LUISS

Department of Economics and Finance

Chair of Money and Banking

Bitcoin's Potential as a Fiat Currency Challenger: An Austrian Viewpoint

Supervisor:
Prof. Paolo Paesani

Candidate:
Gabriel Memet Eraslan, 255751

Academic Year 2022-2023

INDEX

Introduction

The world was introduced to Bitcoin when Satoshi Nakamoto introduced it in 2008. Ever since, the cryptocurrency has attracted the attention of economists, cryptographists, politicians, and the world. Bitcoin uses blockchain technology and cryptography to operate. Blockchain technology allows Bitcoin to have a distributed ledger, where anyone can participate and join the network, creating the first ever user-oriented currency.

Bitcoin can disrupt the traditional financial system we know today, because of how it was designed and what it stands for. This analysis will focus on what these characteristics are and how they pose an innovation to fiat currencies. The first chapter focuses on the traits of Bitcoin. Scarcity, decentralization, and immutability of the blockchain altogether create a secure peer-to-peer payment system that doesn't require the trust or need of a third party. Before Bitcoin, all these traits put together in one single currency are something never seen before. While these form the base layer security of Bitcoin, mining, and miners provide continuous security with an incentive-based system known as proof of work.

Although it has grabbed most of the attention Bitcoin is not the only cryptocurrency, it's just the first successful one. The second chapter focuses on other cryptocurrencies as well, with an emphasis on the differences between Bitcoin and other cryptocurrencies and what must be done to improve Bitcoin. There have been many improvements made since its release and there are many more to come. Since Bitcoin provides users a say in what happens, all these improvements will be made with the consensus from the users, bringing democracy to currency as well.

The final chapter tries to imagine the implications of a hypothetical Bitcoin standard, where Bitcoin is widely used, accepted and seen as a store of value. Before arriving at conclusions about a hypothetical Bitcoin standard, this paper analyses whether Bitcoin could even be considered as money, where money has the traits of a store of value, unit of account and medium of exchange. If we were to consider Bitcoin as sound money, an economy with a finite supply of currency would come with many implications such as deflation and the consequences of this phenomenon are and have been widely discussed by both Austrian and Keynesian economists, who have arrived at two very different conclusions. In this paper, we will look at a more Austrian perspective on Bitcoin.

Because it's still a new development, Bitcoin has a long way to go in terms of acceptance and whether it could have a significant impact on the traditional financial system will depend on the robustness of the system, which this paper focuses on deeply. Only if the market were to recognize the efficiencies made possible by Bitcoin it would be possible for it to achieve wide acceptance, which is a scenario that might not be impossible.

Chapter 1

Nakamoto's innovation and the idea behind it

1.1- Bitcoin and its characteristics

On October 31st, 2008, an anonymous individual or group of persons who goes by the pseudonym of Satoshi Nakamoto published the Bitcoin white paper, which describes the protocol and technical functions of Bitcoin.

Satoshi Nakamoto's first words in the white paper are those that summarize what Bitcoin is: *"A purely peer-to-peer version of electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution"*[1]. While payment systems such as credit cards have middlemen that ensure the transaction is successful, bitcoin operates differently. Bitcoin uses the collaboration of individual miners to validate transactions.[2] Being a peer-to-peer currency, Bitcoin allows payments to be made directly from the sender to the receiver. This makes it like cash since they are both peer-to-peer. A difference between cash and Bitcoin would be the fact that cash is considered anonymous while Bitcoin uses public keys to receive money and this public key number is accessible to anyone. If a government ID was attached to that public key, no transaction made by that account would be anonymous.

Bitcoin was designed to have certain characteristics that differentiate it from most of the resources found on earth and from most types of money used until now. Bitcoin transactions are ensured by a cryptographic algorithm and not the government, differing from the currencies we use today. This characteristic makes Bitcoin entirely decentralized from any public or private entity.

---

[1] Nakamoto S. (2008) Bitcoin: A peer to peer electronic cash system.

[2] See chapter 1.3 mining

Bitcoin's Decentralization: When designing Bitcoin, Satoshi had to overcome the problem of having transactions registered without the assistance of any central authority. For this to be accomplished the system chosen was one where many individuals who don't know each other took on the role of acting as an 'accountant'. The transaction validation process is a perfect example of peer-to-peer decentralization. When a transaction X is made, the information of that transaction[3] is then sent to miners that have the IP of that specific account registered. Miners that have that IP registered will be notified of that transaction and the miner that acts quicker than all the other ones will be the one to register that transaction. Before this happens, the miner will have to check the commission fee and decide if it's rational and incentive compatible. That miner will have to write the transaction on a block it's currently editing. When the block of transactions is filled, that block will be shared on the blockchain for all miners to validate it[4]. This step is crucial for miners, since in order to receive commissions from transactions, they need other miners to validate their work. This last step of unanimous validation is essential to avoid the double spending problem, because if another miner that received the same transaction information tries to add its block to the blockchain, with the same transaction information of the latter, that transaction would be processed twice. Due to other miners' auditing, two blocks that have the same transactions will not be validated.

Decentralization has many benefits to it. This characteristic protects its users against censorship[5] and against manipulation of the currency, perhaps to devalue it. If a single authority becomes corrupt or compromised, the currency that is supported by that authority will likely be manipulated, and its users will probably have to suffer in the form of inflation or censorship. With centralized currencies, one must trust its central authority to know that its transaction is registered accordingly. Bitcoin on the other hand uses an interconnected system of millions of individuals that are economically incentivized to be truthful to each other, making it extremely challenging for an

---

[3] Account number, amount to send, and commission fees

[4] *"Blocks are data structures within the blockchain database, where transaction data in a cryptocurrency blockchain are permanently recorded. A block records some or all of the most recent transactions not yet validated by the network. Once the data are validated, the block is closed. Then, a new block is created for new transactions to be entered into and validated."* Frankenfield J (2022).

[5] Censorship related to money happens when the government or an intermediary has the authority to block anyone from the use of that money. For example, when government dissidents have their bank accounts blocked, they are censored.

individual bad actor to compromise the system. This distribution of vulnerability lowers overall vulnerabilities, because in order to gain control of the Bitcoin network more than 50% of the nodes[6] in the network would have to cooperate, all with the same goal. As the system grows larger, the possibility of this threat becomes almost null[7]. Just as with most things, decentralization presents some challenges as well. The lack of central guidance makes it very difficult for Bitcoin to improve or modify from its current version. For this to happen, each individual node will have to make these modifications for itself. This decreases the likelihood that Bitcoin receives major changes because each node could be any person with a computer, and they are unidentifiable. Although decentralization is both an advantage and a disadvantage for Bitcoin, this is a trade offer that users will have to accept since Bitcoin won't be changing its operating system any time soon.

Bitcoin's Scarcity: Scarcity is one of economics core concepts. Lionel Robbins (1935), for example, describes economics as "*the study of the allocation of scarce resources which have alternate uses[8]".* Humans have infinite wants; however, our world has finite resources. Because resources are finite, or in other words scarce, everybody's demand cannot possibly be met. This forces us to choose economic systems to distribute these resources.

There are two types of scarcity. One is relative scarcity and the other is absolute scarcity.

• Relative scarcity: These resources do not have a fixed supply because when demand for this resource increases, supply will increase for the new demand to be met. Gold is an example of this resource.

• Absolute scarcity: These resources have a fixed supply, so whenever demand for this resource increases, supply can never increase.

Bitcoin fits into the absolute scarcity category because it has a fixed supply of 21 million coins and it can never exceed this number, as this is its protocol. When demand for Bitcoin increases, the only variable that changes to equate demand and supply to reach its equilibrium is its price.[9]

---

[6] "*A node can be described as a device running the software of a specific blockchain"* Till Wendler, Peaq CEO (2022)
[7] The probability of millions of random people that do not know each other acting together with a common goal of distrupting a system which is profitable for most of them can very hardly be above 50%

[8] Robbins L. (1935). *An Essay on the Nature and Significance of Economic Science*. London: MacMillan and Co

[9] Suriyan, S. (2021). Bitcoin's Price Rises Rapidly Due to Absolute Scarcity. *Bitcoin Magazine*

Still, this doesn't mean that Bitcoin is not impacted by inflation. To this day approximately 19 million bitcoins have been mined, leaving 2 million more to be mined. As explained previously, miners receive revenue through commissions from transactions. Another way to earn revenue, is from block rewards which will be explained in chapter 1.3[10]. When 210.000 blocks are found that reward is cut in half until there are no more bitcoins to be mined. Initially, each block rewarded a miner with 50 bitcoins, today this number is 6.25. Based on this schedule, all bitcoins will be mined by the year 2140. The fact that bitcoins are continuously mined[11] automatically implies that there will be inflation attached to it until the year 2140. However, this inflationary effect won't be felt as in fiat currencies, since the amount mined each year is a very small portion compared to bitcoins' total circulating supply.[12]

The quantity theory of money assumes MV=PT where M represents money supply, V represents money velocity, P represents the general price level and T the total volume of transactions in an economy. Assuming V and T constant, an increase in the money supply would directly imply an increase in the price level according to the QTM. This causes a fall in the purchasing power of individuals (1/P). With scarce money, the supply doesn't shift as much as fiat currencies' supply does, implying that the QTM equation remains stable over time (with V and T constant).

The timeline of Bitcoin's supply change is depicted in **Figure 1.** Bitcoin's inflation is described as the relationship between newly issued bitcoins and the already existing ones. This inflation rate is predictable since the amount issued in each period is predetermined. In March 2020 this rate was 1.8%, meaning that an additional 1.8% units of bitcoin have been added to its supply.

---

[11] This causes existing miners' costs to rise as new miners join the network, as seen more in-depth in Chapter 1.3.1.

[12] Khalif, David. (2022). What Happens When All 21 million Bitcoin Are Mined? *Nasdaq*

Figure 1: Bitcoin's predictable supply and decreasing inflation rate
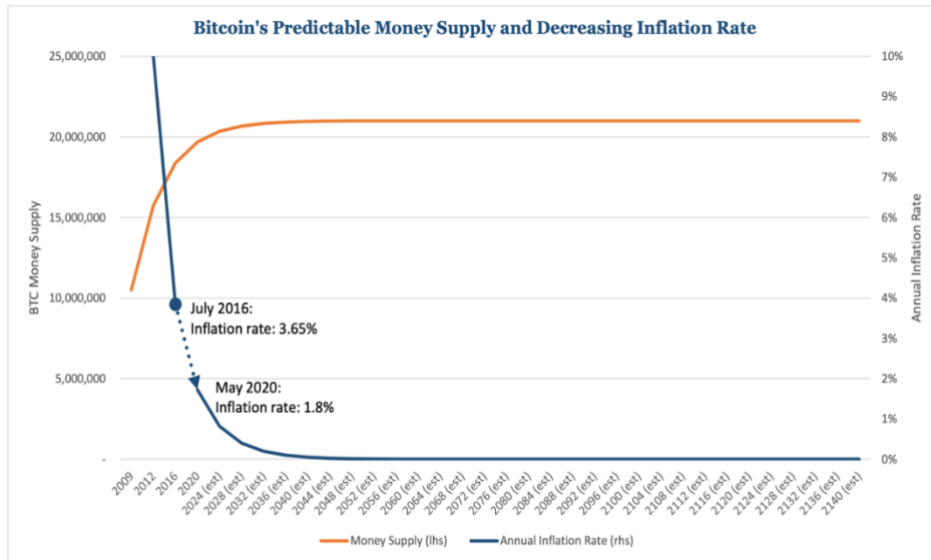
Immutability of the Blockchain: The blockchain is the technology that enables cryptocurrencies to exist. Each cryptocurrency has its own type of blockchain with its own different protocols. With Bitcoin, this technology is almost immutable.

This characteristic exists on two levels, the first being that Bitcoin's consensus protocol is extremely resistant to alterations. This is achieved thanks to its high level of decentralization, and as a result, its scarcity is protected. Each individual runs the same code, and they all agree to the same rules, as they are economically incentivized to do so. This implies that a government or any single entity would have to recruit each node one by one in order to achieve enough nodes for a modification in the blockchain.

Secondly, Bitcoin's blockchain is immutable in the aspect that its history cannot be easily rewritten. Once transactions occur, they are forever registered on the blockchain and can be audited by any individual who wishes to do it. This is how we know exactly when the first ever Bitcoin transaction occurred[14]. If a malicious miner wanted to rewrite a block's content, all blocks after

---

[13] Horizon Kinetics LLC (2020). Bitcoin Supply Curve Over Time

[14] We know from looking back at the blockchain that the first ever bitcoin transaction occured between Nakamoto and computer scientist Hal Finney. However, the first commercial transaction was between Laszlo Hanyecz and Papa John's, where 10.000 bitcoins were traded for two pizzas.

that block would also be altered, since each new block contains the previous block's hash[15]. This would in turn cause all non-malicious miners to correct that alteration, otherwise they would all be negatively affected by it from an economic point of view[16] since they have spent a large amount of resources (energy and the cost with comes with it) in '*mining*' a specific block and a malicious miner trying to rewrite the content of the block nullifies the other miners' efforts to validate that. The case in which these arguments for the blockchain's immutability are rendered invalid is when a 51% attack occurs. A malicious miner must obtain 51% of all the mining power for this to ever be possible. This attack is very hard to implement as previously explained, however, it's still a possibility. Still, the unlikeliness of such an attack makes Bitcoin relatively safe for preserving history, because records could only be falsified if the 51% attack occurs. Anyone that records a message or a transaction on the Bitcoin blockchain will most likely leave that message to the following generations to come, without any modification to it. This allows the Bitcoin blockchain to be a reliable source for past transactions and events since no one can meddle with its content and in this sense Bitcoin preserves history.

A metric to measure the risk of a 51% attack is called 'hash rate'. The hash rate measures the total mining capacity of the Bitcoin network. The higher this rate the better since a high hash rate implies major costs for this attack to be realized[17]. **Figure 2** shows the value of the hash rate together with the market price of Bitcoin. The hash rate has been on a sharp rise since August 2021 even after the drop in the price of Bitcoin. This signals an unprecedented level of security in the Bitcoin blockchain.

---

[15] A hash is a mathematical function that is involved in guaranteeing Bitcoin's security.
[16] Immutability. *River Financial*

[17] "51% Attack | River Financial." *River Financial*, https://river.com/learn/terms/1/51-percent-attack/

Figure 2: Total hash rate and bitcoin's market price

Finally, **Figure 3** makes a comparison of characteristics between bitcoin and gold amongst many aspects, such as decentralization and scarcity which have already been discussed. The comparison between gold and Bitcoin is made often because Bitcoin has many traits like gold such as scarcity, durability and fungibility. Especially the scarcity aspect, and the fact that both gold and Bitcoin are decentralized, have led many to call Bitcoin '*digital gold'*.

