Anarchy in Money
~ On The Ethical Economics of Bitcoin ~

Max Hillebrand

~ Dedicated to ~

Murray
&
Satoshi

Abstract

An act is morally righteous only when it is chosen voluntarily, as there is no violation of property rights and Natural Law. The free market is a complex network of sovereign individuals engaging in mutually beneficial exchange. A money is the store of value, medium of exchange and unit of account chosen by free market participants. As money is half of every transaction, it is of enormous importance to the economy and society at large. A monetary network which is based on voluntary action and with no systematic theft is both economically and morally righteous.

Bitcoin is a money that emerges out of the free and peaceful market, with sovereign nodes declaring their individual monetary rules, presenting themselves to a network of peers and enforcing consensus rules. With a hard and predictable monetary base and equal opportunity for any individual to enter the market of money production, there is no institutionalized theft via inflation. Thus, Bitcoin is true market anarchy and freedom.

Table of Content

List of Abbreviations

BIP	Bitcoin Improvement Proposal
Bitcoin	The monetary network adhering to Nakamoto Consensus
bitcoin	The monetary base unit represented in the n_value field
MoE	Medium of Exchange
No2X	User movement against a hard fork block size increase
PoW	Proof of Work
SegWit	Segregated Witness
SoV	Store of Value
SPV	Simple payment verification
UASF	User Activated Soft Fork
UoA	Unit of Account
UTXO	Unspent Transaction Output

Appendix List

1 Natural Law and Anarchy

"When in the course of human events it becomes necessary for a people to advance from that subordination in which they have hitherto remained, & to assume among the powers of the earth the equal & independent station to which the Laws of Nature & of Nature's god entitle them, a decent respect to the opinions of mankind requires that they should declare the causes which impel them to the change.
We hold these truths to be sacred & undeniable; that all men are created equal & independent, that from that equal creation they derive right inherent & inalienable, among which are the preservation of life, & liberty, & property." [1]

~ Thomas Jefferson ~

Natural Law is a set of universal, inherent, objective, non-man-made, eternal and immutable conditions, that govern the consequence of behavior of beings with the capacity for understanding the differences between harmful and non-harmful action.[2] This law of nature applies to all things objectively and exists independent of human understanding.[3] It is known under several different terms: The Law of Cause and Effect ["Effect invariably follows cause" – "For every action, there exists an equal and opposing reaction"]; the Law of Attraction ["The energy you emit is the energy you attract" – "Energy flows where attention goes" – "As you think, feel and act – so you shall be"]; Karma or Moral Law ["You reap what you sow"]; or the Golden Rule ["Do unto others as you would have done to yourself"]. According to this theory, an action is Right, when it is based in truth and in harmony with Natural Law, this action does not result in harm to other sentient beings. Contrarily, any action is Wrong, when it is not based in truth and in opposition to Natural Law, thus, this action does result in harm to other sentient beings. Natural Law is derived through apophasis,[4] a method of logical reasoning employed when given a limited set of possibilities, in order to arrive at knowledge by way of the exclusion of known negatives. It is describing what something is based on, by what it is not. When eliminating the impossible, the remains, regardless how improbable, must be the truth. Natural Law is thus affirmation through negation.

Any form of initiation of violence is aggression against other sovereign individuals, and also a violation of their Natural Right to property. Murder is theft of another's life. Assault is theft of another's physical wellbeing. Rape is theft of another's sexual consent. Trespassing is theft of someone's home and land. Coercion is theft of another's Free Will.

---

[1] Jefferson (1760), Declaration of Independence paragraph 1-2.
[2] See Aquinas (1485), Summa Theologia-Illea.
[3] See Strauss (1968), Natural Law.
[4] Greek for "to say no".

Theft is taking another's property in goods. Taking something which does not belong to you is always a wrong and immoral act. The initiation of violence is never justifiable. The one single rule of Natural Law is thus: "Do not break Private Property." Any action that does not harm property, is thus rightful and in accordance with Natural Law. Harm no one ~ do everything.

Anarchy is derived from the Greek prefix "an-": "without; the absence of" and the Greek noun "archon": "external master; ruler". It does not mean no rules, rather, it means without imposed rulers, no masters and no slaves, in other words, Freedom. Anarchy is in opposition to authority or the state, as these terms are simply euphemisms for aggression and theft, which are always immoral and in opposition to Natural Law. There is no legitimacy to the mastery over other people. Freedom is based upon the Non-Aggression Principle and the Principle of Self-Defense against the violation of Rights.[5] *"The Natural Liberty of man is to be free from any superior power on Earth, and not to be under the will or legislative authority of man, but only to have the Law of Nature for his rule."* [6]

A sovereign individual has the objective knowledge[7] of which behaviors are Rights because they don't harm others, and which are wrongs, as they do steal from others. Further, once these facts are fully understood and integrated into one's being, and individual action is willfully aligned in accordance to this Will, a state of true Anarchy, Freedom and Peace[8] emerges.

All parts of the economy rely on a fundamental legal and moral framework, just as society in general require such ethical guidelines. This is of course true for the creation of production and consumption goods, where firms can strive to achieve prosperity both economically as well as morally. Most industries are under heavy scrutiny to make sure that no legal or moral code is violated without repercussions. However, one of the most important industries, money production, has so far slipped through the cracks of this due diligence.[9]

---

[5] See Samuel Adams (1772), The Rights of the Colonists.
[6] Samuel Adams(1946), Selections from his Writings.
[7] See Bakunin (1971) On Anarchy.
[8] See Spooner (1882), Natural Law, Chapter 1: The Science of Justice
[9] See Jack Guynn (2005) former chairman of the Federal Reserve Bank of Atlanta, hypocritically stressing the ethical challenges in a market economy, without applying the same rigor to his own instituition. Refer to speech at the Bridgewater College, Bridgewater, Virginia.

2 Sovereign Full Node

Bitcoin is an electronic peer-to-peer cash system.[10] The important aspect is peer-to-peer, that is that the individual user has full control over the system, and doesn't delegate authority to a representative centralized party. However, the system is truly trust less, if and only if the individual user runs a full node. This is a piece of software that can be installed on any hardware, [laptop, raspberry pi,[11] smartphone[12] etc.] and by anyone who wants to, without asking for permission. Ultimately, the end user could write this software from scratch, but this is of course very complex and not reasonable to assume. There are several different clients available, that can be used in order to communicate with the rest of the network, the most advanced of these software is the Bitcoin Core client.[13] It is fully open source,[14] each and every line code can be seen, copied, changed and improved by anyone, without asking for permission, thus everyone can verify the entire software.

When installing the node software, Alice can set any kind of individual rule that she wants. She could increase the number of bitcoin in existence, change the proof-of-work algorithm, change the network routing, or take away control from another UTXO and give herself the control over these coins. There are literally no restrictions on the individual user, she can change anything and everything she wants, as this is her software.

Once the rules are set, the node introduces itself to the network and queries for other nodes to communicate with. Alice's node will receive lots of information from many different participants, and she herself will authoritatively verify the adherence to her individual rules. When the incoming block is valid, for example the coin base reward is 50 bitcoin, halving every 210.000 blocks, she will store it on her drive. However, if according to Alice's rules, the transaction proposed is invalid, for example a double spend, her node will reject it, block the sending node, and tell her peers about the malicious actor. Alice does not need to trust anyone in the validation process, as she has full access and control of the source code rule set. This is a self-sovereign[15] node, a monarch,[16] a single Ruler who rules only the Kingdom of Self. Sovereignty is a state in which one controls one's

---

[10] Satoshi Nakamoto (2008), Bitcoin, a Peer to Peer Electronic Cash System.
[11] Tutorial to install Bitcoin Core on a Raspberry Pi available at http://www.raspberrypifullnode.com/ .
[12] ABCore by Blockstream .
[13] Bitcoin Core Client, latest version available at https://github.com/bitcoin/bitcoin .
[14] See the chapter on Scarcity.
[15] Derived from Latin "super": "above", and "regnum": "rule" or "control".
[16] Derived from Greek "mon-": "one", and "archon": "ruler".

own thoughts [individual rules], emotions [verification of these rules], and actions [enforcement of these rules].

Of course, as soon as one person changes some of the rules, he might violate the rules of other individual nodes, those will recognize him as an aggressor against their individual rules. Because money is a network good, it increases its value exponentially with any additional participants. As soon as someone has different rules in the system, he is excluded from the network. The users with the minority rule change, thus diminish the value of their network money drastically. Therefore, there is a natural incentive for the individual, to use the same rules in his money as the majority of the economy does. Thus, one node software might be used by the vast majority of the network. The Bitcoin Core implementation is very well maintained by the most reputable developers and testers, thus it is running on over 95% of public full nodes.[17] Regardless, the individual user has full control over which rules he wants to comply with, and there is no coercion whatsoever. By definition, anyone who runs a full node thus voluntarily agrees to the rules of the network, nobody is forced to use this software as is. Bitcoin Core is part of the Schelling point of Bitcoin, a solution that peers will tend to use in the absence of communication, because it seems natural, special, or relevant to them.[18]

"The reason why Bitcoin works at all is because users validate blocks and make sure the rules are being followed; every rule that you aren't validating and the economic majority is validating is a potential attack."[19]

A peer who runs a full node thus chooses which rules he likes, verifies if they are uphold, and if not, punishes the nodes that don't comply. He is the judge, jury and executioner. He is the king of his money, the sovereign of his money. And nobody can take this away from him. This is per definition Anarchy, the absence of coercive rule and masters, but only free sovereign individuals in voluntary corporation.

This is why Bitcoin is unique and so innovative. Anyone and everyone has full control over his money, nobody can force him to comply. This is further why closed source and permissions blockchain projects are simply boring and not innovative. They retain the control by the trusted centralized party and don't give the power to the individual user. It's the intranet, filled with stale, boring and old content; to the internet, a network of freedom, ideas and without any censorship.

---

[17] See Bitcoin network, visualized at https://coin.dance/nodes .
[18] See Schelling (1960), The Strategy of Conflict.
[19] Todd (2016), Soft Forks are Safer than Hard Forks.

