

# PARALLAX DIGITAL

## Money, Bitcoin and Time

By: Robert Breedlove, CEO

January 3, 2019

**Abstract (aka TL;DR)**

Money is vital lubricant of human exchange that allows it to flourish globally. Human exchange is the driving force of prosperity, which is expressed in terms of time saved. The hardness of money determines how reliable it is as store of value across time. Money is defined in many ways and by many traits, and competition is at all times alive between different monetary goods. Historically, people have always naturally and rationally chosen the hardest form of money available to them as hard money is resistant to value debasements and thus provides its holders peace of mind. Societies using hard money systems have always flourished, until either they are exposed to a harder form of money or the hardness of their monetary system is technologically compromised. After centuries of monetary competition, the world finally settled on a hard money gold standard in the 19<sup>th</sup> century. During this golden era, the world witnessed unprecedented levels of trade, innovation and peace as a bank-enabled gold standard provided people a self-sovereign, cash money that was beyond the control of any single government. The fatal flaw of this system was the physicality of gold, which led to its centralization within bank vaults. Driven by greed, banks began printing more bank notes than their gold reserves could justify, thus compromising the hardness of the gold standard. Drawn by the practically limitless power provided by the fiat money printing press, governments and newly created entities called central banks began taking over the banking sector. Soon, they began confiscating gold from citizens and forcing them to use valueless money called fiat currency. Virtually all fiat currencies throughout history have had their values completely destroyed by inflation. Further, inflation is the prime driver of all economic inequality in the world, as those privileged few who receive newly printed money the earliest benefit disproportionately. Central banks are the last bastion of socialism in the free world, as their express aim is to centrally plan and manipulate the market for money. Central bank actions are the primary cause of market distortions (aka bubbles), economic recessions and the boom-and-bust business cycle. In the past century dominated by central banking, the world has witnessed unprecedented levels of death in warfare, economic crisis and an ever-growing wealth disparity.

Bitcoin was released in 2009 as an open-source software project in the wake of the Great Recession. Bitcoin is digital cash money, meaning that it is a self-sovereign asset that is beyond the control of any single government, similar to gold. By virtue of being digital Bitcoin is resistant to centralization, can be transmitted at the speed of light and stored in computer or human memory. Similar to the internet, Bitcoin is decentralized which makes it immune to confiscation, counterfeit, inflation and censorship. The hardness of Bitcoin increases relentlessly and will eventually reach infinity, as its supply is absolutely scarce. Its hardness is secured by its immutable rules, which are protected by the energy expenditure necessary to maintain its network. The Bitcoin network is the most powerful, valuable and secure computing network in the history of the world. In the face of adversity it adapts, improves and grows. Bitcoin propagates its network by economically incentivizing everyone who interacts with it. Further, these network participants create multi-sided network effects which fortify Bitcoin's market dominant position and insulate it from competitive disruption. History shows us that every time hard money encounters a softer form of money, it ultimately outcompetes it into extinction. In the digital age, monetary networks are more connected than ever before. There is no way to protect yourself from someone else holding a form of money that is harder than yours – ignore Bitcoin at your own peril.

Time is the only true scarcity we deal with as human beings. Conceptually, money is frozen time that is tradeable for the time of others. Therefore, the finite supply of Bitcoin makes it perfect for freezing and transacting finite time. Diffusion of and trust in innovative technologies like Bitcoin grow over time and benefit early adopters the most. As a purely informational innovation, Bitcoin is protected under Freedom of Speech laws. Looking towards the future, game theory shows us that global Bitcoin adoption is virtually inevitable. As it begins demonetizing government fiat money economies, it is only a matter of time before central banks suffer competitive disruption from Bitcoin. Of course, the future is uncertain and the end could always be near, so only time will tell how this all plays out.



## Table of Contents

### **MONEY**

---

THE SIMPLE TRUTH ABOUT MONEY	5
HUMAN EXCHANGE	5
STORY OF MONEY	7
HARD MONEY	8
MONEY IS A SOCIAL NETWORK	9
MONETARY TRAITS	10
PROSPECTS OF PROSPERITY	10
FOUNDATION OF ECONOMIC GROWTH	13
THE ECONOMIC NERVOUS SYSTEM	14
MONETARY EVOLUTION	16
MONETARY METALS	18
GLOBAL GOLD STANDARD	20
HARDNESS OF GOLD	22
FINAL SETTLEMENT	23
CENTRALIZATION OF GOLD	24
ABOLISHING THE GOLD STANDARD	25
GOVERNMENTS TAKE CONTROL	26
FREE MARKET CAPITALISM VERSUS SOCIALISM	28
FAILURE OF GOVERNMENT FIAT MONEY	31

### **BITCOIN**

---

THE SIMPLE TRUTH ABOUT BITCOIN	33
GRASPING BITCOIN	33
DIGITAL CASH MONEY	33
TECHNOLOGICAL PROPERTIES	35
BLOCKCHAIN, ENERGY AND MINING	36
THE INTERNET OF VALUE	38
THE INFINITE HARDNESS OF BITCOIN	39
BITCOIN'S SOCIAL CONTRACT	43
A NEW FORM OF LIFE	46

THE DECENTRALIZED NETWORK ARCHETYPE	47
ANTIFRAGILITY	51
BITCOIN'S POSITIVE FEEDBACK LOOP	52
BITCOIN'S NETWORK EFFECTS	53
MINORITY RULE	58
A SUPERIOR SPECIES OF MONEY	62
INVESTING IN BITCOIN	64
A MOMENTUS INNOVATION	67

## **TIME**

---

THE SIMPLE TRUTH ABOUT TIME	69
THE ULTIMATE RESOURCE	69
FROZEN TIME	70
TIME ARBITRAGE	71
LINDY EFFECT	73
FUTURE OF REGULATION	74
THE LONG GAME	77
THE EVENT HORIZON	81
REVERSE BANK RUN	83
A PATH TO PROSPERITY	85
TIME WILL TELL	88
SOURCES	89
GLOSSARY	91

## MONEY

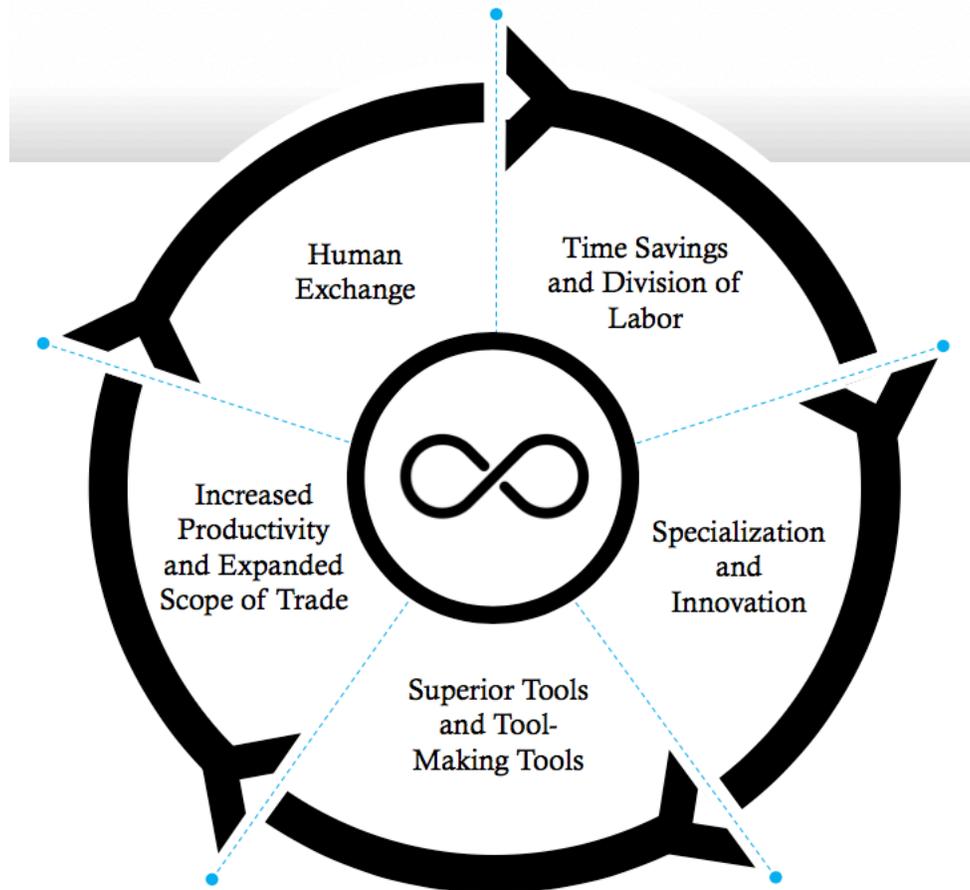
### The Simple Truth about Money

Money is the most successful story ever told by humans. It is a reflexive narrative: meaning it has value only because everyone believes it, and everyone believes it because it has value. Money is a story that continues to be written...

### Human Exchange

Human beings are the networked species. Initially, these were small bands of hunters and gatherers numbering no more than 150 persons strong (Dunbar's number). When humans began to exchange with one another, they intuitively discovered the *division of labor* which allows people to focus on their relative advantages and concentrate on their chosen craft. The division of labor enables the *specialization* of productive efforts for mutual gain. If John makes axes faster than Steve, and Steve makes bows faster than John, then they both are better off by specializing and trading. Interestingly, this holds true even if John is faster than Steve at making axes and bows (up to a point) and, amazingly, this effect compounds.

Tools, or technologies, are mechanisms that increase *productivity* by amplifying the returns on human time directed at production. You can chop more wood per man hour using an axe than you can with your bare hands. As people made and exchanged more tools, time savings increased and specialization deepened. Specialization sparked innovation, because it encouraged the investment of time in tool-making tools, such as whetstones used for making sharper axes. This enabled people to create superior tools, which increased productivity even further. That saved more time, which people used to specialize even further and expand their *scope of trade* by exchanging with an even greater number and variety of people, which increased the division of labor even further, and so on. This recursive dynamic persists to this day as a virtuous cycle with no known natural limit – modern markets in goods, services and ideas allow human beings to exchange and specialize honestly for the betterment of all. In this way, the act of exchange is the incipient force driving all human progress and *prosperity*. Prosperity is simply time saved, which is proportional to the division of labor:



Human exchange is to cultural evolution what sex is to biological evolution. By exchanging and specializing, innovations come into existence and spread. At some point, human intelligence became collective and cumulative in a way that happened to no other animal. Language, and later writing, allowed us to pass our collective learnings to each successive generation. Written language allowed us to manifest and share our belief systems. As the only animal that can tell and believe stories, we learned to organize ourselves using abstractions such as money, mathematics, nations and corporations. Our unique ability to tell and believe stories – as free market capitalists, human rights activists, national citizens or whatever story we accord with – enables us to cooperate flexibly in large numbers and across genetic boundaries. This scale of collaboration, never attained by any other animal before or since, is the reason mankind came to dominate the Earth. We are the networked species, fully interconnected by our acts of exchange. A spontaneous emergent property of these complex human interactions is money, which solved problems inherent to trade and accelerated the rate of human exchange and the division of labor. Money, as the vital lubricant for human exchange, was among the first stories we used to collectively organize ourselves.

## Story of Money

Let's begin with first principles and follow logic from there. The simplest way for people to exchange value is to trade actual goods, say guns for boats, in a process known as *direct exchange* or barter. This is only practical in small groups of people where few goods are exchanged. In larger groups of people, there are more opportunities for individuals to specialize in production and trade with more people, which increases the aggregate wealth for everyone. This simple fact, that exchange enables us to produce more goods per hour of human effort is the foundation of economics itself:

### **Economics is the social science of increasing production per unit of contribution.**

Larger groups of people exchanging goods mean larger markets, but also creates a problem of *non-coincidence of wants* – what you are seeking to acquire by trade is produced by someone who doesn't want what you have to offer. This problem has three distinct dimensions:

- Non-coincidence in Scales – imagine trying to trade pencils for a house, you cannot acquire fractions of a house and the owner of the house may not need such a large amount of pencils
- Non-coincidence of Locations – imagine trying to trade a coal mine in one place for a factory in another location, unless by coincidence you are seeking a factory in that exact location and the counterparty you are dealing with is seeking a coal mine in that precise place, the deal will not be completed since factories and coal mines are not movable
- Non-coincidence in Time Frames – imagine trying to accumulate enough oranges to trade for a truck, since the oranges are perishable they would likely rot before the deal could be completed

The only way to resolve this three-dimensional problem is through *indirect exchange*, where you seek to find another person with a good desired by the counterparty and exchange your good for theirs only to, in turn, exchange it for the counterparty's good to complete the deal. The intermediary good used to complete the deal with the counterparty is called a *medium of exchange* – the first function of money. Over time, people gradually converge on a single medium of exchange (or, at most, a few media of exchange). A good that assumes the role of a widely accepted medium of exchange is commonly called money.

Money offers its users pure optionality, as it can be readily exchanged for any good available in the marketplace. In other words, money is the most liquid asset within a trade network. In this sense, money is said to have the highest *salability*, meaning the ease with which it can be sold on the market at any time with the least loss in price. The relative salability of goods can be assessed in terms of how well they address the three dimensions of the non-coincidence of wants problem:

- Salability across Scales – a good that is easily subdivided into smaller units or grouped together in larger units, which allows the user to trade it in whatever quantity desired
- Salability across Space – a good that is easily transported or transmitted over distances

- Salability across Time – a good that can reliably hold its value into the future by being resistant to rot, corrosion, counterfeit, unpredictable increases in supply and other debasements of value

It is the third element, salability across time, that determines a good's utility as a *store of value* – the second function of money. Since the production of each new unit of a monetary good makes every other unit relatively less scarce, it dilutes the value of the existing units in a process known as *inflation*. Protecting value from confiscation via inflation is a critical feature of money, and money is critical to the existence of flourishing trade networks.

### Hard Money

*Hard money* is more trustworthy as a store of value precisely because it resists intentional debasements of its value by others and therefore maintains salability across time. The hardness of a monetary good, also known as its soundness, is determined by the stock of its existing supply and the flow of its new supply. The ratio which quantifies the hardness of money is called the *stock-to-flow* ratio:

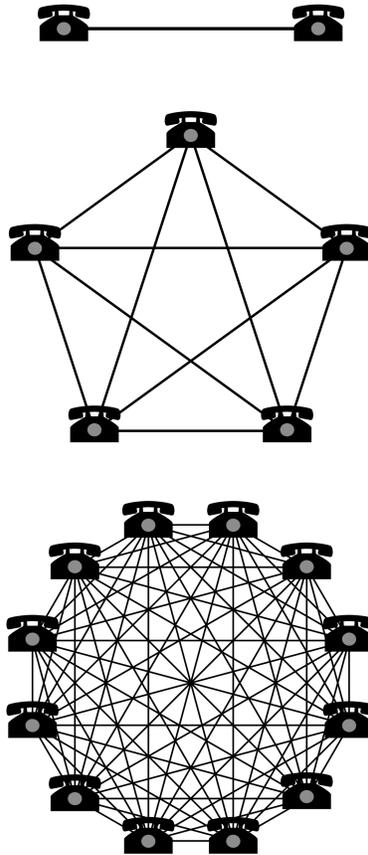
- 'Stock' is the existing supply of monetary units
- 'Flow' is the newly created supply over a specified time period, usually one year
- Dividing the stock of a monetary good by its flow equals its stock-to-flow ratio
- The higher the stock-to-flow ratio, the greater the hardness (or soundness) of money

The higher the stock-to-flow ratio, the more resistant the money is to having its value compromised by inflation. There are no correct choices as to forms of money, however there are consequences to what form a market naturally selects. If people choose to store their wealth in a monetary good which exhibits less hardness, then the producers of this monetary good are incentivized to produce more monetary units, which expropriates the wealth of existing unit holders and destroys the monetary good's salability across time. This is the fatal flaw of *soft money*: anything used as a store of value that can have its supply increased will have its supply increased, as producers seek to steal the value stored within the soft monetary units and store it in a harder form of money. As many historical examples in this essay will demonstrate, any monetary good which can have its supply cheaply and easily increased will rapidly destroy the wealth of those using it as a store of value.

For a good to assume a dominant monetary role within an economy, it must exhibit superior hardness with a higher stock-to-flow ratio than competing monetary goods. Otherwise, excessive unit production will destroy the wealth of savers and the incentives to use it as a store of value. Particular goods achieve monetary roles based on the interplay of people's decisions. It is from the chaos of complex human interactions that monetary orders emerge. Therefore, it is important to consider the social aspects of the spontaneous emergence of monetary orders.

## Money is a Social Network

Money, as a value system which connects people across space and time, is the original and largest social network. The value of a network is a reflection of the total number of possible connections it allows. Similar to the telephone and modern social media platforms, a monetary network becomes exponentially more valuable as more people join it because the number of possible connections it allows is proportional to the square of the number of its total network participants, a relationship defined by *Metcalf's Law*:



In a monetary network, more possible connections mean more salability and a broader scope of trade. Participants in a monetary network are connected by their use of a common form of money to express and store value. *Network effects*, defined as the incremental benefit attained by adding a new member to a network for all existing members in that same network, encourage people to adopt a single form of money. Intuitively, a monetary good that holds value across time (hard money) is always preferable to one that loses value (soft money). This causes people to naturally gravitate to the hardest form of money available to them. Further, since human exchange is a singular communal phenomenon suffering from a three-dimensional non-coincidence of wants problem, any monetary good that can solve all three dimensions of this problem will win the entire (or vast majority) of the market. For these

reasons, a free market for money exhibits a *winner take all* (or, at least, a winner take most) *dynamic*. Network effects accelerate people's natural coalescence around a single monetary technology since larger monetary networks support higher salability of the monetary good involved. However, the selection of a monetary good is limited by the technological realities of the markets selecting. This can impede the winner take all dynamic, since particular monetary goods each satisfy the desirable traits of money to greater or lesser extents.

### Monetary Traits

As we will see, markets have naturally and spontaneously selected for the monetary good which best satisfies a variety of desirable traits that determine how useful a particular monetary good is as a form of money:

- Hardness – resistance to unpredictable supply increases and debasements of value
- Fungibility – units are interchangeable and indistinguishable from one another
- Portability – ease of transporting or transmitting monetary units across distances
- Durability – resistance of monetary units to rot, corrosion or deterioration of value
- Divisibility – ease of subdividing or grouping monetary units
- Security – resistance to counterfeiting or forgery
- Sovereignty – the source of its value, trust factors and permissions necessary to transact with it (natural social consensus or artificial government decree)
- Government Issued – authorized as legal tender by a government

As discussed, hardness is the singular trait that takes primacy over all others in determining a good's suitability for playing a monetary role. Money, as an expression of value, has remained conceptually constant but has evolved to inhabit many different goods over time. Like language, which was first spoken, then written and now typed, the meaning expressed by money remains the same while its modality continually evolves. As the monetary technologies we use to express value change, so too do our preferences.

### Prospects of Prosperity

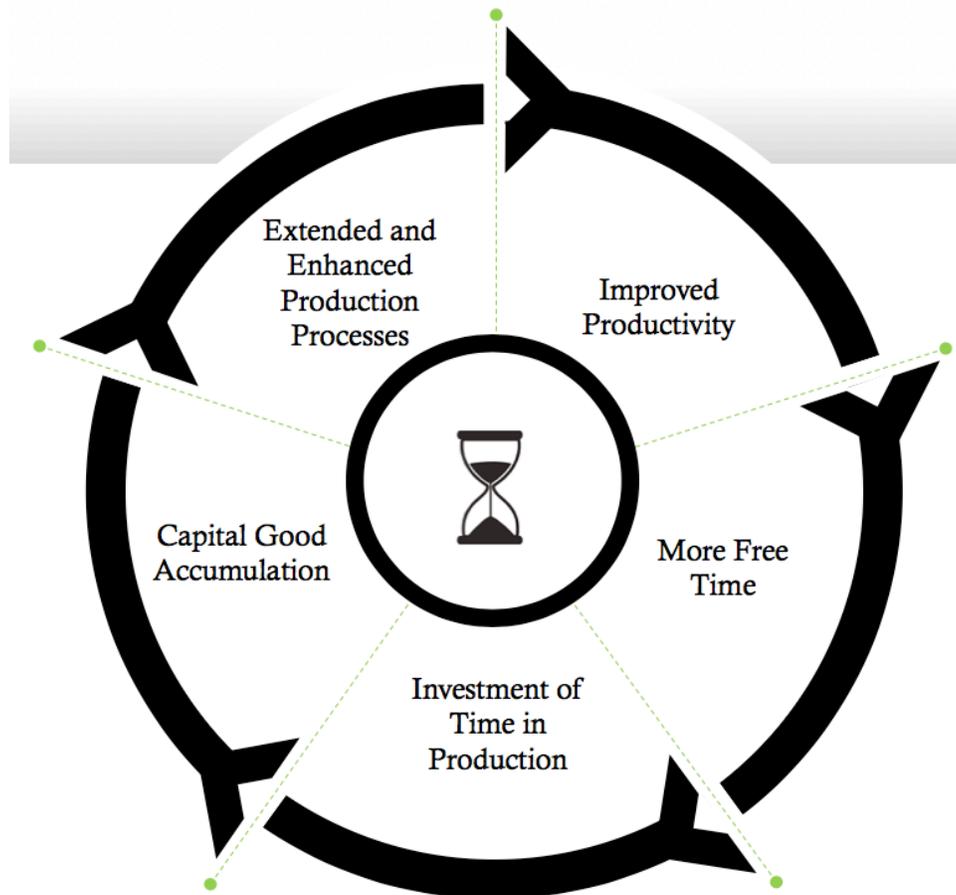
In economics, a critical aspect of human decision making is called *time preference*, which refers to the ratio at which an individual values the present relative to the future. Time preference is positive for all humans, as the future is uncertain, and the end could always be near. Therefore, all else being equal, we naturally prefer to receive value sooner rather than later. People who prefer to defer current consumption and instead invest for the future are said to have a lower time preference. The lowering of time preference is closely related to the hardness of money and is also exactly what enables human civilization to advance and become more prosperous. In regard to time preference, hard money is important in three critical aspects:

- By providing a reliable way to protect value across time, hard money incentivizes people to think longer term and thus lowers their time preferences

- As a stable unit of measurement, hard money enables markets to grow ever-larger by reducing the costs and risks of free trade, which increases the incentives for long-term cooperation and lowers time preferences
- Self-sovereign money (like gold and Bitcoin) that cannot be manipulated by any single party reduces governmental intervention which encourages the growth of free markets, which increases their long-term stability and lowers time preferences

A lower time preference is an important part of what separates humans from other animals. By considering what is better for the future, we can curb our animalistic impulses and choose to act rationally and cooperate for the betterment of everyone involved. As humans lower their time preference, they develop a scope for carrying out tasks over longer time horizons. Instead of spending all our time producing goods for immediate consumption, we can choose to spend time creating superior goods that take longer to complete but benefit us more in the long run. Only by lowering time preference can humans produce goods that are not meant to be consumed themselves but are instead used in the production of other goods. Goods used exclusively for the production of other goods are called *capital goods*.

Only humans with a lower time preference can decide to forgo a few hours of fishing and opt to build a superior fishing pole, which cannot be eaten itself, but in the future will enable better results per hour of human effort spent fishing. This is the essence of *investment*: humans defer immediate gratification and invest their time producing capital goods which will, in turn, make the production process itself more sophisticated, extend it over a longer time horizon and yield superior results per hour of human effort. In this way, investment increases capital good stocks which increases productivity. Amazingly, this effect also transforms into a *positive feedback loop*. Also known as a virtuous cycle or the flywheel effect, a positive feedback loop is a process that is recursively energized (its outputs also serve as its inputs) and therefore creates compounding effects. Positive feedback loops play an important role in biology, chemistry, psychology, sociology, economics and cybernetics. In respect to investment, as more capital goods are accumulated, levels of productivity are increased even more and the time horizon of production is extended even further:



To understand this preference clearly, let's consider two hypothetical fishermen, Harold and Louis, who start out with nothing other than their bare hands. Harold has a higher time preference than Louis and chooses to spend his time catching fish with using just his bare hands. Using this approach, Harold spends about 8 hours per day to catch enough fish to feed himself for one day. Louis, on the other hand, spends just 6 hours per day catching fish, makes do with the smaller amount of fish and chooses to spend the other 2 hours building a fishing pole. Two weeks later, Louis has succeeded in building a fishing pole, which he can now use to catch twice as many fish per hour as Harold. Louis's investment in the fishing pole could allow him to only fish for 4 hours each day, eat the same amount of fish as Harold and spend his other 4 hours in leisure. However, since Louis has a lower time preference, he instead chooses to fish for 4 hours per day and spend the other 4 hours building a fishing boat.

One month later, Louis has succeeded in building a fishing boat, which he can now use to go further out to sea and catch fish that Harold has never even seen. Not only has Louis increased his productivity (fish caught per man hour) but he has also increased the quality of his production (a greater variety of fish from the deep sea). By using his fishing pole and boat, Louis now needs only 1 hour per day to catch a day's worth of food and spends his other 7 hours engaged in further capital accumulation – building better fishing poles, boats, nets, lures, etc. – which, in turn, further increases his productivity and quality of life.

Should Louis and his descendants continue to exhibit a lower time preference, the results will compound over time and across generations. As they accumulate more capital, their work efforts will be ever-further amplified by productivity gains and enable them to engage in ever-larger projects that take ever-longer to complete. These gains are amplified even further when Louis and his descendants begin trading with others that specialize in crafts in which they themselves do not – such as housing, wine making or farming. Successive layers of learning, productivity gains and flourishing trade networks are the foundational sediment upon which all human advancement in terms of knowledge, technology and culture is built. Human advancement is noticeable by the tools we make and the way we relate with one another.

From this perspective, it becomes clear that the most important economic decisions any individual faces are related to the trade-offs they face with their future self. Eat less fish today, build a fishing boat tomorrow. Eat clean today, be healthy tomorrow. Exercise today, be fit tomorrow. Read books today, be knowledgeable tomorrow. Invest money today, be wealthy tomorrow. We can all take solace that this compounding force of nature is always available to each and every one of us. No matter how bad the circumstances are for a man with a low time preference, he will likely find a way to keep compounding his present efforts and prioritizing his future self until he achieves his objectives. Contrarily, no matter how much fortune and wealth favors the man with a high time preference, he will likely find a way to continue squandering his wealth and shortchanging his future self. These individual relationships with our future selves is the microcosm of the societal macrocosm. As society develops a lower time preference, its prospects of prosperity improve in tandem.

### Foundation of Economic Growth

There are many factors beyond the scope of this writing which influence time preference. Most relevant to our discussion is the expected future value of money. As we have seen, hard money is superior at holding its value across time. Since its purchasing power tends to remain constant or grow over time, hard money incentivizes people to delay consumption and invest for the future, thereby lowering their time preference. On the other hand, soft money is subject to having its supply increased unexpectedly. Increasing the money supply is the same as lowering the *interest rate*, which is effectively the price of borrowing money and the incentive to save. By reducing the interest rate, the incentive to save and invest is diminished whereas the incentive to borrow is increased. So, soft money disincentivizes a favorable orientation towards the future. In other words, soft money systems raise society's time preference. For this reason, soft money, once it is sufficiently debased, tends to precede societal collapse (more on this later).

An ideal hard money would be one whose supply is absolutely scarce, meaning no one could produce more of it. The only noncriminal way to acquire money in such a society would be to produce something of value and exchange it for money. As everyone seeks to acquire more money, everyone would become ever-more productive which would encourage capital accumulation, productivity gains and a lowering of time preference. Since the money supply is fixed, economic growth would cause the prices of real goods and services to drop over time, as a fixed quantity of monetary units chases an increasing quantity of goods. Since people could expect to be able to purchase more with the same amount of money in the future, such

a world would discourage immediate consumption and encourage saving and investment for the future. Paradoxically, a world that consistently defers consumption will actually end up consuming more in the long run as its increased savings would increase investment and productivity, thus making its citizens wealthier in the future. This dynamic would spark a positive feedback loop - with present needs met and an ever-greater focus on the future, people naturally begin concentrating other aspects of life such as social, cultural and spiritual endeavors. This is the essence of free market capitalism: people choosing to lower their time preference, defer immediate gratification and invest in the future.

**The foundation of all economic growth is delayed gratification, which leads to savings, which leads to investment, which extends the duration of the production cycle and increases productivity in a self-sustaining, virtuous cycle with no known natural limit.**

Debt is the opposite of saving. As saving creates the possibility for capital accumulation and its associated benefits, debt is what can reverse it by reducing capital stocks, productivity and living standards across generations. As we will show later, when the gold standard was forcibly ended by governments, money not only became much softer, but it also fell under the command of politicians who are incentivized to operate with high time preferences as they strive for reelection every few years. This explains why politicians continue to mandate the use of soft government money, despite the long-term harm it causes to an economy, ensuring that it remains the dominant form of money in the world (we will cover soft government money's unnatural ascent to world domination later).

When a form of money becomes globally dominant, it finally serves the third function of money – *unit of account*. History shows us that this function is the final evolutionary stage in the natural ascendancy of monetary goods that achieve a dominant role – which are first a store of value, then a medium of exchange and finally a unit of account. As economist William Stanley Jevons explained:

“Historically speaking, gold seems to have served, firstly, as a commodity valuable for ornamental purposes; secondly, as stored wealth; thirdly, as a medium of exchange; and, lastly, as a measure of value.”

Today, the US Dollar is dominant and serves as the global unit of account as prices are most commonly expressed in its terms. This consistency of expression simplifies trade and enables a (somewhat) stable pricing structure for the global economy.

### The Economic Nervous System

Market prices are an essential communicative force in economics. As economic production moves from a primitive scale, it becomes harder for individuals to make production, consumption and trade decisions without having a fixed frame of reference (unit of account) which to compare the value of different objects to one another.

In his paper ‘The Use of Knowledge in Society’ Friedrich Hayek elucidated the economic problem as not merely a matter of allocating human effort. More accurately, the economic

problem is one of allocating human effort according to knowledge that is distributed in the minds of people that are each primarily concerned with their respective area in the broader economy. This distributed knowledge includes the:

- Conditions of production
- Availability of the factors of production
- Preferences of individuals

Knowledge, due to its dynamic and fluid nature, cannot be fully known by a single entity as it is constantly in flux and widely distributed within many minds. In a free market economic system prices capture this distributed knowledge, convert it into impartial information and disseminate it widely. *Price signals* are the coordinating force of free market systems. Each individual decision maker can faithfully rely on the prices of goods relevant to their production process, as the prices themselves are a distillation of all known market realities into a single, actionable variable. Each individual's buy and sell decisions, in turn, further shape prices which carry this altered information back out into the market. Price signals are to market participants what light is to the eye.

To understand this point, consider the 2010 earthquake which badly damaged an area in Chile responsible for a great deal of the world's copper production. This earthquake severely damaged copper mines and export infrastructure, which immediately reduced the flow of new supply to the world copper market and resulted in a 6.2% increase in its price. Anyone in the world whose business interfaces with the copper market will be affected by this, but they do not need any specific knowledge about the earthquake in Chile or market conditions to decide how to respond. All the relevant information they need to make effective decisions is contained within the price of copper itself. Immediately, all firms that demand copper are incentivized to demand less, delay purchases or find substitutes. On the other side of the market, all firms that produce copper are incentivized to produce more of it. With a natural shift in price, everyone in the world involved in the copper industry is incentivized to act in a way that alleviates the negative consequences of the earthquake. This is the power of a free market with accurate price signals.