The difference in counterfeit resistance between gold and bitcoin arises from the fact that since bitcoin is a form of code it cannot be counterfeited, because an alteration of code would not give out the same results, making it futile in a transaction. Gold, on the other hand, is a metal which is still very hard to counterfeit however a malicious person could still give out fake gold disguised as true gold.

Portability is a trait that is inversely related to weight. Gold is very heavy to carry and having pockets full of gold is a major risk. On the other hand, bitcoin is carried on a phone or on a ledger which makes it safer to carry.

Divisibility is important for day-to-day transactions, where large currencies have to be divided into smaller ones according to needs. Gold is divisible, but one can only divide it using labor-requiring methods. On the other hand, 1 bitcoin can be divided into 100.000.000 pieces. Each piece is called a Satoshi, and the minimum transferable amount of Satoshi is 546 of them. This is a very small amount, equalling approximately 0.1267 US dollars in January 2023. The smallest gold denomination is a 'grain', which weighs 0.0648 grams and is impractical to use.

Durability is a strong point for both. Bitcoin is code, so it can never deteriorate. Gold is extremely durable, even after hundreds of years it can maintain itself.

Fungibility is the ability for something to be exchanged for other goods or services. Historically gold has always been used for this function, although it is very hard to use for small transactions. Bitcoin could be used for both because of its divisibility characteristic[18]

Figure 3: Bitcoin vs Gold

Trait	Gold	Bitcoin
Scarcity	Scarce, unknown supply	Scarce, limited supply
Counterfeit-resistance	Medium	High
Portability	Low	High
Decentralization	Low	High
Divisibility	Medium	High
Durability	High	High
Fungibility	Medium	High
User-friendliness and awareness	High	Medium

Source: Binance (2020)

---

[18] "Should I Buy Gold or Bitcoin? A Brief Comparison of Intrinsic Traits of BTC vs. XAU | Binance News." *Binance*, 30 July 2020, https://www.binance.com/en/news/top/46385.

1.2- How is Bitcoin's price determined?

The simple answer to this question would be that bitcoin's price is determined by supply and demand forces. This answer is simple and true, just like most things in the free market, however, there is much more to it.

Investors have very differing opinions on Bitcoin. Warren Buffet has criticized it saying that Bitcoin has no intrinsic value, many others don't see any value to it and expect it to go back to zero in the long run. But what is value? Value is a spectrum, there can't be a unit of measurement for value. Water is extremely valuable for us to live; diamonds are not but they cost much more so the price is not a measure of value. Value is for the most part subjective.

What about intrinsic value? "Intrinsic value or fundamental value is the 'true, inherent, and essential value' of an asset independent of its market value."[19] There are for the most part two views on bitcoins' intrinsic value, believers and skeptics. Sceptics would say it is zero since it doesn't exist, it's not real and has no 'value to **it'**. Believers would argue that some of its characteristics are those very things that give intrinsic value to it. These characteristics are those discussed such as decentralization, scarcity and immutability[20]. Gold's initial value came from physical properties like the cost of extraction, purity, and many other factors. Contrary to what skeptics believe, bitcoin has a cost of 'extraction' as well and its scarcity plays a major role in giving value to it. One could argue whether Bitcoin is fairly valued, but to state that its value is zero seems to be a misrepresentation.[21]

Going back to the initial question, the determinants of bitcoins price will be analyzed from 3 different factors[22].

---

[19] "Intrinsic Value. *Wikipedia, the Free Encyclopedia*

[20] *Bitcoin& Intrinsic Value*. Payward.Inc, July 2020, https://www.lopp.net/pdf/Bitcoin-Intrinsic-Value.pdf .

[21] Kelleher, J. P. (2014, October). Why Do Bitcoins Have Value? Bitcoin Explained. *Investopedia*

[22] Ciaian P. et al. (2016). The Economics of BitCoin Price Formation. *Routledge*

1) Market forces: Supply and demand are the main market forces, however when talking about bitcoin the demand aspect stands out because its supply is fixed. Demand will depend on a variety of factors; anyone can have their reason to purchase Bitcoin. The speculative demand is the one that stood out during these years and that is why we have seen many boom-and-bust cycles to it. In the price calculation process supply is determined by bitcoins total circulating stock, and not by the pre-determined final amount of Bitcoin (which is 21 million). Demand is calculated by the volume of transactions and price level of goods and services such as the EUR/USD exchange rate. A more powerful dollar against the euro would appreciate against bitcoin as well and vice versa[23]. Historically the world has seen Bitcoin's demand rise for mostly speculative reasons, although its use as a hedge against inflation might be recognized soon because of its finite supply. Network effects have largely helped Bitcoin demand to rise because as the cryptocurrency becomes more popular, its demand increases[24]

2) Relationship between attractiveness and bitcoin price: As bitcoin becomes more attractive as an investment opportunity and the media starts to focus more on it, its price is positively affected by it. The research conducted by Glaser et al. (2014) indicates that investors intention to which they collect information about Bitcoin has a major impact on its price. At times the media gives false hopes of speedy growth for Bitcoin, which cause investors that seek information on the matter to buy Bitcoin and increase its price and vice versa. Whether the media gives hopeful or negative scenarios, Bitcoin's price might be affected by this emotion swing. Even though bitcoin has been around since 2008, for the mainstream it's still something to research thoroughly, making the gathering of information and the source from which that information is gathered almost as important, if not more important,
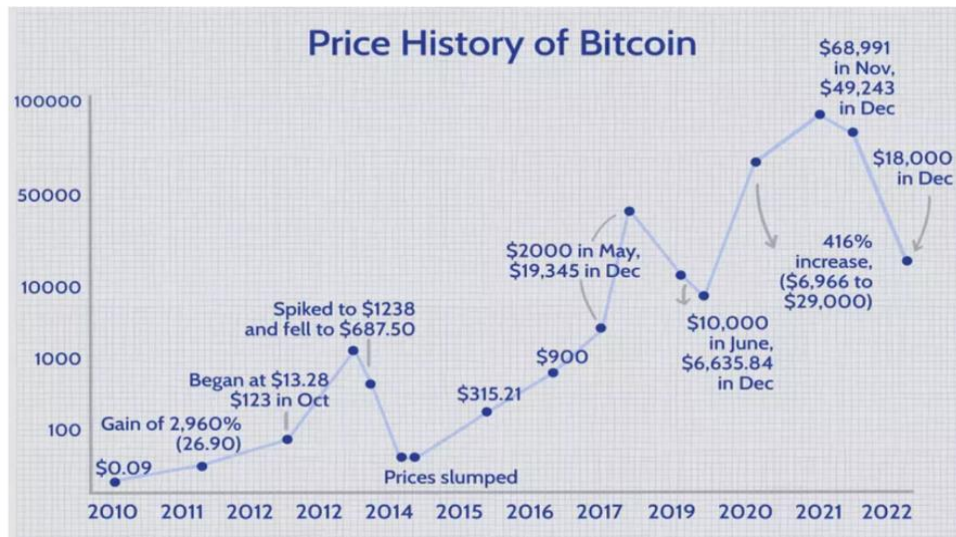
---

[23] Guizani, S. & Nafti I. K. (2019). The Determinants of Bitcoin Price Volatility: An Investigation With ARDL Model. *Elsevier*

[24] Nguyen T. et al. (2018). Factors affecting Bitcoin price in the cryptocurrency market: an empirical study, *International Journal of Business and Economics Perspectives*

than the items characteristics themselves[25]. The research suggests that potential investors can affect Bitcoin positively or negatively depending on the information that the media chooses to circulate in that period[26]. This suggests that speculation has a very important place in determining bitcoins price, implying that the efficient market hypothesis is not always realized[27], especially because of the media's choice of which aspects about determinate things to share and not to share, making economic agents not entirely informed and causing bubbles or cut prices. **Figure 4** depicts bitcoins price history on a logarithmic scale with its many sudden highs and lows. Bitcoin's price has seen a significant amount of volatility over the years, starting from 0.09 cents USD in 2010 up to almost 69.000 USD in 2021. Ever since its 2021 level, the price has decreased significantly. This is a trend that has accompanied Bitcoin almost every 2 to 4 years.

Figure 4: Bitcoin's Price History

Source: Investopedia (2022)[28]

---

[25] Under an efficient market, it would be expected that agents in the economy would decide on purchasing something based on an objective and rational decision-making process. When investors receive information which can be biased, the demand for that product will receive high alterations.

[26] Guizani, S. & Nafti I. K. (2019). The Determinants of Bitcoin Price Volatility: An Investigation with ARDL Model. Elsevier

[27] Since Bitcoin investors might purchase it based on non-objective information spread by different media sources, the efficient market hypothesis which states that agents are well informed about market conditions is not realized.
[28] Edwards J. (2015, December). Bitcoin's Price History. Investopedia

3) Macroeconomic and financial developments and bitcoins price: Bitcoin's price tends to be very related by macroeconomic and financial developments. Wijk (2013) analyzes bitcoins price fluctuations concerning oil, The Dow Jones and Nikkei 225 prices. Both the Dow Jones and the Nikkei 225 are used as financial indicators for respectively the United States and Japan's economic conditions. The Dow Jones is a stock market index of the 30 biggest and most reliable American companies listed on the NYSE and Nasdaq and the Nikkei 225 is the index of the biggest and most reliable Japanese stocks trading at the Tokyo Stock Exchange.

The study has shown, using econometric models, that in the long-run bitcoin has a positive correlation (0.525) with the value of The Dow Jones. This means that if the Dow Jones appreciates, bitcoin tends to move in the same direction, implying that bitcoins worth and the United States economy have a positive correlation[29].

Looking at the correlation with oil prices, this is instinctively negative. Wijk (2013) has shown in his study that the coefficient for the WTI oil price is -0.242. The reason for this is that generally oil is involved in many things, and an increase in oil price will increase costs for producers which in turn will have to reflect this to consumers. When consumers must spend more on other things, bitcoin is negatively affected by it.

Finally, Wijk (2013) shows that the correlation between Bitcoin's price and the Nikkei 225 is negative (-0.438). This means that bitcoin's price and the state of the Japanese economy might be negatively correlated, and that bitcoin is more dependent on the United States economy. He explains that the reason for this might be the fact that most Bitcoin buyers are investors who look for profit opportunities, meaning that when Nikkei 225 has positive prospects, they prefer to leave Bitcoin and invest in the latter.[30]For example, as seen in **Figure 4,** between 2010 and 2012 Bitcoin saw a spike in its price while the Nikkei 225 dropped by approximately 12%.

---

[29] This study looks at correlation, not necessarily causation. Overall the market would expect to see an increase in Bitcoin's price together with The Dow Jones.

[30] Wijk, D. v. (2013). What can be expected from the Bitcoin. *Erasmus University Rotterdam*

These 3 price determinants discussed can be divided into 2 groups: The first is **internal** factors (which are supply and demand) that arise from bitcoins own characteristics, and the other two can be expressed as **external** factors. Bitcoin's price is affected internally by supply and demand since the price tends to meet at the equilibrium between them but can also be affected by external factors that in turn affect the internal factor of demand. While internal factors are core economic concepts, external factors are more an influencing factor.

Figure 5: Bitcoin's price drivers
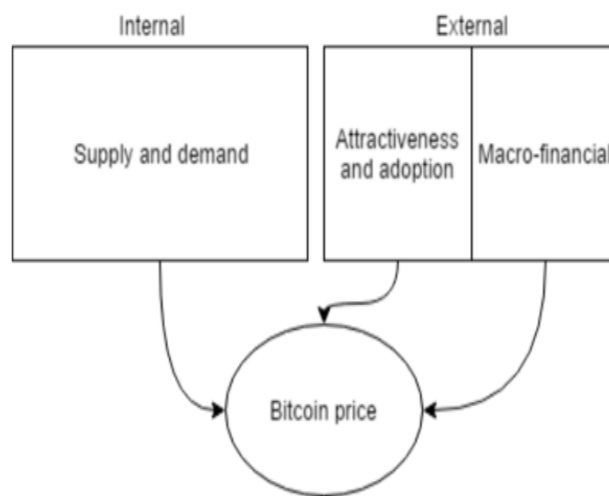
Source: Poyser O. (2017) [31]

1.3- Mining

Bitcoin 'mining' takes its name from real-world mining such as gold or silver mining. Since bitcoin is code, it obviously cannot be mined under any real-world surface so when saying 'mining' what is meant is the process of finding any unfound bitcoins out of the pre-determined 21 million. At its core, bitcoin mining is crucial to avoid double-spending[32] and to create the remaining supply of bitcoins.

---

[31] Poyser, Obryan. (2017). Exploring the determinants of Bitcoin's price: an application of Bayesian Structural Time Series.

Following Kroll J. et al, bitcoin mining is an incentive-based game that requires all players to have consensus.

- Consensus about the rules that determine which transactions are valid
- Consensus about the history of the Bitcoin network, so that the actual owners of the currently existing bitcoins can be determined
- Consensus that bitcoins have value since these miners will receive all their revenue in bitcoin.

A key concept in mining is a 'hash'. As explained by Velde (2013) "a hash function maps text or numbers of arbitrary length into a number of fixed length." The goal for miners is to find a number such that the resulting hash function is less than a set value x. This problem is impossible to solve using the human mind and requires computers with advanced computing power. By trial and error, they try to find the number, making it a game of luck as well. When a miner solves this problem, he is then awarded a block. This system in which miners are rewarded for their work of solving mathematical problems and validating each block is called proof-of-work.

Figure 6: Graphic example of the blockchain
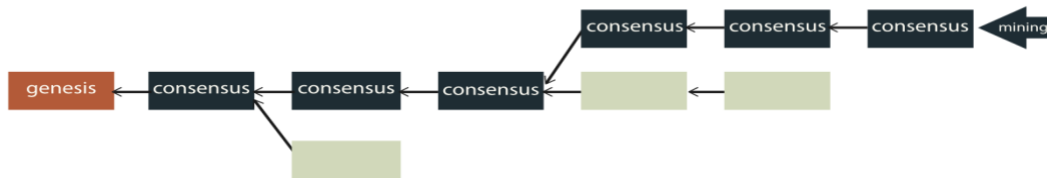
Source: Kroll J. et al (2013)

The blockchain is designed in such a way that any addition of a block to it has a cost attached to it as well. This means that someone who adds a block must also pay a price and this is crucial to avoid falsification of the blockchain, because only those who expect a return would add a block. Miners must solve a complex mathematical problem in order to add a block to the blockchain. Although the cost can vary for anyone, the price of purchasing the hardware, the electricity price and all the time involved in this process is a significant cost. (Velde 2013)

Currently, in 2023 a miner will receive 6.25 bitcoins from 1 block. This number was 50 when Bitcoin first launched. Every 210.000 blocks mined (roughly every 4 years) the award that a block gives is cut in half. Satoshi explained Bitcoin's white paper that when there are no more bitcoins to be mined, miners will receive their revenue from validating transactions and receiving fees based on these.