"[T]he truth that most of the current developers are interested in Bitcoin as a decentralized consensus system existing outside and above the realm of human affairs. Lose that property, and it ceases to be an interesting system. I'm passionate about Bitcoin. I have zero passion for majority-vote to change the rules [of the] system. We have one of those already - it's called fiat." [20]

---

[20] Mark Friedenbach (2016).

3 Forks

All aspects of Bitcoin are fully transparent and open source, thus anyone who is interested has access to the Bitcoin Core implementation and source code[21]. As code is speech and a non-scarce good,[22] it can be copied, adapted, and changed at barely any marginal cost. A problem with altcoins that trade on novelty (rather than utility) is that the market creates novelty faster than these developers can.[23] The code repository can easily be forked off, so to experiment with changes in the code base without affecting the existing consensus implementation. This code fork is not necessarily consensus critical and can be done without permission. A change in the code can be proposed to be pulled back into the reference client, but this is done after rigorous peer review and only when majority consensus is reached. Ultimately, the end user alone is deciding which software he is running and no malicious actor can force him to install any update.[24]

Bitcoin is consensus code that leads to a Schelling point, a standard that people will tend to use in the absence of communication, thus a consensus fork is *"a divergence in the implementation of the verification consensus rules [which] can impede the expected eventual convergence of the network in a single chain that has the most proof of work and also satisfies the rules. This can be intentional or be caused by a bug in consensus validation re-implementations."*[25]

A <u>hard fork</u> is a change to the Bitcoin protocol which loosens restrictions or removes rules, that is that some previously invalid blocks are now considered valid. This might include increase of the block size,[26] signatures operations in the block,[27] or the maximum number of coins,[28] but there are no limits on what could be changed. Because "old" nodes will consider these "new" nodes as violators of the original consensus, each individual node will block and ostracize these aggressors immediately. Even if 99% of nodes accept these new rules and implement the software, they cannot make the 1% upgrade, and these will still run the original individual rules. Thus even with a hyper majority update, the change is a hard fork and the minority network will continue, however, at the immense risk of a

---

[21] https://github.com/bitcoin/bitcoin .
[22] See chapter on Scarcity.
[23] See Tuur Demeester (2014).
[24] See chapter on Sovereign Full Node.
[25] Jorge Timón, (2018) BIP 99, Motivation and deployment of consensus rule changes (soft/hard-forks).
[26] https://github.com/bitcoin/bitcoin/blob/27765b6403cece54320374b37afb01a0cfe571c3/src/consensus/consensus.h#L16 .
[27] https://github.com/bitcoin/bitcoin/blob/27765b6403cece54320374b37afb01a0cfe571c3/src/consensus/consensus.h#L18 .
[28] https://github.com/bitcoin/bitcoin/blob/c0ddd32bf629bb48426b0651def497ca1a78e6b1/src/amount.h#L31 .

51% attack. Because the change is considered invalid by status quo nodes, non-adopting miners build on each other's blocks, creating two separate chains. This is especially concerning, as SPV nodes do not check for the block versioning field, thus they don't see the hard fork blocks at all. After the fork, there will be two different networks and blockchains continuously running. Only the self-sovereign nodes themselves decide which rules to adhere to, and the Schelling point is the Nakamoto consensus. Usually, the UTXO set of the old chain will be utilized as the starting UTXO set of the forked chain, thus every user who had control of bitcoin before the split will gain additional forked coins. These additional UTXO might be considered a gift by the developers and proponents of the new coin to incentivize users to implement the protocol changes. Some projects that fork the Bitcoin consensus argue that this new set of rules is considered to be the true Bitcoin, this is fallacious in many ways. As Satoshi said: *"The nature of Bitcoin is such that once version 0.1 was released, the core design was set in stone for the rest of its lifetime."*[29] A key attribute of Bitcoin is it's unchangeability in consensus, the fact that individual nodes cannot be forced to modify their software and rule set. Once the precedence of a consensus critical change is made, the risk of another change is more likely, as seen with the BCash hardfork with the following splintering and continues forks. Once the precedent of coercive forking as a method of governance is set and nodes give up their sovereignty, it is ever more difficult to reclaim individual control over the protocol. This is in part due to the inherent centralizing nature of a hardfork that is being advocated for by a minority group. Bitcoin does not change precisely because it is leaderless, and any change requires strong avocation of someone.

Due to the monetary value involved in hardforks, a technical debate often shifts to a political one. Individuals who invest much time and effort into developing a hardfork often aspire to become a leader. As humans often look for guidance and leadership, especially in highly complex environments, these people often rise to a new "Satoshi"-like status. They're assumed to be wise and often get a significant say in decisions they shouldn't necessarily be involved in. Many dubious personalities went down this path in the past but haven't been able to gain any long term significant influence in the original Bitcoin project.

A <u>soft fork</u> is a change of the rule set which tightens the parameters or adds rules, this means that the all the new blocks are still considered valid under the original consensus. This means that these new clients are restraining themselves and putting additional rules

---

[29] Nakamoto (2010).

in place which are more constrained than the previous ones. Such a rule change is backwards compatible, because old nodes see this new rule set as valid. Contrarily to a hard fork, a soft fork can be applied by only one individual node, as this node doesn't break consensus. This is an opt in model, thus all users voluntarily agree to constraint their own set of rules. And those that do not want to play by these rules, stick to the original consensus, but stay on the same network and blockchain as those that support the soft fork. Although the full nodes have complete control over their rule set and can change it any time, the resulting blockchain is only secure against reorganization and double spending attacks, if the majority of hashing power is honest. Thus, the nodes have to incentivize enough miners to support this chain, which is done by coinbase reward and transaction fees. A soft fork can introduce radical changes, for example that if >= 95% of the past 2000 blocks signaled for 'Bitcoin v2.0' all blocks must: (i) signal for 'Bitcoin v2.0', (ii) contain exactly one transaction, the coinbase, and (iii) the coinbase must include the hash of a valid 'Bitcoin v2.0' block. This soft fork thus commits to an entirely new 'Bitcoin v2.0' protocol, which could be anything at all![30] Thus, a soft fork is not per definition a positive event for Bitcoin and can be very contentious. All forks degrade security, the question is how badly. When updating the protocol, a softfork is less contentious than a hardfork, thus in general preferable.

Historically, soft forks have been employed after 95% of blocks supported it, signaled by the version field in the block header set by miners, and blocks that don't support the soft fork are considered invalid after the initiation of the soft fork.[31] Blocks from miners that don't adopt the soft fork are still produced 1/20th of all blocks, but they are considered invalid and thus orphaned off.

After years of research and development, it was clear that segregated witness is an overall net positive for the entire network. SegWit fixes the malleability bug, which makes second layers solutions like the lightning network and further complex smart contracts such as Chaumian coin joins[32] possible. Because the signature part is segregated from the transaction itself, this is an increase in the block weight and therefore increases the maximum amount of transactions per second. Furthermore, with the versioning upgrade mechanism, other signature schemes such as Schnorr signature or Boneh-Lynn-Shacham signatures can be added in the future with another soft fork. Only after enough research and with sufficient development and peer review did the core process push for

---

[30] See Todd (2016), Forced Soft Forks.
[31] See Todd (2018) BIP65: CheckLockTimeVerivy, Deployment.
[32] See Fiscor (2017), Zero Link, The Fungibility Framework for Bitcoin

an update in the consensus rules. A dedicated group of individuals can manifest this change in the Bitcoin consensus protocol, as long as they do not violate the rules of other full nodes. Initially, the upgrade mechanism was deployed in a way where miners had to signal the usage and agreement to the SegWit soft fork. As these service providers tried to block and delay the SegWit activation, sovereign nodes banded together and declared to no longer accept PoW of miners who were actively blocking the voluntary soft fork. The act of not doing business with another individual is fundamentally based in voluntary interaction and the Right to be left alone. As long as the user activated soft fork does not break the consensus rules of other individual node it is ethically righteous. The SegWit UASF shows that sovereign full nodes are in full control of their own implementation.

After SegWit got activated, a small group of individuals tried to implement a new code repository as the main consensus reference with a hard fork increasing the block size to 2 megabyte. This hard fork was to be implemented and activated by the hashing power of miners signaling their support. This miner activated hard fork stands as the complete antithesis to the user activated soft fork. A small minority of researchers, developers and enterprise tried to introduce a change to consensus which would break the previously agreed upon rule set, a hard fork. Only after a massive push back from the community [#No2X] did the small minority give up and stop their effort to force a rule change on sovereign nodes. Due to serious flaws in the code and an off by one error, the hardfork would never have taken place anyhow. Regardless, these individuals could never have forced other full nodes to accept and play by these new set of rules, the Schelling point of Bitcoin is the status quo.

As the core attribute of Bitcoin is financial self-sovereignty and therefore the unchangeability of consensus rules, upgrades and improvements to the network are always going to be a contentious matter. It is curious to see how upcoming changes are proposed and handled in the core process. There are still many features to be added to Bitcoin primarily regarding its privacy and fungibility aspects. Although the research and development of tools such as confidential transactions and Schnorr signatures are advanced and currently going through rigorous peer review, implementing these major changes will be a heavily debated topic worth further study. The main challenge will be to introduce these features in a non-contentious but voluntary matter, primarily with a soft fork.

4 Free Exchange and Interventionism

An act is free, when it is entirely unhampered by aggression or the threat thereof. In direct exchange, Alice gives up apples to Bob under the condition that Bob gives his berries to Alice. When neither Alice nor Bob are coerced to partake in this action, but they voluntarily choose to corporate, no harm is done, thus the trade is morally righteous.

Alice is marginally better at picking apples, compared to picking berries, in one hour she can gather 20 apples, or 30 berries. Contrarily, Bob is marginally superior at picking berries, collecting 80 berries or 10 apples per hour. If the two decide to work only for themselves for two hours, Alice can collect 20 apples and 30 berries, Bob can acquire 10 apples and 80 berries. However, they can specialize [33] on the task where they are marginally better at, so Alice gains 40 apples, and Bob 160 berries. On Alice' individual preference scale[34], she prefers 80 berries over 10 apples, on Bob's individual preference scale, he prefers 10 apples over 80 berries. They have a unique opportunity to engage in a voluntary trade of 1 apple for 80 berries. After this exchange, Alice has 20 apples and 80 berries, Bob has 20 apples and 80 berries, both are better off, making the trade mutually beneficial.

