SCHOOL OF BUSINESS ADMINISTRATION

DEPARTMENT OF ACCOUNTING AND FINANCE

POSTGRADUATE PROGRAM IN ACCOUNTING TAXATION AND FINANCIAL MANAGEMENT

Master Thesis

TOKENOMICS AND THE INTRINSIC VALUE OF CRYPTOCURRENCIES

by

STYLIANOS KOUROUMIDIS

Supervisor: Prof. Achilleas Zapranis

Submitted as required to obtain the Postgraduate Diploma in Accounting Taxation and Financial Management

October 2022

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my supervisor, Prof. Achilleas Zapranis, for his invaluable guidance in the writing of this thesis and for his inspiring teaching throughout my studies. This work is dedicated to my family for their encouragement and their never-ending support.

ABSTRACT

The purpose of this Master thesis is to examine the existence of intrinsic value in cryptocurrencies and to provide a framework for their evaluation. I described the unique characteristics, capabilities and disadvantages of the underlying technology and detailed the most common criticisms, especially those regarding their dubious economic premise. I classified tokens by their use case and provided arguments for the existence of intrinsic value in every category. Subsequently, I introduced a theoretical valuation framework, which focuses on identifying the value drivers in each case. Lastly, I used on-chain analysis to reach a rough estimation of the intrinsic value of Bitcoin, followed by sensitivity analysis on the relevant parameters. Results indicate a wide range of possible values, depending on the initial assumptions. Initial assumptions often rely on intuition, while the interpretation of on-chain metrics is not always apparent. I concluded that the biggest challenge lies in assessing the fraction of a cryptocurrency's market capitalization that should be attributed to speculation, rather than utility.

Keywords: DLT, cryptocurrencies, tokens, tokenomics, tokenization, intrinsic value, valuation framework, bitcoin

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

In the last decade, following Bitcoin's implementation in January 2009, thousands of cryptocurrencies have emerged and their underlying value, utility and disruptive potential have been a topic of debate both in popular media and academic literature. While cryptocurrencies can differ vastly in terms of technology, economics, purpose and regulatory status, it's helpful to understand Bitcoin's core principles as an introduction to the concept of decentralized digital currencies.

In 2008, an unknown person or group, under the pseudonym Satoshi Nakamoto, proposed a solution to the double-spending problem [1] by introducing Bitcoin, a purely peer-to-peer version of electronic cash which would allow online payments to be sent directly from one party to another without going through a financial institution. The need for a trusted third party to validate transactions would be replaced by a system based on cryptographic proof. In his paper, he describes the benefits of removing the intermediary, which include the possibility of completely non-reversible transactions and lower transaction costs [2].

Bitcoin uses blockchain technology, which is a form of distributed ledger technology (DLT). Bank of England defines DLT as *a database architecture which enables the keeping and sharing of records in a distributed and decentralized way, while ensuring its integrity through the use of consensus-based validation protocols and cryptographic signatures.* The blockchain is a particular architecture of a distributed ledger whereby blocks of data are linked together, with each block containing information about the block preceding it. Thus, one could not retroactively alter any block without having to alter all subsequent ones as well. The result is a chronological chain of immutable records [3]. In this paper, the terms DLT and blockchain will be used interchangeably, since blockchain is by far the most common form of DLT.

The security and immutability of the Bitcoin blockchain is achieved by implementing a hash-based Proof-of-Work (PoW) mechanism that accepts the longest chain as consensus. In basic terms, decision making is not based on simple majority vote, with each IP having one vote, but on solving complex mathematical puzzles that require immense computational power. As long as the honest nodes have sufficient combined CPU power, attempting to alter the ledger comes at a prohibitive cost [2]. While the threshold to secure the network could be as high as 70% of total computational power [4], it's much less vulnerable than the one IP-one vote alternative, which could be manipulated by a single attacker allocating multiple IPs.

Since the PoW mechanism is energy-intensive and thus costly to individual nodes, incentives are required to secure the network. Each time a block of transactions is created and added to the chain, the creator gets rewarded in Bitcoin. The process of receiving newly minted coins as a reward for validating transactions is termed mining, drawing an analogy between gold miners spending time and resources on adding gold to circulation, and nodes receiving coins in exchange for their time, CPU power and energy consumption. This incentivizes nodes to be honest, as the value of Bitcoin heavily relies on the integrity of the network. At the same time, no central authority is responsible for issuing coins, further reinforcing decentralization [2].