Figure 7 shows which places are optimal for bitcoin mining in the world, considering electricity costs, outside temperatures and internet connection speed. Bitcoin mining is also done by some natural gas companies that divert lost gases during their extraction to generators which in turn mine Bitcoin. As seen in the figure below, the most ideal places for mining Bitcoin are places where there is a low cost of electricity together and fast internet connections. Venezuela, the United States, Canada, Russia and China are all efficient places to mine Bitcoin. The place of production doesn't necessarily affect the demand for Bitcoin. The supply is assumed fixed, while the demand is not affected by the location of production because Bitcoin has no borders so a potential buyer would be able to buy it from anywhere at any time.

Figure 7: Global Bitcoin mining costs

Source: BitcoinWiki 2020

1.3.1- Mining difficulty adjustment

Assuming mining is extremely profitable for Bitcoin, new miners will want to join in and reap some of those earnings. However, the issuance of new blocks is very stable, 210.000 blocks are mined roughly every four years. Expecting to join in and grab high profits from Bitcoin mining perpetually sounds too good to be true, and it is. The more miners decide to join this sector, the harder it is going to be for one single node to solve the computational problem required to mine the blocks. The difficulty is changed every 2016[33] mined blocks, based on how much it took to discover them. Every 2016 block interval is called an *epoch*. A block is found every 10 minutes, so an *epoch* will last 2 weeks. If it took more than 2 weeks, the difficulty would lower and *vice versa.* However, the bitcoins protocol limits how much this difficulty can increase or decrease in order to avoid instantaneous and big changes. The limits are +300% when increasing and -75% when decreasing per *epoch[34]*.

Bitcoin mining is a game characterized by many incentives; this is how the system kept on going for more than 10 years. Since their wealth is involved, miners will need to do an in-depth analysis of these incentives. A measure used by investors to see whether the Bitcoin network is safe from a 51% attack, this metric was the hash rate. This serves a good purpose for investors to decide on whether to trust Bitcoin or not. Miners are going to need metrics as well, because for them mining is also an investment. One of these metrics is the difficulty rate. This will illustrate how saturated the mining market is and how many computations will be approximately required to solve the mathematical problem. With low barriers to entry and perfect competition assumption, we can imagine that in the long run, the difficulty rate will increase to such a level that miners will receive close to zero profit since as long as miners will be making positive profits there will be new entrants to this sector.[35] As shown in **Figure 8**, the difficulty rate has been increasing year after year. This

---

[33] There is no specific reason for Satoshi to have made the adjustment period 2016 blocks. With the assumption that bitcoin stands against fiat currencies and knowing that Satoshi leaves many small messages in what he does, the reason for this to be 2016 can be the fact that 2016 backwards is 6102. This might refer to Executive Order 6102 in the United States, which had the goal of confiscating gold owned by private citizens

[34] Mineur, A. (2021, December). How Are Bitcoin's Difficulty and Hash Rate Calculated? *Miner Daily*

[35] Kroeger, A. & Fuerst T. *Essays on Bitcoin*

increase is also in a direct relationship with the price increase, just as competition models would argue.

Figure 8: Difficulty Rate and Price
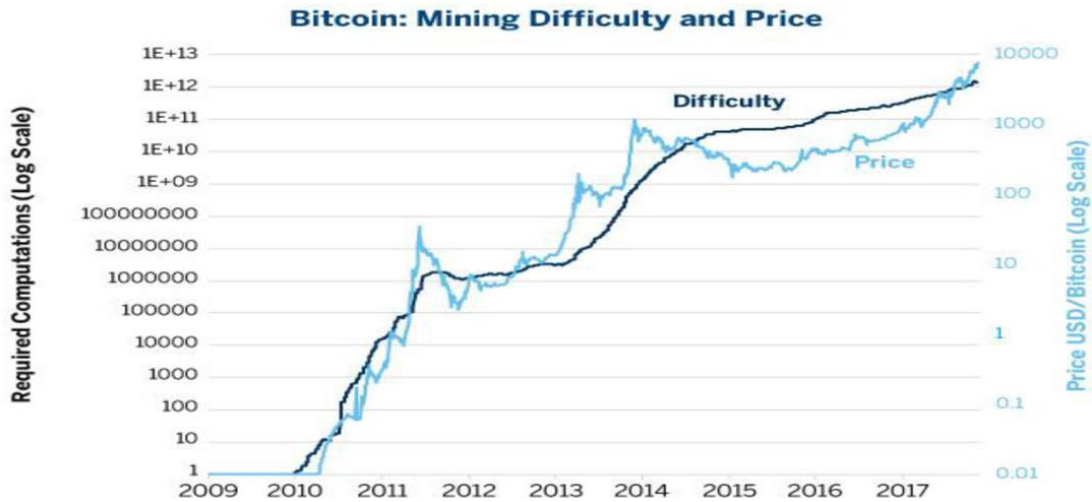
1.4- Austrian school and Bitcoin

The Austrian school of economics is a school of thought which has gone through years of evolution while keeping the same principles. Its founder is considered to be Carl Menger, who wrote *Principles of Economics* in 1871 which became a pillar for the marginalism revolution[36]. Ludwig Von Mises was another major Austrian economist, who wrote the book *Theory of Money and Credit* applying Menger's marginal utility to money theory. The Austrian school also includes Friedrich Hayek, who won a Nobel Prize in Economic Science in 1974. While the heterodox view on money assumes monetary instruments embody an abstract standard of value and money cannot exist without an authority regulating it and enforcing its use, the orthodox view that Austrian economists support says that money develops with time, according to the need of a medium of exchange of the market. Bitcoin is one of the latest developments in money, which emerges with

---

[36] Marginalism theory says that economic decisions and behaviors occur in incremental units and not categorically. This has allowed economists to analyze decisions marginally, introducing terms such as marginal utility, marginal costs, and other core ideas of modern micro and macroeconomics. *Investopedia*

technological evolution and fits the heterodox view of money since there is no enforcer of the currency and only market forces have led to its rise.

Ludwig Von Mises had a basic rule for economists, which was that an economist's first job is to tell governments what they **cannot** do. The Austrian view of economics deeply supported free trade and property rights while strictly opposing taxes, price controls and various regulations that impeded the smooth flow of free trade. Most Austrian economists oppose the government's monopoly on money and high credit expansions, which according to Rothbard, Mises and Hayek amplified business cycles to a point where they were too damaging for the economy.[37]

Many Austrian economists and libertarians have discussed whether Bitcoin fits their narrative. Most agree that bitcoin is a medium of exchange or that it has the potential to be one but to answer whether bitcoin can be fully associated with Austrian economics one must see how bitcoin fits Mises' regression theorem.

The regression theorem was introduced by Ludwig Von Mises in his book *The Theory of Money and Credit* in 1912. In simple words, this theory explains that the value of money can be regressed to its original commodity value. This theory implies that only something which has initial value can be money[38]. For example, gold has a value determined by the market today and it has been used as money for centuries. If we were to trace this back, we would see that gold had value in the sense that it could be used in buildings or for any type of craft. To see if the regression theorem can be applied to Bitcoin, we must trace it back to its origins. What value did Bitcoin have at time zero? According to Graf (2013a, 2013b) bitcoin does not violate the regression theorem because it has an initial use such as the fact that bitcoin has its use within the bitcoin network, or that it was a means for advancing a cause.

Murphy Robert (2013a, 2013b, 2014) also supports the previous claim, by adding that the first buyers of Bitcoin did so for ideological reasons just like giving money to charity. However, the first buyer would be buying Bitcoin only for its potential of being a medium of exchange. This would assume that the initial value given to bitcoin would be that of its potential medium of

---

[37] "What Is Austrian Economics? | Mises Institute." *Mises Institute*, https://mises.org/what-austrian-economics.

[38] Regression theorem, *Wikipedia*

exchange attributes and it would never be valued for anything else other than for this purpose, almost creating a loop in the regression theorem.[39]

One other argument, given by economist Jeffrey Tucker is that the innovation behind Bitcoin is not the coin itself but the payment network behind it. This claim is also supported by Satoshi Nakamoto himself, who emphasized almost entirely on the payment network rather than the coin in his white paper. In other words, the value of Bitcoin does not just represent the value given to one unit of that coin, but to the payment system as a whole and the value of Bitcoin represents this system's value through time.[40]

Discussions on whether the fact that intangible goods such as Bitcoin can ever be considered money according to Mises have also been made. When Mises wrote about the regression theorem the internet, or any type of advanced technology did not exist. The concept of something intangible having value was indeed very hard to grasp. However, to analyze whether a good falls under the regression theorem according to its tangibility is irrelevant. Since a price structure was in existence[41] and value was attributed to it, the regression theorem should not have much to say on this aspect.

The relationship between Bitcoin and the regression theorem is a very complicated one, open to many points of view where many conclusions are exact opposites of each other. What Mises' view of Bitcoin as money would have been is a question that not even the Austrian community can answer without being at odds with one another. There is no specific and definitive reason for Bitcoin not to be money, ever. Thus, arguing about it from a purely philosophical point of view such as the regression theorem has the risk of inserting us in a loop where no conclusions are reached.

---

[39] Davidson L. et al. (2015). Bitcoin, the regression theorem, and the emergence of a new medium of exchange. *The Quarterly Journal of Austrian Economics*

[40] Smith, G. (2019, July). Is Bitcoin Money? Revisiting Mises' Regression Theorem. *Bitcoin News*

[41] A medium of exchange can be a unit of account when this medium of exchange arises from barter or when there is an already existing price structure behind it according to mises.org

1.4.1- Central banks and the inflation tax

Free trade is based on voluntary exchange, where two parties come together and exchange goods only if they require what the other has. Governments don't function this way. Initially, most governments are created for the people with principles of community or liberty. Those that base themselves on free trade usually start with low taxes. This tends to change with time. A silent tax for governments is the inflation tax, which is created by central banks printing unsound money out of thin air. This is not a new phenomenon, it happened thousands of years ago in ancient Rome as well, the emperor would shave off bits of metal from coins. This would allow the emperor to spend more money at the expense of regular citizens who now held inferior coins.[42] The first way this is made today is through central banks as we have seen through the 1914 and 1940s for world war expenses, 70s, and the most recent 2020-22 covid expenses. These are only examples from developed countries. Most developing countries have lived permanently under 2 or even 3-digit inflation, such as Turkey.

According to Hayek changes in relative prices in response to monetary disturbances are not market failures, incomplete information, lags or frictions, but the natural consequence of increasing money supply. The reason is that new money enters the economy through specific channels, where a small number of people receive this money much earlier than others. This is also called the Cantillon effect[43], and it explains why certain sectors are much more affected by inflation than others.[44]

Hayek, in his book '*The Denationalization of Money*' which became a pillar for Austrian economists, said that instead of a government dictating what money is, the private sector should be able to issue their form of money. He then explained that markets would converge on one or a limited number of monetary standards. Bitcoin fits his narrative of private decentralized money; however, bitcoin takes decentralization even further than Hayek would have ever imagined. Hayek

---

[42] What Has Government Done to Our Money? *Mises Institute*

[43] Richard Cantillon analyzed what the effects of an increase in money supply would look like for the economy. He arrived to the conclusion that the effect of the new Money depended on had control of the new Money and where it was injected, thus having a disruptive effect on the economy and causing business cycles. For example, if new Money comes in the hands of entrepreneurs the interest rate would fall but if it came in the hands of consumers the interest rate would rise. The theory suggests that first recipients benefit while the others do not.
Thorton M. (2022). *Cantillon effects: why inflation helps some and hurt others" Mises Institute*

[44] Salerno, J. (2020). Book review: Banking and Monetary Policy from the Perspective of Austrian Economics. *Mises Institute*

also explained that central banks create artificially low-interest rates, making investors too optimistic and thus making them take more risks. This in turn causes malinvestment. Too much inefficiency in investments creates significant bust periods in the economy. While many see these bust periods as a consequence of the free market and call for more government intervention, on the contrary, these bust periods are a cause of central planning and the manipulation of interest rates creating an inefficient

allocation of resources. The resulting bust period is a necessary adjustment of the market, where most inefficiencies are wiped out. [45]

1.4.2- Fractional reserve banking and wallets

Fractional reserve banking is a system where banks only must keep a portion of their deposits ready for withdrawal. The other portion is usually lent to others, for an interest rate. It is the central bank that decides what portion of a bank's deposits must remain as reserves. On the other hand, crypto exchanges that offer wallet services[46] provide a similar service. Crypto exchanges keep the funds of the customers, and just like fractional reserve banks they lend these funds for higher returns, artificially increasing the cryptocurrency supply and posing a risk for customers who might lose their money if the exchange defaults.

This system carries many risks, one of the first examples of this is during the great depression when bank runs caused many banks to fail. Since banks don't hold most of their reserves, when there is a bank run and people demand their money all at once, the bank is unable to pay. Thus, we have the central bank as the lender of last resort, to alleviate liquidity issues. Having a central authority acting as a lender of last resort creates moral hazard problems. Depositors know that the central bank is there to help, so they deposit to less trustworthy banks in return for a higher interest rate on their deposits, or banks lend money to unreliable people. When this is done on a large scale, business cycles and credit expansions will be amplified creating bigger recessions and higher

---

[45]Friedrich August Hayek. *Econlib*

[46] Holding the customers deposits for them

inflationary pressure during the expansion period. Economists know this, and therefore during recession periods the reserve requirement is usually increased by the central bank.[47]

When someone deposits their own money in a bank, they don't have a say on whether that bank will lend out their money or not. Bitcoin enters the discussion of fractional reserve banking when the topic is *choice.* Bitcoin owners can choose to keep their bitcoins on *cold wallets[48]*, while others can choose to keep theirs on exchanges. Cold wallets give the owner the freedom of managing their own money. With gold and fiat, self-custody carries risks such as theft, therefore most people deposit their money in a bank, and no one would prefer to have piles of gold or cash sitting in their home. Self-custody also aligns with the Austrian view, since those coins aren't lent to others using third parties and increasing its supply.

Exchanges usually don't purchase Bitcoin on someone's behalf when that person buys Bitcoin through their platform. That person has a claim on the exchange, but the exchange only has to give it when the owner wants to redeem it. So, when an order for 1 bitcoin is made, the exchange doesn't purchase 1 bitcoin, they only owe the customer 1 bitcoin.[49] Just like fractional reserve banking, these crypto exchanges try to have enough capital to resolve day-to-day liquidity demand however, they either lend money or make their investments. Therefore, crypto exchanges tend to fail. They don't have a lender of last resort and when there isn't a monopoly to protect their operations the fractional reserve system becomes very risky.[50]

---

[47] Alifanov, S. On the Dangers Inherent in a Fractional Reserve Banking System.