The free market is so beautiful, precisely because it's mutually beneficial throughout the entire process. One can only express the individual's preference scale with the action of exchange, and if this is done freely and voluntarily, it implies the higher value of the traded good ex ante. The overall value of all individuals and the entire economy is increased by free exchange. Specialization is encouraged, division of labor is encouraged, free trade is encouraged.

It implies the Natural Right of the individual to do with his property as he pleases, as long as he doesn't harm any other sentient being. Clearly, exchanging the property for a different good is an inherent part of this Right, and to deny it is to imply expropriation and slavery. As Rothbard put it, there are three different types of intervention: autistic, binary, and triangular. Each inherently breaks the beauty of the free market and is not at all mutually beneficial: one individual or group of individuals use violence or the threat thereof to become the master: the tyrant or state, the other individual or group of individuals become the oppressed: the slave. Any form of intervention is thus a violation of property rights and Natural Law, and thus political, uneconomical and immoral.

---

[33] See Rothbard, (1965) Freedom, Inequality, Primitivism, and the Division of Labor, pp. 299–302.
[34] See Rothbard, (1962) Man, Economy, and State, Chapter 1, Section 1.

(i) In an <u>autistic intervention</u>[35] the state denies the individual to use his property in a way that is not in accordance with the states decree, although the individual would not hurt anyone else in his intended action. Prohibition is an example where the state punishes the righteous consumption of a good, such as alcohol or marijuana. Thus, the state implies a higher right to the individuals property and his person, which of course fundamentally breaks the Natural Law. The state gets the outcome it intended and receives its higher value, however the oppressed individual is worse off no matter his intention of adherence of this man made 'law': In the case that he did not want to produce or consume the forbidden good, due to the implied threat of violence; and in the case that he wanted to produce or consume the good, because he is forcefully prohibited from partaking in this peaceful action with his own property to gain additional value. In a free market, the individual will be counseled, suggested and persuaded peacefully and non-coercively without the threat of violence, to stop the action, but the individual can at any time deny and ignore the counseling, he only accepts it if it's of value to him, making it again a mutually beneficial interaction.

(ii) In a <u>binary intervention</u>[36] the state forces or coerces the individual to interact with the state, so the individual has no way of declining. Taxation is an example where the state forcefully expropriates, without the explicit consent, a portion of the individuals income [theft] and product of labor [slavery]. Again the state gets the higher valued outcome, the ownership of the individuals property, and the individual is again oppressed regardless of his intention to exchange or not with the state. Even if the individual was voluntarily intending to pay the contribution, the threat of violence inevitably decreased his wellbeing, and of course if he did not intend to pay the contribution, he was forcefully removed from his rightful ownership and is therefore by definition worse off. In some occasions, the individual or society at large might get some or all of the stolen property back in form of grants or services, public education, roads or security[37]. But nevertheless, the property was first involuntarily stolen and is thus never employed in the individual's highest valuation. Due to costs of bureaucracy the aggregated amount of stolen property is always higher than the aggregated amount of employed public grants and services. In the free market, all exchanges are engaged in voluntarily and are therefore not taxation, but

---

[35] See Rothbard, (1962) Power and Markets, Chapter 2 Fundamentals of Intervention.
[36] See Rothbard, (1962) Power and Markets, Chapter 4 Binary Intervention: Taxation and 5 Binary Intervention: Government Expenditures.
[37] Benjamin Franklin: „those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety and will loose both."

rather a payment for a provided service, exactly the same to the exchange of any other good or service.

(iii) In <u>triangular intervention</u>[38] the stated forces two individuals to only engage in trade with the rules set forth by and the permission of the state, examples are registration, licensing and forced contract covenants. The state gets the higher valued outcome of control, and the individuals get oppressed again even if they intended to obey the 'law' due to the threat of violence; and also if they did not want to engage in the contract forced upon them by the state. Triangular intervention can be sub divided into price controls and product controls. The aggressor can either set a minimum price, which will hurt the customer as he must pay more than he would voluntarily choose to, thus less will be consumed; or a maximum price, which means that entrepreneurs might have to carry a loss as not all their expenses are covered. Regardless, as this dictated price is not the voluntarily chosen market price, it is inherently not mutually beneficial and thus destroys resources and capital. In regards of money, price controls inevitably lead to Gresham's law.[39] Also, the state can manipulate the nature of production directly, rather than the terms of exchange. This is that the aggressor prohibits the production or sale of a certain product, which will again lead to a net loss for all participants. The consumer loses utility as he cannot acquire the good with which he could satisfy his desires, and the producer who is prohibited from earning the revenue that the exchange would have brought him. The only ones that will benefit from this coercion, is the aggressor himself, partly from the tax or licenses which is collected, or from the twisted satisfaction of suppressing others.

---

[38] See Rothbard, (1962) Power and Markets, Chapter 3 Triangular Intervention.
[39] See chapter on Gresham's law.

5 Evolution and Attributes of Money

Only a few times in history has a new money emerged, which is a long lasting phenomenon with a step wise progression. Initially the money is a scarce collectible, then a store of value, later a medium of exchange and ultimately a unit of account.[40]

First, in order for a money to be useful, it has to be exchanged for other goods, where Alice relinquishes control over her money, and Bob gives up the possession of his berries. This aspect of scarcity[41] is essential for a functioning money, as a non-scarce good can be multiplied and shared, so that Alice would retain a copy of that money. The information transmitted on the internet is a non-scarce good, and it is very remarkable, that the Nakamoto Consensus in Bitcoin, morphs this information in such a way, that a scarce good emerges. As Alice is signing the Bitcoin transaction with a non-scarce private key, she has advanced the chain of signatures that represent the UTXO so that it is now pointing to the public address of Bob, and only with control of Bob's private key, can this output be ever spent again. Assuming sufficient fees paid and overall validity of the transaction, this transferal of control is confirmed with accumulated PoW on the Bitcoin blockchain. Alice has given up total control over this bitcoin, and only Bob is in control of it now, thus the aspect of scarcity is fulfilled.

If Alice can take back the good, after giving it to Bob, then she has reversed the trade and broken the private contract that she has initially voluntarily agreed to. Thus, the attribute of scarcity must be upheld not only for a short period in time, but continuously and reliably, even with malicious actors. In Bitcoin, one UTXO must only be used once, and not be double spent, so to prevent the creation of counterfeit currency and inflation of the money supply[42]. Nakamoto Consensus declares a time ordering of transactions in blocks that hash to a value below a certain difficulty target. Once a valid block is found, it can be assumed that the miner proposing the order of transactions, has expending energy and work to do so, he has skin in the game. Each block refers to the previous block, thus creating a chain of accumulated PoW and in order to rewrite this chain, hash calculations have to be performed. It is computationally exponentially more costly to reorganize the chain of blocks, with increasing percentage of honest miners. With an assumption of 50% non-malicious miners, the chain with the most accumulated PoW is considered to be the

---

[40] See Szabo, (2002) Shelling Out: Origins of Money.
[41] See chapter on Scarcity.
[42] See chapter on Money Supply.

one valid chain containing the true transaction history. PoW is thus a tool to defend the attribute of scarcity of bitcoin, so that it can only ever be controlled by one script.

Alice and Bob have unique individual preferences which they will strive to satisfy. They will seek to accumulate scarce goods in order to remove this uneasiness of desire. With the genesis block and the first 50 bitcoin issued in the coinbase reward, Satoshi received the first amount of scarce bitcoin. Ever since then, a new block issues the next set of fresh UTXOs to the database, thus increasing the supply of bitcoin so that more people can accumulate this digital scarce collectible[43] by expending work.

Individuals will continue to intermingle their human ingenuity with the natural resources surrounding them, in order to eventually produce a consumption good with which they can satisfy their desire and remove uneasiness. With increasing productivity, Alice might soon have more apples than she can consume at the current moment, thus she will store some in order to consume them at a later time. With a store of value, individuals can postpone the gratification and plan ahead for an uncertain future. Bitcoin can be bought and held in order to use in a future exchange for good or services. As the supply of bitcoin is predictable and the issuance rate unchangeable,[44] there is no loss of purchasing power through unexpected inflation. Further, as the network continues to grow and expand,[45] the price of bitcoin is likely to increase, and the price volatility will continue to decrease[46]. As Bitcoin is antifragile, the ecosystem has a convex response to a stressor or source of harm leading to a positive sensitivity to increase in volatility,[47] which further enhances its advantages as a store of value.

With direct exchange, Alice has to be willing to trade the good that Bob wants, and vice versa. This double coincidence of wants problem limits the number of total possible trades in the economy, increases the complexity of calculation and introduces general uneasiness. A medium of exchange can be used in indirect exchange, which is a good that is not used up, but rather utilized to acquire a production or consumption good. As individuals will hold some of their wealth in a SoV to postpone their consumption, they can also utilize this good to exchange at a later point for a good they desire. As bitcoin is a useful SoV, individuals will acquire it in order to at a later point in time use it in exchange.

---

[43] See Szabo, (2002) Shelling Out: On the Origins of Money.
[44] See chapter on Money Supply and Inflation
[45] See Van Den Bergh, (2018) On Schelling points, network effects and Lindy: Inherent properties of communication.
[46] See illustration 1 on the purchasing power volatility of bitcoin.
[47] See Taleb, (2012) Antifragility.

Because of the high level of divisibility, it can be used to purchase high value good, but also in micro transactions.

In a simplified barter economy, there is no universal price of any good. One unit of Alice's apple will have several different 'prices': the 'berry price' in terms of Bob's berries and the 'wood price' in terms of Charlie's wood. In a more complex barter economy, every good has a quasi-infinite array of prices in terms of every other good. Each seller has to price his goods in many different goods and keep track on all the exchange values for each and every good. This is of course very cumbersome and costly, deep production stages are very hard to calculate. Because of the limited possible trades and the expensive and recurring adjustments of prices, this is a state of uneasiness which will be relieved in a free market. As more and more people use the same SoV and MoE, the value of that good further increases, thus incentivizing more participants to use it. The more the same good is used in exchange, the more goods are priced in terms of that one good. Thus there is a natural tendency towards one single unit of account in which all goods are being priced. This opens up the possibility of fast and interconnected production stages in a complex economy. As Bitcoin is still at a very early stage, and hold only by few individuals, not everyone is pricing his goods in bitcoin. However, in some selected markets like altcoin trading, bitcoin is already the UoA, and this use can be expected to increase.