The wisdom of the crowd is always superior to the wisdom of the board room. There is simply no way to recreate the adaptivity and collective intelligence of markets by installing a centralized planning authority. How would they decide who should increase production and by how much? How would they decide who should reduce consumption and by how much? How would they coordinate and enforce their decisions in real time on a global scale? In this sense, prices are the economic nervous system that disseminate knowledge across the world and help coordinate complex production processes by:

- Incentivizing supply and demand changes to match economic reality and restore market equilibriums quickly
- Efficiently matching buyers and sellers in the marketplace
- Compensating producers for their work efforts

Without accurate price signals, humans could not benefit from the division of labor and specialization beyond a small scale. Trade allows producers of goods to mutually increase their living standards by specializing in goods in which they have a relative or *comparative advantage* – goods they can produce relatively faster, cheaper or better. Accurate prices expressed in a common, stable medium of exchange help people identify their comparative advantage and specialize in it. Specialization, guided by reliable price signals, enables producers to improve their efficiency of production and accumulate capital specific to their craft. This is why the most productive allocation of human efforts is only determinable by an accurate pricing system within a free market. Also (as we will see later), this is exactly why capitalism prevailed over socialism, because socialism lacked an economic nervous system. But before diving into the economic aspects which underpinned this historic ideological struggle and seeing how it is still relevant today, we first need to understand the evolutionary forces that have shaped money throughout history.

### Monetary Evolution

Throughout history, money has taken many forms - seashells, salt, cattle, beads, stones, precious metals and government paper have all functioned as money at one or more points in history. Monetary roles are naturally determined by the technological realities of the societies shaping the salability of goods. Even today, forms of money still spontaneously emerge with things like prepaid mobile phone minutes in Africa or cigarettes in prisons being used as localized currencies. Different monetary technologies are in constant competition, like animals competing within an ecosystem. Although instead of competing for food and mates like animals, monetary goods compete for the belief and trust of people. Believability and trustworthiness form the basis of *social consensus* – the source of a particular monetary good's sovereignty from which it derives its market value along with the trust factors and permissions necessary to transact with it.

As these competitions continue to unfold in a free market, goods attain and lose monetary roles according to the traits which determine how believable or trustworthy they are and are expected to remain over time. As we will show, free market competition is ruthlessly effective at promulgating hard money as it only allows those who choose the hardest form available to maintain wealth over time. This *market-driven natural selection* causes new forms of money to come into existence and older forms to fade into extinction. Like biologically-driven natural selection, in which nature continuously favors the organisms which are best suited for success in their respective ecologies, this market-driven natural selection is a process in which people naturally and rationally favor the most believable and trustworthy monetary technologies available in their respective trade networks. Unlike ecological competition which can favor many dominant organisms, the marketplace for money is driven by network effects and favors a winner take all (or, at least, a winner take most) dynamic as the non-coincidence of wants problem is universal and if a single hard money is capable of solving all three of its dimensions than it will become dominant (as discussed earlier in the social network aspects of money).

An example of this market-driven natural selection of money comes from the ancient Rai Stones system of Yap Island, located in what is today Micronesia. Rai Stones were large disks of various sizes with a hole in the middle that weighed up to eight thousand pounds each. These stones were mined in neighboring Palau or Guam and were not native to Yap. Acquiring these stones involved a labor-intensive process of quarrying and shipping. Procuring the largest Rai Stones required workforces numbering in the hundreds. Once the stones arrived in Yap, they were placed in a prominent location where everyone could see them. Owners of the stones could then use them as payment by announcing to the townsfolk the transfer of ownership to a new recipient. Everybody in the town would then record the transaction in their individual ledger, noting the new owner of the stone. There was effectively no way to steal the stone because its ownership was recorded by everyone. In this way, the Rai Stones solved the three dimensions of the non-coincidence of wants problem for the Yapese by providing:

- Salability across scales as the stones were various in size and payments could be made in fractions of a stone
- Salability across space as the stones were accepted for payment everywhere on the island and did not have to be moved physically, just recorded by the townsfolk's individual ledgers (remarkably similar to Bitcoin's distributed ledger model, as we will see later)
- Salability across time due to the durability of stones and the difficulty of procuring new stones which meant that the existing supply of stones was always large relative to any new supply that could be created within a given time period (a high stock-to-flow ratio)

This monetary system worked well until 1871, when an Irish-American captain named David O'Keefe was found shipwrecked on the shores of Yap by the local islanders. Soon, O'Keefe identified a profit opportunity in buying coconuts from the Yapese and selling them to coconut oil producers. However, he could not transact with the locals because he was not a Rai Stone owner and the locals had no use for his foreign forms of money. Undeterred, O'Keefe sailed to Hong Kong and acquired some tools, a large boat and explosives to procure Rai Stones from neighboring Palau. Although he met resistance from them initially, he was eventually able to use his Rai Stones to purchase coconuts from the Yapese. Other opportunists followed O'Keefe's lead and soon the flow of Rai Stones increased dramatically. This sparked conflict on the island and disrupted economic activity. By using modern technologies to acquire Rai Stones more cheaply, foreigners were able to compromise the hardness of this ancient monetary good. The market naturally selected against Rai Stones because, as their stock-to-flow ratio declined, they became less reliable as a store of value and thus lost their salability across time, which ultimately led to the extinction of this ancient monetary system.

A similar story played out in western Africa which for centuries used aggr beads as money. These small glass beads were used in a region where glassmaking was an expensive craft, which gave them a high stock-to-flow ratio and made them salable across time. Since aggr beads were small and light they could easily be combined into necklaces or bracelets and transported easily, thus giving them salability across scales and space. In the 16<sup>th</sup> century, European explorers discovered the high value ascribed to these beads by the west Africans

and began importing them in mass quantities; as European glassmaking technology made them extremely cheap to produce. Slowly but surely, the Europeans used these cheaply produced beads to acquire most of the precious resources of Africa. The net effect of this incursion into Africa was the transference its vast natural resource wealth to Europeans and the conversion of aggrary beads from hard money to soft money. Again, the market naturally selected against a monetary good once its stock-to-flow ratio began to decline, as its store of value functionality and, therefore, its salability across time were compromised as a result. Although the details vary, this underlying dynamic of a declining stock-to-flow ratio presaging a good's loss of its monetary role has been the same for every form of money throughout history. Today, we are seeing a similar pattern cause the collapse of the Venezuelan bolivar, (where some Venezuelans are using Bitcoin to protect their wealth as the currency collapses).

As societies continued to evolve, they began to move away from artifact money like stones and glass beads and towards monetary metals. It was initially difficult to produce most metals which kept their supply flows low, thus giving them good salability across time. Gold in particular, with its extreme rarity in the Earth's crust and its virtual indestructability, made it an extremely hard monetary technology. Gold mining was difficult, limiting supply increases relative to its existing supply, which itself could not be destroyed. Gold gave humans a way to store value across generations and develop a longer-term perspective on their actions (a lower time preference), which led to the proliferation of ancient civilizations:



The earliest coins are found mainly in the parts of modern Turkey that formed the ancient kingdom of Lydia. They are made from a naturally occurring mixture of gold and silver called electrum.

### Monetary Metals

Julius Caesar, the last dictator of the Roman Republic, issued a gold coin called the aureus coin which contained a standard 8 grams of gold. The aureus was traded widely across Europe and the Mediterranean, alongside a silver coin called the denarius, which was used for its superior salability across scales. Used together, these coins provided a hard money system that increased the scope of trade and specialization in the Old World. The republic became more economically stable and integrated for 75 years until the infamous emperor Nero came into power.

Nero was the first to engage in the practice of *coin clipping* in which he would periodically collect the coins from the population, melt them down and mint them into newer versions with the same face value but less precious metal content, keeping the residual content to enrich himself. Similar to modern day inflation, this was a way of surreptitiously taxing the population by debasing its currency. Nero and successive emperors would continue the practice of coin clipping for several hundred years to finance government expenditures:



Isaac Newton is attributed with adding the small stripes along the edges of coins as a security measure against coin clipping. These stripes are still present on most coins today.

Citizens gradually wised up to this deceit and began hoarding the coins with higher precious metal content and spending the debased coins, as they were legally required to be accepted at face value in settlement of debts, one of the earliest instances of *legal tender* laws being implemented. This had the effect of driving up the price of coins with higher precious metal content and driving down the price of those with less – a dynamic that came to be known as *Gresham's Law*: bad money (soft money) drives good money (hard money) out of circulation. This is an important law to recall when we look at how modern-day hoarding of Bitcoin impacts its price.

Eventually, a new coin called the solidus was introduced which contained only 4.5 grams of gold, almost half the content of the original aureus coin. With this fall in the value of its money, a cycle familiar to many modern economies running on government money began to take hold – coin clipping reduced the money's real value, increased the money supply, gave the emperor the means to continue imprudent spending and eventually ended with inflation and economic crisis. Analogous to central bank practices today, Swiss banker Ferdinand Lips summarized this era well:

“Although the emperors of Rome frantically tried to ‘manage’ their economies, they only succeeded in making matters worse. Price and wage controls and legal tender laws were passed, but it was like trying to hold back the tides. Rioting, corruption, lawlessness and a mindless mania for speculation and gambling engulfed the empire like a plague.”

Amid the chaos of the crumbling Roman Republic, Constantine the Great took power and would reverse the fortunes of empire by adopting responsible economic policies. He first committed to maintaining the solidus at 4.5 grams of gold, ended the practice of coin clipping and began minting massive quantities of these standardized gold coins. He then moved east and established Constantinople in modern day Istanbul. This became the birthplace of the Eastern Roman Empire, which adopted the solidus as its monetary system.

While Rome continued its economic, social and cultural deterioration until it finally collapsed in 476 AD, Constantinople flourished. The solidus, which eventually became known as the bezant, provided a hard money system with which Constantinople would remain prosperous and free for centuries to come. As with Rome before it, the fall of Constantinople happened only when its rulers began the debasing its currency around 1050 AD. As with Rome, the move away from hard money led to the fiscal, cultural and spiritual decline of the Eastern Roman Empire. After suffering many successive crises, Constantinople was ultimately overtaken by the Ottomans in 1453. However, the bezant inspired another form of hard money that still circulates to this day, the Islamic dinar. Seventeen centuries of people all over the world have used this coin – which began as the solidus before changing its name to the bezant and finally becoming the Islamic dinar – for transactions, thus highlighting the superior salability of a hard money like gold across time.

Following the collapse of the Roman Empire, Europe fell into the dark ages. It was the rise of the city-state (a new story mankind would begin organizing itself around) and its use of hard money systems that would pull Europe out of the Dark Ages and into the Renaissance. Beginning in Florence in 1252, the city minted the florin which was the first major European coinage issued since Julius Caesar's aureus. By the end of the 14<sup>th</sup> century more than 150 European cities and states had minted coins to the same specifications as the florin. By giving its citizenry the ability to accumulate wealth in a reliable store of value which could be traded freely across scales, space and time, this hard money system unlocked scientific, intellectual and cultural capital within the Italian city-states and eventually spread to the rest of Europe. Of course, the situation was far from perfect, as there were still many periods marked by various rulers choosing to debase their currencies to finance war or lavish expenditure.

### Global Gold Standard

When they were being used as physical means of settlement, gold and silver coins served complementary roles. Silver, having a stock-to-flow ratio second only to that of gold, had the advantage of being a more salable metal across scales, since its lower value per weight than gold made it ideal as a medium of exchange for smaller transactions. In this way, gold and silver were complementary as gold could be used for large settlements and silver could be used for smaller payments. However, by the 19<sup>th</sup> century, with the development of modern custodial banking and advanced telecommunications, people were increasingly able to transact seamlessly across scales using bank notes or checks backed by gold:



The US Dollar was once redeemable for gold on demand.

With all of the critical salability characteristics gathered under a gold standard monetary system facilitated by paper bank notes, the superior salability across scales of physical silver lost relevance, setting it up to become demonetized (due to the winner take all dynamic discussed earlier). Ironically, the same banking industry that enabled a global gold standard would in later years see to its elimination (more on this later).

A brief aside on silver: This demonetization dynamic also explains why the silver bubble popped many times throughout history when facing off with gold and will pop again if it ever reflatates. Since silver is not the hardest form of monetary good available, should any significant investment flow into silver, its producers will be incentivized to increase the flow of silver, and store any value expropriated from its increased production in the hardest form of money available to them (which, before Bitcoin, was only gold). This, of course, will bring the price of silver crashing back down, taking the wealth from the investment inflows with it. As a more recent historical example of this dynamic in action: In the 1970s, the affluent Hunt brothers attempted to remonetize silver by buying vast quantities of it in the market. This drove up the price initially, and the Hunt brothers believed they could continue driving up its price until they cornered the market. Their intent was to induce others to chase its appreciation and recreate a monetary demand for silver. As they kept buying and the price kept rising, silver holders and producers kept selling into the market. No matter how much the Hunt brothers purchased, the selling and flow of silver continued to outpace their buying, which decreased its stock-to-flow ratio and eventually led to a dramatic crash in the price of silver. The Hunt brothers lost over \$1B (due to rampant inflation of government money since then, their losses equal \$6.5B in 2019 dollars) in the ordeal, which is likely the highest price ever paid for learning the importance of hard money and its defining metric, the stock-to-flow ratio.

Driven by expanding telecommunication and trade networks, and with custodial banks enhancing its salability across scales by issuing gold-backed bank notes and checks, the gold standard spread quickly. More nations began switching to paper based monetary systems fully backed by and redeemable in gold. Network effects took hold as more nations moved onto the gold standard, giving gold deeper liquidity, more marketability and creating larger incentives for other nations to join.

Those nations which remained on a silver standard the longest before converting, like China and India, witnessed tremendous devaluations of their currencies in the intervening period. The demonetization of silver for China and India was an effect similar to the west Africans holding aggrary beads when Europeans arrived. Foreigners who adopted the gold standard were able to gain control over vast quantities of the capital and resources in China and India. This drives home a key point: every time hard money encounters a softer form of money in a trade network, the softer money is ultimately outcompeted into extinction.

**This dynamic has significant consequences for the holders of soft money and is an important lesson for anyone who believes their refusal of Bitcoin means they are protected from its economic impact. History shows us repeatedly that it is not possible to protect yourself from the consequences of others holding money that is harder than yours.**

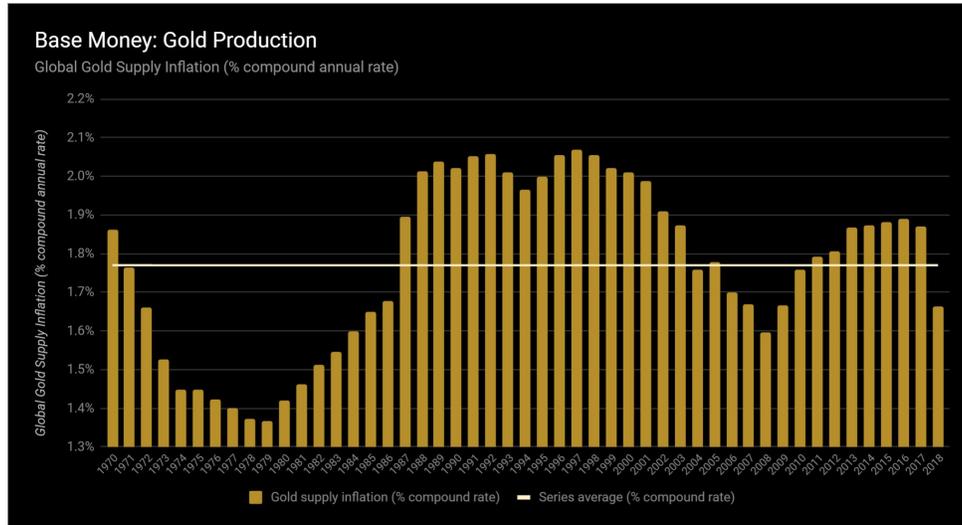
Finally, for the first time in history, the majority of the world economy began operating on a gold-based, hard money standard that was naturally selected for by the free-market.

### Hardness of Gold

By this point in history, virtually everyone had come to fully trust gold's superior stock-to-flow ratio and therefore believed they could use it to reliably store value across time. After thousands of years of mining this chemically stable element, virtually all the gold ever procured by humans is still a part of its extant supply. The stock of all the gold in the world fits into an Olympic-sized swimming pool today and is valued at almost \$8T USD. Gold is rare in the Earth's crust and extraction is costly in terms of time and energy, which keeps its flow predictably low. It is impossible to synthesize gold by chemical means (as alchemy never panned out) and the only way to increase its supply is through mining.

The costliness of gold mining is the *skin in the game* necessary to increase its flow – the risk necessary to procure the reward. Skin in the game is a concept based on symmetry, a balance of incentives and disincentives: in addition to upside exposure, people should also be penalized if something for which they are responsible for goes wrong or hurts others. Skin in the game is the central pillar for properly functioning systems and is at the heart of hard money. For gold, its mining costs and risks form the disincentives which are balanced against the incentives of its market price. Unless consequential decisions are made by people who are exposed to the results of their decisions, the system is vulnerable to total collapse (an important consideration when we discuss soft government money later).

Every market-driven evolutionary step for money has naturally selected the form with the highest stock-to-flow ratio available to its population but stopped when the form lost this key property. With the highest stock-to-flow ratio of all the monetary metals, gold is the hardest physical form of money that has ever existed, which explains its success as hard money throughout history. Even with advances in mining techniques, gold still has a relatively low and predictable flow, as evidenced by its annual supply growth since 1970:



Gold mining, of course, only makes economic sense if the cost of producing an additional ounce of gold is less than gold's market price per ounce. Relatedly, when the price of gold increases, its mining becomes more profitable and draws new miners into the market and makes new methods of gold mining economically feasible. This, in turn, increases the flow of gold until supply and demand forces again reach equilibrium. So, although gold is the hardest form of physical money, it doesn't have perfect hardness as changes in demand for it elicit both a supply and price response, meaning:

- An increase in the demand for gold increases its price,
- An increase in the price of gold incentivizes gold miners to increase its flow,
- An increase in the flow of gold increases its supply
- An increase in the supply of gold puts downward pressure on its price

In this way, changes in demand for gold are expressed partially in its price and partially in its supply flow. This *price elasticity of supply* is true for all physical commodities. For all practical purposes, as we will see later, the Earth always has more natural resources to yield assuming the right amount of time and effort are directed towards their production (this will support an important point later when we look at the impact of changes in demand on Bitcoin's price).

### Final Settlement

Gold also has the advantage of being an instrument of *final settlement*. Whereas the use of government money requires trust in the monetary policy and creditworthiness of the issuing authority or payment intermediaries, known as *counterparty risk*, the act of physically possessing gold comprises all of the trust factors and permissions necessary to use it as money. This makes gold a self-sovereign form of money. This is best understood as an identity of the universal accounting equation:  $\text{Assets} = \text{Liabilities} + \text{Owner's Equity}$

When you own gold free and clear, it is your asset and no one else's liability, meaning that your personal balance sheet includes a 100% gold asset matched by 0% liabilities and 100% owner's equity (since no one else has a claim on your gold asset). This makes gold a *bearer*

*instrument*, meaning that any individual in physical possession of the asset is presumed to be its rightful owner. This timeless and trustless nature of gold is the reason why it still serves as the base money and final settlement system of central banks worldwide.

In the 19<sup>th</sup> century, the term *cash* referred to central bank gold reserves, which was the dominant self-sovereign monetary good at the time. Cash settlement referred the transfer of physical gold between central banks to execute final settlement. Central banks can only settle with finality in physical gold, and still do so periodically in the modern era, since it is the only form of money that requires no trust in any counterparty, is politically neutral and gives its holders full sovereignty over their money. This is why gold maintains its monetary role even today as only the delivery of a bearer instrument can truly be the final extinguisher of debt. In this original sense of the word cash, gold is the only form of dominant cash money that has ever existed (although Bitcoin is well-suited to serve a similar role in the digital age, more on this later). Unfortunately, the combination of gold's self-sovereignty and physicality would lead to the demise of the gold standard.

### Centralization of Gold

By the end of the 19<sup>th</sup> century, all the industrialized nations of the world were officially on the gold standard. By virtue of operating on a hard money basis, most of the world witnessed unprecedented levels of capital accumulation, free global trade, restrained government and improving living standards. Some of the most important achievements and inventions in human history were made during this era, which came to be known as *la belle époque* across Europe and *the Gilded Age* within the United States. This golden era enabled by the gold standard remains one of the greatest periods in human history:

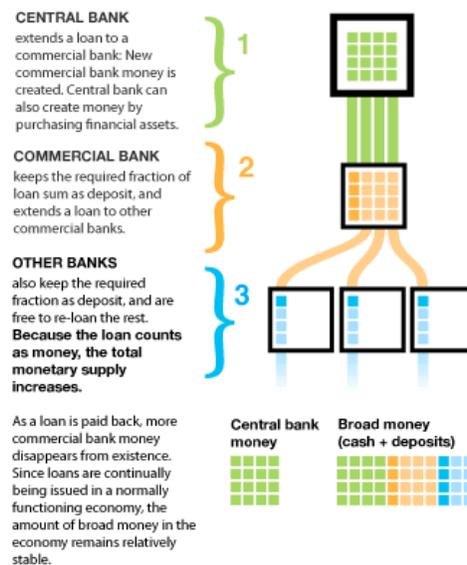
“La Belle Époque was a period characterized by optimism, regional peace, economic prosperity, an apex of colonial empires, and technological, scientific, and cultural innovations. In the climate of the period, the arts flourished. Many masterpieces of literature, music, theater, and visual art gained recognition.”

As multiple societies had now converged on gold as their universal store of value, they experienced significant decreases in trade costs and an attendant increase in free trade and capital accumulation. La Belle Époque was an era of unprecedented global prosperity. However, the hard money gold standard which catalyzed it suffered from a major flaw: settlement in physical gold cumbersome, expensive and insecure. This flaw is associated with the physical properties of gold, as it is dense, not deeply divisible and not easily transactable. Gold is expensive to store, protect and transport. It is also heavy per unit of volume which makes it difficult to use for day to day transactions. As discussed earlier, banks built their business model around solving these problems by providing secure custody for people's gold hoards. Soon after, banks began issuing paper bank notes that were fully redeemable in gold. Carrying and transacting with paper bank notes backed by gold was much easier than using actual gold. Offering superior utility and convenience, the use of bank notes flourished. This, along with government programs to confiscate gold from citizens (such as Executive Order 6102 in the United States), encouraged the centralization of gold supplies within bank vaults all over the world.

Incapable of resisting the temptation of wealth expropriation by tampering with the money supply, banks soon began issuing more notes than their gold reserves could justify, thus initiating the practice of *fractional reserve banking*. This banking model facilitated the creation of money without any skin in the game. Governments took notice and began to gradually take over the banking sector by forming central banks, as this model enabled them to engage in *seigniorage*, a method of profiting directly from the *money creation process*:

## Money creation

through fractional reserve banking (expansionary monetary policy)



The ability to control this process was too tempting for governments to resist. Total control of over the money supply gave those in charge a mechanism to continually extract wealth from its citizenry. The virtually unlimited financial wealth the printing press provided gave those in power the means to silence dissent, finance propaganda and wage perpetual warfare. It is a fundamental economic reality that wealth cannot be generated by tampering with the money supply, it can only be manipulated and redistributed. Civilization itself relies on the integrity of the money supply to provide a solid economic foundation for free trade and capital accumulation. With a firm grip on the prevailing monetary order established, the next logical step for central banks was to begin moving away from the gold standard altogether.

### Abolishing the Gold Standard

By 1914, most of the major economies had begun printing money in excess of their gold reserves at the onset of World War I. Unsurprisingly, this had many negative consequences, some of which were immediate while others came on more slowly. Eliminating the gold standard immediately destabilized the unit of account by which all economic activity was assessed. Government currency exchange rates would now float against one another and

become a source of economic imbalance and confusion. This distorted price signals, which would now be denominated in various government currencies with rapidly fluctuating exchange rates. This made the task of economic planning as difficult as trying to build a house with an elastic measuring tape.

For a world that was becoming increasingly globalized and technologically sophisticated, freely floating currency exchange rates represented a significant step backwards and gave rise to what is commonly called a 'a system of partial barter'. For people to buy goods from other people who lived on the other side of any number of imaginary lines called national borders, they would now be required to use more than one medium of exchange (their own currency and the foreign currency) to complete the transaction. To an extent, this reignited the non-coincidence of wants problem which money was meant to solve in the first place. Today, over \$5T (\$5,000,000,000,000) of foreign currencies are exchanged daily, forming an annual market valued at over 12 times global GDP. This industry is purely parasitic – it enriches bankers and sucks real value out of society in the form of global trade frictions, market distortions and transaction fees. For this reason, it is excluded from GDP calculations and exist solely because of the inefficiencies caused by centrally controlled capital markets and the absence of a global, politically neutral hard money system. The resultant frictions to global trade fanned the flames of warfare.

### Governments Take Control

As 20<sup>th</sup> century wars raged, so did the printing presses. Governments and their central banks continued to grow more powerful with each new bank note printed as their citizens became poorer. The death stroke came when most governments, due to a unilateral decision of President Nixon in United States, finally severed the peg to gold entirely in the 1971. Which brings us to the modern form of dominant money: *government fiat money*. Fiat is a Latin word meaning decree, order or authorization. This is why government money is commonly referred to as fiat money, since its value exists solely because of government decree:



Today, the US Dollar is not redeemable for anything and its value is derived solely from government decree. Paradoxically, people were coerced into adopting soft government fiat money only because of their shared belief in gold as a hard monetary good.

This is an imperative point: it was possession of gold (self-sovereign, hard money) that gave governments the power to decree the value of their fiat money (soft money) in the first place. National governments were only able to achieve “sovereignty” because they drew this power from their possession of gold. Paradoxically, people were coerced into discarding the gold standard and adopting soft government fiat money only because of their belief in gold as a hard monetary good. This is proof that it is possible to create an artificial asset and endow it with monetary properties, whether by decree or by market-driven natural selection. Governments did so by stealing gold from citizens, which gave them the power to create fiat money and decree its value by force. As we will later see, Satoshi Nakamoto did so by creating Bitcoin and releasing it into the marketplace as a self-sovereign money free to compete for the trust and belief of the people based on its own merits.

Central banks also began engaging in propaganda campaigns declaring the end of gold’s monetary role. However, their actions rang louder than their words as they continued to accumulate and hold gold, a practice they continue to this day. Gold remains the exclusive instrument of final settlement between central banks. Strategically, holding large gold reserves also makes sense for central banks since they can opt to sell reserves into the market should gold start to appreciate too quickly and threaten the value of fiat money. With their monopoly position protected and reinforced by legal tender laws, propagandists and sufficient control of the gold market central banks were free to print money at will. This exorbitant privilege gives central banks extraordinary power and made them extremely dangerous entities. In the words of former US President Andrew Jackson spoken at the Constitutional Convention in 1787:

**“I believe that banking institutions are more dangerous to our liberties than standing armies. If the American people ever allow private banks to control the issue of their currency, first by inflation, then by deflation, the banks and corporations that will grow up around them will deprive the people of all property until their children wake up homeless on the continent their fathers conquered. The issuing power should be taken from the banks and restored to the people, to whom it properly belongs.”**

Unlike to the flow restrictions associated with gold mining, there are practically no economic restraints preventing a government from printing more fiat money. Since there is virtually no cost associated with producing additional units (no skin in the game), government fiat money is the softest form of money in the history of the world. Predictably, money supplies grew quickly, especially in the heat of warfare. In the past, for societies operating with hard money systems, once the tide of war had shifted in favor of one belligerent over the other, treaties were quick to be negotiated as war is an extraordinarily expensive endeavor. The fiat money printing press, on the other hand, gave governments the ability to tap the aggregate wealth of entire populations to finance military operations by implicitly taxing them via inflation. This provided a more secretive, implicit method of funding warfare than explicit taxation or selling government wartime bonds. Wars began lasting much longer and became more violent. It is no coincidence that the century of total war coincided with the century of central banking:

**Table 5.1 Conflicts steadily cost more in human lives**

Period	Conflict-related deaths (millions)	World population, mid-century (millions)	Conflict-related deaths as share of world population (%)
Sixteenth century	1.6	493.3	0.32
Seventeenth century	6.1	579.1	1.05
Eighteenth century	7.0	757.4	0.92
Nineteenth century	19.4	1,172.9	1.65
Twentieth century	109.7	2,519.5	4.35

As is to be expected, soft government money has an abysmal track record as a store of value. This becomes abundantly clear when we look at its inflationary effects on the price of gold. An ounce of gold in 1971 was worth \$35 USD, and today is worth over \$1,200 USD (a decrease of over 97% in the value of each dollar due entirely to inflation). Based on these figures, it is easy to see that gold continues to appreciate as its supply is increased less quickly than the supply of \$USD (government fiat money). The constantly increasing supply of government money means its currency depreciates continuously, as wealth is stolen from the holders of the currency (or assets denominated in it) and transferred to those who print the currency or receive it earliest. This transfer of wealth is known as the *Cantillon Effect*: the primary beneficiaries from expansionary monetary policy are the first recipients of the new money, who are able to spend it before it has entered wider circulation and caused prices to rise. Generally, this is why inflation hurts the poorest and helps the bankers, who are closest to the spigot of liquidity (the government fiat money printing press) in the modern economy. A centrally planned market for money like this completely contradicts the principles of free market capitalism.

### Free Market Capitalism versus Socialism

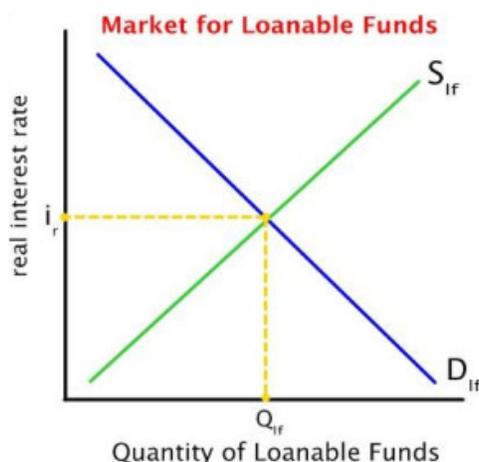
In a socialist system, the government owns and controls all means of production. This ultimately makes the government the sole buyer and seller of all capital goods in its economy. Such centralization stifles market functions, like price signals, and makes decision making highly ineffective. Without accurate pricing of capital goods to signal their relative supply, demand and relevant market conditions, there is no rational way to determine the most productive allocation of capital. Further, there is no rational way to determine how much to produce of each capital good. Scarcity is the starting point of all economics and people's choices are meaningless without skin in the game in the form of price or trade-offs. A survey without a price would find that everyone wants to own a private island but when price is included, very few can afford to own a private island. The point here is not to trumpet free market capitalism over socialism, but rather to clearly explicate the difference between the two ways of allocating resources and making production decisions:

- Free Market Capitalism places trust in Price Signals
- Socialism places trust in Centralized Planning

A free market is one in which buyers and sellers are free to transact on terms determined solely by them, where entry and exit into the market are free and no third parties can restrict or subsidize any market participants. Most countries today have well-functioning, relatively free markets. However, every country in the world today engages in centralized planning of the *market for money* (aka the market for financial capital) itself.