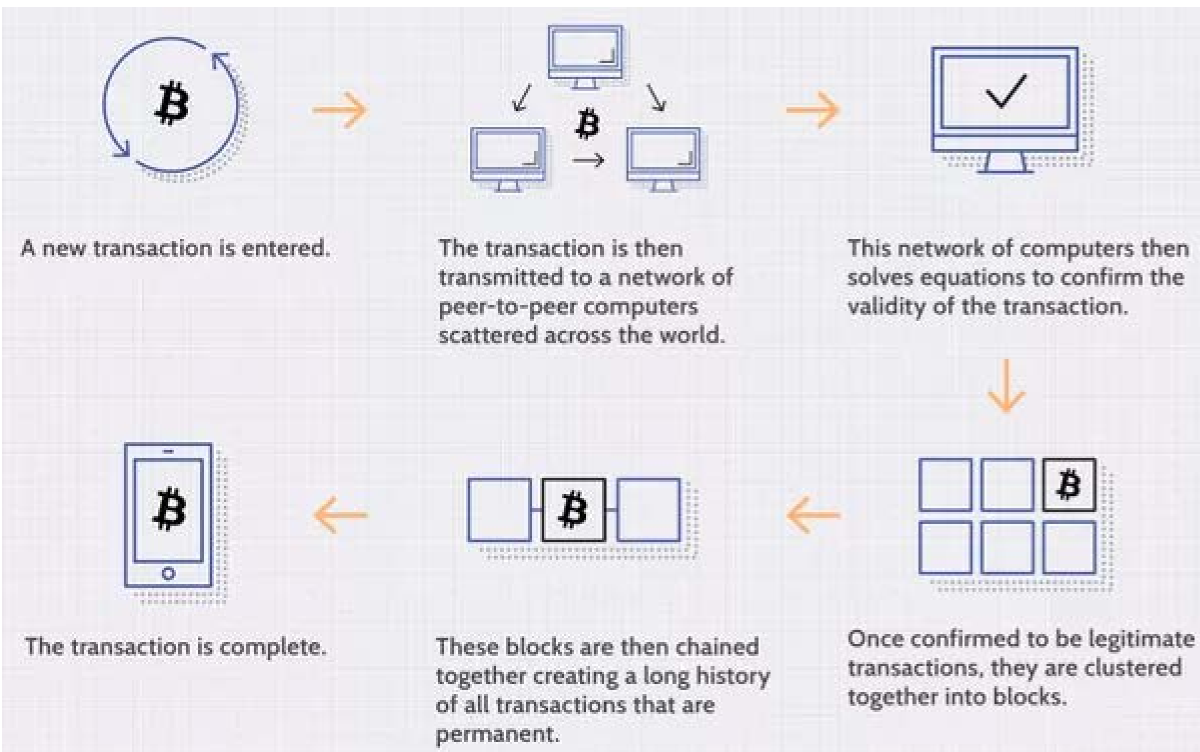


Figure 1: Blockchain Proof-of-Work transaction process (source: investopedia.com)

The protocol determines a 50% decrease of Bitcoins generated per block, every 210,000 blocks, a process known as halving. This is enforced by automatically adjusting the difficulty of the mining algorithm so that the rate of issuance is the one originally intended [5]. As a result, halvings occur approximately every 4 years, until the total supply of Bitcoins asymptotically reaches 21,000,000 around the year 2140. From that point onwards, miners will be rewarded by receiving a commission on transaction fees [6]. This limited supply and issuance rate applies to Bitcoin, but other blockchains may have economics that differ vastly from it. Bitcoin's smallest unit of divisibility is termed Satoshi and is one hundred millionth $\left(1/_{100,000,000}\right)$ of a Bitcoin.