That good, which is the most common store of value, medium of exchange and unit of account in the economy, is called the money. Of course, every good can be money, but that good which is the most saleable will tend to be the single money. Due to the network effect, the saleability of the money increases exponentially with each new participant in the money economy. Thus there is a natural tendency towards one single money on the free and voluntary market. This must not be confused with government legal tender laws, which force market participants to use a currency, and as there are several states haggling for control, several currencies are prevalent in the market place.

"But the expected value will be the decisive factor determining how much of it the public will want to hold, and the issuing bank will soon discover that the desire of the public to hold its currency will be the essential circumstance on which its value depends. [...] The crucial point it must keep in mind will be that to keep a large and growing amount of its currency in circulation, it will be not the demand for borrowing it but the willingness of the public to hold it that will be decisive."[48]

---

[48] Hayek, (1976) The Denationalization of Money.

6 Money Supply and Inflation

An increase in the stock is caused by an increase in the production of money, and decreased by decay, unrecoverable loss and use in production. Because the market will choose a durable money,[49] and because the money itself is not consumed or used up in production, the proportional increase of supply will be quite small.

The question arises, if there exists an optimal quantity of money and how much money should be in supply? Economists argue, whether the supply should move in accordance with population growth, economic growth, volume of trade, velocity of trade, the amount of goods produced or according to demand so to keep a stable purchasing power. Many ignore the possibility of leaving the decision to the free and voluntary market.

Money differs from other goods in one essential attribute: An increase in the supply of consumption goods, leads to more options and a higher living standard for the individual. With more production goods, more consumption goods can be built, thus further increasing future prosperity. Additional land and other natural resources promise more production and consumption, both in the present and the future. Consumption goods are used up by consumers; and capital goods are used up to produce more consumption goods. But money is not used up, it is neither a consumption nor a capital good, but rather a SoV, MoE and UoA used to postpone the gratification of needs and desires, increasing the number of possible trading pairs, and decreasing the complexity and cost of overall trade.

If Alice is willing to trade her apple for 3 money units, the price of the apple is 3 money units. A money is the UoA, thus all prices are denominated in this good. It represents the amount of goods one money unit can purchase, just like the price of the apple represents the amount of money 1 apple can be traded for. The price of money is thus the inverse of the price of all available goods. With an increase in the supply of money, and unchanging demand, the price of money will fall, thus the price of all other goods denominated in this money will increase. The opposite is true for a decrease in the quantity of money.

In the hypothetical construct of helicopter money,[50] each individual will simultaneously receive an equal proportion of new money. Let's assume that Alice has 50 money units, Bob 30 and Charlie 20, and the total supply instantly doubles to 200. Now Alice has 100

---

[49] See chapter on the Evolution of Money.
[50] See Mill, (1884) The Currency Question, Westminster Review, XLI, p. 579-598.

money units, Bob 60 and Charlie 40. Are they now magically twice as rich? Did this increase their purchasing power? Obviously not. Alice still has 50%, Bob 30% and Charlie 20% of the money units and purchasing power in the economy. Only an abundance of goods can increase prosperity, and this is limited by the scarcity of the resources land, labor and capital. Simply increasing the money supply does not bypass economic laws. They might feel more wealthy initially because of the increase in their nominal holdings of money, but soon they will realize, that their percentage of the total quantity of money remains equal. As individuals barter for the price of the exchange following the increase in supply, the demand for all goods will roughly double, which will eventually lead to a doubling, but at least an increase in the price of all goods. The new price is reached when demand is satisfied and new money no longer bids against itself for the goods. Therefore, while the increase in the supply of money will, as with any other good, lead to a decrease in the price of money, but this does not lead to an increase in the benefit for society. Thus, it does not matter what the supply of money is! Any quantity of supply will work just fine, as long as the units can be divided for small transactions. On the free and voluntary market, the individuals will simply adjust the prices to the same degree of purchasing power as before the change in supply. This adjustment process will take a considerable amount of time, effort and cost. Thus, even in this hypothetical construct of helicopter money, changing the money supply is not just useless, but actually spawns unnecessary costs and uncertainty.

However, in the real economy, it is impossible to have an instantaneous increase in the money supply. Some market participants receive the new money before others, the consequences are called Cantillon Effects.[51] Let's again assume the initial state with Alice 50 money units, Bob 30 and Charlie 20, but the 100 inflated money units go directly and solely to Alice. Alice now controls 75%, Bob 15% and Charlie only 10%. It is logical, that Alice having received the money first, benefits at the expense of Bob and Charlie, because her percentage of the total money has risen, while Bob's and Charlie's has declined. Further, Bob and Charlie have not yet adjusted their prices upwards to reflect the delusion of the money supply. Alice purchases some berries from Bob for 10 money units, thus the price per berry increases, which adjusts Bob's purchasing power upwards, but only to 20%, which is still below the initial state. If Bob now purchases wood from Charlie for 5 money units, Bob has the advantage of buying the wood for the not yet adjusted price. After the exchange, Charlie will adjust the price accordingly, and his

---

[51] See Cantillon, (1755) An Essay on Economic Theory.

purchasing power is now higher at 12.5%. Because Alice is the sole money producer, she is stealing purchasing power from Bob and Charlie, who cannot defend against this hidden taxation.

Contrarily, if Alice loses 20 money units, her purchasing power decreases to 37.5%, Bob's increases to 37.5% and Charlie's increases to 25%. Alice has lost both in the quantity of money units, and in her percentage allocation of the total supply. However, Bob and Charlie have not gained additional units, but as the total supply has deflated, their percentage has increased. Alice has to cut her spending and thus suffers the most, Bob and Charlie see their buying prices fall, before their income is cut, thus they benefit.[52] Thus, Bob and Charlie gain at the expense of Alice, but this is entirely due to her fault, and with no wrong doing from Bob and Charlie.

We can observe following law: *"When a change in the money relation causes prices to rise, the man whose selling price rises before his buying prices gains, and the man whose buying prices rise first, loses. The one who gains the most from the transition period is the one whose selling price rises first and buying prices last. Conversely, when prices fall, the man whose buying prices fall before his selling price gains, and the man whose selling price falls before his buying prices, loses."*[53] The greater and longer the positive difference between the selling and buying prices, the greater the gain. The greater and longer that negative difference, the greater the loss. Which participants gain and loose, depends on the relative time that they receive the newly printed money as it gets diffused throughout the economy.

It has to be noted, that the old and new relative prices and valuation are not identical. Even if the individual valuation would be frozen throughout the adjustment process, the shift in relative prices changes the overall demand structure, first for the gainers, later for the losers. The same is the case for the time preference. Even in the helicopter money construct, not all prices will double automatically, because everyone has a unique demand-for-money structure. The exact amount and direction of the shift of the demand structure can of course not be predicted by economists, as they rely solely on the unique individual valuation of countless market participants.[54]

According to Nakamoto Consensus in Bitcoin, there is a set issuance rate for new money units. Initially, 50 new bitcoins every block can be created and given directly to the miner

---

[52] See Mises, (1912) Theory of Money and Credit, Part 2, Chapter 2, §7.
[53] Rothbard, (1962) Man, Economy and State, Chapter 11, Part 7
[54] See Mises, (1912) Theory of Money and Credit, Part 4, Chapter 1, §1

who finds valid proof of work. Every 210.000 blocks or roughly 4 years, this number is halved, first to 25 bitcoin, then to 12.5 bitcoin and eventually, no new bitcoin will be created in the year 2141 with a total number of just shy of 21 Million bitcoin in existence.[55] The issuance schedule is part of the Nakamoto Consensus, and therefore it can only be changed if an overwhelming majority individual nodes agree to such a drastic change. As seen with #No2X, even for a rather trivial change such as the block size security parameter it is nearly impossible to reach consensus. It is safe to say, that such a fundamental change will not be adopted easily and without pushback, if merged at all.

One of the unique attributes of Bitcoin regarding inflation is the difficulty adjustment period of 2016 blocks, where the accumulated proof of work is verified against the targeted time frame of one block every ten minutes. If more hashing power has entered the network over the last two weeks, the difficulty of finding valid PoW is increased; if hashing power has exited the network, the difficulty is decreased. This seems like a trivial procedure, but its effects are brilliant and vitally important.

Individuals value gold, as it is a good SoV, MoE and UoA, thus they are willing to pay a price to acquire this money. Thus entrepreneurs take on capital and production cost of gold in order to sell it at a profit. As more peers use gold as their money, the network expands and the price rises, thus more miners can enter the market and cover their cost with the revenue. This, however, increases the total money supply of gold, increasing the uncertainty in the economy and shifting the purchasing power from the holders to the money producers. This is downward pressure on the price of gold.

Bitcoin is, just as gold, a very useful money, thus individuals value it and acquiring it at a price from the entrepreneurs who are producing bitcoin. These are miners who are packaging individual transactions in their candidate block and hashing it until the difficulty target is met. As a reward, the miner can give himself newly created bitcoin in the coinbase transaction, starting a new chain of digital signatures. As the network grows, more peer will value bitcoin, new miners are incentivized to enter the market and start hashing their candidate block. Now sooner rather than later, a new block will be found, which in the short run, will increase the issuance rate, as the 2016 blocks will be found faster than two weeks. However, for the next period, the difficulty target will be decreased, thus it takes proportionally more hashes until a valid block is found. This stabilizes the stock-to-flow ratio and the uncertainty of a changing issuance rate is drastically reduced. Thus, in the long run, the increase of the money supply is highly predictably, and, the

---

[55] See Illustration 2 on the bitcoin money supply.

security against reorganization attacks is drastically increased. Unlike all previous moneys, with an increase in users and miners, not the money supply, but the security of the network increases! This leads to even more peers using Bitcoin, which starts the cycle all over again. The positive feedback loop increases the security, but leaves the issuance schedule untouched. There is thus no downward pressure on the price due to an increase in the money supply!