**No country in the world today has a free market for money, which is the most important market in any economy.**

In a modern economy, the market for money consists of the markets *loanable funds*. These markets match savers with borrowers using the interest rate as their price signal. In a free market for loanable funds, the supply of loanable funds rises as the interest rate rises, as more people are willing to loan their savings out at a higher price. Conversely, the demand for loanable funds decreases as the interest rate rises, as less people are inclined to borrow funds at a higher price:



Notice that the interest rate in a free market for capital is always positive because of people's naturally positive time preference, meaning that no one would part with money unless they could receive more of it in the future. These natural market forces are artificially manipulated in every market for money in the world. All markets for money in the world today are centrally planned by central banks, who are responsible for "managing" the market for loanable funds using monetary policy tools. Since banks today also engage in fractional reserve banking, they lend out not only customers' savings, but also their demand deposits (monies available to customers on demand, like checking accounts). By loaning out demand deposits to a borrower while simultaneously keeping them available to the depositor, banks can effectively create new, artificial money (a part of the money creation process from earlier). Central banks have the power to manipulate the market for financial capital and can artificially increase the money supply by:

- Reducing interest rates, which increases demand for borrowing and money creation by banks

- Lowering the required reserve ratios, allowing banks to lend more money out than their capital reserves justify
- Purchasing government debt or other financial assets with newly created money in the open market
- Relaxing lending eligibility criteria, allowing banks to increase lending activities and money creation

In a free market for money, the exact amount of savings equals the exact amount of loanable funds available to borrowers for the production of capital goods. This is why the availability of capital goods, as we saw with Harold and Louis, is inexorably linked to a reduction in consumption. Again, scarcity is the starting point of all economics, and its most important implication is the notion that all decisions involve tradeoffs.

**In the free market for money, the opportunity cost of saving is foregone consumption, and the opportunity cost of consumption is foregone saving – an indisputable economic reality.**

No amount of centralized planning can alter this fundamental economic reality. This is why centrally planned markets always suffer from distortions (aka bubbles, surpluses or shortages) as political agendas run up against the underlying free market forces. Undeterred, central banks continually attempt to “manage” these market forces to achieve politically established policy goals. Most often, central banks are trying to spur economic growth and consumption, so they will increase the supply of loanable funds and lower the interest rate. With the price of loanable funds (the interest rate) artificially suppressed, producers take on more debt to start projects than there are savings to finance these projects. These artificially low interest rates don’t provide any benefit to the economy, rather they simply disseminate distorted price signals that encourage producers to embark on projects which cannot realistically be financed from actual savings. This creates a market distortion (in other words, blows up another bubble) in which the value of consumption deferred is less than the value of the savings borrowed. This distortion can persist for some time but will inevitably unwind with disastrous consequences as economic reality cannot be fooled for long.

The excess supply of loanable funds, backed by no actual deferred consumption, initially encourages producers to borrow as they believe the funds will allow them to buy all the capital goods necessary for their project to succeed. As more producers borrow and bid for the same amount of capital goods, inflation sets in and prices begin to rise. At this point, the market manipulation is exposed since the projects become unprofitable after the rise in capital good prices (due to inflation) and suddenly begin to fail. Projects like these would not have been undertaken in the first place absent the distortions in the market for money created by central banks. An economy-wide simultaneous failure of overextended projects like this is called a *recession*. The boom and bust *business cycle* we have all grown accustomed to in the modern economy is an inevitable consequence of this centrally planned market manipulation. The United States and Europe saw a great illustration of this process when the dot-com bubble of the late 1990s was replaced by the housing bubble of the mid-2000s.

**Free market capitalism cannot function without a free market for money.**

As with all well-functioning markets, the price of money must emerge through the natural interactions of supply and demand. Healthy markets require functional nervous systems, as market participants must have accurate price signals to make decisions effectively. Basic economics shows us clearly that central bank meddling in the market for money is the root cause of all recessions and the business cycle. By imposing an artificial price, in this case the interest rate on loanable funds, central banks inhibit natural price signals which coordinate allocation decisions among savers and borrowers. Their market manipulation creates market distortions and recessions. Attempting to remedy a recession by injecting more artificial liquidity into the system will only exacerbate the distortions which caused the crisis in the first place and blow up new bubbles. Only central planning of a soft money supply and its pricing mechanism can cause widespread failures in an economy like this, as an economy based on hard money remains firmly rooted in economic reality and resists market distortions.

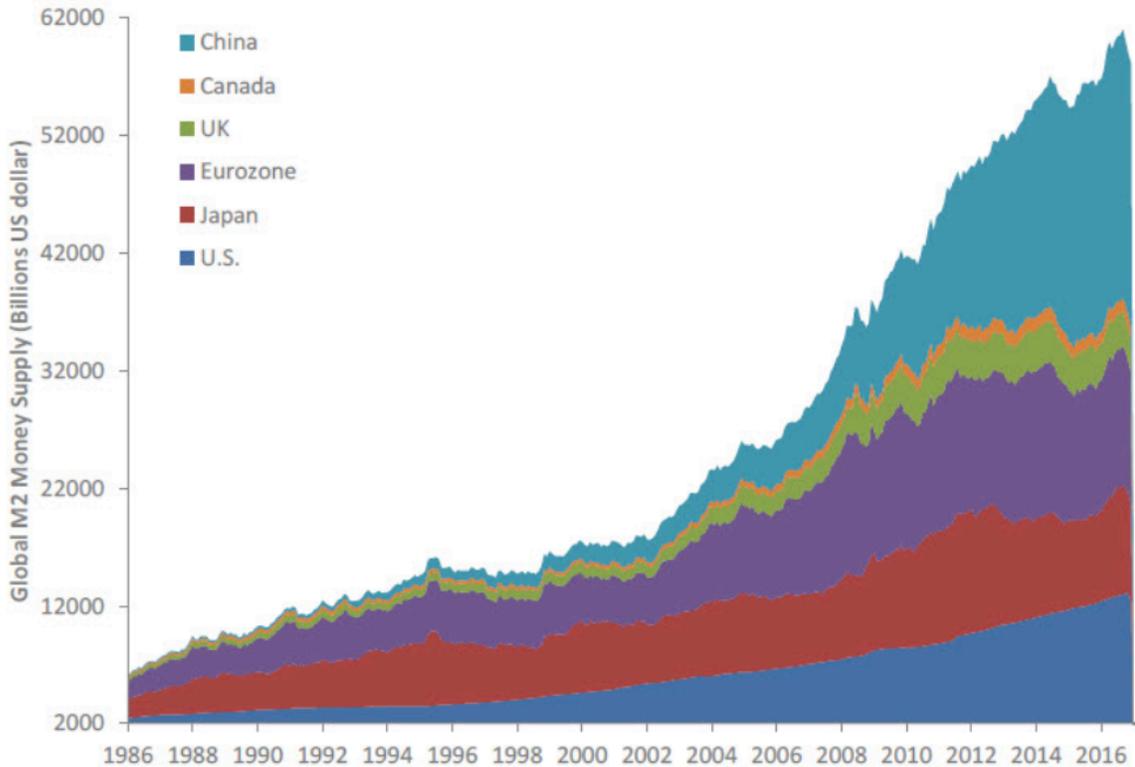
**Alignment with natural market forces like supply, demand and the price signal is the principal reason free market capitalism prevailed over socialism.**

### Failure of Government Fiat Money

Seeing that governments have been forced to use coercive measures, such as confiscating gold and implementing legal tender laws, to enforce adoption of fiat money is a clear indication that soft money is inferior and doomed to fail in a free market. This severe inadequacy of government fiat money came to the forefront of global consciousness in the wake of the Great Recession that began in 2008. Due to gigantic market distortions driven by artificially low interest rates and credit ratings agencies with no skin in the game, US subprime real estate became the largest bubble in modern history. When it bursts, its affects were globally systemic, and central banks all over the world (predictably) began increasing their money supplies in an attempt to reflate their broken economies.

Instead of calling it what really is, central banks now deceptively refer to the act of printing money as *quantitative easing*. As we have learned, increasing the money supply creates no real economic value, it only causes market distortions and furthers the misallocation of capital. Injecting liquidity into an economic system experiencing a recession only provides illusory, temporary relief. Printing money delays and exacerbates the inevitable correction, as economic reality cannot be deceived forever. Despite economic reality, central bank market manipulation is worse than ever.

Here we show the amount of government fiat money printed by the largest economies of the world since 1986:



It was in the depths of the Great Recession that an anonymous individual named Satoshi Nakamoto introduced the open-source software project called Bitcoin to an online group of cryptographers. Many attempts at creating a digital cash had been made over the previous twenty years but none had succeeded. Initially, few in the group took Bitcoin seriously. However, Nakamoto was eventually able to convince a few other cryptographers to join and the Bitcoin network was born.

After ten years of virtually perfect operation, the Bitcoin network has gone from \$0 to \$80B in value stored on its network and has cleared \$1.38T in total transactions. It is clear that this monetary technology is now competing successfully in the marketplace and is being used by many for real world purposes.

## BITCOIN

### The Simple Truth about Bitcoin

Bitcoin is the hardest form of money ever invented. It has successfully brought the advantages of physical cash money into the digital realm. Bitcoin is changing the way people organize themselves. The next chapter in the story of money is being written in a new language...

### Grasping Bitcoin

Bitcoin seems easy to understand at first (it's just magic internet money, right?), however truly grasping its significance is a formidable task. Once you think you have Bitcoin figured out, you'll see it from another perspective and realize how little you actually knew. This pursuit of understanding Bitcoin is like a mountain climber that continually encounters false peaks, which fool him into thinking he has reached the summit, only to realize it is higher still.

It has been said that you can judge the quality and importance of an idea by the vehemence of its opposition. Bitcoin has been called many things – digital gold, tulip mania 2.0, financial revolution, the MySpace of cryptocurrencies, environmental disaster, rat poison squared, libertarian idealism, apex predator of monetary technologies, the biggest bubble in history, the model-T of cryptocurrencies, a superior species of money – but it turns out that, in context of the history and nature of money, Bitcoin appears to be a distinct evolutionary leap forward. Bitcoin is not an internet application like MySpace, it is an internet protocol. Bitcoin is not the model-T of cryptocurrencies, it is a more like a global freeway system. Bitcoin is not like any type of gold coin, Bitcoin is more like the element gold. Its integrity is protected by the inviolable laws of mathematics. Human nature is one of its core components. It is a new form of social institution. Bitcoin is a living system unto itself that adapts to environmental changes.

This may sound mind blowing at first. Most innovations of this magnitude sound this way in the beginning as we struggle to communicate using outdated terms and analogies that cannot possibly convey their importance. However, history shows us that ignoring innovation is a terrible strategy. In light of its inherent complexity and novelty, we will view Bitcoin from many different perspectives in an attempt to create a mosaic of understanding in the minds of our readers. First and foremost, Bitcoin is *digital cash money*.

### Digital Cash Money

As the global economy becomes increasingly digitized and interconnected, new technological realities are taking shape which will cause the market to naturally select for the most effective species of money native to this new digital terrain. Bitcoin is the first truly digital solution to the problem of money. It is the world's first digital cash (in the original sense of the word cash discussed earlier) meaning that it is under the full control of its owner and can be used for final settlement in the same way as gold is today. Put another way, Bitcoin is digital cash money, a self-sovereign asset that contains within it all the trust factors and permissions necessary to transact with it. Bitcoin is not the liability of any counterparty, hence its nickname – digital gold.

Like gold, Bitcoin is a supranational form of money, meaning that no government needs to decree its value or permit its use, nor can it be eliminated unilaterally by regulation. The hardness of Bitcoin is superior to all forms of money, including gold, and its stock-to-flow ratio will eventually reach infinity. As a digital asset, Bitcoin has unprecedented levels of salability across scales, space and time. It is resistant to confiscation, censorship, inflation and counterfeit. Meritoriously, Bitcoin's value is attained entirely from the social consensus it earns by competing freely in the marketplace.

As one perspective of its monetary significance, Bitcoin can be understood as the successful fusion of the advantages associated with physical cash payments with the efficiencies and certainties enabled by digital technology. Cash payments have the advantage of being immediate, final and requiring no trust on the part of either transacting party in each other or any other intermediary. The drawback of cash payments was the need for transacting parties to be physically present in the same space and time, which increases risks associated with physical custody, especially for larger transactions. As more business is conducted remotely, thanks to ever-advancing telecommunications technologies like the internet, physical cash transactions become increasingly impractical.

Since the inception of computers, the nature of all digital objects is that they were infinitely replicable. This meant that no digital object could be provably limited in quantity. For instance, when you "send" an email, you are actually sending a copy, as you still have the email in your sent folder. Before Bitcoin, there was no way to send a digital good that could not also be resent elsewhere at a later time. This presented an intractable issue for direct digital payments known as the *double-spend problem*. Without a trusted third-party intermediary to verify the payer was not double spending, digital payments were not possible. Using intermediated digital payments (like Venmo or PayPal) exposed parties to additional transaction costs, risk of censorship, fraud and transaction disputes.

The nature of digital objects also meant creating a digital cash was impossible, since its monetary units could be reproduced endlessly and would therefore suffer from unlimited inflation. Before Bitcoin, people had to rely on physical laws (rarity and chemistry, in the case of gold) or jurisdictional laws (government and central bank monopolies) to regulate money supplies. Innovatively, Bitcoin relies on mathematical laws to protect its monetary policy. Building on top of decades of innovative trial and error by other programmers and combining a wide range of proven technologies, Nakamoto successfully made Bitcoins the first digital objects that were verifiably scarce. As the world's first instance of *digital scarcity*, Bitcoin was able to solve the double-spend problem and become the world's first functional digital cash.

**"That in order to make a person covet a thing, it is only necessary to make the thing difficult to attain." – Mark Twain**

In this way, Bitcoin would bring the desirous advantages of physical cash to the digital realm and combine them with an immutable monetary policy that cannot be manipulated to benefit any outside party at the expense of Bitcoin holders. Drawing on lessons learned by other

programmers during two decades of attempts at this innovative breakthrough, Nakamoto finally achieved digital cash money by combining four key technologies:

- Proof-of-Work – mathematical puzzles which require energy expenditure to be solved, solutions are rewarded with newly issued Bitcoin and user transaction fees, functions as the skin in the game necessary to keep Bitcoin’s distributed ledger truthful and maintain its monetary hardness
- Distributed peer-to-peer network – a record of Bitcoin’s entire transaction history is maintained by each network participant (known as a node) who mathematically verify each other’s work, making the entire system resistant to censorship and manipulation
- Hashing – a method of computer cryptography that transforms any stream of data into dataset of fixed size (known as a hash), this transformation is irreversible and is the foundation of trustless verification within the Bitcoin network
- Digital Signatures – a method of authentication that relies on a set of mathematically related elements called the private key, the public key and signatures – the private key (which must be kept secret) allows its holder to control the Bitcoin associated with it, meaning that the private key is a bearer instrument (holding Bitcoin is holding its private key, which makes it a self-sovereign monetary good like gold)

In the same way a monetary assessment of gold would not delve too deep into its chemical properties, this essay will not delve too deep into the technological properties of Bitcoin. We will instead focus on its monetary properties and its relevance in the story of money. However, some basic technical knowledge of Bitcoin is warranted to fully appreciate the importance of the innovation that is digital cash money.

### Technological Properties

Bitcoin is *open-source software*, meaning its source code can be inspected by anyone. This makes Bitcoin a language, its source code and transaction history are universally transparent and can even be printed onto paper (interestingly, this makes it protected under the First Amendment in the United States, more on this later). As an open-source software project, Bitcoin is supported by a global network of volunteer programmers. These programmers are self-interested in the sense that they are almost always Bitcoin owners as they are aligned with its purpose philosophically, and therefore stand to gain financially from its expanding network. Their work over the years has greatly enhanced the functionality of the Bitcoin network. However, these programmers are unable to change the rules of Bitcoin (as we will see when we discuss Bitcoin’s social contract).

To become a Bitcoin network member, known as a *node*, all that is necessary is to download and run the software on a computer. Once downloaded, the software will enable you to store Bitcoin and transact it with any other node in the world. Also, by becoming a node, the entire Bitcoin transaction history will be recorded on your machine and updated in perpetuity, just as it is on every other node in the world. This is the essence of Bitcoin’s *decentralized architecture*. The Bitcoin network, similar to the internet, lives *everywhere and nowhere*.

Owning a Bitcoin means owning the private key that can authorize it to be used in a transaction. The private key is purely informational, meaning that it is just a string of alphanumeric characters. This makes it a self-sovereign form of money, giving its holder the presumption of rightful ownership, which makes Bitcoin an instrument of final settlement (like gold). Bitcoin is the world's first global, digital final settlement system.

The core operational feature of Bitcoin is verification, which allows its users to remove the need for trust completely. Every transaction has to be recorded by every node on the network so that they all share one common ledger of balances and transactions (remarkably similar to the Rai Stone system used by the Yap Islanders). Transactions are grouped together approximately every ten minutes in what is known as a *block*. Each block is then added to the previous block of transactions, forming a chronological chain of inextricably linked blocks that stretches all the way back to the genesis block mined by Nakamoto himself exactly 10 years ago today. This is commonly called the Bitcoin *blockchain*. The blockchain is the common ledger of which each node maintains its own copy (commonly known as the distributed ledger). Each node verifies the accuracy of every other node's transaction inputs and truth is established by consensus. In this way, the Bitcoin network relies 100% on verification and 0% on trust. This gives Bitcoin the unique property of *trustlessness*, meaning it is able to operate successfully without the need to trust any counterparty or intermediary whatsoever.

### Blockchain, Energy and Mining

Economic incentives and disincentives are used to maintain truthful records in the blockchain, it what is an ingenious application of the skin in the game concept. Nodes compete to solve complex mathematical puzzles in a process called *proof-of-work*. Nodes are incentivized to perform this computing task because the first one to solve the proof-of-work is awarded a batch of newly issued Bitcoin and the transaction fees generated within the latest block of transactions – called the *block reward*. A block is sealed approximately every ten minutes, which triggers the opening of the next block and proof-of-work competition. Nodes expend processing power (in the form of electricity) to solve these complicated mathematical problems, although considerably less and much more efficiently than the systems that support gold and government money today:

	Annual Cost (\$USD)	Energy Consumption (GJ)	\$USD per GJ
Gold Mining	\$ 105,000,000,000	475,000,000	\$ 221
Gold Recycling	\$ 40,000,000,000	25,000,000	\$ 1,600
Government Fiat Money Production	\$ 28,000,000,000	39,000,000	\$ 718
Banking System	\$ 1,870,000,000,000	2,340,000,000	\$ 799
Governments	\$ 27,600,000,000,000	5,861,000,000	\$ 4,709
Bitcoin Mining	\$ 4,500,000,000	183,000,000	\$ 25

Proof-of-work energy expenditure is the thermodynamic bridge from the physical to the digital world. It transmutes the fundamental commodity of the universe, energy, into digital gold. This energy expenditure is essential to the functioning of the Bitcoin network, as it disincentivizes node dishonesty. If a node attempted to include a fraudulent transaction in a

block, other nodes would reject it and it would incur the cost of processing power without the prospect of earning the block reward. This process is commonly referred to as *mining* and the competing nodes are called miners (or mining nodes). Mining is a truly capitalistic voting mechanism where energy expended equals hashes, which are votes for the proof-of-work solution, generated. The name mining is an ode to the arduous process of mining of gold. As we have learned, the costs and risks related to the mining of this monetary metal is necessary for it to maintain its hardness (skin in the game). Similarly, mining using proof-of-work is the only known method of creating digital cash money.

Money, which is the representation of the work required to generate goods, can also be considered a form of stored energy. In the early 20th century, free market proponents like Henry Ford and Thomas Edison were interested in replacing gold or the US dollar with an energy money. Showing great prescience, they foresaw the day when the world may exhaust its non-renewable energy sources and be forced to switch to alternatives. Convicted in their free market beliefs, they shared this idea and assumed a great deal of reputational risk in the process, as their views ran contrary to the established economic order. The concept of energy money was popular due to its hard money characteristics, as energy is costly to produce. However, energy money was technologically well before its time, as energy could not be transmitted or stored easily using technologies of the day. In championing a novel idea with the greater good at heart, Ford and Edison were exhibiting *soul in the game*, or the exposure to downside risks on behalf of others. As Edison said in 1931:

“I’d put my money on the sun and solar energy. What a source of power! I hope we don’t have to wait until oil and coal run out before we tackle that.”

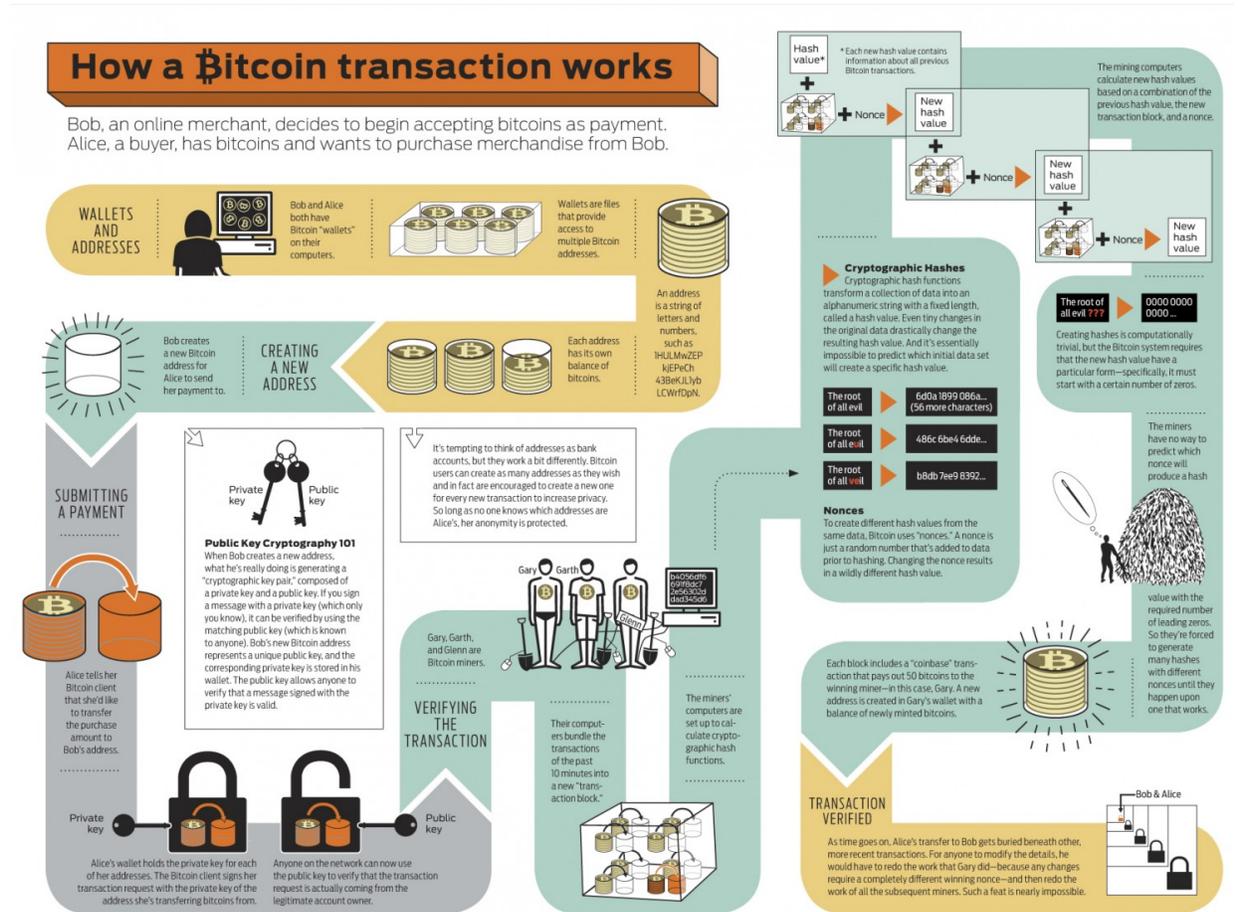
By using proof-of-work, which was originally invented as a measure to mitigate email spam, Bitcoin became the world’s first functional energy money. With physical monetary goods, we were required to build walls to safeguard our money. With the Bitcoin network, we are required to expend energy to preserve the sanctity of its ledger, secure its network and enforce the immutability of its money supply. Proof-of-work is essential for Bitcoin to function as hard, digital cash money and enables it to serve as the buyer of last resort for electricity worldwide. The Bitcoin network provides a perpetual economic incentive for everyone in the world to invent more efficient methods of harnessing energy. This global incentive will increase the rate of innovation in energy technologies. As Bitcoin expert Nic Carter puts it:

“The Bitcoin network is a global energy net that liberates stranded assets and makes new ones viable. Imagine a 3D topographic map of the world with cheap energy hotspots being lower and expensive energy being higher. I imagine Bitcoin mining being akin to a glass of water poured over the surface, settling in the nooks and crannies, and smoothing it out.”

As more nodes compete to solve the proof-of-work puzzle, the difficulty automatically increases so that new blocks are added on average once every ten minutes. This automatic algorithmic change is called the *difficulty adjustment* and is perhaps the most ingenious aspect of Bitcoin. It is the most reliable engineering solution for making and keeping money maximally hard and gives Bitcoin the unique ability to adapt its network security as it grows.

As we have seen, when a form of money appreciates, people are immediately incentivized to increase its new supply flow, which reduces its stock-to-flow ratio and compromises its hardness. With Bitcoin, an increase in its price does not lead to the production of more Bitcoin beyond its transparent and predictable supply schedule. Instead, it simply leads to an increase in processing power committed by miners which in turn makes the network more secure and difficult to compromise. Like a vault that becomes harder to crack the more money that is stored within it, Bitcoin offers people an incredibly effective means of value storage.

Next, we depict the entire process of a Bitcoin transaction:



## The Internet of Value

“The internet of value” is a popular moniker to describe Bitcoin. In reality, the Bitcoin *protocol* can be considered an integral and newly evolved layer of the commercial internet. In computer science, a protocol is a ruleset that governs the transmission of data. The internet as we know it is an integration of four successive layers of open-source protocols, called the Internet Protocol Suite, that maintain constant communication with one another:

- The Link Layer puts data packets on the wire

- The Internet Layer routes data packets across networks
- The Transport Layer persists communication across any given conversation
- The Application Layer delivers software files and applications

In this context, Bitcoin can be considered the fifth layer of the internet protocol suite:

- The Value Layer allocates scarce resources across networks

In the same way the internet is a set of open-source protocols for exchanging data, Bitcoin is an open-source protocol for exchanging value. It is trustless, as any machine can accept it from any other securely and at virtually zero cost. Bitcoin is also global and *permissionless*, meaning that any machine can speak its language and no central bank is required to authorize its use. This means that transactions on its network are essentially unstoppable as all trust factors and permissions necessary to transact with it are intrinsic to the act of holding a Bitcoin private key. Software protocol developments are being implemented that will make Bitcoin transactions even faster, cheaper, anonymous and capable of authentication. These can expand the utility of Bitcoin to enable the allocation of scarce network resources like computing power, verification of contracts or tracking identity and reputation.

Although Bitcoin is the fifth layer of the internet protocol suite, it is the base layer protocol for the value layer itself. This means that second and other higher order protocol layers may be built on top of it. A second layer protocol to Bitcoin, called the Lightning Network, is currently being implemented and is designed to sacrifice some degree of trustlessness to achieve higher transaction throughput, allowing Bitcoin to be used more effectively as a medium of exchange. The Lightning Network is an open-source protocol and functions by establishing trust channels among parties for faster, cheaper transactions that are then settled periodically to the Bitcoin blockchain. Higher order protocol development and integration is one of the many ways Bitcoin adapts to changes in its environment (more on this later).

In the same way that money is an emergent property of complex human interactions, Bitcoin is an emergent property of complex interactions occurring between people, machines and markets. Even if Nakamoto and Bitcoin never existed, it would still be necessary for us to invent the concept of cryptoassets to enable machines to exchange value to facilitate digital economies, use smart contracts and provide the substrate necessary for the 'internet of things' to come into existence. Not only is Bitcoin a prerequisite innovation to the digital economy, it is also the hardest monetary technology ever invented.

### The Infinite Hardness of Bitcoin

Bitcoin is the hardest form of money in existence. Its money supply is enforced mathematically and, like the other rules of Bitcoin, cannot be broken or changed. Only 21 million Bitcoins can and will ever exist:

$$\frac{\sum_{i=0}^{32} 210000 \left\lfloor \frac{50 \cdot 10^8}{2^i} \right\rfloor}{10^8}$$

The monetary policy of Bitcoin is set in (mathematical) stone.

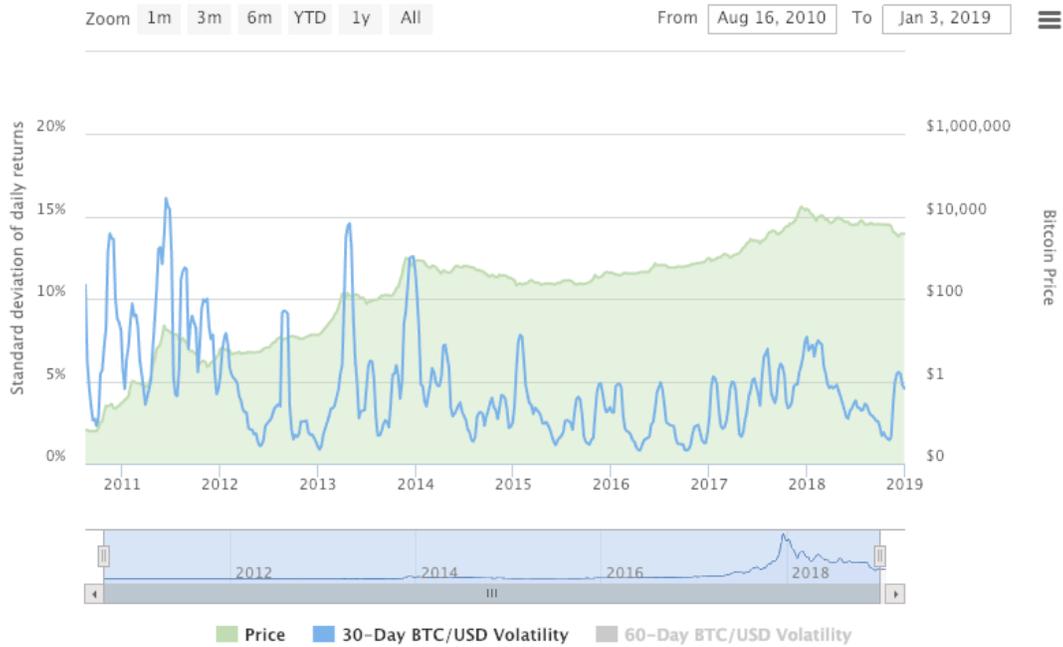
This strictly limited supply makes it the first monetary technology exhibiting *absolute scarcity*. Unlike gold and other monetary metals, no matter how much demand for Bitcoin increases there will never be any units produced in excess of its fully transparent, predictable and unchangeable monetary policy.

**Before Bitcoin, only time itself had achieved the property of absolute scarcity.**

Since increased demand for Bitcoin cannot affect its supply, it can only be expressed in its price. Bitcoin has perfect *price inelasticity of supply*, meaning that it has zero supply-side response to increases in its price. Unlike gold and all other physical commodities, where an increase in demand will inevitably lead to larger supplies being produced over time, Bitcoin can only express an increase in demand by becoming more expensive (and a more secure network). A perfect price inelasticity of supply no doubt contributes to the notorious price volatility of Bitcoin it is exhibiting at the earliest stages of its growth we are witnessing today.