[48] This is a cryptocurrency 'wallet' that is not connected to the internet and is not vulnerable to any kind of online attacks. The owner of this wallet is the only person that can manage the currency inside of it.

[49] This artificially lowers bitcoins price, since someone that wants to purchase the coin gives money to an exchange that doesn't really purchase it. Having a limited supply, this system is not sustainable in the long run since there can only ever be 21 million coins.

[50] Kamau, R. (2022). Why Keeping Bitcoin on An Exchange Is Driving the Price Down. *Forbes*

Chapter 2

Bitcoin's competition

In the first chapter, Bitcoin was introduced by giving details about the characteristics it possesses and the economic school of thought behind it. Bitcoin is not the only cryptocurrency. There are thousands of different coins that try to compete and try to create their eco-system. Bitcoin's characteristics are not unique to Bitcoin, but other coins can also try to replicate them to some degree, or even improve in some respects. However, there are limits to how much a coin can be developed and how much they can differ from one another. The concept in this chapter will be about what these limitations are, and how the various crypto developers chose to do their trade offers in creating their coins. Before talking about the challenge of trying to design the "perfect" coin, it is important to keep in mind that Bitcoin is not the first cryptocurrency ever. Bitcoin is just the product of many prior attempts and trial-and-error processes.

2.1- Trial an error process to create bitcoin

We can trace back the inspiration Nakamoto received to create bitcoin to 1989. In that year the first ever crypto coin was introduced to the world.

Digicash: Digicash was created by David Chaum in 1989. Chaum was concerned with the public nature and open access to online payments and personal information so he proposed a system with cryptographic protocols where a bank or a government couldn't trace any sensitive information. The aim of getting rid of intermediaries and third parties is an idea that has accompanied the cryptocurrency space from its first days and is not unique to Bitcoin. Later, he created this coin to try and earn money on his digital currency knowledge and the coin didn't have much success since it is as centralized as it could be, and the coin wasn't very practical to use as well since the internet was not mainstream when digicash was created. Still, the invention of such a coin was a great development for the future of crypto. [51]

Hashcash: Adam Back proposed this proof-of-work system to limit e-mail spamming. This has been very influential on the creation of Bitcoin because the proof-of-work system that Back

---

[51] Frankenfield J. (2018, June). DigiCash Definition. *Investopedia*

proposed in 1997 went on to become the pillar on which Bitcoin mining was built on. Although it is not a coin, this algorithm deserves recognition since the decentralization characteristic of Bitcoin was developed with hashcash's internal algorithm. [52]

B-Money: B-Money was proposed by computer scientist Wei Dai in 1998. Wei Dai was a major advocate for privacy and as an anarchist he disliked government interference. He criticized payment systems such as Visa because the owner of the funds could be tracked and regulated accordingly, and so he wanted a decentralized coin where its participants couldn't be traced, and a central authority can't regulate the coin's use. These fundamentals are similar, if not the same, with bitcoins.

Wei Dai proposed two protocols for b-money. The first protocol was very impractical since it didn't solve the double spending problem. In the second proposal, he proposed a coin with two participants: users and servers. Users are the normal users we know about. Servers are the ones that keep the ledgers and verify transactions. He added that servers will have to deposit a certain amount of money to pay for fines or rewards. Although Wei Dai proposed this coin, he never actually released it. His efforts were not in vain since Nakamoto would go on and create Bitcoin using some of the same protocols. [53]

Bit Gold: Nick Szabo invented BitGold in 1998. Szabo's coin used a proof-of-work mechanism inspired by hashcash. The main differences from Bitcoin were the scarcity and mining aspect and therefore the decentralization aspect. Bit Gold required more centralization than bitcoin because as per the protocol, a coin stamped in year x would be more valuable than a coin stamped in x+1. This creates fungibility challenges and would require a bank with the purpose of bundling the coins to create a standard value pack. Bit Gold didn't have a pre-scheduled inflation rate and its supply could increase drastically when computing power increased, while the difficulty adjustment in bitcoin prevents this.[54]

---

[52] What Is Hashcash and How Is It Connected to Bitcoin? *Paybis Blog*

[53] Van Wirdum A. (2018). THE GENESIS FILES: IF BITCOIN HAD A FIRST DRAFT, WEI DAI'S B-MONEY WAS IT. *Bitcoin Magazine*

[54] Bitcoin Magazine (2018, July). The Genesis Files: With Bit Gold, Szabo Was Inches Away From Inventing Bitcoin. *Bitcoin Magazine*

All these coins had flaws that Nakamoto learned from and improved on. The characteristic of being completely decentralized not only from governments but from any kind of individual, or the characteristic of being scarce were not inventions by themselves, but the merge of all these characteristics in one single coin was the technological improvement that Nakamoto released. As mentioned before, it's been a trial-and-error process that to this day continues to evolve. However, this process can't go too far in crypto because when trying to improve something in a coin some other things might have to be sacrificed. This is what is called the blockchain trilemma.

2.2- How does bitcoin perform as money?

2.2.1- Store of value

Money is a store of value when it facilitates saving and capital allocation, transferring purchasing power from the present to the future. The function of store of value is critical to a currency. Money should preserve purchasing power from today to the future. This allows for economic long-term decision-making and stabilizes people's time preferences. Theoretically, since bitcoin possesses most of gold's characteristics it could potentially serve as a store of value. With its supply being fixed, ungovernable and decentralized the store of value function could be achieved.

In real life we see a different scenario. Although Bitcoin surpassed most assets as stores of value in the last 10 years, it has extreme volatility attached to it. Something cannot be a store of value and extremely volatile at the same time. However, the overall trend is upward, and if the number of people who think that a bitcoin has value appreciates its value will continue to rise. As demand increases, because of bitcoins protocol its supply cannot adapt to the demand and the result is a steep appreciation in price. When demand reaches a significant portion of the world population its value starts to stabilize. Only at this point can it be considered a proper store of value. However, volatility can never be completely removed as it is a property that comes with demand. If bitcoin adoption doesn't happen at a steady rate volatility will always be a part of the price dynamics[55].

---

[55] Ametrano F. (2016). Hayek Money: The cryptocurrency price stability solution, 18-21

2.2.2- Medium of exchange

Money is considered a worthy medium of exchange when it is accepted as payment from other agents. Someone will accept a form of payment from somebody if they believe that someone else will also accept it from them. Since fiat money is legal tender, and all businesses in each country are required to accept by law that fiat currency because government regulations enforce it. This allows fiat money to be a good medium of exchange. However, Bitcoin isn't backed by any government and unless it becomes legal tender (like El Salvador), it requires most private citizens to accept it for it to become a proper medium of exchange. There have been some examples of Bitcoin being accepted by businesses as payment. Elon Musk's Tesla used to accept Bitcoin as payment up until it announced that it wouldn't until Bitcoin mining became more sustainable. Small businesses in Lugano accept Bitcoin, as it is one of the most Bitcoin-friendly cities in Europe[56].

Bitcoin poses significant incentives as a medium of exchange rather than the traditional banking system when considering large sums of payment, especially international ones. The Bitcoin network doesn't have borders, so transferring Bitcoin from Sevilla to Madrid is the same as transferring it from Tokyo to Moscow. On the other hand, currently, there are significant time delays and banking fees when transferring large sums of money through banks, however bitcoin offers lower fees and faster transactions when dealing with such sums. The same cannot be said for small transactions, which are much faster and cheaper with credit or debit cards, but therefore this chapter focuses on Bitcoin as a reserve currency and not as a daily used one.

A drawback for some micro users would be that the time it takes for a transaction to occur is longer than that of credit cards or national bank transfers. If someone were to buy coffee with Bitcoin, it would probably take more than 10 minutes for the coffee seller to receive the payment. However, this doesn't mean that the customer must wait until the payment arrives. Once the customer makes the payment, the customer can no longer have any claim on those bitcoins and the seller will only have to wait for a miner to verify the transaction.

---

[56]Lo, S. & Wang J. C. (2014). Bitcoin as Money*? Federal Reserve Bank of Boston*

Bearing in mind that bitcoin is completely peer-to-peer and that a transfer of bitcoin requires relatively no effort, it can be considered a relatively good medium of exchange. Better than gold, but not better than fiat currencies. For Bitcoin to be a better medium of exchange than fiat currencies, advancements in intermediaries such as the lightning network must occur.

2.2.3- Unit of account

A unit of account is a standard unit of measurement of the value of goods, services and any transaction. This function of many is fundamental to attach a value to something, to make economic calculations possible. Since Bitcoin is currently very volatile, it doesn't serve as a good unit of account. Even businesses that accept Bitcoin as payment must list prices in their country's respective fiat currencies for customers to understand how much they are spending. Generally, customers learn how much Bitcoin they have spent only when checking out of the store. These real-life examples demonstrate that currently bitcoin lacks this aspect of money. Nonetheless, this doesn't mean that it cannot be a good unit of account. If bitcoins price were to remain stable, since it's perfectly divisible and countable it has the potential to be a very efficient unit of account. Bitcoin is infinitely divisible, since its protocol allows for changes in divisibility. Currently, the smallest unit of bitcoin is 0.00000001, called a satoshi. Since 1 unit of bitcoins price is very high when compared to goods and services, some problems may arise[57]. If someone wanted to buy a 5-dollar coffee, they would have to spend approximately 0,0001781 satoshis. This is clearly not a good way to price goods because it has a lot of decimal numbers. This would be solved if Bitcoin users collectively decided to switch denomination to either bit (0.000001 btc) or millibit (0.001 btc) where prices would look better to the eye and ear. Using a smaller unit to measure value would also allow its acceptance to rise since consumers and producers would have a better idea of how much they are spending. Also, if bitcoin has a stable price, pricing goods and services in smaller units of bitcoin would show those goods and services real value while fiat currencies would only be showing their nominal value. This can occur when citizens start to calculate their worth based

---

[57] Cermak V. (2017) Can Bitcoin Become a Viable Alternative to Fiat Currencies? An Empirical Analysis of Bitcoin's Volatility Based on a GARCH Model. Skimore College

on how much Bitcoin they have and not based on how much fiat they possess. Since no governance structure controls Bitcoin, the users will have to decide on this unit of measurement change for themselves[58].

Surveys and statistical analyses conducted by Andreianova M., with the results shown in **Figure 13**, which consider a pool of almost 70.000 Bitcoin users show that approximately 10.4% of Bitcoin users use it to store the value of their wealth while 9.7% use it for cross border transactions and 13.9% use it as a local payment method as well. Thus, a little more than 20% of users consider Bitcoin to be a medium of exchange. On the other hand, features such as trading and investing capture half of Bitcoin's entire demand. This shows that the use of Bitcoin is noticeably diverse and not constrained to a specific function.[59]

Figure 13: Bitcoin usage categories
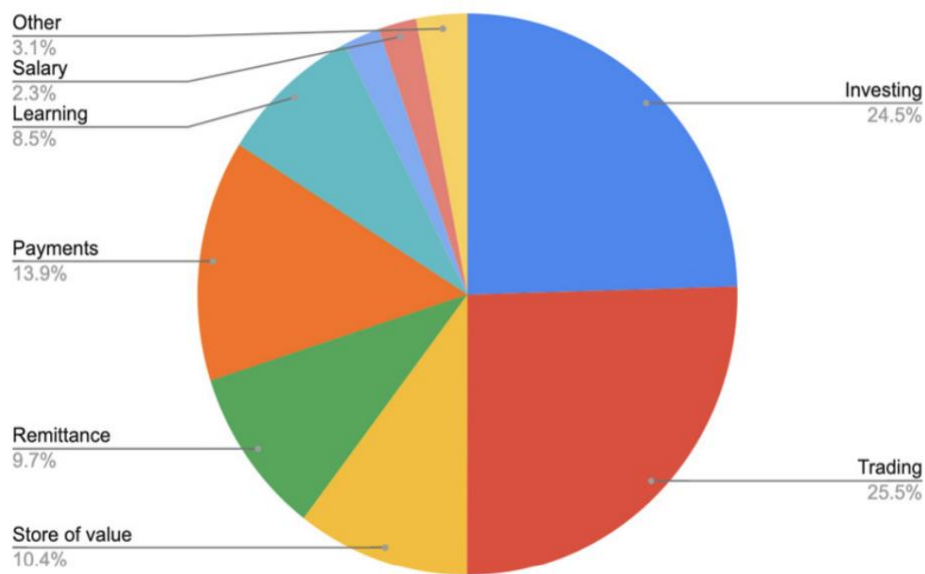
Source: Andreianova M. et al. (2021)

---

[58] Albrecht C. et al. (2020). Legitimizing Bitcoin as a Currency and Store of Value: Using Discrete Monetary Units to Consolidate Value and Drive Market Growth. *Ledger Journal*

[59] Andreianova M. et al. (2021). Bitcoin usage: Study on Bitcoin usage around the World, *The Journal of Fintech*

Bitcoin has the potential to become a store of value. It possesses many of the characteristics necessary for a store of value. The challenge towards this is the volatility aspect, which could decrease as more and more people start using Bitcoin. To become a good medium of exchange for small transactions scalability must be improved, and with projects such as the lightning network, this could occur soon. For large transactions and international transactions Bitcoin is already a reliable payment system. It has very low transaction speeds and feed compared to normal banks. Since Bitcoin is available 24/7 it also allows nightly payments across borders. Bitcoin also possesses the characteristics of becoming a unit of account since it's divisible. The challenge to face is to decide which decimal number to start with, otherwise it becomes too complicated to understand the price since 1 bitcoin is worth almost 30.000 dollars.