"The quantity of bitcoin created is preprogrammed and cannot be altered no matter how much effort and energy is expended into proof-of-work. […] Difficulty adjustment is the most reliable technology for making hard money and limiting the stock-to-flow ratio from rising, and it makes Bitcoin fundamentally different from every other money. […] Bitcoin is the hardest money ever invented: growth in its value cannot possibly increase its supply; it can only make the network more secure and immune to attack. […] Gold became the prime money of every civilized society precisely because it was the hardest to produce, but Bitcoin's difficulty adjustment makes it even harder to produce."[56]

"In this sense, it's more typical of a precious metal. Instead of the supply changing to keep the value the same, the supply is predetermined and the value changes. As the number of users grows, the value per coin increases. It has the potential for a positive feedback loop; as users increase, the value goes up, which could attract more users to take advantage of the increasing value."[57]

"Monopoly prevents people from using what is rightfully their property and thus prevents them from competing with privileged market participants. This is partial theft."[58] Thus, when there exists a state monopoly on the production of money, it is inherently stealing the private property of entrepreneurs seeking to enter this market and provide a service for their customers. It is theft, regardless if the monopoly entity will inflate the money supply. However, those that have the power to print money, are incentivized to misuse this power. In order to prevent this from happening in Bitcoin, anyone can enter the market to produce new bitcoin by performing PoW through hashing. All that is needed in order to calculate this mathematical function, is a piece of paper and a pen.[59] It is neither required to disclose ones identity, nor use any specific hardware or ask for permission. Mining is performed by a dynamic set of unknown entrepreneurs. Not even Satoshi had extra privilege, as he had to proof his work even for the genesis block.

---

[56] Ammous, (2018) The Bitcoin Standard.
[57] Nakamoto, (Feb 2009).
[58] Hülsmann, (2008) Ethics of Money Production, Chapter 9 Legal Monopolies, Part 4 Ethics of Monetary Monopoly.
[59] See Shirriff, (2017) Mining Bitcoin with pencil and paper: 0.67 hashes per day.

Although he was initially the only miner, he could not exclude anyone from competing against him. Precisely because anyone can enter this market place, the issuance rate evident in Bitcoin is neither unethical nor uneconomical!

In a fiat system with legal tender laws, inflation is theft because it shifts the purchasing power from the savers, to the money producers, and the users didn't voluntarily agree to the redistribution and they are forced to use the currency as it depreciates in purchasing power.[60] However, the consensus rules in Bitcoin were set in 2009, and anyone who runs a Bitcoin full node can decide which rules to follow. Any arbitrary change to the open source software is not just possible, but encouraged. Because anyone can adapt the rules, by definition, if an individual node is connecting to the network, it is voluntarily agreeing to the rules in this network, including the issuance schedule. Therefore, the Bitcoin <u>issuance rate is accepted voluntarily</u>, and thus is neither coercion nor theft. There is no inherent moral problem with a voluntary increase in the money supply, however, there might be an economic issue.

As described earlier, the Cantillon effects favor the money producers over the savers, and shift the purchasing power from one to the other. This creates two problems: (i) malinvestment and (ii) over consumption.[61]

(i) On the entrepreneur side, because as the quantity of money increases, more money is available for investments and the new money is allocated to rather less profitable and more risky opportunities, which have a potentially greater return, but also a higher chance of default. In a sound economy, the amount of purchasing power dedicated to new investments is dependent on the savings rate of market participants. Thus entrepreneurs might assume that this additional money available for investments comes from consumers who postpone their satisfaction of needs to an uncertain future. In this case it would be profitable for the entrepreneurs to increase the production stages and build higher order goods. However, as in the case of an inflationary money supply, the additional money is not derived from consumer savings, but rather printed out of thin air. Consumers are actually not saving for future consumption, rather they are consuming more in the present.

(ii) On the other hand, consumers have a choice of satisfying their needs right now, or later in the uncertain future. This time preference is unique to each individual, and is evident in the interest rate, which reflects this postponement of gratification. With an increase in the money supply, its price will decrease, incentivizing the immediate

---

[60] Issing, (1993) Der Zins und sein moralischer Schatten.
[61] Mises, (1949) Human Action, Interest, Credit Expansion, the Trade Cycle.

exchange for consumption goods. Consumers are thus incentives to postpone saving and increase their current consumption. This behavior is rational in an inflationary economy, but is directly contrary to the expectations of the entrepreneurs.

Because everyone can become a miner and create blocks, the new money is spread throughout the economy and not to one central party. Thus, no one is the sole beneficiary of the inflated money, which decreases the Cantillon effects. Further, the issuance rate is set, publicly known and anticipatable by all market participants. Nevertheless, this economic law is prevalent in Bitcoin as well. The goods subsidized by the new bitcoin are (i) security on the production side and (ii) the block space on the consumption side.

(i) Because of the block reward which increases the money supply, entrepreneurs, in this case the miners, invest more than the users are willing to pay for in mining. There is more hashing power in the network, ceteris paribus, compared to a system without such a block reward. Although one might argue, that the additional mining power and security is beneficial and needed to bootstrap Bitcoin, it nevertheless is a malinvestment. More security is being produced than the individual user is willing to pay for. The logical conclusion is, that the current hyper-exponential growth in Bitcoin's accumulated PoW is not in line with the current needs of users. As soon as this subsidy will decrease, the costs for the security has to be carried by the direct transaction costs only. It will become evident that the entrepreneurs have produced too much security and that the Bitcoin users are not willing to pay this much directly with transaction fees. Because users might not increase the Satoshi per virtual Byte transaction inclusion fee as much, miners will no longer be profitable and cannot amortize their investment in mining chips, electricity and knowhow. These miners who have not anticipated the correct demand for security have over invested and will no longer be profitable. They will cease operation, which will lower the total hash rate and thus security. The hash rate will continue to drop to that amount which the users are willing to pay for. This correction is inevitable, but due to the difficulty adjustment not a problem for security and block confirmation time, as explained earlier.

(ii) There are costs in securing the Bitcoin network with mining, and those costs are paid for by the individual user with the transaction fee that goes directly to the miner. The more security the users want, the more transaction fees have to be paid. The additional fees will incentivize new miners to start hashing, which will increase the security against reorgs and double spends. However, the payment for the service security is subsidized by the block reward, which additionally to the transaction fee gives the miner the newly issued bitcoin. The direct costs for the user, the transaction fees, are thus comparatively low

because the miner can pay his production costs in part with the newly issued bitcoin. The block space is thus relatively cheaper for the end user, compared to a network without the subsidy. Therefore, users will consume more of the blockchain, i.e. they will make more transactions than they otherwise would. Apps like SatoshiDice will use up block space although the amount of security in the network might be considered way too high for such a use case. SatoshiDice could work perfectly fine in a network with less security, which would increase efficiency at lower costs, for example the lightning network.

The <u>cultural consequences of inflation</u> are long lasting. When the money supply is continuously increased the purchasing power of the money is continuously depreciated. Thus, with the same nominal amount of currency tomorrow you can purchase less goods and services. Therefore, Alice is incentivized to consume today, thus increases her time preference, and lowering her planning horizon.[62] Because she is fearful that tomorrow she will have less purchasing power to satisfy her needs and desires, she is pushed to consume as much and as soon as possible. Alice no longer plans for future generations as her wealth is degraded over time. As this culture of inflation and theft is manifested across several generations the result is an uncertain and fearful society consuming weak products. Entrepreneurs are incentivized to introduce planned obsolescence so to have recurring consuming customers, offsetting their loss in wealth. A one-time collapse in the value of a monetary medium is tragic, but at least it is over quickly and its holders can begin trading, saving, and calculating with a new harder money. But a slow drain of its monetary value over time will slowly transfer the wealth of its holders to those who can produce the medium at a low cost.

"The real impact of this is the widespread culture of conspicuous consumption, where people live their lives to buy ever-larger quantities of crap they do not need. When the alternative to spending money is witnessing your savings lose value over time, you might as well enjoy spending it before it loses its value. The financial decisions of people also reflect on all other aspects of their personality, engendering a high time preference in all aspects of life: depreciating currency causes less saving, more borrowing, more short-termism in economic production and in artistic and cultural endeavors, and perhaps most damagingly, the depletion of the soil of its nutrients, leading to ever-lower levels of nutrients in food. [...] The culture of conspicuous consumption, of shopping as therapy, of always needing to replace cheap plastic crap with newer, flashier cheap plastic crap will not have a place in a society with a money which appreciates in value over time. Such a

---

[62] Hülsmann, (2009) The Cultural Consequences of Fiat Money.

world would cause people to develop a lower time preference, as their monetary decisions will orient their actions toward the future, teaching them to value the future more and more. We can thus see how such a society would cause people not only to save and invest more, but also to be morally, artistically, and culturally oriented toward the long-term future."[63]

Contrarily, with sound money and an unwavering supply schedule, as the economy grows, the purchasing power of money increases. Because entrepreneurs no longer have the uncertainty of a changing money supply, they can dedicate more of the resources to productive use cases. As there is the potential for multi-generational wealth preservation, individuals are incentivized to decrease their time preference and increase their planning horizon. Long lasting monumental projects can now be focused upon as the need for recurring consumption is decreased. Entrepreneurs can focus on innovating and improving living conditions. Saving and investing ideas for long-term capital accumulation. *"A world of constant money supply would be one similar to that of much of the eighteenth and nineteenth centuries, marked by the successful flowering of the Industrial Revolution with increased capital investment increasing the supply of goods and with falling prices for those goods as well as falling costs of production."[64]* It is no wonder that the golden era of innovation in the nineteenth century, la belle époque, was a world running on a hard money, because that hard money is what allowed all these many inventors and tinkerers the capital and freedom to experiment with outlandish ideas. As Bitcoin is an even harder money compared to gold, it might usher in an era of tremendous prosperity, capital accumulation and wealth preservation. This has long lasting effects, not just on the economy, but on the minds of free sovereign individuals.

---

[63] Ammous, (2018) The Bitcoin Standard, Chapter 7 Sound Money, Part 1, Should the Government manage the Money Supply.
[64] Rothbard, (1976) The Austrian Theory of Money, The Foundations of Modern Austrian Economics.