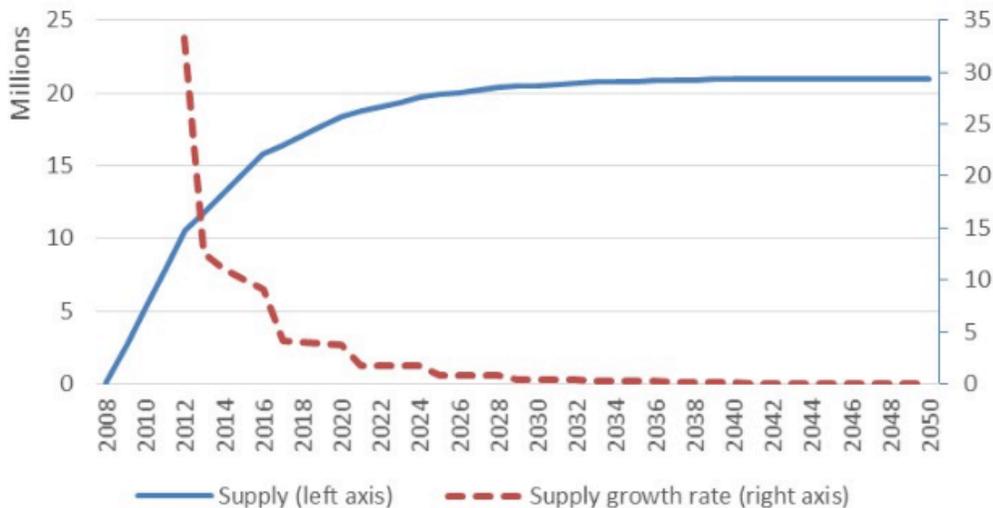
Absolute scarcity greatly exacerbates Bitcoin's price volatility. As its network continues to grow, the value of Bitcoin as an unstoppable payments channel and uninflatable money is steadily increasing over time while its price is constantly attempting to find it, dramatically overshooting and undershooting along the way. With a totally inflexible supply schedule, as long as Bitcoin is growing quickly, its price will behave like that of a startup company stock undergoing meteoric growth. Should Bitcoin achieve sufficient market penetration that its growth slows down, it would stop attracting high-risk investment flows and become a stable monetary asset expected to appreciate slightly each year as demand increases due to productivity and population growth – like any mature hard money should. As expected, over the long-run we are already seeing a decrease in Bitcoin's price volatility:

### Bitcoin Price and Volatility



Bitcoin’s immutable monetary policy ensures that its supply will continue to grow at a decreasing rate and will reach its maximum of 21 million units sometime in the year 2140. To maintain salability across scales, Nakamoto designed each Bitcoin to be further divisible into 100 million units, which are now commonly called Satoshis in his honor. Once the last Bitcoin is mined, its stock-to-flow ratio will become infinite as its flow will completely and irreversibly cease. Beyond this point, miners will be compensated exclusively by transaction fees. Bitcoin’s decreasing growth rate means that the first 20 million coins will be mined by the year 2025, leaving the last 1 million to be mined over the subsequent 115 years:

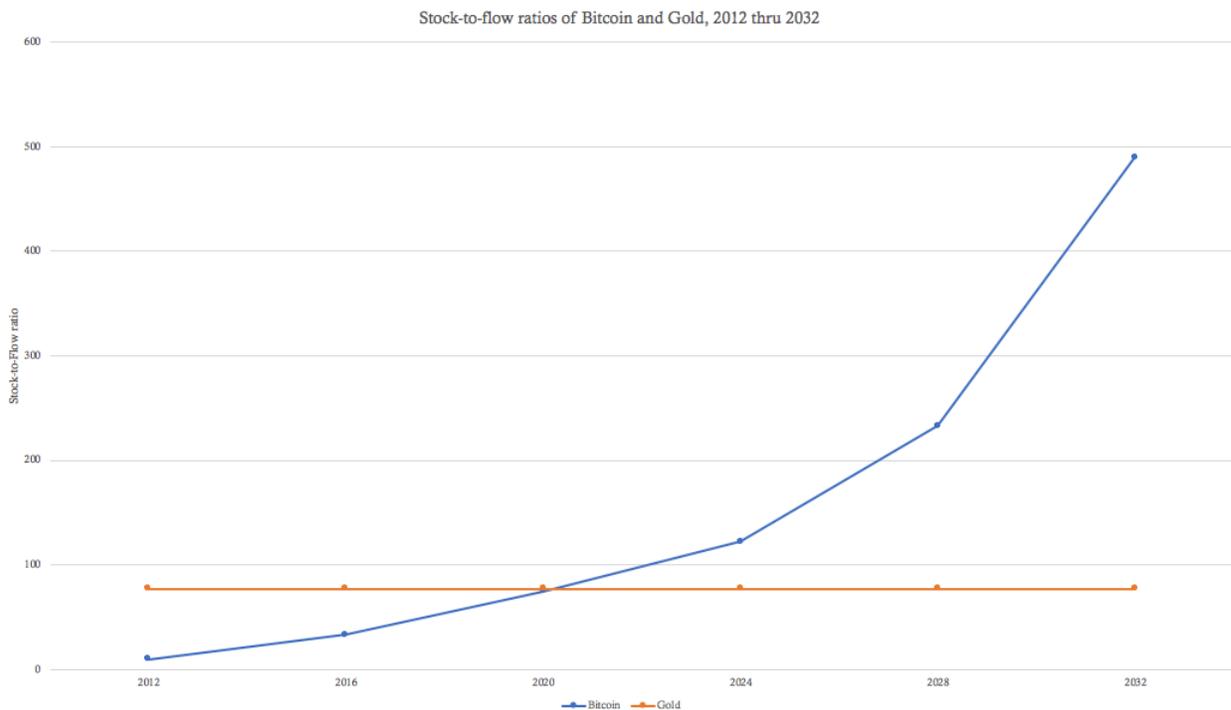
### Bitcoin supply and growth rate



This predictable, transparent and immutable supply schedule gives Bitcoin a significant advantage as it competes for the trust of the people to become a reliable store of value. Unlike government money or even gold, people know with absolute certainty that Bitcoin will never have its salability across time compromised by unexpected supply increases.

**Bitcoin is uninflatable money in a world where wealth is continuously stolen via inflation.**

As is the case with its other immutable laws, Bitcoin’s monetary policy is enforced by the inviolable laws of mathematics. Inevitably, Bitcoin will surpass gold around the year 2020 to become the hardest form of money in history:



By virtue of its natively digital nature, Bitcoin is (critically) highly resistant to centralization. As we have learned, it was the centralization of gold that led to government money backed by gold, which made gold more salable across scales and encouraged a gold standard to flourish throughout most of the world. However, as the temptation to expand money supplies seems to be irresistible for humans, governments soon took control of the banking sector, printed money in excess of its gold reserves, eventually severed their currencies peg to gold and thereby destroyed the hardness of government money completely.

Historically, people who adopted hard money systems flourished – such as the Romans under Caesar, The Byzantines under Constantine and the Europeans under the gold standard – and people who had the hardness of their money compromised suffered enormous consequences – such as the Yap Islanders, West Africans using glass beads and the Chinese under a silver standard in the 19<sup>th</sup> century. Moving a society away from a hard money system has been a

harbinger of economic crisis and societal decay, an outcome that can be explained as a social contract rescission.

### Bitcoin's Social Contract

Social contract theory starts with an assumed hypothetical state of nature full of violence that is unbearable for people to live in. Driven by a desire to improve their circumstances, people come together and collectively agree to sacrifice some of their freedoms to establish a *social contract* and empower an institution to protect them. Government is the result of a social contract: people sacrifice some of their freedoms to give the state control over the monetary system and armed forces. The state, in turn, uses that power to manage the economy, redistribute wealth and fight crime. In the United States, our current social contract grants the government monopoly control of money (via the Federal Reserve) and violence (via the Police and Military).

Similarly, money itself can be thought of as a social contract. If enough people are unhappy with a barter economy, they can collectively agree to use money instead. This social contract entails sacrificing certainty (requiring trust that dollars will maintain their value over time) in exchange for convenience (using dollars as a medium of exchange). The social contract for money, as we have seen, emerges and evolves spontaneously based on market-driven natural selection. Each person continuously decides which outcomes they prefer and how best to achieve them. If enough people seek the same outcome, we call the result a social contract.

Throughout history, almost every government (a form of social contract) put in charge of the monetary system (another, often interrelated, form of social contract) has abused its power by forcibly confiscating assets, censoring private transactions and printing money to steal wealth via inflation. Using the virtually unlimited financial means provided by control over money supplies, these governmental social contracts grew in successive bureaucratic layers. The larger and more valuable these social contracts became; the more freedoms were forfeited and the more others sought control over them. This led to many instances of conflict (warfare or social revolution) in which old social contracts (dictatorships or tyrannical regimes) were rescinded in favor of new ones (new laws, treaties or governments). The principal point here is that people can agree they are in a terrible situation and come together to change it, but the resultant social contract is only as strong as its credibility and enforceability.

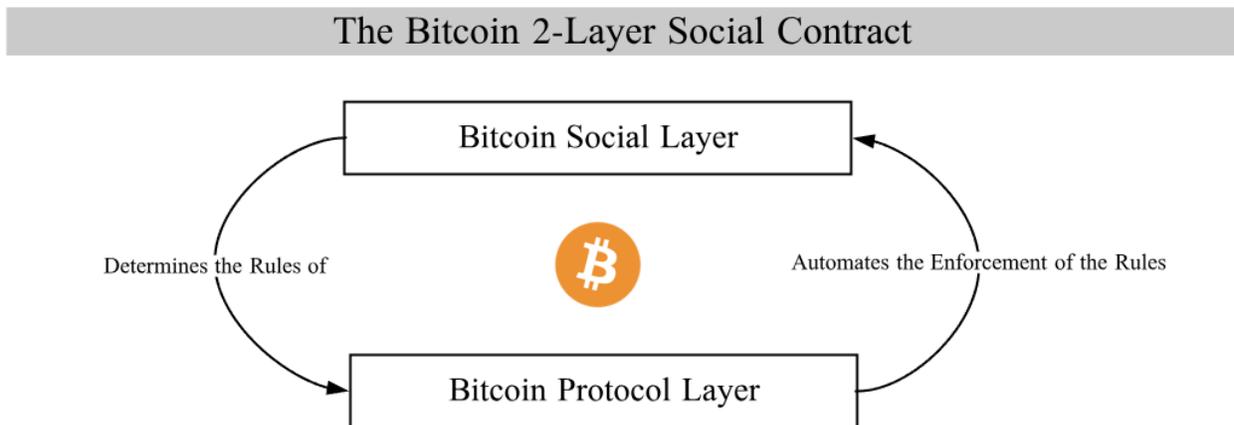
The invention of Bitcoin can be regarded as a new implementation of the social contract for money. Nakamoto settled on the following rules for this new implementation:

- Only the owner of a Bitcoin can produce the digital signature to spend it (confiscation resistance)
- Anyone can transact and store value in Bitcoins without permission (censorship resistance)
- There will only be 21 million Bitcoins, issued on a predictable schedule (inflation resistance)
- Anyone will always be able to verify all the rules of Bitcoin (counterfeit resistance)

Historically, social contracts intended to protect people, such as governments and their central banks, eventually became controlling and ultimately turned abusive. When a social contract loses sufficient trust of the people, it falls apart or is overthrown, by ballot or by bullet. This dynamic has resulted in a continuous cycle of rising and falling social contracts throughout history. Bitcoin is intended to break this cycle in two ways:

- Instead of seeking security from a powerful central entity (like a government or central bank) that can be corrupted or overthrown, Bitcoin creates a hypercompetitive market for its own protection. It turns security into a commodity and the security providers (miners) into harmless commodity producers.
- By requiring its security market participants (miners) to incur real world costs to generate their economic reward (skin in the game), Bitcoin incentivizes the market to reach consensus over who owns what at any given point in time.

In this sense, the Bitcoin social contract is composed of two distinct, self-reinforcing layers: the social layer and the protocol layer. The social layer is the social consensus itself, which determines the rules of Bitcoin and establishes its value. The protocol layer simply automates the enforcement of the rules set by the social layer:



In this sense, Bitcoin is more than just a technology. Indeed, it is a new institutional form. Viewing it in this way, we are better able to answer some of the more existential questions about Bitcoin:

*Who Can Change the Rules of Bitcoin?*

Since the rules of the Bitcoin social contract are decided at its social layer and enforced at its protocol layer, who can actually change its rules? Bitcoin, as computer network, comes into existence when people run implementations that follow the same ruleset (think of these rulesets as speaking the same language). You remain in the network by following the same rules as everyone else. If you decided to change the ruleset on your local computer, you would simply be evicted from the network (you no longer speak the same language as everyone else).

Your unilateral decision to change the rules would not impact the actual Bitcoin network in any way whatsoever.

The only way to change the rules of the Bitcoin social contract is to convince people to voluntarily accept your proposed rule changes at the social layer. As each network member is self-interested, they will only adopt rules that benefit them. Seeing as its current rules are already optimal for Bitcoin holders (resistance to confiscation, censorship, inflation and counterfeit) it would be extremely difficult to convince a majority of the approximately 30 million network participants to change rulesets. This asymmetrical governance dynamic virtually rules out any contentious changes from succeeding, as they would never get broad social consensus. Therefore, the Bitcoin network can be upgraded in ways that align with the collective best interests of its members and is at the same time highly resilient to changes that contradict these interests.

### *Can a Software Bug Kill Bitcoin?*

In September 2018, a software bug arose in the main implementation of Bitcoin that opened up two potential attack vectors which theoretically could have been exploited to circumvent its counterfeit and inflation resistance properties. Bitcoin developers quickly fixed the bug before either vector was exploited, however this event left many people wondering what would have happened had the vulnerabilities not been discovered in time.

Any time the social layer and protocol layer diverge in the Bitcoin social contract, the protocol layer is always wrong. Again, all rules are set at the social layer whereas the protocol layer is only responsible for automating their enforcement. Had the software bug not been discovered in time, Bitcoin's blockchain would have undergone a *fork* – meaning its protocol layer would have been split into two networks, one with the bug and one without it. Every Bitcoin holder would then have an equal number of coins in each network, but the value of these coins would be determined solely by the free market. This is true for all forms of money, as social consensus determines the value of money. At the social layer, each Bitcoin owner would then choose either the implementation with or without the bug. To protect the value of their Bitcoin, holders would rationally choose to migrate to the mended network and its blockchain would continue without interruption.

When the Bitcoin protocol layer successfully automates the enforcement of the rules determined at its social layer, the two layers are in sync. If they diverge for any reason, the social layer supersedes, and the protocol layer is mended to reflect the economic reality of the social consensus surrounding Bitcoin. Software bugs are inevitable, and Bitcoin's 2-layer social contract construction ensures that it can withstand them.

### *Can Forks Compromise the Immutability of Bitcoin's Rules?*

Since Bitcoin is open-source software, anyone in the world can copy its code, change it and launch their own version. This is also a chain fork which, as established earlier, affects only the protocol layer of the Bitcoin social contract. Without changing the rules at the social layer first, a protocol layer fork only evicts you from the true Bitcoin network. To successfully

change the rules of Bitcoin, you must successfully fork its social layer first. To accomplish this, you would need to convince as many people as possible that your proposed ruleset is meaningfully better for them, so that they take the risk of adopting your proposed software changes. Forks like these are difficult to pull off in reality because they require buy-in from thousands of people to be successful. This asymmetry between the cost of campaigning for ruleset changes and their potential benefit to network participants makes the Bitcoin network exhibit an extremely strong status quo bias when it comes to governance.

The key to understanding this is that the value of any form of money is purely a social construct or, in other words, is derived from social consensus. Individual Bitcoins, like US dollars or any other currency, receive their value exclusively from the shared belief of their users. Forking Bitcoin's protocol layer is worthless without forking the social layer from which it derives its value. In the rare cases that the social layer itself splits, as was the case with the Bitcoin Cash fork, the result is two weaker social contracts, each agreed upon by fewer people than before. The complete failure of the Bitcoin Cash fork (its price has declined from 0.21 to 0.04 Bitcoin over the past year) is yet another battle scar for Bitcoin that pays testament to its governance model and exemplifies the winner take all dynamics inherent to monetary competition.

So long as Bitcoin network participants continue to act in accordance with their own individual self-interest, the rules of Bitcoin (resistance to confiscation, censorship, inflation and counterfeit) are immutable and, therefore, as reliable as the laws of mathematics. It's clear from this perspective that Bitcoin is more than just a technological innovation. Although Bitcoin as a network and monetary technology is groundbreaking in many respects, its social contract implementation is revolutionary. Bitcoin is the first technology that incorporates human nature as one of its core moving parts.

**In essence, by believing that mathematics and individual self-interest will persist, we can reliably believe in Bitcoin's value proposition and its ongoing successful operation.**

Over the past 10 years, by inventively aligning human self-interest with its own self-interest, the Bitcoin network has managed to grow organically from \$0 to \$80B in value.

### A New Form of Life

Although Bitcoin is intended to be a monetary technology, it is a totally unique compared to other forms of money. Ralph Merkle, famous cryptographer and inventor of the Merkle tree data structure, has a remarkable way of describing Bitcoin:

“Bitcoin is the first example of a new form of life. It lives and breathes on the internet. It lives because it can pay people to keep it alive. It lives because it performs a useful service that people will pay it to perform. It lives because anyone, anywhere, can run a copy of its code. It lives because all the running copies are constantly talking to each other. It lives because if any one copy is corrupted it is discarded, quickly and without any fuss or muss. It lives because it is radically transparent: anyone can see its code and see exactly what it does.

It can't be changed. It can't be argued with. It can't be tampered with. It can't be corrupted. It can't be stopped. It can't even be interrupted.

If nuclear war destroyed half of our planet, it would continue to live, uncorrupted. It would continue to offer its services. It would continue to pay people to keep it alive.

The only way to shut it down is to kill every server that hosts it. Which is hard, because a lot of servers host it, in a lot of countries, and a lot of people want to use it.

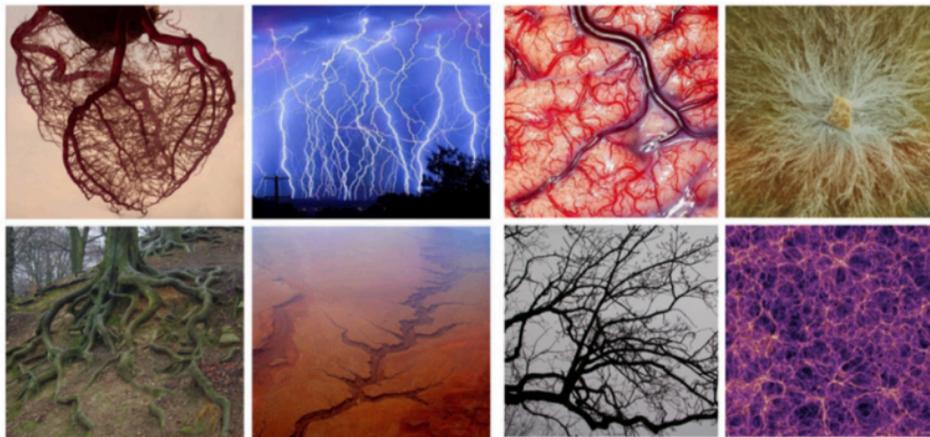
Realistically, the only way to kill it is to make the service it offers so useless and obsolete that no one wants to use it. So obsolete that no one wants to pay for it, no one wants to host it. Then it will have no money to pay anyone. Then it will starve to death.

But as long as there are people who want to use it, it's very hard to kill, or corrupt, or stop, or interrupt.”

Bitcoin is a technology, like the hammer or the wheel, that survives for the same reason any other technology survives: it provides benefits to those who use it. It can be understood as a spontaneously emergent protocol that serves as a new form of uninflatable money and an unstoppable payments channel. Structurally, the Bitcoin network reflects a quintessential manifestation commonly found in nature.

### The Decentralized Network Archetype

The Bitcoin network mirrors one of the most successful evolutionary structures found in nature, the *decentralized network archetype*:



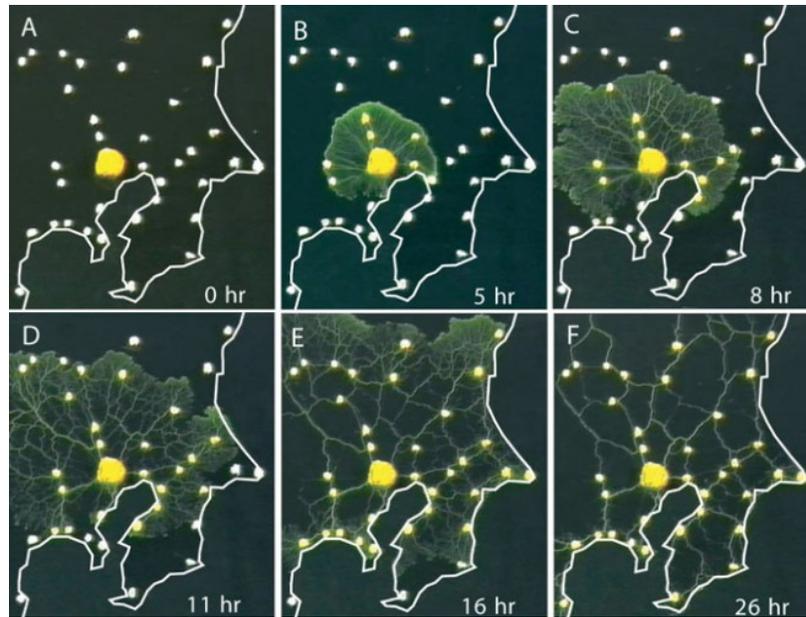
Clockwise from the top left: the human heart, lightning, the human brain, a fungal mycelium network, roots from a tree, an aerial view of the Grand Canyon, branches from a tree and a cosmic web of galactic superclusters in the deep Universe (which is the largest observable structure in the known Universe at over 1 billion lightyears across).

The decentralized network archetype is prevalent in nature because it is one of the most energy efficient structures possible. Energy is the fundamental commodity of the universe and nature always optimizes for its utilization. Atoms, bubbles and stars (in a state of equilibrium) always form spherical shapes, which is the most energy efficient form for minimizing surface area, precisely because they are energy conservation structures. Minimal surface area output per unit of energy input ensures that these structures optimally expend the finite energy of which they are composed. Spheres are figures of equilibrium with equal distribution their own inherent energy.

Conversely, decentralized networks always form in these tendrilled, circuitous and redundant shapes, which is the most energy efficient form of maximizing surface area, precisely because they are energy exchange structures. Maximal surface area output per unit of energy input ensures that these structures achieve the highest degree of spatial exposure to optimize the likelihood of successful exchange – whether their purpose is pumping blood, imbibing groundwater or seeking sunlight. Spheres and decentralized networks are antithetical in purpose and archetype. Decentralized networks are figures of disequilibrium which both disperse and gather energy within their environments. A decentralized form in organic systems confers advantages such as distributed intelligence, invulnerability to singular attack vectors and accelerated adaptivity.

**The decentralized network archetype found in nature is the antecedent to paradigm shifting innovations throughout history such as the railroad system, the telegraph, the telephone, the power distribution grid, the internet, social media and now Bitcoin.**

To illustrate the power of this natural archetype, let's consider the story behind the design of the Tokyo subway system. Scientists conducted an experiment where an ancient fungus, the slime mold, was incentivized to recreate the Tokyo subway system. Each subway stop (node) was marked with oat flakes, the favorite food of the slime mold. In a single day, the slime mold grew to connect all the subway stops in a more energetically efficient design than that proposed by the central planning committee of engineers who spent many months at great expense to the Japanese government in the design process:



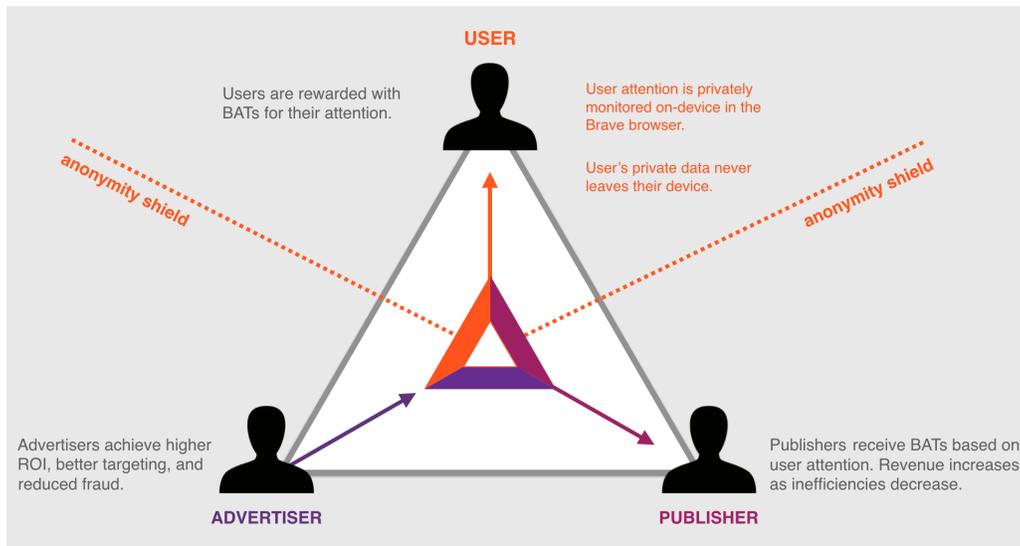
As the Scientists later reported:

“Transport networks are ubiquitous in both social and biological systems. **Robust network performance involves a complex trade-off involving cost, transport efficiency, and fault tolerance. Biological networks have been honed by many cycles of evolutionary selection pressure and are likely to yield reasonable solutions to such combinatorial optimization problems. Furthermore, they develop without centralized control and may represent a readily scalable solution for growing networks in general.** We show that the slime mold *Physarum polycephalum* forms networks with comparable efficiency, fault tolerance, and cost to those of real-world infrastructure networks—in this case, the Tokyo rail system. The core mechanisms needed for adaptive network formation can be captured in a biologically inspired mathematical model that may be useful to guide network construction in other domains.”

In a similar vein, Bitcoin and its network participants receive signals from the market to create features that satisfy unmet demands or improve the functionality of its network. When block space demand exceeds capacity, as it did in late 2017, transaction fees spike and encouraged the development of a second layer protocol to increase transaction throughput (the Lightning network discussed earlier). As rent-seeking businesses, like Western Union, continue charging exorbitant fees for international remittances, market demand shifts to Bitcoin’s much more cost effective and permissionless payment channel. When governments crack down on Bitcoin exchanges, trading volume on peer-to-peer exchanges like LocalBitcoins.com flourishes. To enhance Bitcoin network accessibility, Blockstream launches satellites that provide global coverage for node synchronization. The Bitcoin network is constantly adapting to optimize for its own expansion and the interconnectedness of its participants. Perhaps Bitcoin is less so digital gold, and more so digital slime mold (just kidding, or am I?).

In most forms of life, genes are only passed from parent to offspring in a process called *vertical gene transfer*. Certain fungal networks, which are modeled after the decentralized network archetype, are able to steal competitive advantages directly from physical contact with other similar organisms in a process called *horizontal gene transfer*. These fungal networks can grow to gargantuan sizes – indeed, the largest organism on Earth, at nearly 4 kilometers across, is a honey fungus in Oregon that is slowly consuming an entire forest. Fungal networks live in constant competition as they fight off predators, pests and pollutants. This environmental stress causes them to naturally synthesize a variety of enzymatic and chemical countermeasures and, when one of these measures is successful, it is stored in the distributed mind of the entire fungal network. The next time it encounters a menace for which it has even once synthesized an effective countermeasure, the fungal network will use it to neutralize the threat, no matter where the latest encounter occurs. Amazingly, these fungal networks are capable of absorbing countermeasures created by competitors in the same ecosystem purely from physical contact. Such organisms exhibit distributed intelligence, meaning they learn at the edges and distribute the lessons throughout their vast networks.

There is a common misconception that an alternative cryptoasset could develop a superior feature that will eventually outcompete Bitcoin. Similar to certain fungal networks, Bitcoin is able to subsume features that have been proven in the marketplace from cryptoasset competitors. For example, an alternative cryptoasset called Basic Attention Token (BAT) is designed to power an internet browser called Brave that allows users to shield themselves from advertisements:



Brave users are then given the option to open their browsing sessions up to advertisements and are paid in BAT for their attention. This blockchain-based digital advertising solution is intended to allow users to monetize their own attention, whereas in most browsers advertising revenues are allocated mostly to the content publishers. Given Bitcoin’s open-source nature, it is able to absorb competitive features like this in a process similar to horizontal gene transfer. Today, by using the Lightning Joule browser extension and running a full Bitcoin node, you

can perform browser-based microtransactions similar to BAT but using Bitcoin instead. This effectively eliminates the need for a cryptoasset like BAT. Further, the technologies combined to make Bitcoin all came from previous attempts at digital cash, reiterating the point that open-source software is amenable to feature absorption. This ability accelerates the adaptivity of the Bitcoin network and insulates it from competitive disruption which further reinforces its position as the market leader.

### Antifragility

Seeing the ubiquity of the decentralized network archetype throughout nature in this way makes the invention of decentralized digital money seem less novel and more inevitable. An open and decentralized nature also enables Bitcoin to benefit from adversity. In light of its track record, Bitcoin is an excellent incarnation of Nassim Taleb's concept of *Antifragility*:

“Wind extinguishes a candle and energizes fire... Some things benefit from shocks; they thrive and grow when exposed to volatility, randomness, disorder and stressors and love adventure, risk and uncertainty. Yet, in spite of the ubiquity of the phenomenon, there is no word for the exact opposite of fragile. Let us call it antifragile. This property is behind everything that has changed with time: evolution, culture, ideas, revolutions, political systems, technological innovation, cultural and economic success, corporate survival, good recipes, the rise of cities, legal systems, equatorial forests, bacterial resistance... even our own existence as a species on this planet.”

Fragility can be defined as sensitivity to disorder, whereas robustness is insensitivity to disorder. Antifragility is a property of anything that benefits from disorder, stress or adversity. The many failed attempts at killing Bitcoin thus far have only made it stronger by drawing attention to attack vectors or vulnerabilities that its global team of self-interested, volunteer programmers can then fix. These improvements have only increased the network's operational efficiency. Also, each time it withstands an external attack or a chain fork (as we are witnessing with the abject failure of Bitcoin Cash), its reputation for network security and immutability is strengthened. The resiliency of Bitcoin is hardened by hostility.