2.3- Blockchain trilemma

When discussing cryptocurrencies, it is rare, if not impossible, to describe a coin as the perfect currency. By perfect currency, what is meant is a currency that is entirely decentralized, entirely secure and with a very high level of scalability. There is always a tradeoff that must be made. If one were to increase one of the three factors, they would have to sacrifice, to some degree, one of the other three. This phenomenon was called the *"blockchain trilemma"* by Vitalik Buterin, the co-founder of Ethereum. [60]

---

[60] Binance Academy (2022) "What Is the Blockchain Trilemma?" *Binance*

Figure 9: Blockchain trilemma
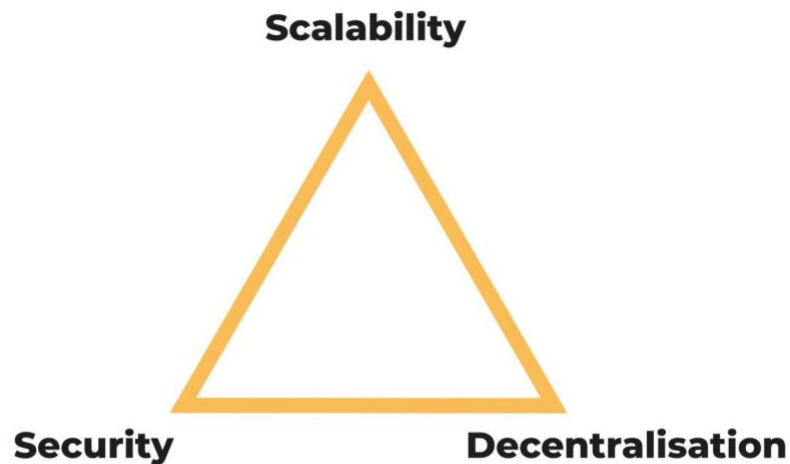
In **Figure 9**, decentralization refers to the trait of not being controlled by any central authority, where the network relies on its stakeholders. Decentralization is characterized by the number of active miners, the geographical distribution of the miners, etc.

Scalability in blockchain technology refers to the capability of the network to handle a larger number of transactions efficiently and without any negative impact on its performance or security. The third factor, security, is the ability of the network to safeguard the integrity and confidentiality of the data stored on the blockchain. This includes protection against various attacks, such as double spending, data alteration and malicious network disruption.

For example, increasing the level of decentralization in a blockchain network can increase security by reducing the risk of a single point of failure or attack. However, this also decreases scalability, as more nodes may be required to validate transactions. Similarly, increasing scalability by using a more efficient consensus mechanism may come at the expense of security.

When designing Bitcoin, Nakamoto prioritized decentralization and security by sacrificing scalability. This is why the Bitcoin network can handle roughly five transactions per second, which is extremely low considering that Visa and Mastercard can both process thousands of transactions per second. Similarly, Ethereum also prioritizes mostly decentralization and security by having a network that can process roughly double the transactions per second that Bitcoin can. On the other

---

[61] Guazzo, G. (2020, November). Bitcoin e Trilemma Della Blockchain: Cosa è e Possibile Soluzione. *Investire.Biz*

hand, other cryptocurrencies such as Ripple prioritize scalability and security over decentralization.[62]

Bitcoin is meant to be used as a decentralized and secure cryptocurrency, independent from any institution or person, where participants can be a part of the transaction validation. Together with its scarcity feature, this is also why it has appreciated significantly in price over the years. Sacrificing decentralization to increase the scalability of Bitcoin is a solution that would mostly bring damage to the cryptocurrency, as its purpose would be altered, and therefore other cryptocurrencies are developed. Each cryptocurrency is developed with its own tradeoff in the blockchain trilemma to develop a relatively good balance.

While Bitcoin disappoints from the scalability perspective, previous attempts to change this feature have proven that the market overall prefers Bitcoin as it is[63].

We can arrive at this conclusion because there have been past attempts to change Bitcoin, but the original coin has always been preferred over the others, as seen by the appreciation in price[64]. Currently, technological advancements are not enough to solve the trilemma so improvements can be made only through forks and second-layer solutions like the lightning network.

---

[62] Longchamp, Y. et al. (2020). The Blockchain Trilemma. *SEBA Swiss*

[63] Bitcoin as a decentralized and secure cryptocurrency, and not a highly scalable one where more transactions can be made.

[64] By original what is meant is the first and non altered coin developed by Nakamoto.

2.4- Attempts to improve bitcoin

2.4.1- Forks

There have been some attempts to achieve a different tradeoff in bitcoins blockchain trilemma position ever since Bitcoin started. By attempting to change Bitcoin and not creating another cryptocurrency from scratch, developers used a method in blockchain technology called a fork, which could be used to increase scalability, decentralization or security.[65]

In the context of blockchain, fork means a deviation from the original technology where miners validate a new block by adding to it an updated set of predetermined rules, instead of validating the block that is supposed to be continued. Forks can be either "hard fork" or "soft fork". A hard fork is made when the upgrade is incompatible with the existing blockchain implementation. This type of fork is not backward compatible and any miner that validates the old network will consider the new one invalid. In other words, a semi-separate cryptocurrency is created. Semi-separate because the original coin and the new one will have a common ancestor, which is the genesis block, however they are different coins with different implementations in the present. On the other hand, a soft fork is a backward-compatible upgrade where the upgraded nodes can communicate with the old ones. **Figure 10** gives us a more visual explanation of what a fork is in blockchain technology

Figure 10: Forks
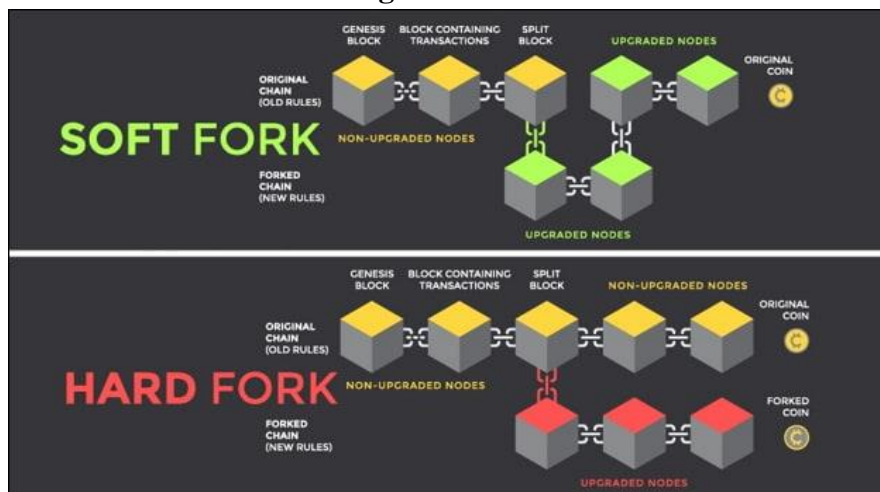
Source: Finance Magnates/ Types of blockchain forks[66]

---

[65] Whatever upgrade is made, it is always done at the expense of one of these three traits.

[66] What Is a Blockchain Fork & How Do They Work? (2022, September). *Shardeum*

Hard forks have been used frequently on Bitcoin's blockchain however, their names are mostly unknown since they haven't been influential. The first major fork came in 2014. This fork was a soft fork that aimed at adding a new protocol to the network. This soft fork attracted notable attention within the community at the time. Another significant soft fork was the SegWit fork where developers aimed at improving scalability and managed to do this successfully.

Those that found the limits of soft forks within the Bitcoin protocol not enough, applied hard forks to the network. The most significant hard fork is Bitcoin Cash. [67] These forks are made by developers, who are usually miners, and are hard to implement with Bitcoin because these miners would need a 51% approval rate from all the computational power devoted to the blockchain. Without a governance mechanism, which Bitcoin does not have, it is a struggle to do any kind of forks.

Bitcoin Cash is one of Bitcoin's hard forks, which was proposed and implemented by developers to solve the scalability problem. They did this by raising the sizes of the blocks within the blockchain. Block size went up from 8Mb to 32Mb, allowing a single block to have supplemental transactions and thus allowing to make transactions in a matter of seconds and reducing transaction fees to pennies. Other than the block size and difficulty adjustment protocol, Bitcoin Cash shares almost an identical protocol to the Bitcoin generally known.[68]

Although higher scalability gives Bitcoin Cash a higher utility for day-to-day and small transactions, this improvement was made at the sacrifice of security. The side effect of a higher block size is that because of the increase in size, transactions can be validated very quickly and with less computational power, making a 51% attack more likely than Bitcoin. A bigger block also incentivizes more miners to come together and operate a common mining "*pool*", instead of mining individually and in a decentralized way. Bitcoin developers aim at having a decentralized and secure payment system, and any sacrifice to those two aspects has the potential of destroying the

---

[67] Neo C.K. Yiu. (2021). An Overview of Forks and Coordination in Blockchain Development. *University of Oxford*

[68] Shaw, B. (2022). Bitcoin vs. Bitcoin Cash: What's the Difference and Which Is Better? *Nasdaq*

coins' purpose. Bitcoin Cash developers prefer faster transactions and lower fees since their vision for Bitcoin was for it to become an efficient medium of exchange. This consequence of an increase in block size can be considered a reason for why Bitcoin Cash didn't reach the heights it was envisioned to.[69] **Figure 11** shows the history of Bitcoin Cash's exchange rate in terms of Bitcoins. When it was first forked, one Bitcoin Cash could purchase almost 0.2 Bitcoins, as of 28/03/2023, this number is around 0.0044.

Figure 11: Bitcoin Cash to Bitcoin price

Source: Yahoo Finance

Other than Bitcoin Cash, another discussed hard fork was the Bitcoin Gold fork. This fork was made to improve decentralization in Bitcoin but was widely criticized and isolated by investors because its developers pre-mined 100.000 units of it before opening to the public.[70] In addition, the Bitcoin Gold network has received many 51% attacks where malicious miners successfully stole some coins from investors, increasing doubt around the coin. On the other hand, no one has ever successfully attacked Bitcoin in its history[71]. **Figure 12** illustrates all major forks that occurred in

---

[69] Lucena, J. Advantages And Disadvantages Of Bitcoin Cash. *FLAUNT*

[70] Neo C.K. Yiu. (2021). An Overview of Forks and Coordination in Blockchain Development. *University of Oxford*

[71] Reiff N. (2018, March). Bitcoin Gold: Distribution, Protection, and Transparency. *Investopedia*

Bitcoin. The Bitcoin Cash and Gold forks were the first two major ones and many other forks occurred after those, however none of them were able to receive wide acceptance.

Figure 12: Bitcoin forks since 2017
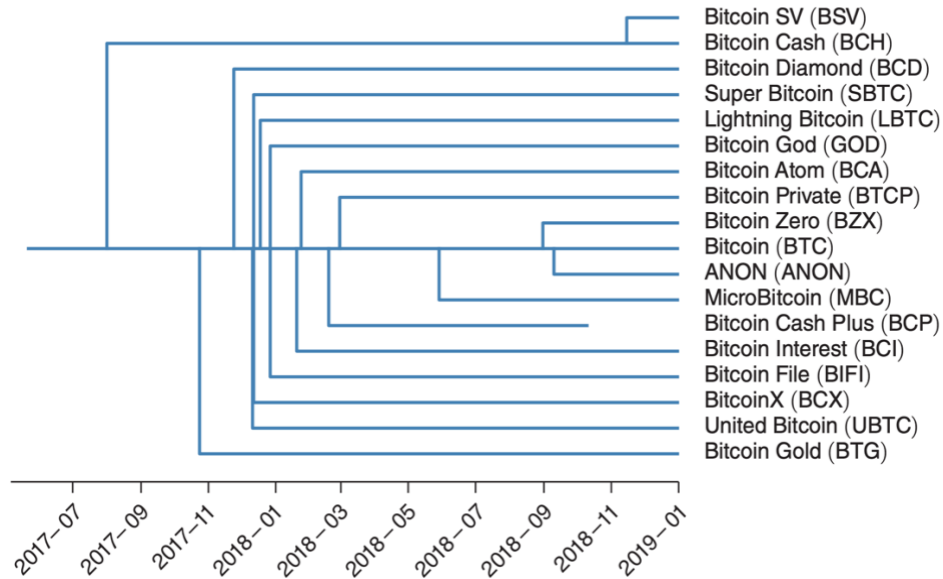
Bitcoin sits in a very balanced position within the triangle for its purpose. Those purposes are being independent and secure from any central authority. Market participants, developers and miners who acknowledge this aspect are likely to reject any new fork or alternative if the core concepts of Bitcoin's creation must be altered. Bitcoin Cash developers wanted Bitcoin to be highly scalable to be able to purchase even goods that are worth pennies, however Bitcoin as a day-to-day medium of exchange idea has not received the acceptance as the Bitcoin as a digital gold idea has.

---

[72] Biais B. et al. (2019) Blockchains, Coordination, and Forks. *AEA Papers and Proceedings*, *American Economic Association*, 88–92.

2.4.2- A solution to scalability: Lightning Network

The lightning network is an overlay of the Bitcoin network powered by smart contracts and it's not a blockchain of itself. This is also called a layer 2 solution to scalability. This was introduced by Thaddeus Dryja and Joseph Poon in 2016 to overcome Bitcoin's limits.

The lightning network is not a fork to the blockchain, but it's a second layer that is added to the Bitcoin blockchain so the Bitcoin blockchain remains untouched. The lightning network allows instantaneous Bitcoin transactions, but it doesn't solve the blockchain trilemma because it still loses in decentralization while increasing scalability. However, it is deemed to be beneficial for Bitcoin transactions because the Bitcoin blockchain can remain secure and decentralized, while allowing faster payments to be made by this second more centralized layer that doesn't affect the original layer 1 Bitcoin blockchain. Summarized, the lightning network allows instantaneous transactions by allowing transactions to occur outside of the blockchain and keeping a record of all these off-chain transactions. These transactions are then pooled together to be confirmed on the Bitcoin blockchain as a single transaction. The lightning network also allows exponentially cheaper transaction fees, down to 1 satoshi (1/100.000.000th of a bitcoin). Without this solution a person would have to wait for months or even years in order to get their transaction approved if everybody used bitcoin.[73]

The lightning network has drawbacks as well. There are various participants in various channels in the lightning network. If a participant in a payment channel within the network decides to close that channel while the other participant is offline, the one that closes the channel can also withdraw all the money from the channel as well. These scams might occur with the lightning network. Some transactions sometimes do not occur because of errors within the payment channel and subsequently the person who sent the money will have to wait until that lost transaction is found and refunded. All these drawbacks, combined with a high level of anonymity in the lightning network[74] create an environment that will require and will be affected from regulation[75]. Although

---

[73] Kaloudis, G. (2021). A Deep Dive into Lightning as a Bitcoin Scaling Solution. *Coin Desk Research*

[74] All transactions in one payment channel are recorded as one big transaction in the bitcoin network, not allowing anyone to see the various senders of those multiple transactions

[75] Rowden S. (2022, November). What is Lightning Network? What are pros and cons of Lightning Network. *BITKAN*

this solution is very new, it might have a lot of potential in terms of solutions to scalability without the need of doing a fork by changing the original blockchain of Bitcoin but only by adding a second layer to the blockchain. There have been cases in which some have lost their money in the lightning network because the channel was closed and all the funds were withdrawn, so in terms of security this project still has a long way to go before being considered for worldwide use.

