesses integrity.

10. That the main part of integrity is to keep people consuming efficiently and producing productively and that this can be reduced by poor monetary-system design, counterfeiters, and government policies that warp or cloud the true state of the economy.

11. That the economy does not run like "clockwork" where equations with known values return predicted results. Instead, the economy is chaotic. Small variations can have large effects that cause friction, feedback loops, dead locks, unexpected results and unintended consequences.

12. That government monetary policy and public policy can destroy, block, and hide information that will make the economy productive, efficient, and just.

13. That empirical evidence is the proof of truth and that nothing can be true simply by thinking it true.

14. That in general, price controls and price subsidies block information that tell people to consume less and produce more. This results in consumers consuming inefficiently by over-consumption leading to shortages and for producers to become unproductive by under-producing also leading to shortages and economic decay.

15. That in general, forcing the price of something to go up by taxing, regulating and restricting causes inefficiency because people are required to substitute inefficient actions with efficient ones and this inefficiency will lead to feedback that reduces future improvements in efficiency causing the economy to decay.

16. That governments should not create monetary systems as monetary systems created by governments and banks are likely to be subverted so that governments can do things that their people would not normally allow them to do and the same with banks.

17. That there is technology to create "perfect" monetary systems and that this system is theoretical in nature and should not be forced upon people but should be adopted voluntarily.

18. That the use of money is a natural right and that we should not be forced or prohibited to use monetary systems or their exchanges.

20. THIS AUTHOR'S JOURNEY

I have a master's degree in Computer Information Systems and have finished all my courses for a PhD in Computer Information Systems, but I have not finished my dissertation. After teaching computer science for 22 years, I retired in 2023.

The best thing about being a college instructor is that you get summers off. On the first day of summer in 2016, I lay in the bath for hours thinking about the nature of money. Bitcoin was becoming a big thing. Contemporary philosopher Stefan Molyneux said Bitcoin was money. Nobel Prize-winning economist Paul Krugman indicated that Bitcoin was not money. People like Congressman Ron Paul said that only gold and silver were money. The chairman of the Federal Reserve Ben Bernanke said in a congressional hearing that gold was not money. Why was there so much disagreement?

In college, I was interested in economics and took close to 30 units. I was never satisfied with the definition of money, so I decided to

give it some hard thought that day. The year before, I had studied philosophy with my daughter as part of her home schooling. We read together from a philosophy 101 textbook. I knew nothing of the subject. While thinking in the bathtub, I discovered that my studies in philosophy had changed the way I thought about things. I reflected on Plato's forms as I considered the "essence" of money. I concluded that a major part of money is that it cannot be counterfeited easily.

I then turned my attention to the money on the Island of Yap. I learned about this money in college. The Yapese used great round stone coins to show which family-owned money. If you wanted to pay someone, you would roll a stone coin from your family's platform to the platform of the seller. You would need a lot of help rolling it because these stones are heavy.

Suddenly it clicked in my mind: This was a database made out of stone. It was a public ledger like Bitcoin. The platforms were like cells in a table. The stone disks were used as data. The size of the stone symbolized its numeric value. This was an information system to track who had spending rights.

Could it be that other monetary systems like cash are databases too? What about the US Dollar? After a few more days of thinking, I realized that the US Dollar was a database, except the cells of the table were not grouped together on a ledger. The cells were in our pockets, wallets and banks, while the dollars were the data. More specifically, the numbers on the paper were the data. Soon I realized that in a blockchain public ledger system, the owner of the money is symbolized by numbers, also known as account numbers. With cash, the owner of the money is symbolized by a self-representing symbol, the people themselves. To make Blockchain work, everyone who wants to participate needs a symbol, in this case a "public key." And in a cash system, people do not need symbols because they themselves are the symbol and they can show ownership simply by physically possessing other symbols (money).

Now this was significant. As part of my study of philosophy, I

learned about "Normative Philosophy." Normative philosophy is when we make claims about how things should be, what is good and bad, and which actions are right and wrong. We in the field of information systems have been developing a normative philosophy about information systems for decades. For example, in the study of databases, we have "Database Normalization." Database normalization is a concept that was first published in a scholarly journal [1] in 1970. For the past 50 years, the subject has been the study of hundreds of scholarly papers with much argument and debate among computer scientists. The concept has stood the test of time and is likely to be around for another 50 years, if not more.

In the study of information security, we have the "Security Triad." This concept was first discussed in scholarly papers in 1977. Over time, scholars have come to accept the security triad as part of the "right" way of thinking about information systems and that we should take actions to implement the security triad.

The idea is that monetary systems are information systems and that money is data. The significance of this is that people like me, who have been studying information systems for decades and have come up with very good ideas about how information systems should be and contribute to the field of economics. Because monetary systems are information systems, we can use this knowledge to create a "normative philosophy" on how money should be. In other words, we can have a theory of perfect money.

Economists were never able to understand this before because economists always studied human behavior and not information systems. The greatest economists in the world don't know anything about database normalization. Like many technological advancements, combining disciplines can lead to new discoveries and the combination of economics and information systems has produced this book!

From here, I tried to determine what was special about Bitcoin. I concluded that it had no owner and could not be tampered with. I called this property data supremacy. I discovered that the

Blockchain was just one of 16 exotic data structures that no one else seemed to be aware of.

I looked around for other databases that also had data supremacy and could only find one: The Root DNS servers. The Domain Name System has never gone down since the day it was created in 1985. That is a track record better than Bitcoin. I coined a name for these root servers: A redundant array of independent domain agents or RAIDA for short.

The RAIDA uses the second of the 16 exotic data structures that I discovered earlier.

Using this data structure, I invented CloudCoin. The most perfect currency in the world (at least in my opinion). You can try it yourself by going to https://CloudCoin.com

I hope this book has been thought provoking and that it will add to your approach to monetary thinking. May it help make the world a better place!

Join the discussion on https://perfectmoneybook.com
Contact the Author at CloudCoin@Protonmail.com
Invest in RAIDA-based technologies: https://Raidatech.com
Try out CloudCoin: https://CloudCoin.com

We Read Perfect Money in One Weekend!

THE END