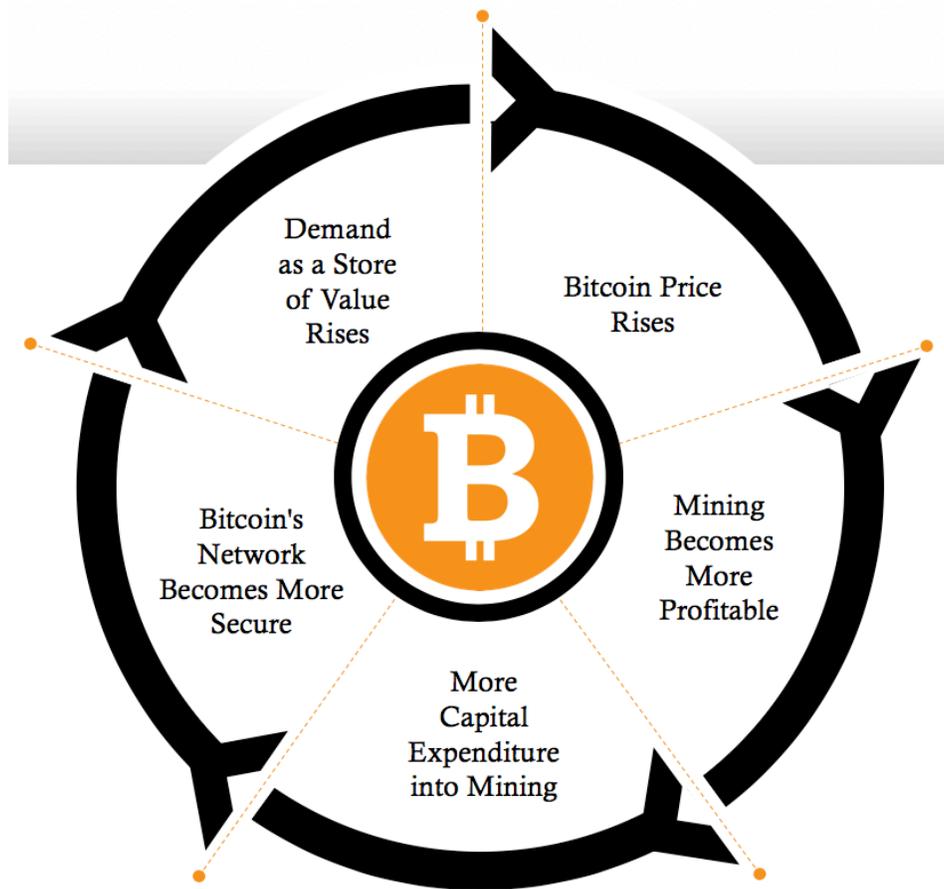
As Bitcoin has fluctuated wildly in price over the years, each new crash has triggered widespread declarations of its demise. Over 330 prominent articles declaring the death of Bitcoin, known as Bitcoin obituaries, have been written over the past 10 years. These publicity attacks on Bitcoin brought it to the attention of ever-wider audiences. As obituaries intensified, Bitcoin's network processing power, transaction volume and market capitalization all continued to ascend relentlessly – a confirmatory example of the saying 'all publicity is good publicity'.

When China took a heavy-handed approach to regulation by shutting down Bitcoin exchanges in 2017, we witnessed several informal exchanges and OTC markets appear following the demise of each centralized exchange. Although the liquidity for Bitcoin was negatively impacted initially, soon transactions started happening off exchange in China, with volume on websites like localbitcoins.com exploding. The regulatory attack also encouraged people to hold Bitcoin for longer periods, as evidenced by a steep decline in sell volumes,

which only reduced the amount of Bitcoin being traded and put upward pressure on its price. Also, these regulatory actions backfired by triggering the *Streisand Effect*, which is a phenomenon whereby an attempt to hide, remove or censor information has the unintended consequence of publicizing the information more widely, usually facilitated by the internet. As the world watched the situation in China unfold, both the Bitcoin price and global internet searches for the term Bitcoin reached new all-time highs.

Bitcoin’s Positive Feedback Loop

All of the adversity Bitcoin has faced so far has only fed its growth. Absent any top-down authority, Bitcoin is organic in the sense that it has grown from the bottom-up based solely on its own merits as money. Bitcoin perpetuates the expansion of its network and maintains truthful records by relying on asymmetric economic incentives that make fraud far costlier than its potential rewards. Network participants are all rewarded economically for their interactions with Bitcoin, which creates a flywheel effect on its price and network security:



As the Bitcoin network adapts to better meet the demands of its constituents, it in turn recruits more network participants. This positive feedback loop promotes the sustained growth of its network and fuels powerful, multi-sided network effects.

## Bitcoin's Network Effects

Bitcoin's meteoric growth has been both supported and protected by its unique multi-sided network effects. The basic example of a powerful 1-sided network effect is a social network (or a telephone network, as outlined earlier). The more people on a social network, the more valuable it is for others to be on it, as there are exponentially more possible connections. It can, however, be disrupted by a competitor that provides a more valuable service to its single customer cohort, the users, who might then transition to the new service (as happened when Facebook disrupted MySpace).

Successful 2-sided markets (like eBay or Craigslist) are significantly more difficult to disrupt. Consumers want to be there because merchants are there, and merchants want to be there because consumers are there. To disrupt a 2-sided network, you have to simultaneously introduce a superior value proposition for both parties, otherwise nobody moves. That is why Craigslist, despite its limited innovation over the years, has been able to leverage its early 2-sided lead and is still a dominant website today.

Bitcoin has a unique 4-sided network effect that insulates it from disruption and supports its growth. These are the four constituencies that participate in expanding the value of Bitcoin as a result of their own self-interested interaction with its network:

- Consumers who pay with Bitcoin
- Merchants who accept Bitcoin
- Nodes that maintain the distributed ledger
- Developers and entrepreneurs who are building onto and on top of Bitcoin

This 4-sided network effect makes Bitcoin's first mover advantage seemingly indomitable. As an adaptive monetary technology, its network effects encompass the liquidity of its market, the number of network participants, the community of software developers who support it and Bitcoin's brand awareness. Large investors will always seek the most liquid market for ease of entry and exit. Consumers, merchants and developers tend to join the largest of each of their respective Bitcoin communities, which only reinforces their social interconnectivity and cohesion. Brand awareness is innately self-reinforcing, as any cryptoasset competitor will inevitably be mentioned in comparison to Bitcoin.

An aside on Bitcoin's brand awareness: As we have learned, the value of any money is derived from its social consensus, or the mutual beliefs of its users. The notion of a "believer" has religious connotations, as the notion of one having an epiphany once the "truth" is revealed. Such religious undertones are prevalent in most forms of money (In God We Trust on the US Dollar) and they are also part of Bitcoin's aura (The Genesis Block, Bitcoin Evangelists). The most important of these quasi-religious ideas is the mythological bedrock Nakamoto laid with his enigmatic appearance in 2008 and then with his mysterious disappearance 3 years later. Whoever he/she/they were, Nakamoto gave Bitcoin its *creation myth*. As market strategist Nicolas Colas said:

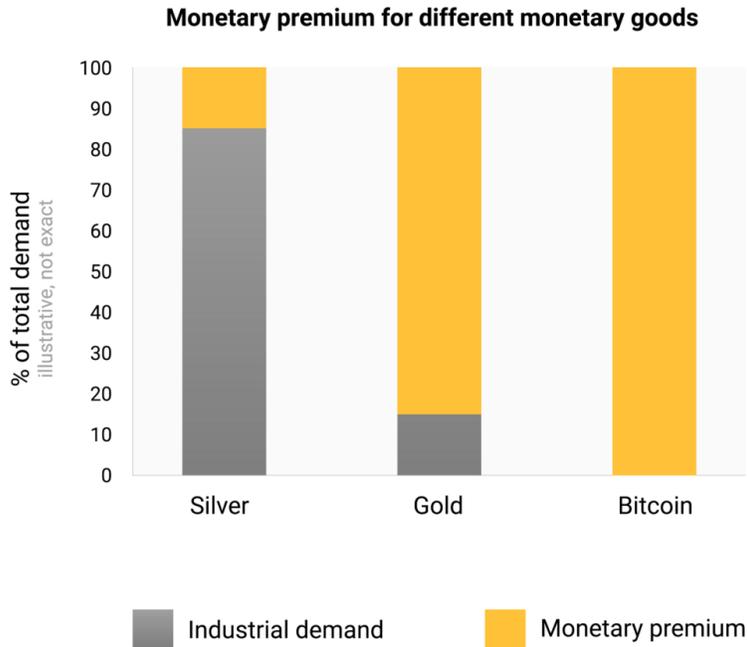
**“In business, creation stories reinforce the role of the individual as a societal agent of change and speak to a core audience of customers. They are the bedrock for what marketers call a brand and the source waters for Wall Street’s shareholder value.”**

Assuming Nakamoto was a lone wolf, it is arguable that his disappearance transformed him from a person into a mythological figure. This mystery fuels the brand awareness of Bitcoin and reinforces its quality of decentralization, as there is no single individual to vilify, denigrate or otherwise target in an attempt to tarnish Bitcoin’s symbolism. Like a super hero with a secret identity, all we have is the icon of Nakamoto as a cryptic genius – the godhead of Bitcoin.

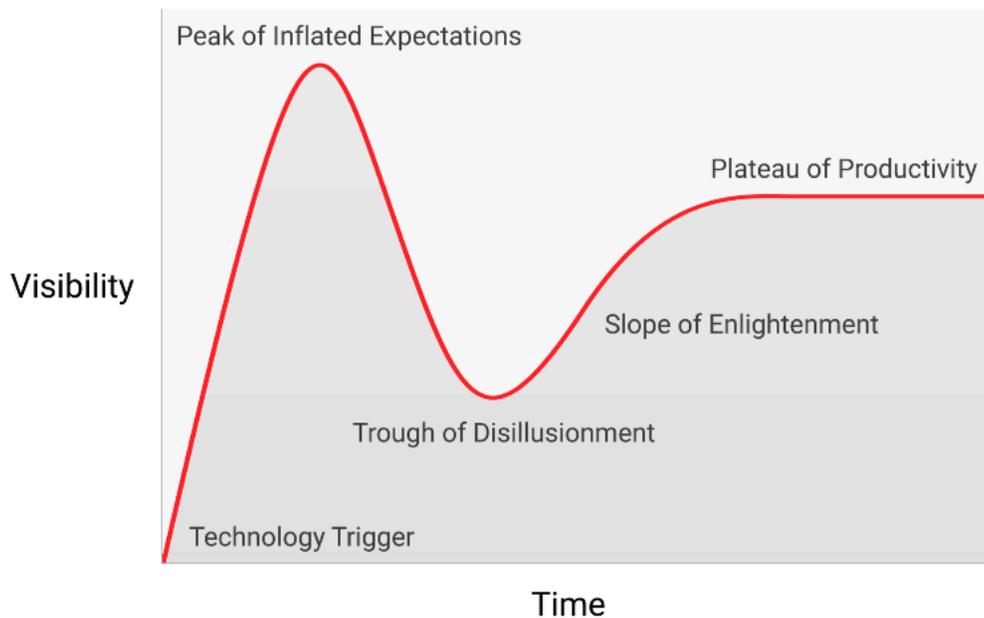
As we have learned, the value of a network is a reflection of the total number of possible connections it allows. Therefore, each new Bitcoin owner increases the value of the Bitcoin network, which benefits all existing owners. This new owner is then incentivized to evangelize the benefits of Bitcoin to others, creating the next wave of new owners, and the cycle continues. As the price increases, so too do the incentives to secure the network which draws in more capital expenditure from miners, making Bitcoin’s network effects even stronger and self-reinforcing as price appreciation reflexively energizes Bitcoin’s positive feedback loop outlined earlier.

Since money is a social network, the price of a monetary good is a reflection of how widely adopted it has become or is expected to become. The price of a monetary good in excess of its industrial demand is its *monetary premium*. This is the only rational basis for the common criticism that Bitcoin is a bubble, as it is purely a monetary technology and has no industrial demand whatsoever. However, this premium is the defining characteristic of all forms of money, as all monetary value is based on the optionality it gives its user for exchange across scales, space and time.

Actual bubbles occur when price exceeds fair value, such as the market distortions created by central bank monetary manipulation. However, some mistake monetary premia for bubbles since they cause prices of monetary goods to exceed their underlying industrial values. If monetary premia are bubbles, then money is the bubble that never pops. Paradoxically, in this sense a monetary technology can presently be both a bubble and significantly undervalued if it later achieves widespread adoption:



Although there is no established price pattern for a digital good that is becoming monetized, Bitcoin’s price appears to follow a fractal (a recursive, self-similar shape) wave pattern of increasing magnitude commensurate with its level of user adoption. The volatility of this price pattern is exacerbated by Bitcoin’s perfect price inelasticity of supply (as discussed earlier). Each iteration of the *fractal wave pattern* appears to match the standard shape of the *Gartner hype cycle*, which provides a graphical and conceptual representation of emerging technologies undergoing five phases of maturation:

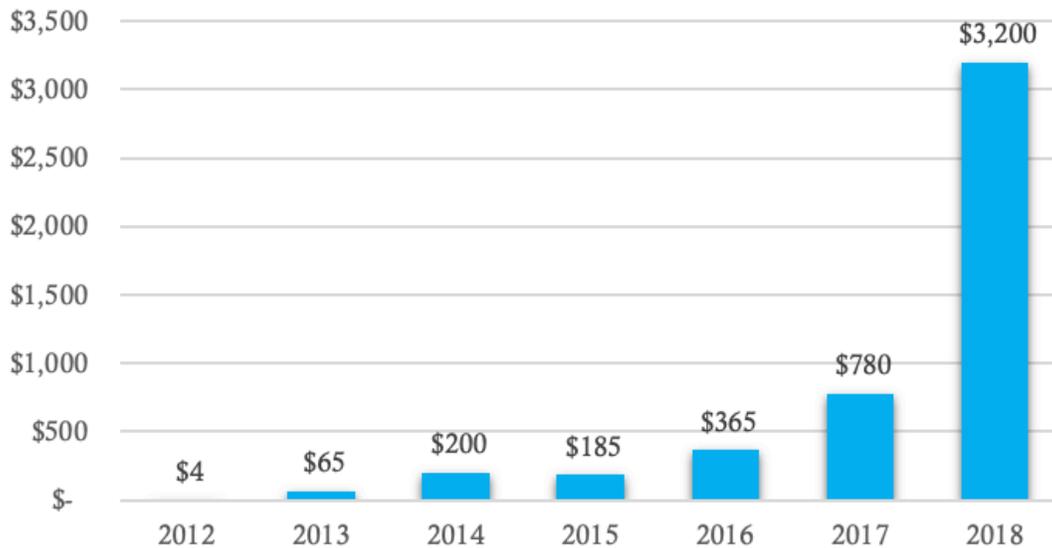


Bitcoin’s growth, in terms of price and transactions, has been dramatic to say the least. Indeed, it is the fastest growing asset in history. Its price has gone from \$0.000994 on October 5, 2009, in its first recorded transaction, to about \$4,000 today – a total increase of over 400,000,000% in 10 years. By its 10<sup>th</sup> birthday, Bitcoin had processed about \$1.38T USD worth of transactions, with USD value calculated at the time of each transaction. Here we show Bitcoin’s entire price history, from a logarithmic perspective, with the Gartner hype cycle fractal wave pattern iterations located inside boxes:

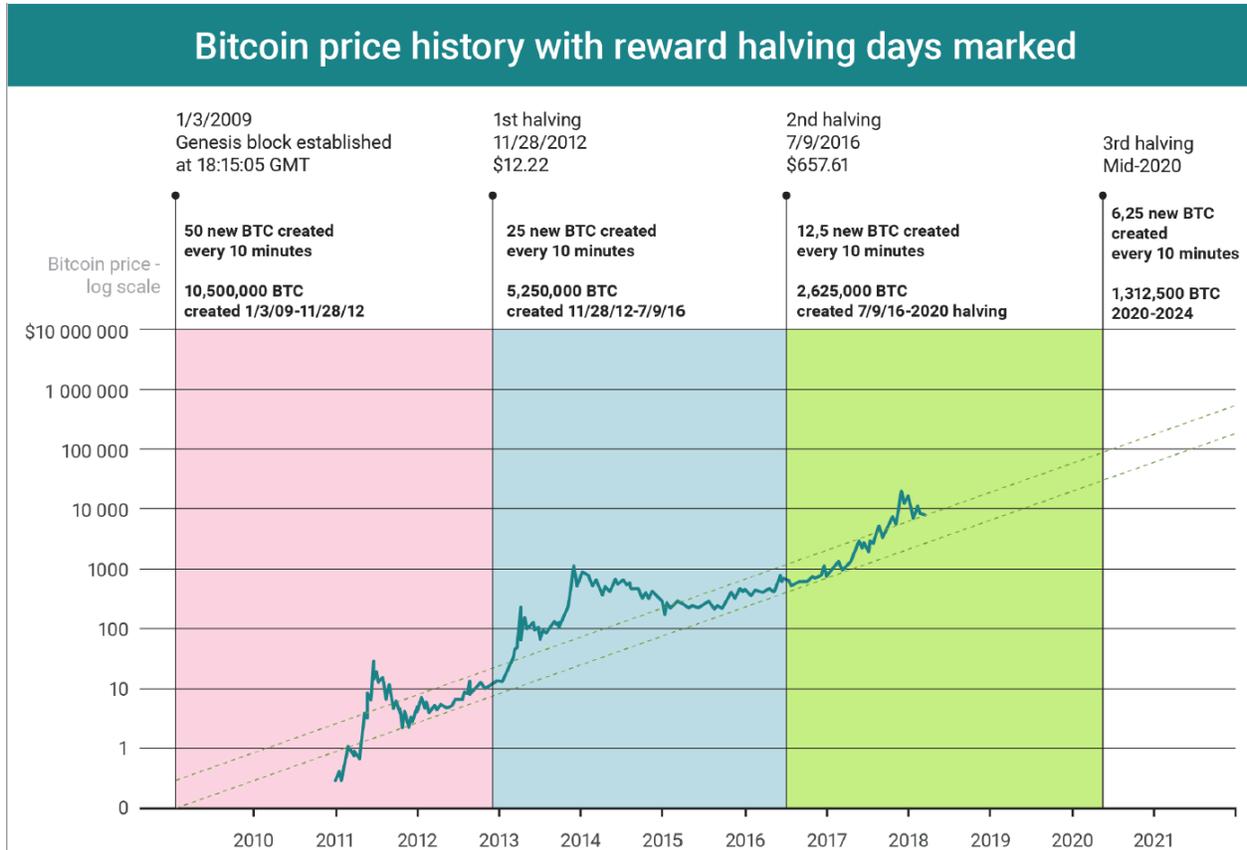


These extreme price cycles draw in new Bitcoin owners as each fractal wave crests. Some of these new owners buy in near the peak, only to be crushed in the trough. Most will capitulate, but those who remain because of their long-term conviction in Bitcoin (typically the most studious of history and monetary evolution among them) become the newest *hodlers of last resort*. Hodl, which began as a chat room typo in the early days of Bitcoin, has morphed into a memetic phrase that denotes “hodling” Bitcoin long term without regard to its price volatility. Layers of these stubborn hodlers have been added throughout each of Bitcoin’s four major price cycles. A good proxy for the depth of these layers is the lowest price Bitcoin hits each year, which indicates the rising collective obstinacy of these hodlers:

## Lowest Bitcoin Price Points 2012-2018



These layers form the base for the next iteration of each fractal wave pattern. As more observers recognize the survivability of Bitcoin following each price crash, they realize that investing in it may not be as risky as they once thought. This larger base of believers sets the stage for the next iteration of the fractal wave pattern which will support a much larger set of newcomers at a far greater magnitude of peak price. Few people are able to accurately predict how high prices will go in each fractal wave cycle, and they usually reach levels that would seem absurd to most investors at the earliest stages of the cycle. The best proxy for the timing of these fractal wave patterns has been the quadrennial Bitcoin inflation rate adjustment, when the amount of new Bitcoin rewarded at the close of each block is reduced by half, an event commonly known as the *halving*. Historically, Bitcoin achieves a new all-time high price within 18 months of its last halving. The next halving will occur in May 2020:



The fractal wave patterns inevitably crescendo and begin to crash, usually attributed to myriad factors by mainstream media. However, the Gartner Hype cycle is an archetypal market pricing pattern that is driven entirely by human psychology, game theory and the ultimate exhaustion of market participants reachable in each iteration. The magnitude of each cycle is exacerbated by Bitcoin’s absolutely fixed supply schedule, as increases in demand are expressed exclusively through its price, which historically leads to market frenzies at each peak. The long game for Bitcoin, and its final fractal wave pattern, will begin when and if central banks begin accumulating it as a reserve asset (more on this later). In this way, the bedrock of the Bitcoin network’s expansion is the intransigency of its hodlers of last resort. Although they constitute a small minority of the whole, these stubborn hodlers will contribute to ongoing Bitcoin adoption in a meaningful way.

### Minority Rule

When it comes to group preferences, certain types of minorities – those who stubbornly insist on a particular preference – that constitute even a small level of the total population (often less than 4%) can cause the majority to submit to their preferences. Another clever concept from Nassim Taleb, called the *minority rule*, is the result of complex system dynamics, like those inherent to human interaction.

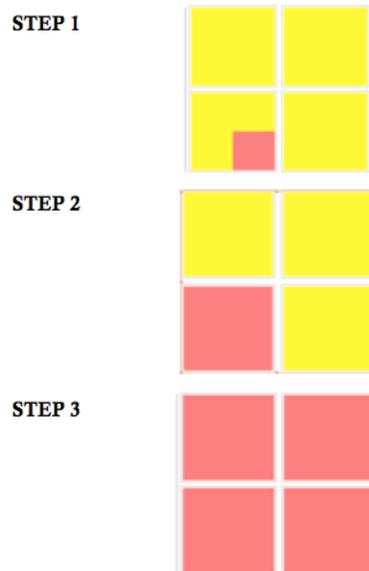
The nature of complex systems (society) is that the collective behaves in a way not predicted by its individual constituents (people). The interactions between its constituents matter more

than their individual natures. Studying individual ants will never give us an idea on how the ant colony operates. For that, one needs to understand an ant colony as an ant colony, not just a collection of ants. This is called an emergent property of the whole. In other words, the whole is more than the sum of its parts because what matters is the interactions between the parts. These interactions, while complex, can obey simple rules, like the minority rule (or the rule that barter economies settle on a medium of exchange or that the hardest form of money always outcompetes). Many domains are impacted by the minority rule such as:

- Markets – Market prices are not the consensus of market participants, but instead reflect the activities of the most motivated buyers and sellers. In 2008, a single \$50B order, less than 0.2% of the stock market’s total value of about \$30T, caused the market to drop by almost 10%, causing losses of around \$3T. The order was activated by the Parisian Bank Société Générale who discovered a hidden trade by a rogue trader and wanted to reverse the purchase. The market reacted disproportionately because there was only a desire to sell and no way to change the stubborn seller’s mind.
- Science – Similar to markets, science is not the consensus of scientists, it is the minority body of knowledge remaining after removing disproven hypotheses.
- Law – A law abiding citizen will never commit criminal acts but a criminal will readily engage in legal acts, and criminal behavior has been shown to be contagious within certain social groups.
- Imports – In the United Kingdom, where the (practicing) Muslim population is only around 4%, a very high proportion of the meat we find is halal (or Kosher). Close to 70% of lamb imports from New Zealand are halal. The same population and import proportions hold true in South Africa (the case of imports is closely related to the example below).

Today, in the United States and Europe, companies are selling more and more non-GMO food precisely because of the minority rule. Given the possibility of food containing GMOs, food not bearing the label “non-GMO” may be assumed by some to contain GMOs which, according to the minority, contain unknown risks. People who eat GMO food will readily eat non-GMO food, but not the reverse. Assuming the price and distribution costs differences between GMO and non-GMO are sufficiently small and the intransigent minority is distributed somewhat evenly throughout the population, this will have the effect of disproportionately increasing the demand for non-GMO food in the long run. This dynamic of scale can be explained quantitatively. In mathematical physics, renormalization groups are an apparatus that allow us to see how things scale up or down.

Now an example:



Here we show how the minority rule can renormalize the preferences of the majority. Our graphic depicts:

- Three vertically-stacked large boxes, each representing one sequential step in the minority rule renormalization process
- Four medium boxes in each step, each representing a family of four
- Four smaller boxes contained within each medium box, each representing an individual member within each family of four

Assume that in Step 1, the daughter in the family of four is the intransigent minority (the small pink box) who eats only non-GMO food. As we move to Step 2, the group renormalizes as the stubborn daughter manages to impose her rule on her three family members (who are now all pink) as they are flexible on the matter and consistency simplifies their grocery shopping and administrative process. In Step 3, the family of four goes to a backyard barbeque attended by three other families. As their family is known for their strict eating habits, the host will only serve non-GMO food as the other families are flexible and consistency simplifies the food preparation process, thereby making all four families (which are now all pink) adopt the minority rule originally set by the intransigent daughter in Step 1.

This minority rule will continue imposing and proliferating itself as these families attend other social events, which gradually shifts customer preferences in the neighborhood and eventually causes the local grocery store to switch to non-GMO foods to simplify its procurement processes, which impacts the local wholesaler, and so on up the supply chain. The real world result of this dynamic is the preferences of 4% of a population (practicing Muslims) driving the market preferences of 70% of their respective populations (in the UK, New Zealand and South Africa). As we can see, the minority rule spreads by interaction and renormalizes the entire group to conform with its preferences. Its proliferation is accelerated if there are incentives to switch, low switching costs or anticipated future benefits from switching (as superiorly hard digital cash money, Bitcoin offers all three). In this example, a minority

constituting 6.3% of the total population imposed its rules on the majority using pure intransigence. In reality, the minority rule often takes effect when minorities become 4% or less of the total population.

Languages also often adhere to the minority rule. For instance, French was originally intended to be the language of diplomacy as civil servants from aristocratic backgrounds used it, while English was reserved for those engaged in commerce. In the rivalry between the two languages, which are still considered two of the international languages (a third, Spanish, was added later because of its widespread use), English won as commerce came to dominate modern life. This gives us some intuition as to how the emergence of *Lingua Franca* languages, those commonly spoken across cultures, can come from minority rules. As Taleb puts it:

“Aramaic is a Semitic language which succeeded Canaanite (that is, Phoenician-Hebrew) in the Levant and resembles Arabic; it was the language Jesus Christ spoke. The reason it came to dominate the Levant and Egypt isn’t because of any particular imperial Semitic power or the fact that they have interesting noses. It was the Persians –who speak an Indo-European language –who spread Aramaic, the language of Assyria, Syria, and Babylon. Persians taught Egyptians a language that was not their own. Simply, when the Persians invaded Babylon they found an administration with scribes who could only use Aramaic and didn’t know Persian, so Aramaic became the state language. If your secretary can only take dictation in Aramaic, Aramaic is what you will use. This led to the oddity of Aramaic being used in Mongolia, as records were maintained in the Syriac alphabet (Syriac is the Eastern dialect of Aramaic). And centuries later, the story would repeat itself in reverse, with the Arabs using Greek in their early administration in the seventh and eighth’s centuries. For during the Hellenistic era, Greek replaced Aramaic as the lingua franca in the Levant, and the scribes of Damascus maintained their records in Greek. But it was not the Greeks who spread Greek around the Mediterranean – Alexander (himself not Greek but Macedonian and spoke a different dialect of Greek) did not lead to an immediate deep cultural Hellenization. It was the Romans who accelerated the spreading of Greek, as they used it in their administration across the Eastern empire.”

There is an asymmetry that those who do not have English as their first language usually know basic English, but native English speakers knowing other languages is less likely. If a meeting is taking place in an international office in say, Istanbul, among twenty executives from a sufficiently international corporation and one of the attendees does not speak Turkish, then the entire meeting will be run in English (the commercial *Lingua Franca*). This is the minority rule in action.

Money is an emergent property, as it is an expected result of complex human interactions within a barter economy. Similar to language, it is a means of expression, only it is used to express value instead of information or emotion. The US Dollar is the *Lingua Franca* of money today, as it belongs to one of the world’s largest economies (an economy which also happens to effectively control the global banking system).

As the digital age matures and the world becomes increasingly interconnected, ever-more commerce and administration will be conducted over the internet. Also, fully interconnected trade networks will level the terrain of commerce and increase free market competition among different forms of money. Considering the significant market lead already enjoyed by Bitcoin, its superior hardness, its multi-sided network effects, the impotency of capital controls on digital cash and the winner take all dynamic inherent to monetary competition; it's likely that Bitcoin will continue to outcompete and its adoption rate will increase. By considering the application of the minority rule to adoption of Bitcoin in the digital age, we can reasonably expect the following:

- Once a sufficient minority of the world's population, say 4% or less, have realized the advantages of hard money and digital cash money, their intransigent hoarding of Bitcoin will drive its price upward (Gresham's Law) and begin imposing itself economically on all other holders of money in the world. This will put downward price pressure on government fiat money, further accelerate Bitcoin's adoption rate and drastically improve Bitcoin's chances for global acceptance over the long run.
- As the first natively digital form of cash money, Bitcoin will become the Lingua Franca of digital commerce and the dominant value exchange protocol, thereby capturing nearly all the value transacted online (e-commerce alone is estimated to be nearly \$5T annually by the year 2021) over the long run.
- Bitcoin may also become the base layer for other tools of cryptographic certainty in commerce, such as smart contracts and TrustNet applications (more on these later).

The minority rule is based on a fundamental asymmetry between the intransigence of the minority and the flexibility of the majority. The minority rule shows us that a small number of unyielding people with skin or soul in the game can change the shape of the majority. Bitcoin already has the advantage of being the hardest form of money ever invented, and its rules are immutable, which is the highest form of intransigency possible. It also has unrivaled brand awareness, fed by the mystery of its creation myth, and the support of free market fanatics all over the world. Once its obstinate minority reaches a certain size, the unbreakable rules of Bitcoin will begin to stubbornly impose themselves on the established economic order. In the words of Margaret Mead "Never doubt that a small group of thoughtful, committed citizens can change the world; indeed, it's the only thing that ever has."

### A Superior Species of Money

Bitcoin also introduces three new traits of money never before seen – censorship resistance, adaptivity and programmability. Censorship resistance means that no group or individual in the world can stop payments made on its network. Bitcoin gains censorship resistance by virtue of its decentralized architecture. Adaptivity refers to the ability for Bitcoin's network to become more secure as it stores more value, its open-source nature which aligns the incentives of its global team of volunteer programmers with its own to ensure it is always up to date with state-of-the-art software enhancements and its ability to subsume features from competitors that have been proven in the marketplace. Programmability refers to the digital nature of Bitcoin and its ability to interface with smart contracts and other decentralized applications. As we have learned, the free market for money is a competitive environment that is shaped

by continuous market-driven natural selection; as a competitor in this domain Bitcoin is a superior species:

Bitcoin is a Superior Species of Money

---

**Money is a social technology used to solve a problem which has persisted for all of humanity's existence: how to move economic value across time and space.** Competition is at all times alive between different forms of money, subject to market-driven natural selection.

Traits of Money	Gold	Government Money	Bitcoin
Fungibility (interchangeable units)	High	Medium	High
Hardness (stock-to-flow ratio)	Medium	Low	High
Portability	Medium	High	High
Durability	High	Medium	High
Divisibility	Low	Medium	High
Security (cannot be counterfeited)	Medium	Medium	High
Easily Transactable	Low	High	High
Scarcity (predictable supply)	Medium	Low	High
Self-Sovereign (permissionless)	High	Low	High
Government Issued	Low	High	Low
Decentralized (censorship resistant)	Low	Low	High
Smart (adaptive & programmable)	Low	Low	High

The technology that is enabling Bitcoin to compete effectively in the market for money is also being applied to create new markets or disintermediate other existing markets. In technical parlance, the Bitcoin network is the world's first decentralized application. A decentralized application is a service that no single entity owns or operates. It is a new form of software and human organization that eliminates single points of failure, resists external attacks and reduces the need for intermediaries. Decentralized applications are enabled by cryptoassets. In the same way corporate equities serve companies and government bonds serve nations, cryptoassets serve decentralized applications. Owning a cryptoasset (like Bitcoin) is the only way to own a piece of a decentralized application (like the Bitcoin network). Technically, a cryptoasset is a cryptographically protected digital token representing rights within an economic network. A cryptoasset is to a decentralized application what oil is to an engine; it provides functionality and liquidity for the network and its constituents. A defining feature of cryptoassets and decentralized applications, and arguably their most alluring, is their organic nature; they are not centrally owned, governed or developed – making them highly resistant against censorship and manipulation.