2.5- Other major cryptocurrencies

There are thousands of cryptocurrencies other than Bitcoin why try to compensate for some of its drawbacks or exist to be used as a token inside a blockchain system where the main goal is to design decentralized applications. In this section I will try to explain the differences of other major cryptocurrencies such as Ethereum, BNB and XRP from Bitcoin. These three cryptocurrencies are one of the biggest *altcoins*[76] and they are among the five biggest cryptocurrencies by market capitalization. They summarize quite well the distinction between Bitcoin and most altcoins, since they share the same use and purposes as most cryptocurrencies. I chose these three cryptocurrencies to compare with Bitcoin among the thousands of cryptocurrencies that exist because each one of these three represent the best cryptocurrency among the group they belong. Ethereum is a token for the Ethereum blockchain used to create decentralized applications, Ripple is a centralized token designed to ease bank settlements while Binance coin was designed to be the token of the centralized exchange Binance for transaction fees and other exchange related purposes. On the other hand, Bitcoin was designed for none of these reasons but only to become a form of money to be used by anyone for anything.

• The Ethereum blockchain was released on the 30th of July 2015. While Bitcoin aimed at becoming a decentralized peer-to-peer currency, Ethereum had a much broader aim. Ethereum was created to be a platform that facilitates smart contracts and the creation of decentralized applications, where data is not stored in a centralized server but in a decentralized manner within blockchain technology. Ethereum is the name of the platform and at the same time the name of the token that

---

[76] A cryptocurrency other than Bitcoin

platform uses to exchange value in those smart contracts or applications. While Bitcoin uses the proof-of-work consensus mechanism to secure the network, Ethereum uses proof-of-stake. This consensus mechanism removes the need for miners and solving complex mathematical problems in order to validate blocks. POS validators are required to stake their own Ethereum to certify that transactions are genuine. If a malicious validator tried to disrupt the network, because the majority of validators are genuine they will most likely lose all their tokens, and this is how POS guarantees security. While POW rewards miners when they find a block in the blockchain, POS rewards validators only when they approve transactions and smart contracts. A major difference between POS and POW is the amount of energy they use. POW uses significant energy to validate blocks while POS uses only a fraction of what the latter uses. Although Ethereum uses less energy to validate transactions, the trade-off is between that of less energy and security. Since in POS users earn in proportion to what they staked, if there were an owner or a pool of owners of Ethereum that surpass 50% they could easily take control of the network. With POW miners would need to obtain more than 50% of the computing power, which is much more difficult to obtain. To disrupt Bitcoin, there would have to be a cross-country wide effort in order to obtain the energy, but with Ethereum's current market cap[77] the union of a handful of billionaires could gain control over the network.[78] Tokens such as Ethereum obtain their value from supply and demand like Bitcoin, but they also obtain value from the growth of the platform and applications that are within that eco-system, which makes the token susceptible to developments within its network.

• Binance coin, also known as BNB, is a cryptocurrency issued by the biggest crypto exchange in the world, Binance. BNB used to be part of the Ethereum blockchain until it became the coin used in the Binance blockchain. The purpose of this coin was initially to sell it to investors to be able to afford larger marketing operations in order to grow their company and as a utility token to use in transactions as transaction fees for Binance. Today it is also used as a token for decentralized applications just like Ethereum. Its use and purposes are similar to Ethereum, and it receives its

---

[77] 217 billion

[78] Harm, Julianne, et al. Ethereum vs. Bitcoin. *Creighton University*

value from its use in decentralized applications and from the Binance exchange itself. This coin can't be considered decentralized, as most of its use comes from the issuer itself as well. [79]

• The cryptocurrency XRP was created by Ripple to have a currency that would allow payments to be made in real time. Ripple, like Ethereum, uses proof-of-stake. Thus, with a very low power consumption compared to Bitcoin, it can verify transactions in a matter of seconds. XRP is well designed for the needs of financial intermediaries. The Ripple company built a blockchain network for banks together with its rules and frameworks. Banks that use the Ripple blockchain can finalize transactions faster and with a very low security risk. Prestigious banks like Bank of America and HSBC also support this cryptocurrency.

While Bitcoin and Ethereum are constantly mined, all Ripple coins were pre-mined. A portion of these coins were sold to the market, while the majority remains with the creator company. So just like in many other cryptocurrencies, the extremely high scalability came at the cost of decentralization.[80]

Ethereum, BNB and XRP have many differences among them such as Ethereum being created to facilitate decentralized applications and smart contracts, BNB has also this use, while also being the official Binance cryptocurrency for transaction fees. XRP was created to facilitate international and national transactions with high speed and has a different consensus algorithm called RTP. What they all have in common is that they are different from Bitcoin. All of these cryptocurrencies are deemed decentralized from any public authority, and while this holds true, they are not decentralized from individuals or corporations. Ethereum has Vitalik Buterin, BNB has Binance and XRP has Ripple. Most cryptocurrencies have these same goals and purposes. Bitcoin doesn't have a flexible platform for smart contracts or decentralized applications, making Bitcoin relevant only for the digital currency argument. Most other cryptocurrencies are irrelevant when discussing a widely recognizable, secure and decentralized digital currency. These characteristics are why the

---

[79] Frankenfield J. (2018, April). Binance Coin (BNB) Uses, Support, and Market Cap. *Investopedia*

[80] Ahmadova S. & Erek S. M. (2022). Finansal Aracılık Koini Olan Ripple Üzerine Bir Değerlendirme (A Review on Ripple, a Financial Intermediary Coin). *Journal of Academic Projection (Akademik İzdüşüm Dergisi)*

only cryptocurrency comparable to gold has been Bitcoin until now. Ethereum, BNB and XRP are blockchain technology innovations and developments that aim at improving blockchain technology to also broaden its use, while Bitcoin is a monetary innovation with the main scope of being a potential store of value.

Nicholas Weaver (2022) argues that most cryptocurrencies are disguised as securities. Currently, the SEC doesn't have regulations in place for these cryptocurrencies but it's important to note that most of them pass the Howey Test[81]. What makes them a security is that tokens such as Ethereum are not simply cryptocurrencies that have no other use than behaving as a medium of exchange, they also give the holders governance rights in that cryptocurrency's platform. Additionally, many cryptocurrencies are issued through ICO's[82] which is how blockchain projects raise funds. Those who purchase these tokens expect a return for their initial investment, which makes the tokens disguised securities. Bitcoin doesn't fit the description of a security since there is no implicit or explicit investment contract and no one to expect a return from. Weaver (2022) then suggests that cryptocurrencies who aren't currently regulated as securities might be committing security fraud. Once the realization of this occurs these cryptocurrencies will be much more regulated, and this is expected to happen soon. This is also why they cannot compete with Bitcoin in the context of money. It's only a matter of time before regulations start taking place and the difference between Bitcoin and

tokens will become greater since tokens will have to adhere to much more regulations than Bitcoin.[83]

---

[81] The Howey test is a legal test used in the United States to determine whether a transaction qualifies as an investment contract and thus is considered a security under federal law. (Kaur G. *Cointelegrpah*)

[82] Initial Coin Offering, where new blockchain developers give their token in exchange for fiat currencies to develop their project.

[83] Weaver N. (2022) The death of Cryptocurrency: The case for regulation. *Yale Law school Information Society Project*

Chapter 3

Hypothetical Bitcoin Standard: An Austrian perspective

This chapter introduces the idea of a hypothetical bitcoin standard. A world where governments and central banks approve of Bitcoin and where people use it as a medium to measure value. After all the contexts given in the previous chapters, this chapter will focus on trying to imagine bitcoin as everyone's daily currency. From its properties as a store of value, medium of exchange and unit of account to an analysis of how a decentralized and void of inflation economy would look like to political and libertarian implications of a bitcoin standard will be the main arguments discussed.

In the book "*The Bitcoin Standard*" Saifedean Ammous talks about the importance of sound money[84]. Ammous (2018) tells us that the best measure of hardness in money is the stock-to-flow ratio[85]. Historically, money has taken many forms such as seashells or crafted rocks however with advancing technology it becomes easier to produce those currencies, significantly lowering their stock-to-flow ratios. After a long process, humans started collectively accepting gold as form of payment because of its indestructibility and scarcity. Gold has been used up until the end of the gold standard. Ammous (2018) further explains that the gold standard had been replaced with non-sound fiat money, and ever since World War 1 there have been fifty-six cases of hyperinflation. Considering that most people live under almost at or even above double-digit inflation, and the risk of hyperinflation is historically high for countries, the risk of such a thing outweighs any benefits. Ammous (2018) elaborates on the gold standard. This used to be a monetary standard where the value of the currency was pegged to gold and paper currencies represented checks for a fixed amount of gold. Ammous believes that this monetary system had its flaws. For example, he argued that settlements in gold were expensive and risky. This forced gold users to centralize it in banks and central banks where governments could have almost a monopoly on the country's gold. On the

---

[84] Money that is salable and functions as a store of value

[85] The total existing supply divided by the annual production of that money

other hand, bitcoin was designed to incorporate the best features of gold while also avoiding its physical drawbacks such as storing it or transporting it. Making bitcoin a form of currency fit to be a global reserve.[86]

3.1- The Austrian theory of money

The Austrian Theory of money is a discussion that starts and ends with Ludwig Von Mises' book *Theory of Money and Credit.* Mises' took the theory of marginal utility developed by other Austrian economists and applied it to money. Mises used the Wicksteedian concept which says that the price of a resource equals the value that a marginal unit adds to the output it produces. This concept is appropriate to money because money is not a good that is bought and consumed but it's a good held for future exchange. When the theory of diminishing marginal utility is applied to money, as someone spends their wealth at some point, they will want to stop spending and start saving because the marginal utility they will receive from that extra spending becomes null.

Austrian economists find money to be that object which every other object has its value denominated at. Assuming every object has its value denominated in dollars, then the purchasing power of that dollar would be all the goods and services that can be purchased for that dollar in the economy.

Mises argues that with inflationary money having a unitary price level where an increase in something's price is accompanied by an increase in everything's price is fallacious. This is because each person has its own demand curve, and everyone has their own desires. Also, since the newly issued money is generally created to be spent on specific goods and services, those industries that are left out of this stimulus are generally those that are hurt by inflation. However, even though relative nominal prices change disproportionally, real relative prices tend to be stickier. Mises argues that therefore purchasing power of money tends to be uniform in a trading area. For example, the purchasing power of money is much higher in rural Louisiana than in Manhattan and this is seen for almost every good sold in both markets. Although the US is a single trading area with many states that vary in purchasing power of money, the US still tends to have a uniform

---

[86] Ammous S. (2018), *The Bitcoin Standard*, New Jersey: Hoboken

purchasing power, but it is not achieved because of the different valuations of goods[87]. In case there is more than one currency in the world, the tendency of having uniform prices still holds. Mises used the Ricardian analysis for this argument where it is said that the market exchange rate between two currencies will tend to be the ratio of their purchasing powers. This theory is also called the purchasing power parity theory of exchange rates.

Mises managed to overcome one of the challenges that trapped Austrian economists. This trap is called 'the Austrian circle' and it refers to the circular problem that money is valuable not because it has a prior exchange value but because it will be exchangeable in terms of other goods in the future. However, if demand depends on its preexisting purchasing price, then how is the price itself explained by demand? This question trapped Austrian economists up until Mises answered the question by developing his regression theorem. Mises said that what determines the purchasing power of money on day X is determined by its supply and demand, and that in turn depended on the fact that money had purchasing power on day X-1. This process is long, but not circular. The regression theorem looks at the origin of money. It looks at when the commodity known as money today was not used as money. For example, gold can be traced back to barter days where it was used only for consumption and not as a medium of exchange. The regression theorem also shows that for money to be money must have originated from the market itself, discarding fiat currencies as a good form of money[88].

3.2- Sound money and the economy

Sound money, or in other words money with a high relative scarcity such as gold has been around for thousands of years. Most civilizations had sound money at some point in their history. While sound money has a rooted past, fiat money is the type of money that can be considered an experiment. Money not being pegged to something scarce is an experiment that for some countries worked relatively well, but for most it caused either double-digit inflation, hyperinflation, or increased government presence in the markets. As Mises and Hayek argued, the key elements of a

---

[87] Land in Manhattan is much more valuable than land in Ohio because of the vast services and opportunities that Manhattan offers.
[88] Rothbard M. N. (2011). *Economic Controversies.* Ludwig von Mises institute

functioning economy are private ownership of the means of production, capital, monetary calculation, and sound money. Without private ownership of the means of production, there are no markets, and without markets there are no prices reflecting the scarcity of these resources and thus there is no economic calculation. However, there is also another element that is crucial for economic calculation and that is sound money. Economic calculation is best achieved only when prices reflect the real value of the market[89] and sound money is the most reliable form of money for this, as the money itself is scarce too[90]. With Bitcoin as a currency, prices would thus reflect true valuations, and allow for an efficient allocation of resources. In today's world new money constantly enters the economy. When this happens interest rates are artificially pushed down and as a result economic agents begin to have a higher time preference because of the ease of obtaining credit. This causes a distorted calculation by economic agents, because the fall in the interest rate before any modification to prices creates a less efficient allocation of capital to resources. At the start, this causes a boom in the economy where unemployment falls, and real wages begin to rise. However, this type of growth becomes unsustainable. When investments made during the boom turn out to be malinvestments, the boom turns into a bust. Sound money prevents this from happening[91]. With scarce money like bitcoin, boom and bust cycles would not happen systematically. They might happen in individual industries, but not systematically as the current boom and bust cycles occur.

Murray Rothbard explains in his book "*Man Economy and State"* that "*A change in the money relation necessarily involves gains and losses because money is not neutral and price changes do not take place simultaneously"[92]*. Rothbard (1962) further explains that when the money supply in an economy is increased, the changes in the demand for money don't happen suddenly, but step by step. This happens because the market is a complex network where some agents react quicker than

---

[89] The price where supply and demand are in equilibrium and not where the good is over or under-consumed.

[90] Cochran, J. P. (2004). Capital, Monetary Calculation, And the Trade Cycle: The Importance of Sound Money. *The Quarterly Journal of Austrian Economics Vol.7 No.1*

[91] Chamberlin A. & Manish G. P. (2018). Savings, Private Property and Sound Money: An Austrian Perspective on the Essential Pre-Requisites to Economic Growth and Development. *MISES: Interdisciplinary Journal of Philosophy Law and Economics*.

[92] Rothbard, Murray N. *Man, Economy, and State with Power and Market, Scholar's Edition*. Second Edition, Ludwig Von Mises Institute, 2009. pp 811

others so the movements in prices will differ from good to good. Rothbard provided an example of this situation. If Jones were to find some unknown hidden gold, he would have an excess of gold compared to his demand for it. Jones would then look to spend the excess gold he possesses, by buying something from Smith. Smith now finds his gold balance in excess of his demand for it, and he would assume that if this trend were to continue, he would face shortages in his store, so he increases his selling prices. Smith then spends his excess gold with Robinson who goes through the same thought and action process as Smith and so on. As this process continues, more and more stores increase their price, lowering purchasing power. However, the individuals who get the new discovered gold through the end of this process find that prices have mostly increased but the gold balance in their hands still hasn't. This is a very simplified example. In real life, if money supply were to increase since people have different sorts of demands and preferences the price of some goods will increase relatively more and some relatively less.[93]This process, which increases inequality in countries, is not needed with Bitcoin. Resources that have scarcity cannot be printed, only produced. Gold supply increase currently averages 2% per year while bitcoin averages 1.6%, and this will fall as the supply cap of bitcoin is reached allowing for a resource to reflect the equilibrium of supply and demand when pricing goods and services.