7 Gresham's Law

On the free market, a good will always be valued according to the individuals subjective preferences. Assuming two goods are exactly equal, they will be valued the same. If there are two almost identical gold coins, each in pristine conditions and with precisely one ounce of gold, they will be valued equally by any market participant, thus the coins are fungible. Suppose these coins have experienced degradation and clipping,[65] now only containing 0.9 gold ounces. In a voluntary exchange, the coin will only be worth 90% of the previous one ounce of gold. However, if the government introduces legal tender laws as a form of price control[66], it decrees that the worn coins have to be valued equally to the new ones and they must be accepted as equal in payment of debts. The old coins are thus artificially overvalued, and new coins artificially undervalued. This act sets a maximum price on one type of money in relation to another. Maximum prices usually cause a shortage, that is the undervalued good coin will be hoarded while the overvalued old coin will be solely used in exchange.[67]

Gresham's law[68] says that *"money overvalued artificially by government will drive out of circulation artificially undervalued money."* Thus *"there is nothing less fit to be left to the action of competition than money."*[69] It is important to emphasize that Gresham's law only applies to different kinds of money in between which is a fixed rate of exchange enforced by state edict.[70,71] If due to the law two different moneys are treated as substitutes for the payment of debts, creditors are being forced to accept a coin of smaller gold content in place of one with a larger content. Thus, debtors will only pay with the smaller coin and use the larger as a store of value.

As the crypto currency market is free from most state interventions, Gresham's Law does not apply to the different digital assets. However, there is government coercion with legal tender laws in fiat money, which artificially overvalues state currencies. If Alice has both fiat and bitcoin in her possession, and she is seeking to exchange them for goods and services, it is rational that she will first spent the fiat money, as its price is artificially

---

[65] See Rothbard, (1994) Case Against the FED, Chapter on Legalized Counterfeiting.
[66] Refer to chapter on Free Exchange and Interventionism, Triangular Intervention.
[67] Hazlitt, (1960) What You Should Know About Inflation, Chapter False Remedy: Price Fixing.
[68] See Rothbard, (1962) Man Economy and State with Power and Markets, Chapter 12 The Economics of Violent Intervention in the Market, Part 5 Triangular Intervention: Price Control.
[69] Jevons, (1875) Money and the Mechanism of Exchange.
[70] Hayek, (1967) Studies of Philosophy, Politics and Economics.
[71] Fetter, (1931) Some Neglected Aspects of Gresham's Law.

increased. Further, as the fiat money base is continuously inflated, it will continue to depreciate in purchasing power, thus incentivizing spending over rational saving.[72] Alice will retain her sound and hard bitcoin, until she no longer has any artificially overvalued fiat. At the point where she has fully moved to the voluntary and sound economy of Bitcoin, her time preference has decreased accordingly and she will adjust her spending patterns. Now she will willingly exchange her sound bitcoin for precious goods and services which she actually needs, and not because she is artificially incentivized to over consume. So far, few individuals have fully thrown off all their fiat bags, but those that did, now experience the total realignment of their time preference to a voluntary market economy.

"Historically, it has been good, strong currencies that have driven out bad, weak currencies. Over the span of several millennia, strong currencies have dominated and driven out weak in international competition. The Persian daric, the Greek tetradrachma, the Macedonian stater, and the Roman denarius did not become dominant currencies of the ancient world because they were 'bad' or 'weak'. The florins, ducats and sequins of the Italian city-states did not become the 'dollars of the Middle Ages' because they were bad coins; they were among the best coins ever made. The pound sterling in the 19th century and the dollar in the 20th century did not become the dominant currencies of their time because they were weak. Consistency, stability and high quality have been the attributes of great currencies that have won the competition for use as international money."[73]

---

[72] See Hülsmann, (2009) The Cultural Consequences of Fiat Money.
[73] Mundell, (1998) Uses and Abuses of Gresham's Law in the History of Money.

8   Speculative Attack

As the demand for fiat currency increases, it will initially increase its value, which will incentivize central banks and governments to produce additional units of money. This will increase the money supply, lowering the stock-to-flow ratio and thus decreasing the purchasing power of the fiat currency. As the money is now less valuable, it is also cheaper to borrow money and pay back at a later point in time at a further decreased purchasing power. The increased inflation rate will thus incentivize the accumulation of additional debt, which will again increase the money supply, further weakening the fiat currency. Thus, the liabilities side of Alice's balance sheet will increase in mortgages and consumer loans. Fractional reserve based credit creation does not just increase the money supply, the flip side of this coin is that money supply increases and lower interest rates drive demand for more credit creation.

Let's assume that there is a sound and hard monetary alternative to the fiat money, and that the fiat debtors will exchange their fiat currencies for the sound money. This increases the demand for the sound money, which will due to a unchanging stock-to-flow ratio increase its purchasing power. Thus simultaneously, the fiat currency will decrease in purchasing power as additional debt is taken on, and the sound money will increase in value. Those speculators now hold more valuable money and have to pay back the less valuable money, netting a substantial profit. Thus, the asset side of Alice's balance sheet will increase in total bitcoin hodlings.

"The effect of people, businesses, or financial institutions borrowing their local currency to buy bitcoins is that the bitcoin price in that currency would go up relative to other currencies. […] The central bank would have to either increase interest rates to break the cycle, impose capital controls, or spend their foreign currency reserves trying to prop up the [fiat] exchange rate. Only raising interest rates would be a sustainable solution, though it would throw the country into a recession." [74]

The rational action for economic participants would thus be to go into debt in the weak currency and accumulate sound money. *"As soon as the public became familiar with the new possibilities, any deviations from the straight path of providing an honest money would at once lead to the rapid displacement of the offending currency by others."* [75]

---

[74] Rochard, (2014) Speculative Attack.
[75] Hayek, (1974) Denationalisation of Money, Free trade in Money, p.23.

This is not just a hypothetical construct, as there are countless examples of people taking on fiat debt and mortgaging their house to buy even more bitcoin. Curiously, so far the stock-to-flow ratio of fiat money was higher than that of Bitcoin, but only in the early days. Especially with the next halving in 2020, the issuance rate of bitcoin will be much lower than that in fiat, further increasing this effect.

"A hyperbitcoinization event will be much quicker than a hyperinflation event. I have two reasons for this. First, the government will have a much greater difficulty preventing bitcoins from entering the country due to the impotency of capital controls upon it. Second, hyperinflation is inherently an attempt to fool people, whereas hyperbitcoinization is quite regular and predictable (at least by comparison). Therefore people will more easily see that they had better switch over. Thus, as fast as hyperinflation is, hyperbitcoinization will be even faster.

Hyperbitcoinization will not disrupt the economy to nearly the same degree as hyperinflation. The currency is the instrument of the division of labor, and hyperinflation makes it unreliable and forces people to use worse alternatives. In a hyperbitcoinization event, people switch from a fundamentally inferior currency to a superior one, whereas in a hyperinflationary event people will only switch to a new currency once the old currency becomes worse than the next best alternative, such as gold or detergent. Hyperbitcoinization should be accompanied by a rapid improvement in productivity and wealth."[76]

---

[76] Krawisz, (2014) Hyperbitcoinization.

9 Scarcity

There are two different type of goods, scarce and non-scarce. If taking the original good eliminates the possession of the previous owner, it is a scarce good; but if a good can be taken without displacing the original, it is non-scarce. Most goods however, are a combination of both types.[77]

A 3D tangible[78] good is scarce, there can be conflict over who has the right to own and use such good. The very possibility of such a conflict makes economical and ethical rules over who controls that good necessary. Property rights are the fundamental tool to organize such scarce goods and prevent never-ending conflicts over resources. Hoppe writes*: "only because scarcity exists is there even a problem of formulating moral laws; insofar as goods are superabundant ('free' goods), no conflict over the use of goods is possible and no action-coordination is needed".[79]* Property is a concept or a mutually binding rule that enables conflict-free interaction in a scarce world. At the minimum, there exists scarcity in the body and time of humankind, even in a hypothetical construct of superabundance.[80] Property right in body and time are thus the precondition for all sovereign human action. Only the true owner of the body can by sheer power of will directly coordinate and manage it. Scarcity does not automatically create a price of the good, as that also presupposes demand for such a good. A mud pie is by definition scarce, there can be conflict over who owns and controls it, but most likely, it will not have a price in the market. Nor does scarcity refer to the quantity available of the good, or the rarity of it.

Scarcity is thus defined by the possibility of arising conflict over the true owner and manager of a finite thing. It applies to anything and everything that cannot be simultaneously owned, i.e. one's ownership and control excludes others, social ownership doesn't apply. Scarce goods can only be acquired either by the homesteading unused resources, by the economic mean, i.e. trading in a voluntary market, or by the political mean, i.e. forcefully stealing the good from an unwilling subject. Scarce goods are allocated and rationed by prices in the free market.

---

[77] A book has scarce pages, but conveys non-scarce knowledge
[78] Scarcity is not limited to tangible goods though, as it also applies to radio waves or airspace
[79] Hoppe, (1989) Theory of Socialism and Capitalism, p.158, n.120.
[80] Hoppe, (1989) Theory of Socialism and Capitalism, p.20-21.

On the other hand are non-scarce goods, which due to their super-abundance are not subject to desire and choice. Those free goods don't have value in the classical sense, but they exist in superfluity, they gratify and also satisfy all desires which depend on them.[81] It is thus a nonfinite good, which can be replicated without limit, so that everybody can satisfy his desire for it and there is no conflict over ownership. No additional copy will replace the previous copies, nor degrade the quality of the copied good. Ideas can be kept exclusively by the owner as long as he keeps it to himself, but as soon as he utters the thoughts, they force themselves into the possession of everyone that hears the words. The peculiar attribute is that the 'original' thinker still holds full possession over his idea, and all others receive the full expression without any loss. Similar to a match that can light another, without becoming extinct by passing on the flame. This is a benevolent design of Nature, that ideas can be shared freely and openly without lessening the quality, and at no costs to the original thinker.[82] *"When speaking words, they can be taken all to oneself, yet leave all to others and unless the memory fades away, everyone who can hear those words, can take them all and go on each separate way."*[83] *"A teachers time and body is limited and scarce, thus his payment is not for the sharing of non-scarce ideas, but for the presentation and his labor service, which is of course a scarce good."*[84]

With the advent of the printing press, a sheer limitless number of books could be copied without losing any quality in content and without destroying the original book. With new technologies today such as laser and 3D printers, we can manufacture various tangible objects by using a recipe.[85] The same is true for a song, which anyone can sing after it is initially performed. The concept further applies to all digital information, for example a pdf document, mp3 music files or jpeg picture can be copied perfectly ad infinitum for near zero cost. In general, the World Wide Web is an interconnected network of nodes copying and sharing non-scarce goods, sending them to anyone who is interested in receiving this knowledge. As we continue moving towards a digital world, the number of non-scarce goods will continue to increase drastically.