Bitcoin (the OG cryptoasset) is superior in the market for money because it possesses all the ideal features of digital cash money and enjoys a market dominant position by virtue of its serendipitous first mover advantage which is fortified from disruption by its open-source

design and multi-sided network effects. With the invention of Bitcoin, the world finally has a synthetic form of money with a stock-to-flow ratio that is guaranteed to increase (until it reaches infinity) and an unstoppable, permissionless payments channel. Its digital nature makes it salable across space in a way never before seen, as it can be stored in the human mind and transmitted at the speed of light. The deep divisibility of each Bitcoin into 100 million Satoshis makes them supremely salable across scales. Its informational and nonperishable nature, when considered in combination with its superior hardness, gives Bitcoin unprecedented salability across time. This design makes it an impeccable store of value. Finally, by eliminating all intermediary control (which is inherent to government money) Bitcoin resists debasement, censorship and confiscation. It removes the central banks, macroeconomists, politicians, presidents, dictators and military leaders from monetary policy and payments authorization once and for all. The masterful book (which guided and inspired much of this essay) titled “The Bitcoin Standard” by Saifedean Ammous sums up Bitcoin’s historical relevance nicely:

**“If the modern world is ancient Rome, suffering the economic consequences of monetary collapse, with the dollar our aureus, then Satoshi Nakamoto is our Constantine, Bitcoin is his solidus, and the Internet is our Constantinople. Bitcoin serves as a monetary lifeboat for people forced to transact and save in monetary media constantly debased by governments... the real advantage of Bitcoin lies in it being a reliable long term store of value, and a sovereign form of money that allows individuals to conduct permissionless transactions.”**

Bitcoin is a tool for freedom. As the most accessible asymmetric bet in history, Bitcoin is also a unique investment opportunity.

### Investing in Bitcoin

Investing is all about taking intelligent risks. As Daniel Kahneman, a Nobel Prize-winning psychologist, describes it:

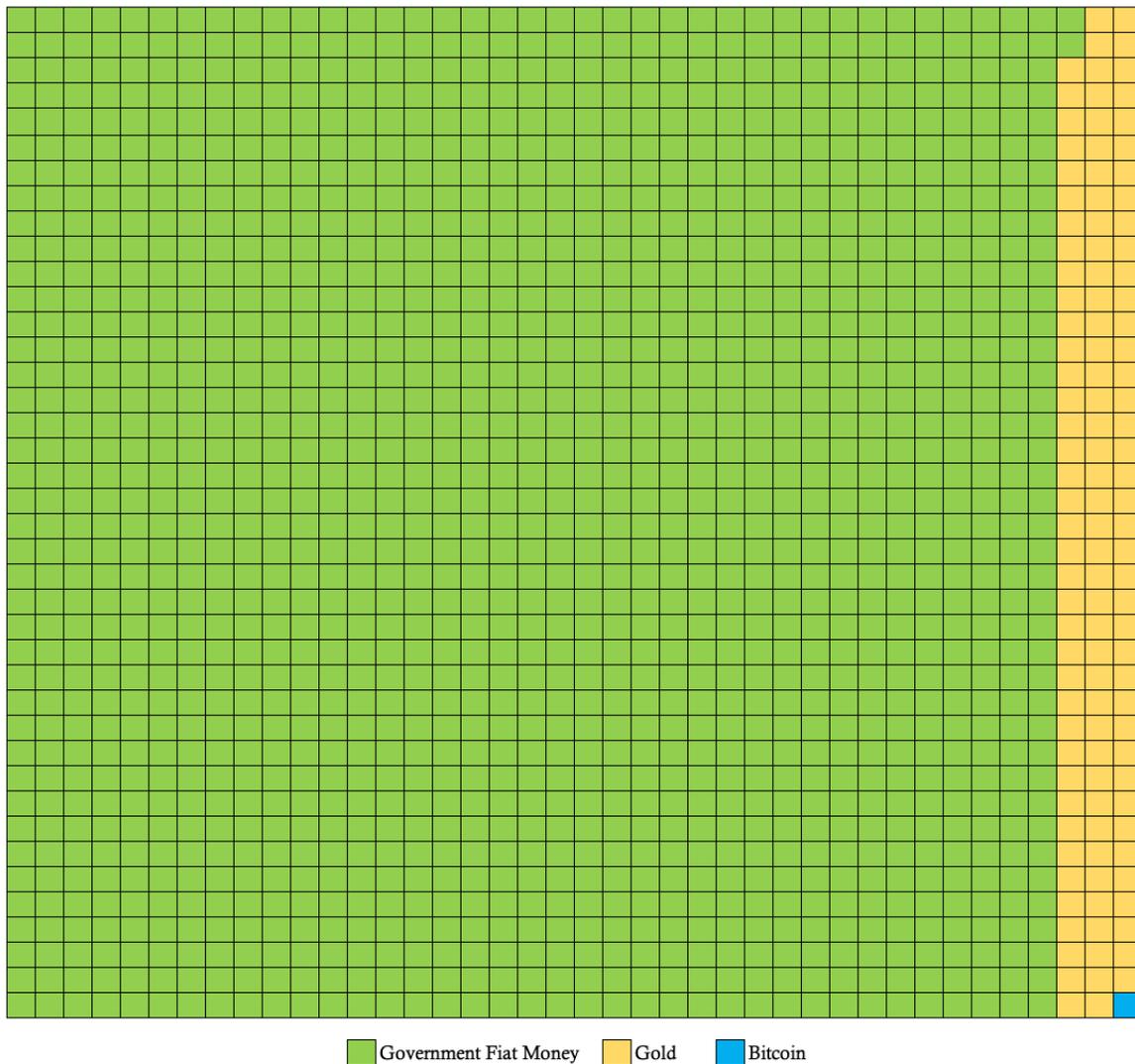
“Intelligent risks are based on wide and voracious data gathering checked against gut instinct; while dumb decisions are built from too narrow a base on inputs.”

Bitcoin is often referred to as digital gold, in reference to its hardness, self-sovereignty and as an instrument for final settlement. Following this analogy, there will only be one digital equivalent to gold (due to winner take all dynamics inherent to the free market for money), and if you were going to bet on which one will succeed you’d want to bet heaviest on the biggest (due to its deep liquidity and multi-sided network effects), most renowned (due to the minority rule) and the longest lived (due to the Lindy Effect, more on this later). As people tend to think by analogy, this comparison to gold mostly works well, although it is incomplete.

As we have seen, Bitcoin is a far superior monetary technology to the golden inert metal. Technologically, Bitcoin needs little to no protocol improvement to continue to compete effectively in the market for money. There are no unsolved computer science problems standing between Bitcoin and its widespread adoption. Therefore, its primary aim is to remain

extant as digital cash money, hence its minimal level of protocol functionality and the status quo bias it exhibits in relation to governance. By merely existing, Bitcoin provides a gateway for people to opt out of the prevailing inflationary monetary order. As long as it continues to operate successfully in its current form, Bitcoin will function healthily as the stateless base money protocol for the digital age – which makes it a viable contender in the \$100T market for global money:

Relative Market Sizes of Government Fiat Money, Gold and Bitcoin as of January 3, 2019



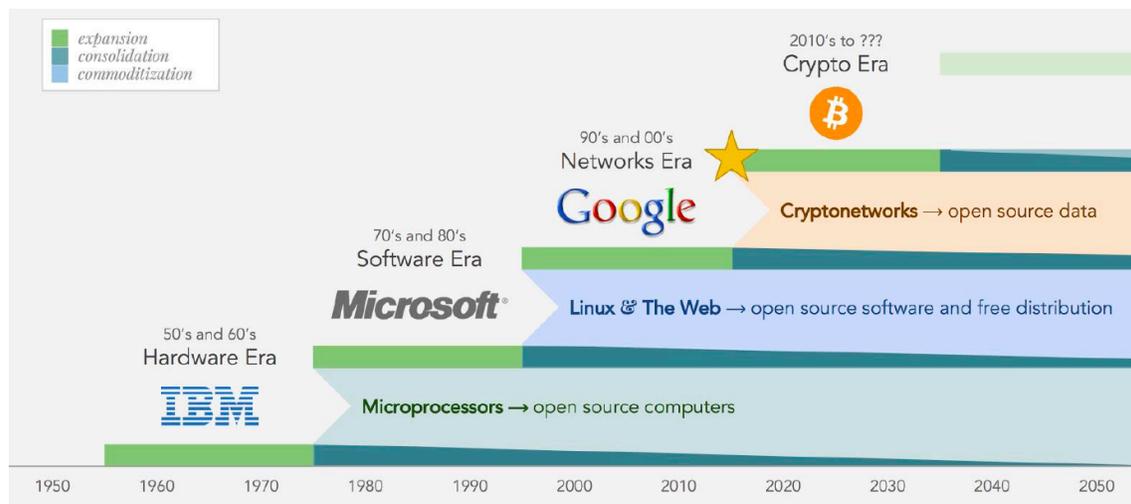
Since it is still extremely small relative to its total addressable market, which consists mostly of gold and government fiat money, Bitcoin still has room to grow by orders of magnitude in both its network size and price. Like a call option, a bet on Bitcoin is asymmetric, meaning that an investor’s downside is limited to 1x whereas their potential upside is 100x or more. Should Bitcoin achieve a majority share of the global market for money, its level of demand will become far more predictable and steady, leading to a stabilization in its price.

**Investing in Bitcoin can be considered a bet on its adoption as an uninflatable, politically neutral store of value and as an unstoppable, permissionless payments channel.**

Bitcoin may also become part of a much bigger wave of innovation. Although the Bitcoin network and the decentralized applications it has inspired are poorly understood by most today (similar to the internet in the early 1990s) we believe that the world will gradually awaken to the paradigmatic shift that is underway for money and markets in general. The greatest wealth is created by being an early investor in innovation. Making such investments requires believing in something before the majority of people understand it – which also often entails enduring mockery, ridicule and criticism for your non-consensus perspective. As Mark Yusko, one of my favorite hedge fund managers, describes the coming crypto era:

“Technology follows 14-year innovation cycles. These began with the Mainframe in 1954, then the Microchip in 1968, the Personal Computer in 1982, the Internet in 1996 and most recently the Mobilenet in 2010. As a result of the innovations introduced by Bitcoin, soon we will christen 2024 as the dawn of the Trustnet.”

The *TrustNet* can be thought of as the dawn of trustworthy computing. In theory, it will enable new technologies such as the internet of things, decentralized autonomous organizations, self-owning commercial assets, decentralized internet provisioning, decentralization of energy distribution, reputation markets, computing power markets, stateless identity, immutable media, AI-run organizations, token curated registries, prediction markets and circles of trust. This anticipated innovation wave is consistent with a multi-decade cycle of information technology expansion, consolidation and commoditization:



Bitcoin, as the original and driving force of this innovation expansion cycle, will likely function as the systemic core and base money system of the Trustnet. During this cycle, all markets that are enabled by this technology will likely rely on the Bitcoin blockchain as a common value system, final settlement mechanism and temporal anchor point.

## A Momentous Innovation

Bitcoin is a momentous innovation of the digital age. As such, it has many unique characteristics, properties and capabilities never before seen in a monetary technology:

- Immutable Monetary Policy – Predictable, transparent and unchangeable money supply schedule. The most critical aspect to outcompeting in the free market for money, as people will naturally come to favor the hardest form of money available to them (uninflatable money).
- Digital Scarcity – Necessary to solve the double-spend problem and bring the speed and finality of physical cash settlement into the digital realm.
- Absolute Scarcity – The only asset in the world which has an absolutely finite supply, like time itself.
- Global Final Settlement System – A permissionless, unstoppable payments system with zero counterparty risk (like gold, only digital) that can be used to quickly and efficiently provide finality of settlement across scales and space.
- Self-Sovereign Network – A self-sovereign monetary good (an informational bearer instrument) whose network operates autonomously in full accordance with its own immutable rules as reliably as the laws of mathematics.
- Stateless Money – The first globally connected payments system that is politically neutral. Possible catalyst for the separation of money and state over the long run.
- Revolutionary Social Contract Implementation – A unique 2-layer social contract implementation that decentralizes power among its constituents and creates a hypercompetitive market for its own network security. A new form of social institution.
- Global Consensus – Perhaps the only truly objective set of facts in world history, its distributed ledger is created by converting processing power into indisputable truth.
- Global Energy Buyer of Last Resort – Enables anyone in the world to convert excess electricity into digital gold on demand. A perpetual incentive for everyone in the world to develop more energy efficient innovations.
- A New Form of Life – Feeds on human self-interest and electricity to provide uninflatable money, an unstoppable payments channel and immutable governance.
- Adaptive Security – By virtue of the mining difficulty adjustment, as more value is stored on its network, the network adapts to become more secure.
- Adaptive Functionality – As an open-source software project, programmers around the world are constantly improving Bitcoin's codebase, however it is up to the users to adopt these changes, which creates a governance equilibrium in which only those changes that are in the collective best interests of users will be adopted. Enables Bitcoin to subsume superior features from competitors that are market-proven, making it highly resilient to disruption.
- Programmability – As a digitally native form of money, it can be used as a form of payment, collateral or fuel for a variety of smart contracts (self-executing software or commercial agreements). Can interface with other decentralized applications. Could function as the core value system for the TrustNet, the anticipated wave of innovation triggered by the emergence of Bitcoin.

Bitcoin has made a major impact in the world in its 10 years of existence, and it still holds a great deal of promise for the future. All in good time. Given its inextricable relationship with money and Bitcoin, the concept of time is worth exploring more deeply. It turns out that time's role in our lives, individually and collectively, is the key to understanding prosperity and the ways in which Bitcoin could play a key role.

## TIME

### The Simple Truth about Time

Time is the ultimate resource. Its absolute scarcity bounds the entirety our stories, both as individuals and societies. With economics, we strive to use it more effectively. As the destroyer of all things and the healer of all wounds, it is the grand paradox of nature.

### The Ultimate Resource

Scarcity is the starting point of all economics. It is commonly believed that natural resources are inherently scarce, which is true in a sense, as there is only so much gold within the Earth, for instance. However, this finite quantity of gold in the Earth is still too large for humans to even measure and in no way constitutes an actual limit to the amount we can conceivably mine. We have literally ‘just scratched the surface’, as our mining efforts haven’t even taken us half way into the Earth’s crust, its thinnest and outermost layer. Driven by need, humans have always found a way to explore farther and dig deeper to uncover ever-more natural resources. Therefore, the actual practical limit to the quantity of any natural resource is always and only the amount of human time, effort and ingenuity devoted to its production. For human beings then, the only truly scarce resource is time.

Individually, the only scarcity we face is our limited time on Earth. As a society, the only scarcity we deal with is the total amount of human time, effort and ingenuity available to be directed at the production of goods. This scarce resource, which we will call *human time*, is the ultimate societal means of production. Humans have never fully exhausted any single natural resource. The price of all natural resources, in terms of human time, has always decreased steadily over the long-run as our technological advancements have dramatically increased our productivity. Not only have we not depleted any natural resource, but the proven reserves (the amount of natural resources still within the Earth) continue to increase despite our increasing rates of production, as new technologies enable us to discover and excavate ever-more natural resources.

Oil, the lifeblood of the industrial economy, is a great example of this concept. Even as oil production has increased every year, its proven reserves increase at an even faster rate. According to data from BP’s statistical review, annual oil production increased 50% from 1980 to 2015. Oil reserves, on the other hand, have increased 148% during the same 35 year period, around triple the increase in oil production. Similar statistics exist for all natural resources prevalent in the Earth’s crust. Some are more common (iron, copper) and some are rare (gold, silver) but the limit of how much we can produce of any particular natural resource is always and only the amount of human time directed at its production. The best evidence of this simple fact is gold: if the annual production of the one of the rarest metals in the Earth’s crust goes up every year, then it makes no sense to consider any other natural resource being scarce in any practical sense. Echoing back to the fundamental market realities related to deferred consumption and investment – the real cost of anything is always its opportunity cost in terms of goods forgone to produce it. In terms of natural resources, only human time is truly scarce, which makes time the ultimate resource.

## Frozen Time

As more humans exist, there is more human time to direct towards the extraction and production of natural resources. As we have learned, productive output per unit of human time (productivity) can be amplified by leveraging technological solutions to problems (tools). In economics, a tool or technology is considered to be both:

- A non-excludable good – once one person invents something, all others can copy it and benefit from it
- A non-rival good – a person benefiting from an invention does not reduce the utility that accrues to the others who use it

For example, once one person invented the wheel, everyone else could copy its design and make their own, and their use of this design would in no way reduce others' ability to benefit from it. Innovations like this spread and their benefits compound over time, leading to ever-higher productivity and division of labor. Like the candle whose flame burns undiminished even after igniting a thousand others, the benefits of innovation ultimately accrue to everyone without detracting from the innovator in any way.

Natural resources and innovation are always and only the product of human time. Therefore, in terms of production, human time is the ultimate resource and essence of value. To keep score, people needed a way to reliably store the value they produce with their time, so that they can exchange it in the future for other peoples' time, effort and ingenuity. Conceptually then, money is frozen time. It is earned by sacrificing human time and can be traded for commensurate sacrifices from others. The age-old problem faced by people is collectively deciding which monetary technology can best serve this purpose.

Technologically, money is a spontaneous emergent property that humans ascribe to a particular good. People, acting in self-interest, live within technological and economic realities that shape their decisions and provide them incentives to persist, adapt, change or innovate. It is from the countless collisions of these complex human interactions that spontaneous monetary orders have emerged and decayed. History has shown us myriad cases of a good being subjected to market-driven natural selection, achieving a monetary role and subsequently having its role taken by a superior technology.

Whatever monetary media people chose as a store of value was always subject to being produced in greater quantity, so the producers could acquire the value stored in it. The Yapese witnessed this play out when O'Keefe produced Rai Stones using explosives. West Africans had their wealth confiscated by Europeans who shipped in boat loads of cheaply produced glass beads. Citizens in modern economies continuously have their wealth usurped as central banks gradually or quickly erode the value of government fiat money. Gold came close to solving this problem as it is indestructible, expensive to mine and its flow is relatively predictable. However, gold's physicality led to its centralization within bank vaults and its compulsory replacement with soft government money.

Until the invention of Bitcoin, all forms of money were subject to having their value stolen by producers of the monetary good. This made all monetary technologies before Bitcoin imperfect in their ability to store value across time. Bitcoin's finite supply makes it the best medium to store the value produced by finite human time. In other words, Bitcoin is the best store of value humanity has ever invented, as it is the only monetary technology that cannot be debased over time. The informational, intangible and purely digital nature of Bitcoin enables it to achieve absolute scarcity, a property that was previously exclusive to time itself.

**The absolute scarcity of Bitcoin makes it the perfect modality for freezing and transacting the only other absolutely scarce resource – time.**

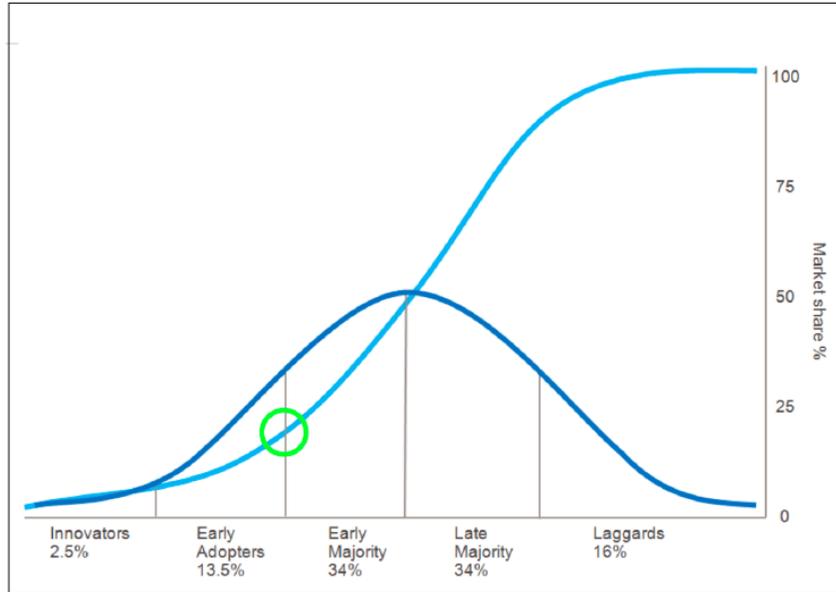
No matter how many people use the network, how advanced mining equipment becomes or how much its price increases, there can only ever be 21 million Bitcoins in existence. In time, it is likely that Bitcoin will be regarded as the best technology for saving ever invented.

### Time Arbitrage

Innovations of this magnitude are virtually impossible to predict; however, they do follow a familiar adoption pattern. The book titled 'Diffusion of Innovations' lays out a framework that seeks to explain how, why and at what rate new ideas and technologies spread. Diffusion is the process by which an innovation is communicated and adopted by participants in a social system over time. There are four main elements that influence the spread of the new idea:

- The nature of the innovation
- Communication channels
- Time elapsed since ideation
- The social systems under which it is adopted

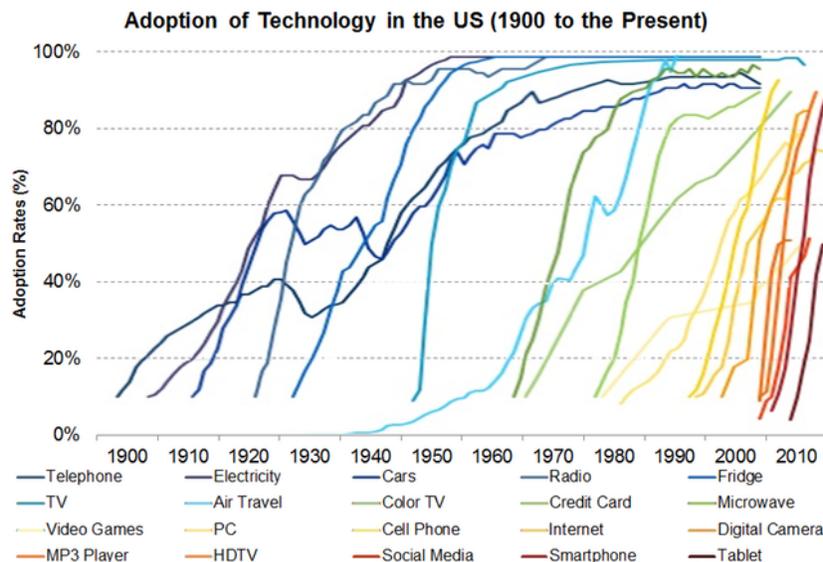
Once a certain rate of adoption is achieved, the innovation reaches a tipping point and its continuous spread becomes practically unstoppable (a concept of preferences closely related to the minority rule discussed earlier) as people naturally prefer superior technology solutions. Such an adoption curve is especially true of, and often completed faster for, network-based technologies such as the internet and Bitcoin; as their general acceptance is driven harder and faster by network effects. Based on its estimated number of users, we are just beginning to enter the early adopter phase for Bitcoin:



The S-curve of adoption. As successive groups adopt a new technology or idea market share rises. The tipping point (green circle) marks an inflection point and leads to rapid growth in adoption.

In investing, the concept of *time arbitrage* refers to an asset becoming oversold based on a short-term or emotional market sentiment despite its long-term outlook or investment fundamentals remaining unchanged or even improving. Time arbitrage is essentially another form of the old investment adage “Buy on bad news, sell on good news”. Times such as these present savvy investors with an opportunity to enter a position with the same or improved value fundamentals at a lower price point.

All ubiquitous technologies today, beginning as fledgling innovations themselves, have traversed this path to mainstream adoption. Here we show some of the most impactful innovations since the year 1900 and the rapidity with which they were adopted:



As we can see, advances in telecommunications and distribution methods have accelerated the pace with which new innovations are adopted. Today, the internet causes breakthrough innovations to spread like a wildfire throughout the minds of people all over the world. Since it is a nascent monetary technology that is not fully understood by the vast majority of the world, Bitcoin still has low levels of adoption and therefore significant upside prospects. Also, owning a piece of the Bitcoin network today is over 80% cheaper than about a year ago even though its utility in terms of throughput, transaction fee efficiency and network security have all improved substantially over the same period. This confluence of factors indicates that now is an opportune time to take advantage of time arbitrage and invest in the Bitcoin network. Also, as a technology, the Bitcoin network's value will continue to grow with every passing day that it successfully operates.

### Lindy Effect

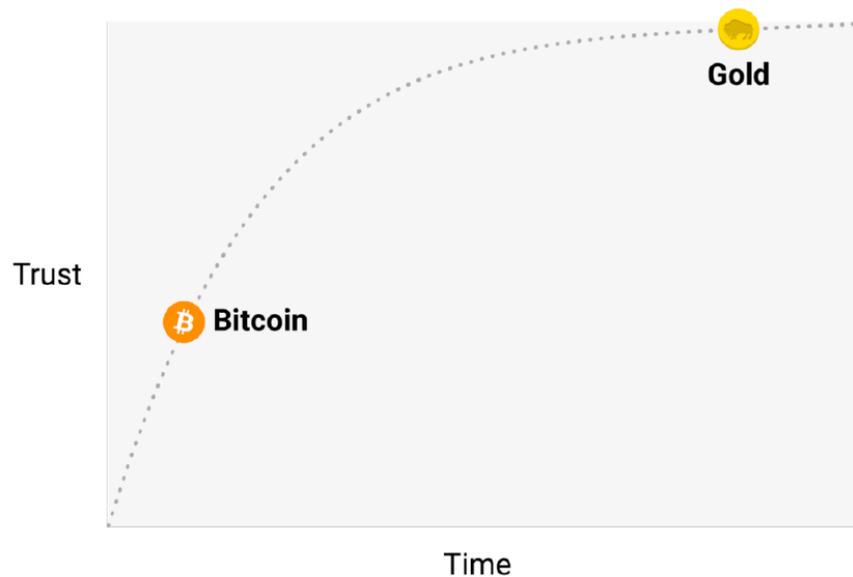
Things in this world fall into one of two general categories: perishable and nonperishable. The distinction between the perishable (humans, single items) and the nonperishable is that the latter does not have a natural, unavoidable expiration date. The perishable is typically physical in nature, meaning it is subject to physical degradation, whereas the nonperishable is typically informational in nature. A single car is perishable, but the automobile as a technology has survived for a century and can be reasonably expected to persist for at least another one. An individual man will die, but his genes (which are digital) can be passed on for innumerable generations. This heuristic from Nassim Taleb, known as the *Lindy Effect*, can be summarized as follows:

- For the perishable, every additional day of life translates into a shorter additional life expectancy.
- For the nonperishable, every additional day of life may imply a longer life expectancy.

The only effective judge of things is time, as time is the ultimate destroyer of all things. The Lindy Effect is closely related to antifragility, as the ravages of time are a potent form of adversity. Anything that gains from temporally-driven increases in disorder is antifragile and benefits from the Lindy Effect. Using arbitrary math for simplicity, if a book is still in print after 50 years, it can be expected to remain in print for another 50 years. If it's still in print for another 50 years after that, then perhaps it can then be expected to remain in print for at least an additional 120 years. At some point, the Lindy Effect may imply an unlimited life expectancy. A book like the Bible, which has been in print for thousands of years, can be reasonably expected to remain in print for the rest of human history.

If you had conducted a survey in 1995 and asked people whether they believed the internet would be a permanent feature of their lives, you would have probably received mixed responses. If you conducted the same survey today, people would resoundingly agree that the internet is here to stay. A technology, being informational rather than physical in nature, does not age in the same way humans do. A technology like the wheel is not "old" in the sense of experiencing degradation, it is a technological design that has persisted for millennia and can be reasonably expected to persist for many more.

So, the longer a technology lives, the longer it can be expected to live. Since Bitcoin is a technology, every day that it continues to successfully operate increases its life expectancy. Further, as we have learned, the core moving parts of Bitcoin are mathematics and human nature – two concepts which are very “Lindy” and can be reasonably expected to persist for the rest of human history. Bitcoin’s ever-growing life expectancy increases its perceived trustworthiness and eventually it will be regarded as a permanent feature of our modern lives in the same way the internet is today. This heuristic helps explain why gold will likely continue to be regarded as a monetary metal for many years to come, whereas Bitcoin is still in the process earning people’s trust:



The Lindy Effect is universally applicable across time. The same competitive dynamics that caused the ascent of gold into a dominant monetary role are now driving Bitcoin adoption. In this sense, the future is in the past. As the Arabic proverb says: *he who does not have a past has no future*. Notwithstanding the past century of central bank coercion, hard money is the norm of human history and we are witnessing its reemergence with the rise of Bitcoin. As Bitcoin continues to persist, knowledge of its fundamental nature and functional capabilities will continue to spread. Threatened by its continued growth, incumbents will ratchet up their efforts to prevent Bitcoin’s ascent and protect the monopoly on money they have enjoyed over the past century.

### Future of Regulation

There is a good reason why the gold standard was forcibly ended and no good store of value has yet risen to fill the void. To preserve seigniorage profits governments must enforce an inflationary monetary policy. Otherwise, if a sound store of value existed that was accessible to its citizenry, their business model would be jeopardized as people would exit depreciating fiat currencies to shield their wealth from further confiscation. As Alan Greenspan, former Chairman of the Federal Reserve (the central bank of the United States) said in 1966:

**“In the absence of the gold standard, there is no way to protect savings from confiscation through inflation. There is no safe store of value. If there were, the government would have to make its holding illegal, as was done in the case of gold. If everyone decided, for example, to convert all his bank deposits to silver or copper or any other good, and thereafter declined to accept checks as payment for goods, bank deposits would lose their purchasing power and government-created bank credit would be worthless as a claim on goods. The financial policy of the welfare state requires that there be no way for the owners of wealth to protect themselves.”**

Clearly, central banks are aware that free market competition against hard money poses significant risk to the continuity of their socialistic business model. To protect central bank monopoly positions, governments have resorted to passing onerous laws against their citizens. Governments seek to insulate their national currencies from free market competition employing legal measures such as:

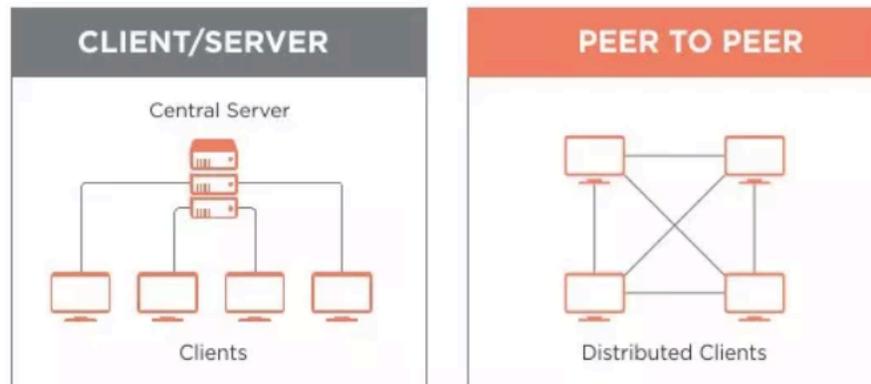
- Capital Controls – which prohibit the movement of money into or out of a country
- Confiscatory Orders – forceful seizure of assets, like Executive Order 6102 in 1933 which outlawed private ownership of gold in the United States
- Legal Tender laws – which create artificial demand for government fiat money by requiring that it be accepted in settlement of debts

With Bitcoin, regulators face a unique dilemma. Bitcoin exists orthogonally to the law, and there is virtually nothing that any authority (or anyone for that matter) can do to affect its operation. Regulations were designed to govern people and entities and are not equipped to deal with a decentralized network that autonomously proliferates itself. Regulators are really good at targeting centralized marks, like an individual business or its CEO, and enforcing laws against them. However, regulations have proven to be largely impotent against decentralized services.