Rothbard goes on by explaining the harms of an interventionist and inflation-seeking government. For the government or a central bank, the issue of new money is costless or even positive. Because of the diffusion effect the first holders of newly issued money gain the most, while each next agent gains less until there is an actual loss by some agents. This is described as a social waste and only advantages some at the expense of others. Most gains obtained during a credit expansion period that the increased money supply cause, are only short-run and will cease once the new monetary equilibrium is reached. However, since some prices rise more than others, inflation will always have permanent gainers and losers. Most victims of inflation are those that have fixed salaries like pensions or yearly un-adjustable salaries, while the other victims are creditors that won't be able to receive the purchasing power-adjusted premium on their loans. Rothbard argues that the new creation of money blinds the businessman, which buys equipment. When the businessmen sell their product, the inflationary gain is recorded as profit, but it isn't, because he would then have to repurchase the capital good at a higher price because of inflation. The businessman that sees extra

---

[93] Rothbard, Murray N. *Man, Economy, and State with Power and Market, Scholar's Edition*. Second Edition, Ludwig Von Mises Institute, 2009. Chapter 11

profits, will go on to increase capital consumption while not considering that the real purchasing power he holds is unchanged or negative. This is especially felt in industries that acquire equipment when prices were lowest. As inflation goes on that industry will seem to have higher profits than usual and it will attract new entrants. At the same time, there will be a deficiency in investment in other industries.[94] This will hurt worker wages of under-invested industries and cause imbalances in the economy. When money is not sound average workers face these risks, since devaluation by the government and boom and bust cycles are never in their favor. This could keep their real wages depressed, while nominal wages rise.

According to Mises a worker has a higher remuneration from his occupation when he can produce more. This increase in productivity is what drives real wages to increase. American wages are better than most wages because the US has allowed for an economic environment for entrepreneurs to invest more capital per worker, which allows them to have more efficient machines. Credit expansion creates an illusion of increasing funds available for production, which drives investments that wouldn't have happened otherwise. These investments create also artificial demand for labor, which will have higher nominal wages, but real wages will be depressed[95]. The United States went off the gold standard in 1971, when President Nixon decided that the convertibility from the dollar to gold would be canceled. Ever since 1971, there have been imbalances between productivity and real remuneration. Although the 1970's and 1980s were full of economic shocks, ever since the sovereignty of fiat money the relationship between productivity and real remuneration appears to be broken. **Figure 14** depicts this divergence.

---

[94] Rothbard, Murray N. *Man, Economy, and State with Power and Market, Scholar's Edition*. Second Edition, Ludwig Von Mises Institute, 2009. Chapter 11

[95] Hickling, M. (2013). Inflation and Other Risks of Unsound Money. *Actuaries Institute*

Figure 14: Divergence of productivity and remuneration

Note: FTE= Full time equivalent worker
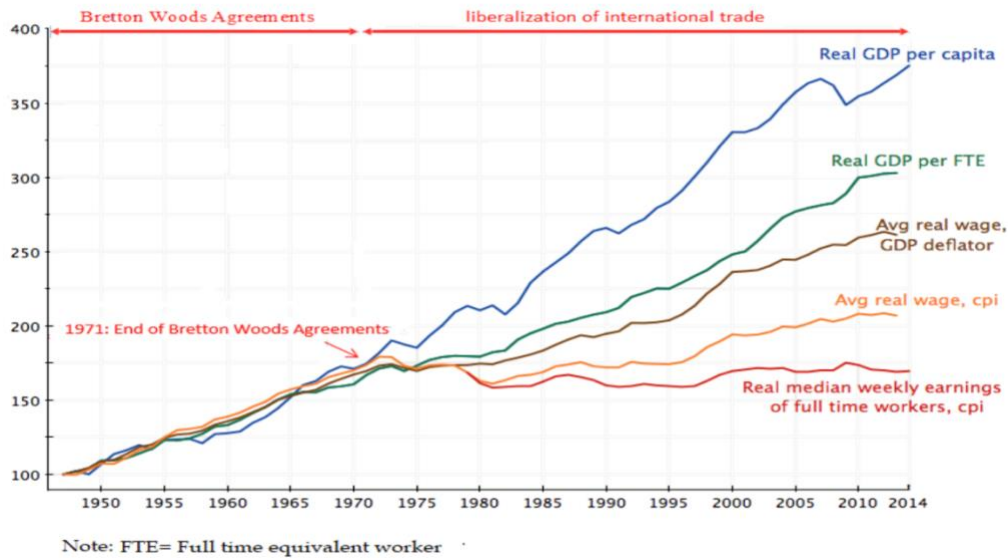
Source: Bureau of Economic Analysis, Bureau of Labor Statistics [96]

With non-sound money when currencies inflate, tangible assets like real estate appreciate notably. This happens because while real estate is finite, paper money is not so an increase in moneys supply will cause real assets to appreciate relatively to it. This hurts average workers, which are unable to afford homes because they are always last in line in the distribution of the newly issued money. Under a Bitcoin standard, where families held Bitcoin to preserve their wealth, the fluctuation between individuals' wealth and real assets would significantly decrease since Bitcoin is as scarce as land. This would end speculation on properties and allow more land to be devoted for housing. Currently those who can own assets are able to rely on their inflated returns. Those who can live with these returns aren't incentivized to do honest knowledge seeking work. With sound money firms would invest in honest, knowledge and skill creating projects to develop new goods and services. Because with no oversupply of money, speculative markets shrink[97]. While countries like the US or EU don't live and haven't recently lived under a hyperinflationary environment, history tells us that devaluation of the currency and hyperinflation is the expected result. The United States has been able to print significant amounts of dollars without significant impacts on their inflation levels thanks to their currency having the world reserve currency status, so they are able to "export"

---

[97] Heung- No, Lee, et al. (2022). Green Bitcoin: Global Sound Money. *The Journal of Digital Assets*

their inflation. Other countries that must keep within their borders all the money they print live under poor economic conditions. For example, currently Turks live with more than 80% inflation levels. Even if during the beginning of the twentieth century Turkey had better levels of inflation that weren't double digits, Turks have lived through double-digit inflation levels every year since the 1970's. Instead of populations arguing about who should better manage the economy, in countries like Turkey the focus must be on solving the chronic disease that has kept the country behind which is a government monopoly on money. Bitcoin wouldn't allow politicians to give empty promises of growth and damaging stimulus plans, because they wouldn't be able to collect the bitcoin needed. Politicians would thus be incentivized to reach a state where productivity and investments keep on growing thanks to a sustainable and free market. Furthermore, bailouts of inefficient banks or industries would drastically decrease since they are only sustained by increasing money supply.

3.3- Consumer behavior without inflation

One of the implications of a Bitcoin standard would be that there would be no inflation, since Bitcoin is a deflationary currency because of its finite supply. This would cause an economic environment where deflation is present. Opinions on deflation vary in economics by the school of thought, for example Austrians usually believe it to be beneficial while modern economics find deflation to be extremely harmful to an economy and try to avoid it through a moderate expansion of the money supply. There still may be times in certain industries where inflation may happen. If trends and preferences were to change, certain products would see an increase in demand that would evolve into higher prices for these products unless production is increased. Inflation could also be caused by supply chain issues which would decrease the quantity of needed materials for production. However, deflation would be a general concern if fiat money continued to inflate relative to Bitcoin. If the overall money supply were to be unvaried or varied in accordance with the Bitcoin held in reserves, the economy would experience mostly 0% inflation rates in the money supply. Not an increase and neither a contraction.

If deflation were to be a reality, Modern economic theory would suggest that deflation would harm the economy in 3 ways. The first being that falling prices would hurt businesses, the second that an increase in real debt would negatively affect production and the third being that credit contraction would amplify the bust cycle. These three phenomena would be destructive for an economy and would significantly lower living standards. This is also why central banks try to achieve an inflation of 2%, for it not to be too high to lower purchasing power and to leave a buffer zone between deflation and the real rate. The Austrian view makes different points, for example according to Rothbard, there are also counterarguments to these three predicted effects. About the prevailing view that falling prices hurt businesses, Rothbard says that for businesses what matters is the difference between selling prices and costs, not the general price level. Businesses would also prepare for deflation, as it becomes predictable. The anticipation of falling prices would immediately decrease factor prices and this anticipation would adjust the purchasing power to the changing conditions.

Addressing the second argument that deflation would hurt businesses since their real debt would increase Rothbard argues that creditors are different types of owners. Meaning that creditors collect money and invest that money in a business, making them not so different from stockholders. Both usually get to have a claim on the business. A change in the price level might not affect a business when these owner-creditors simply divide their gains in different proportions until the debt is repaid. Addressing the third argument that credit contraction would deepen depressions Rothbard says that a credit contraction would speed up the recovery process of that depression. When banks expand credit, the interest rate artificially lowers, and this distorts the free market. When credit contraction follows a credit expansion, this would allow the equilibrium to achieve free market levels. Additionally, a beneficial effect of credit contraction would be that inefficient businesses would have to be liquidated, and this adjustment of malinvestments would speed up the recovery process. Thus, having a view consistent with the Austrian economic belief, Rothbard is not troubled by deflation as others would be[98].

According to Hayek, deflation is a possible effect of a depression that can be cured by the readjustment of the structure of production and not by inflating the country's currency. Since

---

[98] Bagus, P. (2003). Deflation: When Austrians Become Interventionists. *The Quarterly Journal of Austrian Economics*, no. 4, Mises Institute, 19–35.

deflation is a symptom and not a cause, trying to cure it with expansive monetary policies prolongs the depression and avoids the real adjustments of the free market[99].

Deflation or a non-inflationary economy could notably lower individuals time preferences. Time preferences affect behavior across many dimensions. A consumer who has a low time preference would likely save money to then spend it on future satisfaction. With inflation, everyone is implicitly forced to immediately seek an investment with relatively good returns in order to preserve purchasing power, so time preferences will be higher when inflation exists. A lower time preference would significantly contribute to making decisions for the future. As time preference declines, consumers start to defer consumption and keep more money on hand, which will make them more willing to lend money for projects. With lower time preferences and increasing savings and investments, countries can increase their steady state and productivity. Since a high time preference is a consequence of fiat money, it isn't a phenomenon commonly seen in centuries before. Usually, high time preferences used to occur when there were plagues or wars which created a future difficult to foresee. Bitcoin would restore this way of economic planning by emphasizing on long-term planning and growth rather than a short-term one[100].

Countries that are deemed not to have efficient and economically responsible policies like Turkey, Argentina, Lebanon and many others have never ended their inflation. Nearly half of the world's population lives under high levels of inflation as of 2023. In countries like Turkey people are now forced to purchase gold, bitcoin, real estate and other scarce assets for survival. With inflation rates like those in Turkey it is impossible to make decisions even for the medium term.

The current inflationary regime indirectly steals people's labor since payment is the reward of labor. The notion that one's labor reward will be less valuable in the future because central planners want to achieve better growth rates on paper for political purposes is immoral. While under an optimistic view it is possible to achieve 2% inflation as central banks currently aim, it is more realistic to limit politicians' power to increase the money supply for most countries. Because the EU and the US have free markets that contributed to their fast growth relative to the rest of the world that had interventionist policies. Since the US and the EU have a functioning economic

---

[99] Bagus, P. (2003). Deflation: When Austrians Become Interventionists. *The Quarterly Journal of Austrian Economics*, no. 4, Mises Institute, 19–35.

[100] Ammous S. et al (2022) Hard money and time preference: A Bitcoin perspective. *MISES*: *Interdisciplinary Journal of Philosophy Law and Economics*

system, it is unrealistic to imagine a smooth and rapid transition to a Bitcoin standard, while for third world countries or developing countries that have traditionally struggled to improve their living standards there would be fewer trade-offs in switching to a Bitcoin standard. This transition is seen in countries like El Salvador or the Central African Republic.

3.4- Economic and political freedom implications

Using Bitcoin under a Bitcoin standard gives anyone regardless of their nationality, religion, race, or beliefs the privilege of holding on to their wealth without the risk of debasement or censorship. Alex Gladstein, Chief Strategy Officer at the Human Rights foundations[101], explains Bitcoin's contribution to freedom by giving real-life examples. For example, Venezuelans currently live under an authoritarian regime and are forced to flee desperately with nothing in their pockets. Many Venezuelans who still reside in Venezuela are now slowly switching to Bitcoin. Their government set a limit on the money that could come from abroad and Venezuelans are now forced to go through banks for foreign transactions. These banks are then forced by the government to provide information of these transactions, always keeping an eye on their citizens. These intermediaries and the tight surveillance that is made by them also comes with a very high transaction fee for bank users that are trying to send money abroad. Faced with these circumstances, some Venezuelans chose to send their money in Bitcoin. With Bitcoin, Venezuelans can simply contact their family member abroad and receive money within minutes with a significantly smaller transaction fee, without the government knowing anything about it. Government censorship is not possible for these transactions, since the users are both anonymous. Venezuela isn't the only country that faces these problems. In Zimbabwe, the government has printed an endless amount of money, which famously caused the emergence of the famous one hundred trillion dollars banknote, a Bitcoin standard would have prevented this because of its scarcity. In China, the government tracks everyone's bank accounts, but it can't track the accounts of those who use Bitcoin. While currently

---

[101] The Human Rights Foundation is a non-profit, nonpartisan organization established in 2005 in New York with the support of many tyranny victims such as Elie Wiesel who lived through the Nazi dictatorship in Germany and eventually won a Nobel peace prize. Their difference from other human rights organizations is that their focus is on dictatorships.

the use of cash is being de-incentivized year by year, with plans using CBDC's in the future, the use of an impartial peer to peer payment system becomes crucial. Without cash, if someone wanted to give money to the person in front of them, they would have to go through an intermediary like Venmo, which in turn goes through other financial intermediaries. Each intermediary that a person would have to go through could potentially censor, surveil and profit. According to the Human Rights Foundation nearly half of the world's population lives under an authoritarian government and Bitcoin could act as insurance against these regimes[102].