There is no conflict of ownership and control, and thus no property rights apply in this cyberspace. Prices arise in scarce goods to ration the unique goods and allocate them to the most urgent need. Because free goods are only guides for human action and can be

---

[81] Fetter, (1915) Economic Principles, Chapter 1, §3.
[82] See Jefferson, (1813) Letter from Thomas Jefferson to Isaac McPherson.
[83] Wills, (1999) St. Augustine, p. 145.
[84] Kinsella, (2014) A Libertarian Theory of Contract: Title Transfer, Binding Promises, and Inalienability", Journal of Libertarian Studies 17, no.2, pp. 24-26.
[85] Kinsella, (2008) Against Intellectual Property.

copied to satisfy each and every desire, there are no property rights and no need to economize and ration them based on price. Although there is no structure of production when sharing non-scarce goods, they can be economized and commercialized.

Non-scarce goods are all kinds of information like thoughts, ideas, or art, and therefore essential to everyday life. Without these free gifts, there would be no innovation, learning nor advancement. Society can only progress through imitation of accumulated knowledge. Entrepreneurs emulate the success of others and gather experience also from failings. Profits of one peer incentivize new entrepreneurs to copy the successful business model and adapt it to their unique circumstances. Non-scarce goods are thus the driver of all competitive business. *"These designs – the recipes, the formulas, the ideologies – are the primary thing; they transform the original factors – both human and nonhuman – into means."* [86] Once the idea is 'produced' it no longer has to be produced, it is an unlimited factor of production. Ideas themselves don't create wealth, but rather the action that arises out of the initial thought.

Now that we have established that ideas are non-scarce goods and should therefore be shared openly with anyone, let us consider government enforced intellectual property rights. The name itself already contains a fallacy, as only scarce goods give rise to property rights, in order to organize and allocate resources. Because ideas are non-scarce, there are no property rights necessary to ration the good, it can be shared endlessly at almost no cost to the 'original' thinker. Rather, sharing an idea and propagating it throughout society increases the value of the idea, as more people know about it, can understand it and eventually act upon them accordingly.[87] Only when the thought is shared can it outlive the 'original' thinker. With intellectual property rights, not the 'original' thinker, but the person that first registers the idea at a state institution, receives the monopoly right to 'use' this idea. Only he has the legal 'right' to manifest the thought into reality. If anyone else dares to act upon this idea, the patent holder is supported by government thugs in aggressively stopping or hindering that manifestation. This also applies, even though another person might come up with the idea independently and without any knowledge of the previous thinker. If this person, who possesses the rightful property in the original factors, with the application of the idea turns them into means, the patentee is supported in violating the property rights and confiscating or destroying the property or otherwise extracting wealth from the second thinker. Intellectual property rights thus break the fundamental nature of non-scarce goods and

---

[86] Mises, (1949) Human Action, p. 142.
[87] McLuhan, (2006) The Classical Trivium.

tries to introduce artificial scarcity where none exists. A good that can be gifted freely and openly to anyone, is limited without any need to do so, nobody is stolen from when sharing an idea. Furthermore, the person that apparently 'stole' the idea, is violated in his property rights and liberty. Thugs literally steal his property on the basis, that some other person had a thought before him. This regulation not only hinders the general advancement of society, through the artificial scarcity of a free and limitless good, but further breaks the Natural Law inherent in creation. Intellectual Property is thus neither economically sound, nor morally righteous.

Cypherpunks realize the economic and moral fallacies of intellectual property, and see the immense potential of creating a community in cyberspace where free non-scarce goods can be shared as open and as widely as possible. A fundamental building block of today's Internet is the realization, that code is non-scarce speech and therefore protected by the Natural Law of freedom of speech and expression. This especially applies to privacy enhancing technologies such as encryption.

The natural conclusion of this realization is, that the code of each and every application should be open source, that it is shared and that anyone can see and edit the source code of the software. Only this way can the sheer limitless potential of non-scarce goods be reached. Once the code is written, it can be shared at no cost to the creator. It is evident, that there is no perfect and bug-free code. Thus the more developers take a look at the code and check for validity and security, the more the refined the code will be. Permissionless innovation means, that anyone can work on any problem and try to solve it. Nobody has to ask for permission in order to fix or break the code, just like nobody has to ask for permission to write a poem or sing a song. This creates countless black swan events, where a seemingly unsolvable problem is solved in an unexpected but brilliant approach. Nobody thought about this, but one peer somewhere on the interwebs did. As soon as this hidden genius shares his solution to the problem, he has unleashed the power of the non-scarce idea and everybody can copy, adapt and improve the approach. Only one person in a billion needs to find the solution, if he freely shares it with the world, everybody will benefit. Therefore, free software will always outperform any guarded and closed source software: open software wins.[88]

Further, the software user should have full control and trust in the hard- and software that he is running. In a closed source system, there is no possibility of the user to check if the software is doing, what it is advertised to do. He has to blindly trust the intransparent

---

[88] Rosenberg, (2009) The Meaning of Open.

developers. Contrarily, in an open source system the user can, if he has the ability, verify for himself, what the code is and if the software is running secure and sound. Even if the user himself does not have the ability to verify the codes validity, he can verify if there are developers working on improvements and bug fixes. If those developers are reputable and the user can trust their skill and dedication, he has a much higher insurance that the code is clean. Don't trust ~ verify.

Bitcoin is entirely and relentlessly open source. Each and every line of code is auditable. Several thousand volunteers work on the code in an equal and transparent process. Everybody can fork the code, make changes and issue a pull request to merge the code. However, this does not mean that anyone can easily change the code of the Bitcoin core client, or even the protocol rules. There is a rigorous peer review process[89] where even the most trivial of changes gets audited by several different developers, nobody trusts anyone. Bitcoin spawns out of the internet of open source non-scarce goods, a protocol on the network. The software running the consensus code is fully transparent and auditable buy every single full node. It can be downloaded and installed on any scarce hardware that the individual owns. Because of the open source code, and the general attitude of 'don't trust ~ verify' of Bitcoin, the user has full control over which software they deploy on their own hardware.

A private key is only a large random number, a piece of information that is non-scarce and can be copied endlessly, without any cost and at no loss to anyone. However, in the Bitcoin script corresponding to a UTXO can be the requirement to prove control over this private key with an elliptic curve digital signature. Thus, only with knowledge of the private key, can the bitcoin be spent. Other Bitcoin script programs can assign the claim to the bitcoin, to anyone who can fulfill all the conditions, like proof of knowledge of several private keys with a multi signature, or a time delay in check sequence verify. Further advanced smart contracts such as the lightning network can shift the state of a MultiSig off chain. All these scripts provide a clear set of rules over who has access and the right to control these specific bitcoin. With the brilliant pattern of speech, Nakamoto Consensus emerges cryptographically proven scarcity.

In order to secure this attribute of scarcity, Bitcoin employs a plethora of economic incentives and applies monetary theory. In order to secure Bitcoin against a double spend, the duplication of one UTXO, miners order and timestamp transaction and accumulate cryptographic proof of work. Because miners gain economic financial gains and profits

---

[89] Bitcoin Improvement Proposal

with scarce bitcoin in the coinbase reward, they are incentivized to adhering to consensus rules. With a majority of miners accepting consensus as defined by individual sovereign nodes, the chain with the most accumulated PoW contains the valid time order of transactions. PoW is needed to defend bitcoins scarcity even against malicious actors trying to use the same UTXO twice. Running a node and accumulating valid PoW is a tool for defending the Nakamoto consensus which upholds the attribute of scarcity of bitcoin.

10 Conclusion

Money is a tool to postpone the gratification of desires into an uncertain future, this aspect as a store of value is enhanced with a predictable and hard money supply. In Bitcoin, the issuance rate is set by Nakamoto Consensus, which is voluntarily agreed upon and unchanging, thus no violation of property rights. This decreases the time preference of peers and increases overall capital accumulation and savings. However, due to an initially low stock-to-flow ratio, malinvestments and overconsumption have manifested, which will be readjusted as the issuance rate of bitcoin decreases exponentially. A non-scarce piece of information, the private key, can be used to transfer control of a scarce bitcoin, thus fulfilling the medium of exchange function. Due to the sound monetary theory, hyperbitcoinization will occur sooner rather than later and Bitcoin will function as a reliable unit of account, decreasing the complexity of deep production stages and reducing entrepreneurial calculation costs.

Self-sovereign nodes make up their own individual set of rules, query the network and only connect to those peers that voluntarily agree upon the same monetary consensus. No one represents these users, as they are in full control over their open source software and secure their own private keys. There is no theft of private property whatsoever, all actions are agreed upon voluntarily and are mutually beneficial. Thus, Bitcoin is fundamentally based in the moral principles of Natural Law and Liberty.