To understand this point, consider the case of BitTorrent, a decentralized peer-to-peer file sharing service. In the earlier days of the internet, file sharing platforms like Napster and Kazaa had become an extremely popular way for users to share movies, music and other media directly with one another. With these free services, users would upload media to and download media from the companies’ computer servers. This client-server file sharing directly threatened media monopoly profits, as it completely circumvented copyright law. Incumbent organizations quickly responded with heavy litigation. Since services like Napster and Kazaa were hosted by centralized companies complete with a headquarters, executive team and computer servers, they were vulnerable to being shut down. Filing a lawsuit, knocking on some doors, levying some fines and decommissioning some computer servers was all it took to shut down these services and protect media industry monopolists.

The introduction of BitTorrent, an open-source decentralized protocol for peer-to-peer file sharing, was a game changer. Once installed on a computer, BitTorrent enables user nodes to upload and download movies, music and other media directly from one another using encrypted communication channels. Since files on its network do not come from a single

source, BitTorrent was also able to offer superior download speeds by fragmenting the media files and pulling from multiple nodes simultaneously. Unlike the failed client-server models of centralized platforms, the BitTorrent protocol never holds any of the media files, it only facilitates the transfer of files between individual users:



Architecturally, the entire software codebase of the protocol exists on every user machine that downloads it, making it virtually impossible for a regulator to target and shutdown as there is no single point of vulnerability (censorship resistance). The BitTorrent protocol exists everywhere and nowhere by virtue of its decentralized network architecture, a model that would be later employed by Bitcoin. Indeed, without a centralized target to shut down, regulators were incapable of stopping BitTorrent and the other protocols it inspired. By 2009, peer-to-peer file sharing using decentralized protocols like BitTorrent accounted for up to 70% of internet traffic worldwide.

Bitcoin has already exhibited similar properties to BitTorrent as regulators have been incapable of containing the expansion of its network or shutting it down. It cannot be contained by capital controls, as it exists entirely outside the legacy financial system. Confiscation of Bitcoin, unlike that of gold, is extremely difficult given its informational nature. This leaves legal tender laws, which are still enforceable and could therefore require Bitcoin users to convert some of their holdings into government fiat money to pay their taxes. So, the exchanges and OTC markets where Bitcoin is traded are the only viable targets for regulators. As such, these financial gateways that connect Bitcoin to the traditional financial system are likely to see continuous intensification of regulatory scrutiny and enforcement actions. However, as we saw in China, escalated efforts will likely only highlight the need for Bitcoin, expand its brand awareness and spawn off exchange transactions (Streisand Effect).

In essence, open-source software projects like Bitcoin are just information – software written in a computer language called code. Since it is just code, Bitcoin can be printed out, written down, spoken or memorized. Bitcoin is also a form of money, so it makes money and information the same thing. This concept was summed up nicely by Naval Ravikant in 2017:

**“This is one of the crazy things about this concept because money and speech turned out to be the same thing – money, information and math – they’re the same thing. In a Bitcoin world, I can literally write down my Bitcoin address and keys on a**

**piece of paper and put it in a safety deposit box. It's basically in cold storage, I could even put it in my head. I can memorize the key phrases and I could cross national borders with \$1 billion in my brain. It's a very powerful but literally mind bending concept in that sense."**

The First amendment of the United States Constitution guarantees that all Americans have the power to exercise their right to publish and distribute anything they like, without restriction or prior restraint – which includes software code like that which constitutes Bitcoin. Established legal precedent in the United States explicitly protects software code under the First Amendment. Consider the case of PGP:

"In 1995, the US Government had on the statute books, laws that restrict the export of encryption software products from America without a license. These goods are classified as 'munitions'. The first versions of the breakthrough Public Key Encryption software "Pretty Good Privacy" or "PGP", written by Philip Zimmerman had already escaped the USA via Bulletin Board Systems from the moment it was first distributed, but all copies of PGP outside of the United States were "illegal". In order to fix the problem of all copies of PGP outside of America being encumbered by this perception, an ingenious plan was put into motion, using the first Amendment as the means of making it happen legally. The source code for PGP was printed out. It's as simple as that. Once the source code for PGP was printed in book form, it instantly and more importantly, unambiguously, fell under the protection of the First Amendment."

### **Bitcoin unambiguously falls under the Freedom of Speech Protections offered by the First Amendment to the United States Constitution.**

For these reasons, it is unlikely that any major government would attempt to ban Bitcoin outright as, not only would it contradict with freedom of speech laws, it would also create a tidal wave of publicity (again, Streisand Effect). Central banks have acknowledged this reality. Former chairwoman of the Federal Reserve Janet Yellen confirmed "The Federal Reserve simply does not have the authority to supervise or regulate Bitcoin in any way." So, Bitcoin can't be shut down, is virtually immune to regulation and leverages economic incentives to grow relentlessly. Its very existence is a game changer for almost everyone in this world, especially central banks who now face an existential threat to their business model.

### The Long Game

Money is how we keep score in the game of life. *Game theory* explores how rational people make strategic decisions in different scenarios. It is based in purely mathematical terms and has applications in any domain where people must choose whether to cooperate or compete with each other. The standard game analyzed by game theory is the Prisoner's Dilemma:

*Two members of a criminal gang, Alex and Bobby, are arrested and imprisoned. Each prisoner is in solitary confinement with no means of communicating with the other. The prosecutors lack sufficient evidence to convict the pair on the principal charge, but they have enough to convict both on a lesser charge. Simultaneously, the prosecutors offer each prisoner a bargain. Each prisoner is given the*

opportunity either to betray the other by testifying against them, or to cooperate with the other by remaining silent. The possible decisions and outcomes are:

- If Alex and Bobby both betray each other, each of them serves 2 years in prison
- If Alex betrays Bobby but Bobby remains silent, Alex will be set free and Bobby will serve 3 years in prison
- If Bobby betrays Alex but Alex remains silent, Bobby will be set free and Alex will serve 3 years in prison
- If Alex and Bobby both remain silent, both of them will only serve 1 year in prison (on the lesser charge)

This game decisions and its outcomes are summarized in this table:

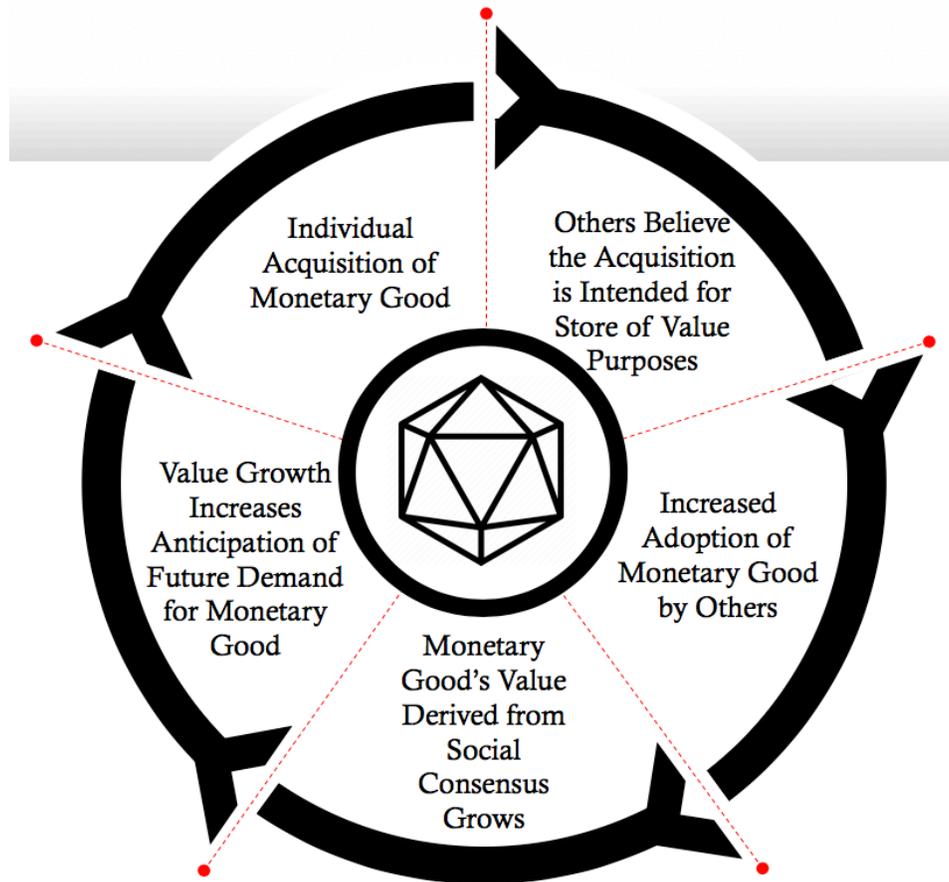
		Bobby's decisions	
		Bobby stays silent (cooperates)	Bobby testifies (betrays)
Alex's Decisions	Alex stays silent (cooperates)	Alex and Bobby each serve 1 year	Alex serves 3 years, Bobby goes free
	Alex testifies (betrays)	Alex goes free, Bobby serves 3 years	Alex and Bobby each serve 2 years

This Prisoner’s Dilemma game converges on a *Schelling Point*, which is a solution that people will tend towards in the absence of communication or definitive trust (in other words, in an adversarial environment). The Schelling Point in the Prisoner’s Dilemma is that Alex and Bobby both choose to betray each other, as each would risk 3 years in prison if one chose to remain silent and the other testified. Since both have an incentive to testify, the optimal strategy for this game is that they both betray, despite their mutual silence offering the best outcome for them both.

Since money is an adversarial game (there are winners and losers) express communications between players cannot always be trusted. Therefore, the Schelling Point of monetary competition is to choose the available good which exhibits the highest hardness, because people (potential adversaries) must be restrained from creating new monetary units to steal the value stored within them. This is exactly the reason market-driven natural selection is so ruthlessly effective at promulgating hard money, as people are constantly seeking to acquire value and store it in the most reliably hard monetary technology available.

Monetary goods, like Bitcoin, are valued based on their game theoretic qualities – meaning each market participant values a monetary good based on their appraisal of whether and how much other participants will value it (in the same way that prisoners Alex and Bobby must anticipate each other’s decisions to make effective decisions of their own). The earlier one is able to anticipate the future demand for a monetary good, the greater the advantage conferred to the prognosticator; as it can be acquired more cheaply than when it becomes widely

demanded at a later time. Further, when one acquires a good expecting that it will be demanded as a future store of value, it actually hastens the adoption of the good by others for that particular purpose, as their selection of a store of value is partly influenced by their perception of your intentions which drove you to acquire the monetary good in the first place. This seeming circularity is another positive feedback loop that drives societies to converge on a single store of value (another aspect of the winner take all dynamic):

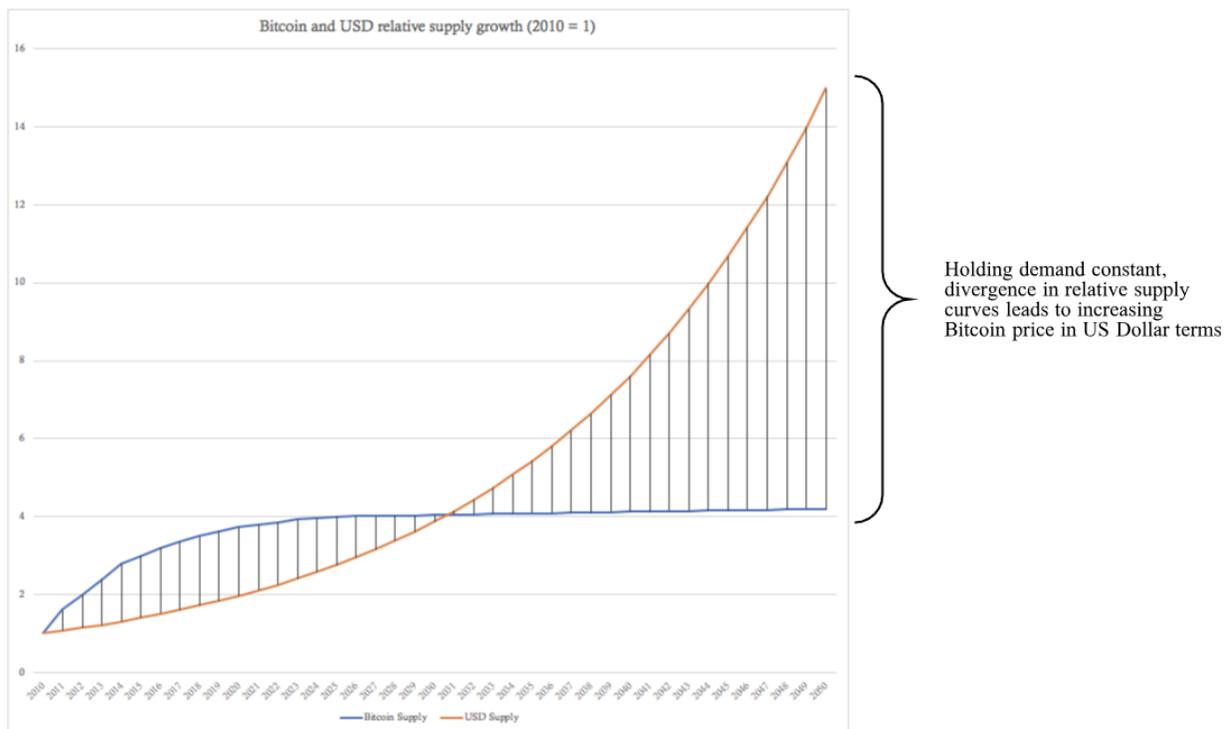


In game theoretic terms, total market dominance by a single store of value with a superior stock-to-flow ratio is known as a *Nash Equilibrium* – a game state where no player has an incentive to deviate from his chosen strategy after anticipating the most likely choices of all his opponents. Throughout all human history, societal convergence on a single form of superiorly hard money is the Nash Equilibrium of monetary competition. As we saw with gold in the 19<sup>th</sup> century, when multiple societies converge on a single store of value, they see a substantial decrease in trade costs and an attendant increase in free trade and capital accumulation (La Belle Époque). Only the past century, dominated by government fiat money, is anomalous in this respect.

**Hard money is the norm of human history, and we are seeing its reemergence with Bitcoin.**

The monetization process, as we saw with gold and are now seeing with Bitcoin, is game theoretic. People must decide individually how best to store the value created by their time spent in production. This decision is based on the anticipated beliefs, decisions and actions of others in relation to the monetary technologies available to them. The complex interaction of these decision dynamics is how people spontaneously ascribe a good the role of money and why the hardest money always wins. In this way, hard money is an emergent property of indirect exchange just like money is an emergent property of direct exchange.

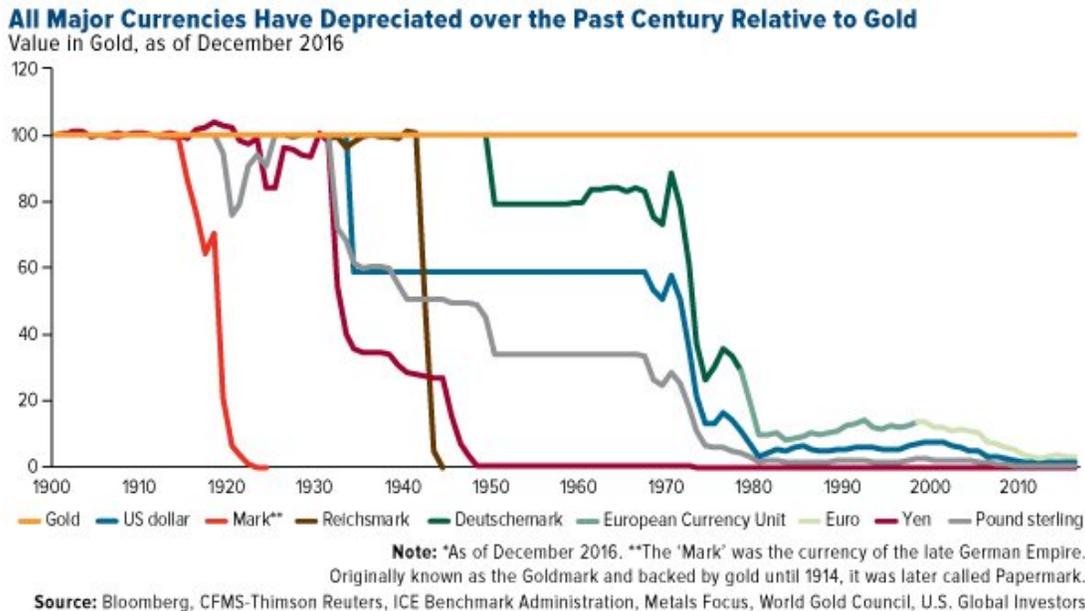
This emergent property perspective is exactly why value stored in softer forms of money is totally absorbed by hard money every time they interact within an economic network. Existing amid the expansionary monetary policies being practiced by every central bank in the world today, Bitcoin's price will continue to increase as the ratio of government fiat money in circulation to Bitcoin units in circulation diverges ever-further:



This graphic, which is strictly illustrative, simply shows that divergence in supply curves of Bitcoin and US Dollars will lead to the appreciation of Bitcoin in US Dollar terms, even without any increase in the demand for Bitcoin (as we have seen, demand for Bitcoin has been surging). The same dynamic is applicable to all modern government monies, as every central bank in the world is engaged in aggressive expansionary monetary policy. In the game of international government fiat monetary competition, the Nash Equilibrium is all currencies inflated into worthlessness. On this race to the bottom, those with easiest access to freshly printed money will expropriate as much value as possible (via the Cantillon Effect) and use it to acquire real estate, gold or other inflation resistant assets (such as Bitcoin). This game

theoretic perspective clearly explains why virtually all soft government fiat currencies have trended towards eventual worthlessness.

Next, we show how all major fiat currencies have depreciated almost completely against gold since 1900 (notice the steep decline in 1971 when the peg to gold was completely severed):



As we have seen throughout history, every time hard money encounters soft money in a trade network, it has outcompeted it into extinction. We saw earlier how gold, possessing superior hardness, demonetized silver with dire economic consequences for those societies that remained on a silver standard the longest, such as China and India. Now it is gold that faces a monetary competitor with superior hardness, and it is likely that it will gradually become demonetized as people convert to Bitcoin for its unparalleled store of value properties. This will happen slowly, and gold may indeed maintain some of its monetary use case given the vast holdings of central banks, mankind's deep history with the monetary metal (Lindy Effect), its relatively high and predictable stock-to-flow ratio and the fact that some people may always prefer a tangible store of value over a digital alternative. For government money, the competitive situation is much more dire.

The Event Horizon

Hyperinflation is a particular type of demonetization, unique to government fiat money, that did not exist under the gold standard. Hyperinflation occurs when a government produces new monetary units at an accelerating pace to finance expenditures or service debt burdens, which pushes the value of its currency down at the same accelerating rate. The value of a hyperinflating currency collapses against the most liquid goods available to the society first (like gold or the US dollar) and then, depending on relative availability, against real goods such as real estate and commodities. This sequence is caused by individual's attempting to maximize their exchange optionality as they escape their failing currency and prepare to navigate highly uncertain economic conditions. When hyperinflation intensifies, currencies

begin falling against perishable goods. It is common to see grocery stores completely emptied out in societies suffering from the late stages of hyperinflation. Eventually, the society will either devolve to a barter economy or adopt a new medium of exchange, as we saw in Zimbabwe when its failing dollar was ultimately replaced by the US dollar. This process is arduous as the replacement currency is often scarce as foreign banking institutions are either reluctant to or restricted from providing liquidity.

As Bitcoin is the hardest form of money in existence, it will continue to appreciate against a backdrop of hyperinflating, soft government fiat currencies even without any increase in demand for Bitcoin (as illustrated in the above graphic). Eventually, this will lead to an inflection point in some economies where users rush to exit from their failing currency to get into Bitcoin to protect their wealth from further confiscation. This transition will have similar dynamics to other demonetization and hyperinflation events, however it will also be different given Bitcoin's unique properties as a monetary technology. A Bitcoin-induced currency demonetization is called a *hyperbitcoinization event* and is different from hyperinflation in two critical respects.

First, hyperinflation occurs with restricted competition with other fiat currencies, since a government can easily enforce capital controls that selectively prohibit inflows or outflows of government money, whereas hyperbitcoinization occurs because of direct competition with Bitcoin, which can easily cross borders as it is immune to capital controls. This will cause hyperbitcoinization to happen much faster than a hyperinflation event, since governments will have great difficulty preventing Bitcoin trading within their borders due to its purely informational nature. Given governments' inability to shield their local currencies from direct competition with Bitcoin and the high opportunity cost of holding a depreciating form of money, once a hyperbitcoinization event reaches a critical mass it will happen quickly.

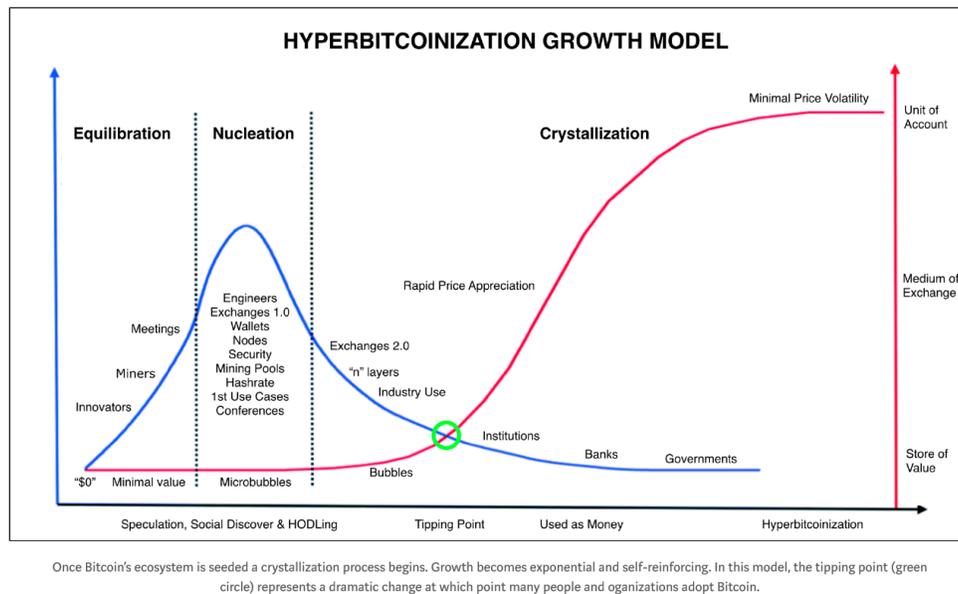
Second, in hyperinflation, the governments expand money supplies in an attempt to outpace people's inflation expectations. As governments forms a habit of inflating money supplies, people form a habit of anticipating rising prices and seek alternative stores of value. Governments, in turn, must print incrementally more money to stay ahead of inflation expectations and generate the same economic effect with each new monetary unit produced. With no alternative monetary media in which to escape, prices surge until a breaking point is reached. Hyperinflation is extremely disruptive to an economy as it forces people to switch from the worst form of government fiat money available to them to some other soft government fiat money (at best) or ends in total economic collapse (at worst). In hyperbitcoinization, users have a supranational monetary media in which to escape centrally planned economies. Therefore, a hyperbitcoinization event should be much less disruptive to the economy, as people will be trading in an inferior form of money for a superior one. Seeing as hyperbitcoinization should happen fast, people will quickly become accustomed to dealing in Bitcoin, which will protect deteriorating wealth and stabilize economic conditions.

Hyperbitcoinization will likely be a confusing, potentially chaotic, time for many people. Initially, it will probably occur at the periphery, with the countries inflating their currencies the fastest experiencing it first. Stories of this will spread quickly in the digital age and add to the believability of Bitcoin, all while it continues to benefit from the resultant increases in

demand, network effects and the Lindy Effect. As more people wake up to the reality of hard money, we would expect the pace of this global transition to accelerate until all soft money is outcompeted into extinction. Fortunately, it will happen relatively quickly, since Bitcoin is immune to capital controls, and act as a stabilizing force for the world economy going forward (since hard money resists market distortions and remains firmly rooted in economic reality).

**Like a star orbiting a black hole, any established monetary order that goes beyond the event horizon of hyperbitcoinization will inevitably collapse into Bitcoin’s singularity.**

Next, we show how a hyperbitcoinization event is likely to unfold:



The estimates of how valuable Bitcoin would become after global hyperbitcoinization vary based on what weighting is included for different stores of value (gold, government money, real estate, stocks, bonds, art, oil and other commodities are all used for this purpose today) but, using simple math for our directional analysis, if Bitcoin demonetizes just gold it would be valued at about \$400K per coin (\$8T/20M coins in 2025). If it demonetizes government money as well, it would be valued at about \$5M per coin (\$100T/20M coins in 2025). As awareness of Bitcoin and its potential impact spread, the long game becomes even more interesting. Considering Bitcoin represents an existential threat to government fiat money and central banks, we must also consider their decisions from a game theoretic perspective.

Reverse Bank Run

Although it is still considered magic internet money by most people today, its continued existence and appreciation will attract more attention from high-net-worth individuals, institutional investors and then, possibly, central banks. As we have learned, central banks still rely on gold as a means of final settlement, as it was (before Bitcoin) the only monetary

medium entirely free of counterparty risk (cash money). However, transporting and securing gold is an extremely expensive process fraught with operational risk. These costs and risks are the reason final settlements between banks occur very infrequently.

With the transaction throughput available on the Bitcoin network today, the global group of 850 central banks can perform daily final settlement with one another. With each central bank serving an average of 10 million customers, this would more than cover the entire world's population. In a world in which central banks adopted a Bitcoin standard, governments would no longer have the ability to increase the money supply and banks would begin to compete freely with one another by offering various physical and digital Bitcoin-backed monetary instruments and payment solutions. By using the technologies introduced by Bitcoin, cryptographic digital certainty can be applied to bank accounting and help expose those that engage in fractional reserve banking. This may lead to Bitcoin realizing its ultimate use case: the fastest and most efficient system for global final settlement across long distances and national borders. Despite the clear advantages of a system such as this, central banks are unlikely to give up their monopoly control over the existing monetary order willingly.

As people begin to voluntarily exit fiat currencies into Bitcoin to protect their wealth, as is already taking place in countries like Venezuela today, it will likely grab even more attention from central banks. As central banks are effectively losing customers, they will need to hedge the *going concern risk* posed to their business model. Central banks today hold reserves mainly in US Dollars, Euros, British Pounds, IMF Standard Drawing Rights and gold. These reserves are used to settle accounts and defend the market price of their respective currencies. Should Bitcoin remain on its current trajectory, and considering its superiority as a final settlement layer, it is possible that at least one central bank somewhere in the world will add Bitcoin to its reserves, if for no other reason than to defend the market price of its government fiat money, as is consistent with their strategy for gold.

The most likely scenario is that a central bank will seek to own part of the Bitcoin network as an insurance policy against it succeeding. Strategically, it makes sense for a central bank to spend a small amount acquiring some of Bitcoin's supply today. For example, consider that the authorities of a central bank today judge that, although chances of a hyperbitcoinization event are extremely remote, it would represent an extinction-level event for their business. Mathematically, using Bitcoin's approximate price today of \$4K and its expected post-hyperbitcoinization price of \$5M, unless the central bank is more than 99.92% certain that this event will NOT happen then it is prudent to allocate at least 0.08% of their assets into Bitcoin as a perfect hedge against its success (since price growth from \$4K to \$5M is a 1250x increase, an allocation of 0.08% of assets would keep a central bank at even-money should a hyperbitcoinization event play out).

Game theory tells us that the first central bank to buy Bitcoin will trigger a reverse bank run, as its decision will alert the rest of the central banks who will be compelled by self-interest to follow suit. The first purchase by a central bank will cause the price of Bitcoin to rise significantly, causing others to move in based on their anticipation of future demand and compounding the effect as more central banks enter the market; making it progressively more expensive for later entrants. As central banks keep trying to anticipate the moves and strategies

of one another, a game theoretic positive feedback loop will ensue that converges on a hard money Schelling point similar to that of free market monetary competition, thus triggering a global competition among central banks for maximal Bitcoin accumulation. A smart play for a central bank under the circumstances would be for it be the first to buy a small share of the Bitcoin network. An even smarter play would be for a central bank to purchase Bitcoin without announcing it, allowing it to begin accumulation at lower prices.

Similar to the transition to the gold standard in the 19<sup>th</sup> century, network effects would eventually take hold as more central banks bought some Bitcoin, increasing its liquidity and making it more marketable, thus creating ever-larger incentives for other central banks to join. After a sufficient minority of central banks have purchased part of the Bitcoin network, the minority rule will reach its final step and begin imposing the immutable rules of Bitcoin on the established monetary order. Once this reverse bank run on Bitcoin became public knowledge (as tends to happen easily in the digital age), it would be the ultimate seal of legitimacy for Bitcoin adoption and would add even more force to its ascent in the marketplace as this global game of Bitcoin accumulation would reach a fever pitch. Even at the largest scales of the financial system, Bitcoin converts individual self-interest into the growth of its network.

You may find this prospect hard to believe. About 25 years ago, handheld touchscreen supercomputers with wireless global interconnectivity were hard to believe too. Change keeps happening faster and faster. Remember, each central bank will value Bitcoin based on its appraisal of whether and how much other central banks will ultimately value it. As they will all be conducting the same strategic analyses, they will undoubtedly realize the dilemma they face – either ignore Bitcoin and watch it continue to outcompete and accelerate the failure rate of fiat currencies thereby loosening their control over the established economic order or choose to adopt Bitcoin as a reserve asset and trigger a game of accumulation against other central banks and legitimize it as an asset which will culminate in the loss of their monopoly position in the market for money. Operating in an adversarial environment, game theory tells us that so long as Bitcoin continues to operate in its current form, central banks (like the prisoners Alex and Bobby) will eventually be faced with strategic choices such as these to protect their own interests. At some point, the substantial advantage imparted to the central bank that moves first will become an overwhelming incentive to at least one, causing it to be the first to make its move, thereby triggering the reverse bank run on Bitcoin.