In Nigeria, the population started acquiring Bitcoin once they realized that inflation wasn't transitory and that the government wouldn't protect human rights. In 2017, the "End SARS[103]" movement began, after this special unit started extorting its citizens for money while imposing roadblocks, torturing dissidents and even killing people without any due legal process. Protestors used to receive funds from foreign donors, which sent the money to the protestors bank accounts. After a while, protestors noticed that their transactions were slowing down, until one day all donations were blocked by the banks. Although the Nigerian government said they weren't involved in the blocking of donations towards protestors, naturally many doubts arise. After the protestor's bank accounts were blocked, they chose the only option that would give them the freedom necessary to receive donations without government involvement, which is Bitcoin. Thanks to Bitcoin they were able to receive the funds necessary at the time to continue promoting against police brutality and according to their accounts summary they received approximately 40% of all donations in Bitcoin[104].

Cryptocurrencies such as Bitcoin have also had an influence in today's Russia-Ukraine war. During the war, both Ukraine and Russia had difficulty accessing traditional banks. Ukraine had difficulty with traditional systems since they were under attack. While normal banks are closed at night and weekends Bitcoin is active 24/7 making the reception of funds much more efficient and easier.

---

[102] Gladstein, A. (2018). Why Bitcoin Matters for Freedom. *TIME Magazine*

[103] In 1992, the Nigerian government established the Special Anti-Robbery Squad (SARS) to fight against armed robbery and other major crimes.

[104]Kazeem, Y. (2020) How Bitcoin Powered Nigeria's #EndSARS Protests. *Quartz*

Ukraine received more than 200 million dollar's worth of cryptocurrencies up until February 2023. On the other hand, Russians couldn't access any international bank because of sanctions. Even they received funds through Bitcoin[105]. In a free marketplace of ideas, the right thing gets rewarded. Therefore, Ukraine received many times more donations than Russia did in Bitcoin. Fiat money is used as a tool against Russia to disincentivize it from continuing the war, but the only damage done is towards its citizens. While this sounds like justice, this is a dangerous tool that could fall in the wrong hands[106]. Bitcoin would simply act as money, not as anyone's political tool. Fiat money has the risk of being too politicized because most of the times it is the politicians who decide when to print, how much to print and how to distribute it. Right or wrong Bitcoin gives everyone the right of willfully exchanging goods, even to two different extremes such as Russia and Ukraine because while fiat money is political, Bitcoin is apolitical.

---

[105] Chipolina S. (2023), The two sides of crypto in the Ukraine war. *Financial times*

[106] If the ability of destroying a country's production through fiat money sanctions exist, it is more than likely that this will be used for political purposes rather than for justice.

Conclusions

Bitcoin has brought to life a debate that seemed settled after the exit from the gold standard. Supported by cryptography and blockchain technology, Bitcoin came into the world as the first completely peer-to-peer digital currency. Currently, it promises to offer an alternative to the third party requiring traditional financial system.

All of Bitcoin's core characteristics such as scarcity, decentralization, the immutability of the blockchain, and many more can play a crucial role for its future success. Innovation is about bringing new ideas or improving those already existing to the marketplace. A competing innovation for Bitcoin seems to be a Central Bank digital currency (CBDC), which is nothing more than a digital fiat currency and Bitcoin's decentralized nature could provide what these CBDC's would lack. Having no single entity in control over the network and thus protecting the users from censorship gives Bitcoin much more intrinsic value than a traditional fiat currency. A world that gets increasingly fed up with government fiat currencies would eventually transition a portion of its wealth to Bitcoin. Even a slight mainstream recognition would imply very high returns for Bitcoin holders, considering that even though it has been around for more than 10 years most people have never bought Bitcoin. This presumption does not mean that a global Bitcoin standard is probable. For this to happen anytime in this century there would have to be something like a revolution, therefore until this point in time, a Bitcoin standard remains entirely hypothetical.

On whether Bitcoin could ever challenge fiat currencies, with the volatility seen in Bitcoin these years, it is difficult to certainly predict if this could happen. The volatility seen until now has been almost always on an upward trend, but this is not an assurance of the future. Nonetheless, a contributor to higher Bitcoin usage would ultimately also depend on individual countries monetary and public policies. If governments were to mismanage fiat currencies by inflating them too much, this would be a strong incentive to store Bitcoin for its scarcity.

The future of cryptocurrencies is also unclear. Currently, Bitcoin and the crypto industry altogether lack regulations. Although Bitcoin doesn't fit the description of a security and should not be regulated as so, the regulations that are predicted to arrive might make it harder for Bitcoin to maintain its status as a truly decentralized and anonymous currency. Other challenges such as

scalability are also going to shape Bitcoin's future. Without a solution for scalability issues, it's hard for Bitcoin to ever permanently replace fiat currencies.

With many challenges ahead, Bitcoin has the potential to become a widely used currency, where freedom is given to users and taken from central planners since it was designed to incorporate many of the characteristics needed for this to be possible. Whether this will happen or not will depend on how circumstances change with time, however the prerequisites to replace or challenge fiat money are undeniably there.

Bibliography

- Ahmadova S. & Erek S. M. (2022). Finansal Aracılık Koini Olan Ripple Üzerine Bir Değerlendirme (A Review on Ripple, a Financial Intermediary Coin). *Journal of Academic Projection (Akademik İzdüşüm Dergisi)*

- Albrecht C. et al. (2020). Legitimizing Bitcoin as a Currency and Store of Value: Using Discrete Monetary Units to Consolidate Value and Drive Market Growth. *Ledger Journal*

- Alifanov, S. On the Dangers Inherent in a Fractional Reserve Banking System.

- Ametrano F. (2016). Hayek Money: The cryptocurrency price stability solution, 18-21

- Ammous S. (2018), *The Bitcoin Standard*, New Jersey: Hoboken

- Ammous S. et al (2022) Hard money and time preference: A Bitcoin perspective. *MISES: Interdisciplinary Journal of Philosophy Law and Economics*

- Andreianova M. et al. 2021 Bitcoin usage: Study on Bitcoin usage around the World, *The Journal of Fintech*

- Bagus, P. (2003). Deflation: When Austrians Become Interventionists. *The Quarterly Journal of Austrian Economics*, no. 4, Mises Institute, 19–35.

- Biais B. et al. (2019) Blockchains, Coordination, and Forks. *AEA Papers and Proceedings*, *American Economic Association*, 88–92.

- Burgers J. W. (2021) Understanding Bitcoin's Scarcity. *Bitcoin Magazine*

- Cermak V. (2017) *Can Bitcoin Become a Viable Alternative to Fiat Currencies? An Empirical Analysis of Bitcoin's Volatility Based on a GARCH Model*. *Skimore College*

- Chamberlin A. & Manish G. P. (2018). Savings, Private Property and Sound Money: An Austrian Perspective on the Essential Pre-Requisites to Economic Growth and Development. *MISES: Interdisciplinary Journal of Philosophy Law and Economics*.

- Chipolina S. (2023), The two sides of crypto in the Ukraine war. *Financial times*

- Cochran, J. P. (2004). Capital, Monetary Calculation, And the Trade Cycle: The Importance of Sound Money. *The Quarterly Journal of Austrian Economics Vol.7 No.1*

- Ciaian P. et al. (2016). The Economics of BitCoin Price Formation. *Routledge*

- Daisyme, P. (2022) Why Decentralization Is Crypto's Greatest Strength and Greatest Threat. *Nasdaq*

- Davidson L. et al. (2015). Bitcoin, the regression theorem, and the emergence of a new medium of exchange*. The Quarterly Journal of Austrian Economics*

- Davidson L. & Walter B. (2015). The Relevance of Bitcoin to the Regression Theorem: Reply to Pickering. *The Quarterly Journal of Austrian Economics*

- Gladstein, A. (2018). Why Bitcoin Matters for Freedom. *TIME Magazine*

- Guizani, S. & Nafti I. K. (2019). The Determinants of Bitcoin Price Volatility: An Investigation With ARDL Model. *Elsevier*

- Harm, J. et al. Ethereum vs. Bitcoin. *Creighton University*

- Heung- No, Lee, et al. (2022). Green Bitcoin: Global Sound Money. *The Journal of Digital Assets*

- Hickling, M. (2013). Inflation and Other Risks of Unsound Money. *Actuaries Institute*

- Horizon Kinetics LLC (2020). Bitcoin Supply Curve Over Time

- Kaloudis, G. (2021). A Deep Dive into Lightning as a Bitcoin Scaling Solution. *Coin Desk Research*

- Kamau, R. (2022). Why Keeping Bitcoin on An Exchange Is Driving the Price Down. *Forbes*

- Kazeem, Y. (2020) How Bitcoin Powered Nigeria's #EndSARS Protests. *Quartz*

- Khalif, David. (2022). What Happens When All 21 million Bitcoin Are Mined? *Nasdaq*

- Kroeger, A. & Fuerst T. *Essays on Bitcoin*

- Kroll, J. A. et al. (2013) The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. *Princeton University*

- Lo, S. & Wang J. C. (2014). Bitcoin as Money*? Federal Reserve Bank of Boston*

- Longchamp, Y. et al. (2020). The Blockchain Trilemma. *SEBA Swiss*

- Nakamoto S. (2008) Bitcoin: A peer-to-peer electronic cash system.

- Neo C.K. Yiu. (2021). An Overview of Forks and Coordination in Blockchain Development. *University of Oxford*

- Nguyen T. et al. (2018). Factors affecting Bitcoin price in the cryptocurrency market: an empirical study, *International Journal of Business and Economics Perspectives*

- Robbins L. (1935). *An Essay on the Nature and Significance of Economic Science*. London: MacMillan and Co

- Rose, C. (2015) The Evolution of Digital Currencies: Bitcoin, A Cryptocurrency Causing A Monetary Revolution. *International Business & Economics Research Journal vol.14*

- Rothbard, M. N. (1962) *Man, Economy, and State, Scholar's Edition* (2nd ed)*,* Ludwig Von Mises Institute

- Rothbard M. N. (2011). *Economic Controversies.* Ludwig von Mises Institute

- Shaw, B. (2022). Bitcoin vs. Bitcoin Cash: What's the Difference and Which Is Better? *Nasdaq*

- Salerno, J. (2020). Book review: Banking and Monetary Policy from the Perspective of Austrian Economics. *Mises Institute*

- Suriyan, S. (2021). Bitcoin's Price Rises Rapidly Due to Absolute Scarcity. *Bitcoin Magazine*

- Van Wirdum A. (2018). THE GENESIS FILES: IF BITCOIN HAD A FIRST DRAFT, WEI DAI'S B-MONEY WAS IT. *Bitcoin Magazine*

- Velde, F. R. (2013). Bitcoin: A Primer. *Chicago Fed Letter*, *The Federal Reserve Bank of Chicago*

- Weaver N. (2022) The death of Cryptocurrency: The case for regulation. *Yale Law school Information Society Project*

- Wijk, D. v. (2013). What can be expected from the Bitcoin. *Erasmus University Rotterdam*

Sitografy

- Binance Academy (2022) "What Is the Blockchain Trilemma?" *Binance* https://academy.binance.com/en/articles/what-is-the-blockchain-trilemma

- Bitcoin Magazine (2018, July). The Genesis Files: With Bit Gold, Szabo Was Inches Away From Inventing Bitcoin. *Bitcoin Magazine* https://www.nasdaq.com/articles/the-genesis-files%3A-with-bit-gold-szabo-was-inches-away-from-inventing-bitcoin-2018-07-12

- Chen J. (2022, April). Nikkei. *Investopedia* https://www.investopedia.com/terms/n/nikkei.asp

- Daisyme P. (2022) Why Decentralization Is Crypto's Greatest Strength and Greatest Threat. *Nasdaq* https://www.nasdaq.com/articles/why-decentralization-is-cryptos-greatest-strength-and-greatest-threat

- Edwards J. (2015, December). Bitcoin's Price History. *Investopedia* https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp

- Favole J. (2021, December). It Can't Be Decentralization or Bust. *CoinDesk* https://www.coindesk.com/policy/2021/12/16/it-cant-be-decentralization-or-bust/

- Frankenfield J. (2014, June) What Is a Block in the Crypto Blockchain, and How Does It Work? *Investopedia* https://www.investopedia.com/terms/b/block-bitcoin-block.asp

- Frankenfield J. (2018, April). Binance Coin (BNB) Uses, Support, and Market Cap. *Investopedia* https://www.investopedia.com/terms/b/binance-coin-bnb.asp

- Frankenfield J. (2018, June). DigiCash Definition. *Investopedia* https://www.investopedia.com/terms/d/digicash.asp

- Ganti A. (2003, November). What Is the Dow Jones Industrial Average (DJIA)? *Investopedia* https://www.investopedia.com/terms/d/djia.asp

- Guazzo, G. (2020, November). Bitcoin e Trilemma Della Blockchain: Cosa è e Possibile Soluzione. *Investire.Biz* https://investire.biz/analisi-previsioni-ricerche/bitcoin-e-criptovalute/criptovalute-bitcoin-trilemma-blockchain-cosa-funzionamento-soluzione-lightning-network

- Kelleher, J. P. (2014, October). Why Do Bitcoins Have Value? Bitcoin Explained. *Investopedia* https://www.investopedia.com/ask/answers/100314/why-do-bitcoins-have-value.asp

- Lucena, J. Advantages And Disadvantages Of Bitcoin Cash. *FLAUNT* https://flaunt.com/blog/by-bit

- Mineur, A. (2021, December). How Are Bitcoin's Difficulty and Hash Rate Calculated? *Miner Daily* https://minerdaily.com/2021/how-are-bitcoins-difficulty-and-hash-rate-calculated/

- Nevil S. (2006, August). Fractional Reserve Banking: What It Is and How It Works. *Investopedia* https://www.investopedia.com/terms/f/fractionalreservebanking.asp

- Reiff N. (2018, March). Bitcoin Gold: Distribution, Protection, and Transparency. *Investopedia* https://www.investopedia.com/tech/what-bitcoin-gold-exactly/

- Rowden S. (2022, November). What is Lightning Network? What are pros and cons of Lightning Network. *BITKAN* https://bitkan.com/learn/what-is-lightning-network-what-are-pros-and-cons-of-lighting-network-6445

- Smith, G. (2019, July). Is Bitcoin Money? Revisiting Mises' Regression Theorem. *Bitcoin News* https://news.bitcoin.com/is-bitcoin-money-revisiting-mises-regression-theorem/

- What Is a Blockchain Fork & How Do They Work? (2022, September). *Shardeum* https://shardeum.org/blog/what-is-a-blockchain-fork/

- What Is Hashcash and How Is It Connected to Bitcoin? *Paybis Blog* https://paybis.com/blog/what-is-hashcash/

- Yanay, A. Bitcoin: Money Decentralization (Understanding the Process). https://www.vpnmentor.com/blog/bitcoin-money-decentralization/