References

Adams, Samuel   The Rights of the Colonists, The Report of the Committee of Correspondence to the Boston Town Meeting, 1772

Adams, Samuel   Selections from his writings, Edited, with an introduction, by Elizabeth Lawson, New York: International Publisher, 1946

Ammous, Saifedean   The Bitcoin Standard: The Decentralized Alternative to Central Banking, 2018

Aquinas, Thomas   Summa Theologia-Illea, 91,1, 1485

Bakunin, Michael   On Anarchy, Edited, with an Introduction and Commentary, by Sam Dolgoff, 1971

Cantillon, Richard   An Essay on Economic Theory, 1755

Fetter, Frank Albert   Economics, Volume 1, Economic Principles, 1915

Fetter, Frank Walter   Some Neglected Aspects of Gresham's Law, Quarterly Journal of Economics, 1932

Friedenbach, Mark   Comment from the /r/BTC sub-Reddit, https://www.reddit.com/r/btc/comments/415vme/ now_that_real_consensus_is_forming_be_ready_for/cz0bejv/?context=3, 2016, Sourced on 29.11.2018

Guynn, Jack   Speech at the Bridgewater College, Bridgewater, Virginia, April 11, 2005

Hayek, Friedrich August von   Denationalisation of Money: The Argument Refined, An Analysis of the Theory and Practice of Concurrent Currencies, 1976

Hayek, Friedrich August von   Studies of Philosophy, Politics and Economics, Routledge & Kegan Paul, London and Chicago, 1967

Hazlitt, Henry   What You Should Know About Inflation, 1960

Hoppe, Hans Hermann   Theory of Socialism and Capitalism, 1989

Hülsmann, Jörg Guido   The Ethics of Money Production, 2008

Hülsmann, Jörg Guido   Lecture on the Cultural Consequences of Fiat Money, 2009

Issing, Otmar   Der Zins und sein moralischer Schatten, Frankfurter Allgemeine Zeitung, 1993

Jefferson, Thomas   Rough Draught of the Declaration of Independence, The Papers of Thomas Jefferson, Volume 1: p. 423-28, 1760-1776

Jefferson, Thomas	To Isaac McPherson Monticello, 1813
Jevons, William Stanley	Money and the Mechanism of Exchange, 1875
Kinsella, Staphan	A Libertarian Theory of Contract: Title Transfer, Binding Promises, Inalienability, 2014
Kinsella, Staphan	Against Intellectual Property, 2008
Krawisz, Daniel	Hyperbitcoinization, 2014
McLuhan, Marshall	The Classical Trivium: The Place of Thomas Nashe in the Learning of His Time, 2006
Menger, Carl	On the Origins of Money, 1892
Mill, John Stuard	The Currency Question, p. 579-598, 1884
Mises, Ludwig von	Human Action, 1949
Mises, Ludwig von	Theory of Money and Credit, 1912
Mundell, Robert	Uses and Abuses of Gresham's Law in the History of Money, 1998
Nakamoto, Satoshi	Bitcoin: A Peer to Peer Electronic Cash System, 2008
Nakamoto, Satoshi	BitcoinTalk.org thread, June 2010 https://bitcointalk.org/index.php?topic=195.msg1611#msg1611, Sourced on 29.11.2018
Rochard, Pierre	Speculative Attack, 2014
Rosenberg, Jonathan	The Meaning of Open, 2009
Rothbard, Murray	Freedom, Inequality, Primitivism, and the Division of Labor, in Egalitarianism as a Revolt Against Nature, and Other Essays, 1965 (Auburn, Ala.: Mises Institute, 2000), pp. 299–302.
Rothbard, Murray	Man, Economy, and State with Power and Market, 1962
Rothbard, Murray	What Has Government Done to Our Money? 1963
Rothbard, Murray	The Austrian Theory of Money, 1976
Rothbard, Murray	The Case Against the Fed, 1994
Schelling, Thomas	Schelling, Thomas C., The strategy of conflict(First ed.). Cambridge: Harvard University Press., 1960
Shirriff, Ken	Mining Bitcoin with pencil and paper: 0.67 hashes per day, 2017
Spooner, Lysander	Natural Law; or the Science of Justice: A Treatise on Natural Law, Natural Justice, Natural Rights, Natural Liberty, and Natural Society; showing that all Legislation whatsoever is an Absurdity, a Usurpation, and a Crime. Part First. 1882

Strauss, Leo	Natural Law, International Encyclopedia of the Social Sciences, 1968
Szabo, Nick	Shelling Out: The Origins of Money, 2002
Taleb, Nassim	Antifragility: Things that Gain from Disorder, 2012
Timón, Jorge	BIP 99, Motivation and deployment of consensus rule changes (soft/hard-forks), 2015, https://github.com/bitcoin/bips/blob/master/bip-0099.mediawiki , sourced 29.11.2018
Todd, Peter	Soft Forks are Safer than Hard Forks, 2016
Todd, Peter	Forced Soft Forks, 2016
Todd, Peter	BIP 65, OP_CHECKLOCKTIMEVERIFY, 2014, https://github.com/bitcoin/bips/blob/d37084d4baba1b88a84-9f1a7131f9e7c65dd0850/bip-0065.mediawiki#Deployment , sourced 29.11.2018
Van Den Gergh, Willem	On Schelling points, Network Effects and Lindy: Inherent Properties of Communication, 2018
Wills Garry	Saint Augstine: A Life, 1999

Appendix

1. Price Volatility BTC/USD

Latest 30-Day Estimate

4.58%

Latest 60-Day Estimate

3.46%

Bitcoin Volatility Time Series Charts

Zoom 1m 3m 6m YTD 1y All   From Aug 16, 2010 To Nov 27, 2018 ≡

Standard deviation of daily returns

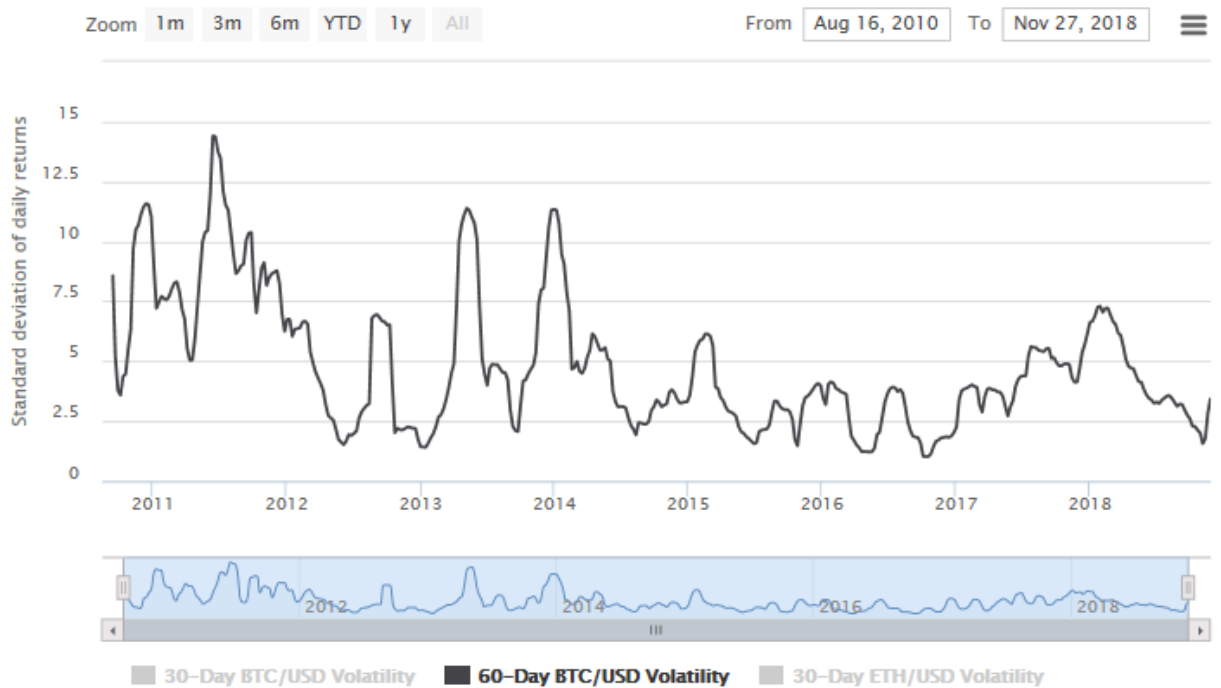30–Day BTC/USD Volatility   **60–Day BTC/USD Volatility**   30–Day ETH/USD Volatility

Illustration 1: Bitcoin Price and 30-Day BTC/USD Volatility

Source: www.buybitcoinworldwide.com/volatility-index/ 28. November 2017
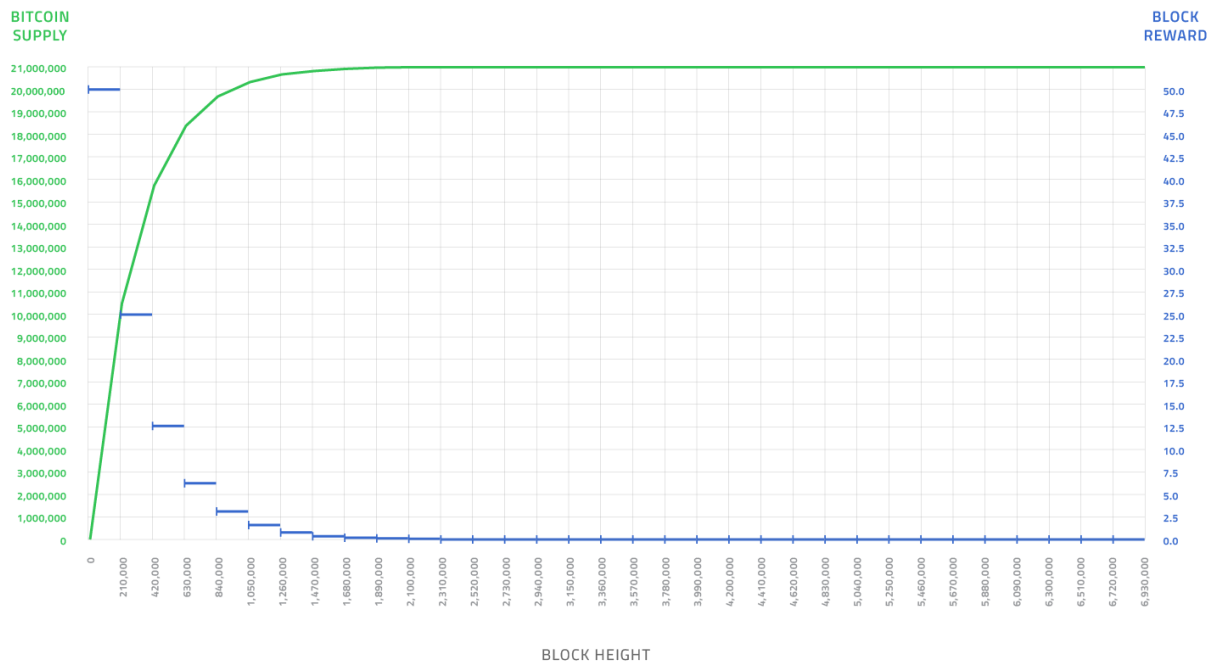
2. Bitcoin Money Supply and Issuance Rate

Illustration 2: Bitcoin Money Supply and Issuance Rate
Source: Nakamoto Consensus, verified on the authors full node.