### A Path to Prosperity

Making predictions is risky business, wrong answers are innumerable, and the right answer is singular. Accurate predictions are rare. By weaving together historical knowledge and awareness of current trends, one can develop a perspective on what technological innovations are possible. The biggest mistakes people make when making such predictions are:

- Forming an opinion on the innovative potential without considering it deeply (Blockbuster quickly reaching a decision to pass on buying Netflix for \$50M)
- Disregarding an innovation because it contradicts a closely held worldview (Kodak refusing to accept the disruptive potential of digital photography as they spent 100 years building a business model centered on chemical film)

- Overlooking an innovation because it is too small or threatens a position of power (major newspapers refusing to develop an online presence early on)

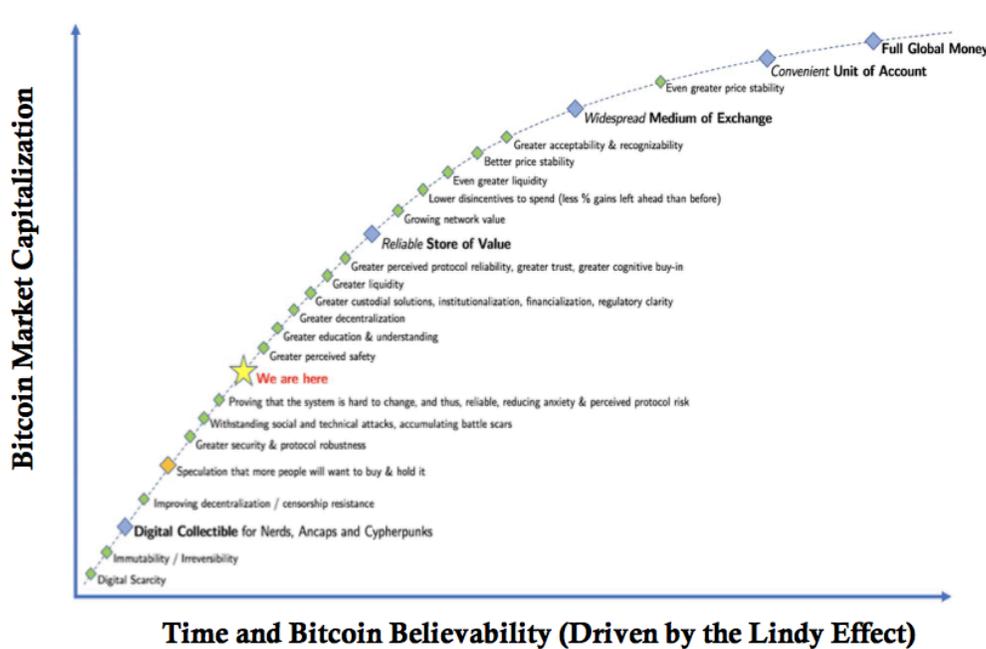
Practicing a beginner's mindset and reasoning from first principles is critical for effective foresight. Pulling together everything we have discussed in this paper, we will now propose a potential path forward for Bitcoin based on the historical competitive dynamics of money, current macroeconomic trends and game theory. We will start from the inception of Bitcoin:

1. Bitcoin is first perceived as an internet toy for cryptographers (Minority Rule – Step 1)
2. Its rapid price increase makes a small group of people rich, engages free market fanatics and brings media attention. Its hyper-volatile price presents itself early (Hodlers of Last Resort – Layer 1).
3. The media, financial and tech establishments - having failed to buy Bitcoin early and benefit from its meteoric rise - denounce it as a Ponzi scheme, the MySpace of Cryptocurrencies and the greatest bubble of all time (Streisand Effect).
4. A large number of scammers jump onto the Bitcoin hype-train and create their own cryptocurrencies claiming to be superior though lacking critical qualities including decentralization, security and immutable governance. Bitcoin's serendipitous first mover advantage, multi-sided network effects and its brand awareness fueled by the Nakamoto creation myth preserves its market dominant position.
5. Retail investors, venture capitalists and hedge funds - lacking understanding of monetary economics and applying inappropriate valuation models - invest into other cryptocurrencies, creating more noise and confusion as the prices of these altcoins increase at a rate higher than Bitcoin.
6. Well-connected venture capitalists and hedge funds are given discounts on the investments only to then dump much of what they bought onto retail investors.
7. Given their high correlation to Bitcoin and lacking utility, the world watches as the bear markets continue to wipe out more and more alternative cryptoassets as most fail to deliver any useful product, although some succeed in other market spaces. Features that are proven in the market by other cryptoassets are subsumed by Bitcoin (Decentralized Network Archetype). Bitcoin price volatility persists but annual low prices continue to ascend relentlessly (Holders of Last Resort – Layer 2).
8. Trust in Bitcoin increases over time (Lindy Effect) and its market price continues its upward yet volatile trajectory (Fractal Wave Patterns).
9. People, burned in the altcoin craze, witness and learn about Bitcoin's undisputed superiority across all monetary characteristics, especially its hardness (Holders of Last Resort – Layer 3).
10. On the eve of and during the next bull markets, Bitcoin's absolute scarcity and antifragile characteristics exacerbate investor FOMO (Game Theoretic Positive Feedback Loop). Some investors are inevitably caught in the subsequent Bitcoin price crash (Fractal Wave Pattern)(Hodlers of Last Resort – Layer 4).
11. Hyperinflating fiat currencies are further contributing to the adoption of Bitcoin as it becomes the only means of preserving wealth for many people, making Bitcoin a legitimate store of value. Governments scramble to try and enforce capital controls and create propaganda against Bitcoin, just like they did to gold in the 20<sup>th</sup> century. Capital controls prove to be impotent and the propaganda against Bitcoin incites

- internet and media narratives that regard it as a tool for freedom (Antifragility). Government dissent highlights the need for Bitcoin in the first place (Streisand Effect).
12. Investors and high net-worth individuals are convinced to allocate a small portion of their assets into Bitcoin to capture further growth, hedge against inflation and increase the risk adjusted returns of their traditional portfolios (Minority Rule – Step 2)
  13. Increases in demand for Bitcoin necessarily involve a reduction in demand for fiat currencies, causing even higher inflation rates (Gresham’s Law). At great expense and effort, governments messily issue their own cryptocurrencies but fail to relinquish control over monetary policy, which makes them uncompetitive against Bitcoin (Market-Driven Natural Selection). Governments covertly attempt to attack the Bitcoin network, which only strengthens it (Antifragility). Media coverage about Bitcoin shifts towards its use as hard money (Skin in the Game) and its importance for prosperity (Hodlers of Last Resort – Layer 5).
  14. Activists share the message that soft money creates social inequality (Soul in the Game) by disproportionately taxing the poorest via inflation (Cantillon Effect). This message spreads fast in a world of ever-more crashing fiat currencies and people rush to exit their local currencies for the safety of Bitcoin, triggering the first hyperbitcoinization events (Hodlers of Last Resort – Layer 6). Bitcoin mining hardware becomes commoditized and many citizens join mining pools (Decentralized Network Archetype)(Skin in the Game).
  15. Central banks, in an attempt to adapt to the new conditions and hedge going concern risks, quietly start to accumulate Bitcoin as a reserve asset, consistent with their gold strategy. A former central bank employee leaks a confidential strategy document regarding Bitcoin (Soul in the Game) which triggers other central banks to begin purchasing Bitcoin, causing its price and perceived legitimacy to increase at an accelerating rate (Game Theoretic Positive Feedback Loop)(Final Fractal Wave Pattern)(Hodlers of Last Resort – Layer 7).
  16. Bitcoin’s market capitalization reaches tens of trillions in US Dollar terms. Bitcoin’s volatility subsides as both its market capitalization and liquidity are larger than ever (Mature Hard Money).
  17. Early Bitcoin investors are now sitting on significant unrealized gains and are willing to part with some of their Bitcoin to pay for their purchases. With its purchasing power stabilized, the opportunity cost of transacting with Bitcoin is diminished and its use as a Medium of Exchange increases.
  18. With the world more digitized than ever before, people increasingly demand to be paid in Bitcoin now that it has proven to be a good store of value given its disinflationary, and later deflationary, monetary policy (Schelling Point)(Hodlers of Last Resort – Layer 8).
  19. With the addition of highly performant transaction layers, Bitcoin’s use as a Medium of Exchange becomes a widespread. Bitcoin, functioning as the core of a new innovation wave called the TrustNet, is christened as a momentous innovation.
  20. As more consumers and merchants become accustomed to transacting in Bitcoin, it gradually becomes used as a Unit of Account.
  21. Due to the emergence of a superior, uninflatable monetary standard, people increasingly store their wealth in Bitcoin rather than fiat currencies (Minority Rule – Step 3)(Hodlers of Last Resort – Layer 9).

22. Central bank monopolies on money are described by historians as a relic of the past. Bitcoin is regarded as the catalytic innovation of the separation of money and state. A free market for money is now the defining feature of free market capitalism (Nash Equilibrium).

This path to full global money will take Bitcoin through many stages:



Time Will Tell

All time beyond the present is unknown. All predictions should always be taken with a grain of salt. The future is uncertain, and the end can always be near. Anyone who claims they can tell you what is going to happen in the future is wrong. All we can do is study the patterns of the past and use them as our map to navigate the ever-advancing territory of the future.

In a free market, hard money has always outcompeted soft money into extinction. Hard money has been the norm throughout all of human history, except for the past 100 years in which we have been coerced into using soft government fiat money. Societies operating on hard money systems optimize for the allocation of the ultimate resource, human time, which increases prosperity for everyone.

In the digital age, markets are increasingly interconnected. Bitcoin is digital cash money. It is a new social institution that lives in accordance with its own laws. Its core components are human self-interest and mathematics. Bitcoin is the hardest monetary technology in history. Will it continue to outcompete and win the throne of full global money?

Only time will tell.

**Sources:**

1. The Bitcoin Standard by Saifedean Ammous (highly recommended; this essay is largely inspired, guided and adapted from this masterful book)
2. Antifragile by Nassim Nicholas Taleb
3. Skin in the Game by Nassim Nicholas Taleb
4. The Rational Optimist by Matt Ridley
5. The Age of Cryptocurrency by Paul Vigna and Michael J. Casey
6. The Truth Machine by Paul Vigna and Michael J. Casey
7. Sapiens by Yuval Harari
8. The Bullish Case for Bitcoin by Vijay Boyapati  
<https://medium.com/@vijayboyapati/the-bullish-case-for-bitcoin-6ecc8bdecc1>
9. World Gold Council <https://www.gold.org/>
10. Why America Can't Regulate Bitcoin <https://hackernoon.com/why-america-cant-regulate-bitcoin-8c77cee8d794>
11. Yellen: Fed Doesn't Have the Authority to Regulate Bitcoin  
<https://blogs.wsj.com/economics/2014/02/27/yellen-fed-doesnt-have-authority-to-regulate-bitcoin/>
12. Misir Mahmudov [https://twitter.com/misir\\_mahmudov](https://twitter.com/misir_mahmudov)
13. Bitcoin's Incentive Scheme <https://medium.com/@hugonguyen/bitcoins-incentive-scheme-and-the-rational-individual-dc20effa4715>
14. Bitcoin obituaries <https://99bitcoins.com/bitcoin-obituaries/>
15. Naval Ravikant <https://twitter.com/naval/status/877468095236849664>
16. The Trade of the Decade: Betting on Bitcoin  
<https://www.forbes.com/sites/katinastefanova/2018/11/28/the-trade-of-the-decade-betting-on-bitcoin/#11a541df458a>
17. The Fed has Lost Control <https://seekingalpha.com/article/4229687-sentiment-speaks-clearly-fed-lost-control?ifp=0>
18. Bitcoin's Social Contract <https://medium.com/s/story/bitcoins-social-contract-1f8b05ee24a9?sk=27e8cf65d45c46ffa1466ce2ac31b48>
19. Bitcoin: A Decentralized Super-Organism  
<https://medium.com/@BrandonQuittem/bitcoin-is-a-decentralized-organism-mycelium-part-1-3-6ec58cdcf6aa6>
20. What I mean by Skin in the Game <https://medium.com/incerto/what-do-i-mean-by-skin-in-the-game-my-own-version-cc858dc73260>
21. La Belle Époque [https://en.wikipedia.org/wiki/Belle\\_%C3%89poque](https://en.wikipedia.org/wiki/Belle_%C3%89poque)
22. United Nations Development Programme's Human Development Report 2005  
[http://hdr.undp.org/sites/default/files/reports/266/hdr05\\_complete.pdf](http://hdr.undp.org/sites/default/files/reports/266/hdr05_complete.pdf)
23. DAOs, Democracy and Governance by Ralph Merkle  
<http://merkle.com/papers/DAODemocracyDraft.pdf>
24. Diffusion of Innovations by Everett Rogers <https://www.amazon.com/Diffusion-Innovations-5th-Everett-Rogers/dp/0743222091>
25. An Expert Called Lindy <https://medium.com/incerto/an-expert-called-lindy-fdb30f146eaf>

26. The Most Intolerant Wins: The Dictatorship of the Small Minority <https://medium.com/incerto/the-most-intolerant-wins-the-dictatorship-of-the-small-minority-3f1f83ce4e15>
27. Bitcoin Market Price (USD) Log Scale <https://www.blockchain.com/charts/market-price?scale=1&timespan=all>
28. PoW is Efficient <https://blog.picks.co/pow-is-efficient-aa3d442754d3>
29. How a Bitcoin Transaction Works <https://visual.ly/community/infographic/technology/bitcoin-infographic>
30. Rules for Biologically Inspired Adaptive Network Design <http://science.sciencemag.org/content/327/5964/439>
31. Bitcoin is a Decentralized Organism <https://medium.com/@BrandonQuittem/bitcoin-is-a-decentralized-organism-mycelium-part-1-3-6ec58cdcfaa6>
32. Basic Attention Token (BAT) <https://basicattentiontoken.org/>
33. Blockstream Bitcoin Network Satellites <https://blockstream.com/satellite/#>
34. The Fifth Protocol [www.startupboy.com](http://www.startupboy.com)
35. Bitcoin Obituaries <https://99bitcoins.com/bitcoin-obituaries/>
36. The Functions of Money [https://www.econlib.org/library/YPDBooks/Jevons/jvnMME.html?chapter\\_num=4#book-reader](https://www.econlib.org/library/YPDBooks/Jevons/jvnMME.html?chapter_num=4#book-reader)
37. Bitcoin Adoption Price Theory <https://medium.com/@mcasey0827/speculative-bitcoin-adoption-price-theory-2eed48ecf7da>
38. Has Bitcoin surpassed the OTC Gold Market in Settlement volumes? <https://bitcoinexchangeguide.com/crypto-researcher-nic-carter-says-bitcoins-settlement-value-has-passed-gold/>
39. The Ultimate Resource by Julian L. Simon
40. BP Statistical Review of World Energy <https://www.bp.com/en/global/corporate/energy-economics/statistical-review-of-world-energy.html>
41. Current Thinking <https://www.nytimes.com/2007/06/03/magazine/03wwln-essay-t.html>
42. Bitcoin Price and Volatility Chart <https://www.buybitcoinworldwide.com/volatility-index/>

**Glossary (terms are in the same order as they are explained within the essay):**

1. *Division of labor* – A natural outcome of human exchange, the division of labor is the assignment of different aspects of the production process to different people to improve efficiency and drive specialization. Since not all productive efforts are laborious, especially in a knowledge economy, this is also referred to as the division of knowledge.
2. *Specialization* – A natural outcome of the division of labor in which people begin to focus on and specialize in particular crafts or productive processes. Since people are able to focus their energies on a narrower set of productive skills, they are able to come up with better ways to producing. In this way, specialization drives innovation.
3. *Productivity* – The effectiveness of productive effort, measured as the rate of productive output per unit of human time. Productivity is improved by specialization, tools and other technological innovations.
4. *Scope of Trade* – The amount and variety of people reachable within an economy for purposes of exchanging goods and services.
5. *Prosperity* – Driven by an increasing division of labor and knowledge, prosperity is measured by the aggregate time savings of a society. Time saved is freedom to spend it otherwise, therefore free societies are prosperous.
6. *Direct Exchange* – Exchanging one good for another directly, commonly called barter.
7. *Non-Coincidence of Wants* – A problem inherent to direct exchange in which what you are seeking to acquire by trade is produced by someone who doesn't want what you have to offer. The non-coincidence of wants can occur in any of three distinct dimensions: scales, locations and time frames. The effectiveness of money can be assessed by how well it satisfies these lacking coincidences.
8. *Indirect Exchange* – A method of exchange where one uses an intermediary good, a medium of exchange, to overcome the non-coincidence of wants problem.
9. *Medium of Exchange* – The first function of money. Any good used as an intermediary good in an indirect exchange is a medium of exchange. Over time, people naturally converge to a single or a few media of exchange to simplify trade.
10. *Salability* – The ease with which a monetary good can be sold on the market at any point in time with the least loss in price. Salability of a good is assessed in terms of how well it addresses the three dimensions of the non-coincidence of wants problem.
11. *Store of Value* – The second function of money. It is determined by how well a monetary good can maintain its value and salability over time.
12. *Inflation* – A dilution in the value each unit of a monetary good as new units are created. Inflation transfers value from existing holders of of monetary units to those with the ability to produce additional monetary units of the same kind. Common with government money, inflation is a stealthy form of theft from savers.
13. *Hard Money* - A form of money that is more trustworthy as a store of value because it resists debasements of value and therefore maintains salability across time. The hardness of a monetary good, also known as its soundness, is determined by its stock-to-flow ratio. Bitcoin is the hardest form of money that has ever existed.
14. *Stock-to-Flow Ratio* – The stock of existing monetary units divided by its newly created supply flow over a certain time period, usually one year. This ratio is the key metric in determining a money's relative hardness and therefore its salability across time.

15. *Soft Money* – A form of money used as a store of value that can have its supply increased easily. Soft money always suffers from supply increases as producers of the new supply flow seek to steal the value stored within it, which ultimately destroys the wealth of those using it as a store of value. Government fiat money is the softest form of money that has ever existed.
16. *Metcalf's Law* - A concept used in computer networks and telecommunications to represent the value of a network. Metcalfe's Law states that a network's impact is the square of the number of nodes in the network. For example, if a network has 10 nodes, its inherent value is 100 ( $10 * 10$ ).
17. *Network Effects* - The incremental benefit attained by adding a new member to a network for all existing members in that same network. Similar to the telephone and modern social media platforms, money is a network that becomes exponentially more valuable as more people join it because the number of possible connections it allows is proportional to the square of the number of its total network participants
18. *Winner Take All Dynamic* – A competitive dynamic inherent to monetary evolution. If all three key salability characteristics can be gathered under a single monetary technology, then that technology will acquire all (or, at least, most) of the market share when competing with other forms of money.
19. *Time Preference* - The ratio at which an individual values the present relative to the future. A lower time preference indicates a longer term orientation, whereas a higher time preference indicates a shorter term orientation. Societies run on hard money systems are incentivized to have lower time preferences.
20. *Capital Goods* - Goods used exclusively for the production of other goods. Capital goods increase productivity and enable a more sophisticated production process that can be extended over longer time horizons.
21. *Investment* – The deferral of consumption to invest time in producing capital goods.
22. *Positive Feedback Loop* - A process in which its outputs also serve as its inputs. Also called a virtuous cycle or flywheel effect, this process creates compounding effects over time. Positive feedback loops play an important role in biology, chemistry, psychology, sociology, economics and cybernetics.
23. *Interest Rate* – The price of borrowed money. Provides an incentive for savers to loan money to borrowers. The interest rate is the price point at the intersection of the supply of and demand for loanable funds. This price is artificially manipulated by central banks.
24. *Unit of Account* – The third function and final evolutionary stage of money. When a form of money becomes dominant prices are most commonly expressed in its terms, thus making it a unit of account.
25. *Price Signals* - The coordinating force of free market systems. Each individual decision maker can faithfully rely on the prices of goods relevant to their production process, as the prices themselves are a distillation of all known market realities into a single, actionable variable. Price signals are the nerve signals of the economic nervous system.
26. *Comparative Advantage* – Also known as a relative advantage, any producer that can produce a good relatively faster, cheaper or better than another is said to have a comparative advantage in that particular good.
27. *Market-Driven Natural Selection* – The evolutionary force that shapes societal ascription of monetary roles to particular goods. A process in which people naturally and rationally

- favor the most believable and trustworthy monetary technologies available to them. In free markets, the hardest forms of money available have always been naturally selected.
28. *Social Consensus* – A stock of values, ideas or beliefs shared among members of certain groups or communities. Social consensus is the source of a monetary good's market value along with the trust factors and permissions necessary to transact it.
  29. *Coin Clipping* – The ancient practice of collecting coins, melting them down and reminting them into newer versions with the same face value but less precious metal content. The residual metal content would be used to enrich the issuing authority. This thieving practice is remarkably similar in economic effect to modern government fiat money inflation.
  30. *Legal Tender* – Forms of money legally required to be accepted if offered to settle a debt.
  31. *Gresham's Law* – A monetary principle stating that "bad money drives out good". For example, if there are two forms of commodity money in circulation, which are accepted by law as having similar face value, the more valuable commodity will gradually disappear from circulation.
  32. *Skin in the Game* – A balance of incentives and disincentives used to regulate behavior. Those who have the ability to make consequential decisions must be exposed to the consequences of such decisions for a system to function properly. Skin in the Game is at the heart of hard money, as evidenced by the costliness of gold extraction and Bitcoin mining.
  33. *Price Elasticity of Supply* – The rate at which new supply of a good changes in relation to changes in its price.
  34. *Final Settlement* – Payment with a self-sovereign form of money (or bearer instrument) that represents the final extinguishment of debt since it is settled with money that is the liability of no one else (free of counterparty risk). Central banks still use gold to perform final settlement with one another today.
  35. *Counterparty Risk* – The risk inherent to transacting with forms of money that are the liability of someone else, such as government fiat money or gold certificates.
  36. *Bearer Instrument* – A self-sovereign monetary instrument that contains within the act of its physical possession all the permissions necessary for transacting with it. The possessor of a bearer instrument is presumed to be its rightful owner. Physical gold and Bitcoin are both bearer instruments.
  37. *Cash* – In its original sense, cash referred to central bank gold reserves, which was the dominant self-sovereign form of money during the 19<sup>th</sup> century. Therefore, gold was the cash money of that era. The word cash is derived from the French word *caisse* which means "money box".
  38. *La Belle Époque* – An era between the end of the Franco-Prussian War and the outbreak of World War I characterized by optimism, regional peace, economic prosperity and innovations. This era was made possible by the global hard money gold standard and ended when the Federal Reserve was established and World War I commenced.
  39. *Fractional Reserve Banking* – A form of banking in which banks lend out more money than their reserves can justify, which facilitated the creation of artificial money whose producers completely lacked skin in the game.
  40. *Seigniorage* – A method of profiting directly from the money creation process employed by governments and central banks. The profit equals the difference between the face value of a monetary unit and its production cost.

41. *Money Creation Process* – A process by which the money supply of an economy is increased artificially through both the printing press and credit creation. This is only possible with government fiat money and fractional reserve banking.
42. *Government Fiat Money* – The dominant form of money in the world today that is backed by absolutely nothing other than government decree. Government fiat money is the softest form of money that has ever existed.
43. *Cantillon Effect* – The transfer of wealth from the holders of government fiat money to those who receive new units freshly printed the same type of government fiat first. Since the earliest recipients can spend the newly printed money while it has its highest purchasing power, they are able to effectively steal wealth from those who receive it later. This effect is at the heart of the economic inequalities created by inflation.
44. *Market for Money* – The market for financial capital, which consist of the markets for loanable funds. No country in the world today has a free market for money, which is the most important market in any economy.
45. *Loanable Funds* – The amount of money owned by savers that is available to be loaned out to borrowers. In a free market, the price in this market (the interest rate) changes according to natural supply and demand forces. In central bank managed economies, the interest rate is artificially manipulated which leads to market distortions, capital misallocations, recessions and the business cycle.
46. *Recession* – An economy-wide, simultaneous failure of overextended projects as a result of centrally planned manipulation in the market for money.
47. *Business Cycle* – The cycle of economic boom and bust which has become the norm in the modern era as a result of government fiat money dominance and central bank market manipulation.
48. *Quantitative Easing* – A euphemism for the act of increasing money supply.
49. *Digital Cash Money* – A natively digital, self-sovereign monetary technology. Offers unprecedented levels of salability across scales, space and time.
50. *Double-Spend Problem* – A problem which prevented all other attempts at digital cash money from succeeding, since digital goods were infinitely replicable they could be spent more than once. Bitcoin solved this problem by combining proven technologies and economic incentives in a novel way.
51. *Digital Scarcity* – Digital items that are provably limited in quantity. Bitcoin is the world's first instance of both digital and absolute scarcity.
52. *Open-Source Software* – Software with a codebase that is fully accessible and transparent.
53. *Node* – A member of the Bitcoin network.
54. *Decentralized Architecture* – A form of networked software architecture in which the codebase and records are distributed amongst every node in the network.
55. *Everywhere and Nowhere* – A key property of decentralized software architecture, refers to the distributed nature of the information making the network resistant to censorship and regulation. It's everywhere in the sense that it is on every computer, it's nowhere in the sense that there is no central point to attack.
56. *Block* – A group of Bitcoin transactions that is sealed every 10 minutes.
57. *Blockchain* – A chronological chain of Bitcoin transaction blocks that are inextricably linked together all the way back to the genesis block mined by Satoshi Nakamoto. Once data is appended to the Bitcoin blockchain and sufficiently confirmed, it is impossible to erase.

58. *Trustlessness* – A property that refers to the ability of a Bitcoin owner to transact it successfully without the need to trust in any counterparty or intermediary. Can also refer to Bitcoin's immutable monetary policy, meaning there is no need to trust a central party not to debase Bitcoin since its laws are fixed mathematically. Before Bitcoin, only cash (in its original sense) money and transactions could be considered trustless.
59. *Proof-of-Work* – Complex mathematical puzzles which mining nodes compete to solve first to earn the block reward.
60. *Block Reward* – The reward a mining node receives when successfully solving proof-of-work. It consist of newly issued Bitcoin and the transaction fees generated within the latest block of transactions. The block reward is the incentive aspect of the Skin in the Game balance of incentives and disincentives inherent to Bitcoin mining.
61. *Mining* – The process by which nodes are incentivized (in the form of proof-of-work competition and the block reward) to expend processing power to secure the Bitcoin network. The expenditure of processing power is the disincentive aspect of the Skin in the Game balance of incentives and disincentives inherent to Bitcoin mining.
62. *Soul in the Game* – Accepting exposure to downside risks on behalf of others.
63. *Difficulty Adjustment* – An automatic adjustment of the Bitcoin proof-of-work algorithm that adapts to become more difficult as more miners compete for the block reward. The actual adjustment occurs every two weeks for added network security purposes. An ingenious feature of the Bitcoin network that makes it more secure as more value is stored within in.
64. *Protocol* – In computer science, a ruleset that governs the transmission of data. A standard for how computers exchange information. By bringing the quality of scarcity into the digital realm, Bitcoin is the first protocol that is capable of storing and transmitting actual value.
65. *Permissionless* – A property of protocols with open access to everyone that does not depend on receiving permission from a network gatekeeper, a government or an intermediary. As with human languages, permissionless protocols can be learned and used by anyone.
66. *Absolute Scarcity* – Refers to the absolutely fixed supply of Bitcoin. Before Bitcoin, the only thing in the world that exhibited absolute scarcity was time itself.
67. *Price Inelasticity of Supply* – Bitcoin is the only asset in history with perfect price inelasticity of supply, meaning that there is zero supply-side response to increases in its price. Therefore, increases in demand are expressed exclusively through its price with no offsetting increase in new supply. This is a consequence of its fixed supply schedule and absolute scarcity.
68. *Social Contract* – an implicit agreement within a society whereby citizens agree to sacrifice certain freedoms to empower an institution to assist or protect them. Conceptually, both money and government are forms of social contracts.
69. *Fork* – A split in the Bitcoin blockchain resulting from code changes to the underlying protocol. A fork does not increase the supply of Bitcoin or dilute its value, as its rules are set and maintained by social consensus.
70. *Decentralized Network Archetype* – A design archetype prevalent in nature that is the antecedent to many paradigm shifting innovations such as the telephone, the internet, social media and now Bitcoin.
71. *Vertical Gene Transfer* – Genes passed from parents to offspring.

72. *Horizontal Gene Transfer* – Genes passed between competitors in an ecology as a result of physical contact.
73. *Antifragility* – A property of anything that benefits from disorder, stress or adversity. Antifragility is common in organic systems. Since the ravages of time introduce all these forms of adversity, antifragile things tend to become stronger over time – as the old saying goes, “what doesn’t kill me, makes me stronger”.
74. *Streisand Effect* – A phenomenon whereby an attempt to hide, remove or censor information has the unintended consequence of publicizing the information more widely. This effect is usually facilitated by the internet. It is named after American entertainer Barbra Streisand, whose 2003 attempt to suppress photographs of her residence in Malibu, California inadvertently drew further public attention to it. Similar attempts have been made, for example, in cease-and-desist letters to suppress files, websites, and even numbers. Instead of being suppressed, the information receives extensive publicity and media extensions such as videos and spoof songs, often being widely mirrored on the Internet or distributed on file-sharing networks
75. *Creation Myth* – The mythological significance ascribed to the creator of Bitcoin, Satoshi Nakamoto, who mysteriously appeared and disappeared from cryptographer chat rooms without ever being identified personally. This creation story is an important aspect of Bitcoin’s symbolic value, brand recognition and unique claim on true decentralization.
76. *Monetary Premium* – The price of a monetary good in excess of that justified by its industrial demand. Can be thought of as the additional value ascribed to a monetary good based on its socially perceived salability across scales, space and time. Bitcoin is the first monetary good whose value is made up entirely of monetary premium, as it is a technology designed to serve purely as money.
77. *Fractal Wave Pattern* – A fractal is a recursive, self-similar shape that occurs at varying scales – for example pebbles, boulders and mountains could be considered fractal as they are structurally similar only at vastly different scales. A fractal wave pattern refers to the self-similar Bitcoin price pattern which has been established at varying scales in its short history, with each iteration appearing to match the shape of the Gartner hype cycle.
78. *Gartner Hype Cycle* – A standard graphical and conceptual representation of five phases of emerging technology maturity.
79. *Hodlers of Last Resort* – Bitcoin “hodlers” who refuse to sell despite its price volatility. A good proxy for the growth of this cohort is the annual low price Bitcoin hits each year.
80. *Halving* – Every four years the rate of new Bitcoin awarded with the closing of each block is reduced by half. This inflation rate reduction continues until the total supply of Bitcoin issued hits 21M around the year 2140.
81. *Minority Rule* – A dynamic in complex systems in which the preferences of an intransigent few, often less than 4% of the total population, can sway the preferences of the many. The minority rule has been observed across many domains including markets, science, law, imports and spoken language.
82. *Lingua Franca* – A language commonly spoke across cultures that do not share a common ancestry. English is the Lingua Franca of the world today as commerce has come to dominate much of modern life and its communications.
83. *TrustNet* – A potential future wave of innovation, enabled by decentralized applications and cryptoassets, which represents the dawn of trustworthy computing. As Nick Szabo says, computers today are a computational etch-a-sketch, whereas blockchains are

computational amber. This wave of innovation is consistent with past multi-decade cycles of information technology expansion, consolidation and commoditization. Bitcoin will likely function as the systemic core and base money protocol for the TrustNet.

84. *Human Time* – A representation of the amount of human time, effort and ingenuity available to be directed at production. This is the only societal resource that is actually scarce, and it is increased as innovations amplify it to enable higher rates of productivity.
85. *Time Arbitrage* – Buying an asset that is oversold based on short-term market sentiment despite unchanged or improved value fundamentals.
86. *Lindy Effect* – For nonperishable things, such as technologies or concepts, every additional day of life may imply a longer life expectancy. At a certain point, this effect can imply a practically unlimited life expectancy.
87. *Game Theory* – The study of mathematical models related to the strategic interactions between decision makers.
88. *Schelling Point* – A game theoretic solution that decision makers will tend towards in the absence of communication or reliable collusion.
89. *Nash Equilibrium* – A game state where no player has an incentive to deviate from his chosen strategy after anticipating the most likely choices of all his opponents.
90. *Hyperbitcoinization Event* – A Bitcoin-induced demonetization of government fiat money.
91. *Going Concern Risk* – The risk that a company, central bank or other entity will not be able to continue operating into the future.

# Gain Perspective. Change Reality.

Discover more about Bitcoin, cryptoassets and the decentralized future at:

[www.ParallaxDigital.io](http://www.ParallaxDigital.io)