In the traditional financial system, information relevant to the transaction is known only to parties involved, plus the trusted intermediary, so privacy is a given. In the Bitcoin network, this information includes the time and size of the transaction as well as the public keys of the sender and the receiver*. Since the ledger is public, this information is broadcasted to all nodes, however, the public key is not linked to an individual, therefore anonymity is preserved [2]. The concept of privacy includes confidentiality of transactions, anonymity of users' identity and unlinkability of transactions to a specific user [8]. This does not mean that it's impossible for authorities or malicious hackers to track the source of a transaction in a roundabout way. One notable case is the arrest of Ross Ulbricht, the operator of a dark web marketplace named Silk Road, in which payments for illegal substances were made in Bitcoin [9]. While anonymity is lucrative for participants in illegal activities, the fact that all transactions will be forever public on the ledger, may ultimately hinder Bitcoin's use in the black market [10].

Bitcoin rose in popularity in the last decade, but its invention was the product of many years of research and digital cash attempts within the computer scientist and cypherpunk community. Its traits of decentralization, anonymity and resistance to censorship made it attractive to early adopters and contributors, who were intrigued by the socioeconomic implications of it and that, arguably, shared a common philosophy aiming to disrupt established institutions. Bitcoin could offer access to financial services for the unbanked population, provide censorship resistant financial infrastructure against authoritarian regimes and upset the status quo of the fractional-reserve banking system, by introducing a currency whose issuance is not controlled by a central government. Nowadays, as institutional and retail adoption increases and as the percentage of the population that owns cryptocurrencies is higher than ever, it's safe to assume that Bitcoin has largely moved beyond its ideological past and has become an investment for the majority of its users, essentially, a new asset class. It has been also considered a possible hedge against inflation, due to its fixed total supply, in contrast with an ever-increasing fiat money supply in the post-Bretton Woods economy. Today, Bitcoin is considered primarily a store of value with some

*a string of numbers and letters, 264-520 bits long, that is unique to each Bitcoin address [7] labelling it digital gold, in reference to its scarcity, divisibility, portability, fungibility, durability and resistance to counterfeiting.

The revolutionary invention of Bitcoin triggered the appearance of numerous imitations and technology pioneers aspiring to expand on the original idea. Thousands of digital currencies, with different technology, consensus mechanisms, degrees of decentralization and purposes appeared. However, the vast majority of them either lack an actual use case or are doomed to fall behind to competition.

In July 2015, the Ethereum network, the first blockchain to support smart contracts, went live. Computer scientist and cryptographer Nick Szabo defined smart contracts in 1996 as: *a set of promises, specified in digital form, including protocols within which the parties perform on these promises* [11]. In layman terms, smart contracts not only include the agreed-upon terms in lines of code, but these terms are also automatically executed via the network, once certain criteria are fulfilled. While Bitcoin is limited, in the sense that one can only store, send or receive coins, the Ethereum platform, utilizing smart contracts, gives users the ability to create decentralized applications (dApps) with their own rules, transaction mechanisms and a wide range of use cases. Such use cases include Decentralized Finance or DeFi applications (financial derivatives, stable-value currencies, decentralized marketplaces etc.), decentralized file storage, distributed computing, identity and reputation systems and decentralized autonomous organizations (DAOs) [12]. This allows for the existence of an ecosystem where all data is stored and controlled by users, without the need for a third party.

While the prospect of trustless transactions is appealing, it faces serious challenges and critical issues need to be solved before DLT achieves mainstream adoption. Arguably, the Holy Grail of DLT today is solving the Scalability Trilemma: achieving scalability, security and decentralization at the same time [13]. In simple terms, that means that the network is capable of handling a high number of transactions per second (TPS), comparable to centralized networks[*], while its security or degree of decentralization is not compromised. The tradeoff between increased TPS and security has been well established [15][16][17] and while numerous solutions have been proposed

[*]Visa, for example, processes around 1,700 transactions per second on average and claims that it could handle more than 24,000 if needed [14]

[18][19][20], as of 2022, there is no network that has achieved all three properties at an adequate degree, with many networks suffering from congestion, high transaction fees [22] and outages [23].

In order to solve the Scalability Trilemma, many blockchains are using variations of Proof-of-Stake (PoS) consensus mechanism. In PoS, nodes have voting power proportional to the amount they have deposited in order to secure the network. The incentive in this case is a consensus participation reward that is proportional to the amount staked. If a node is being dishonest, there are penalties that involve loss of the staked amount. PoS is much less energy-intensive than PoW and allows the network to scale more easily [24]. That also alleviates one of the common criticisms of DLT, that it lacks environmental sustainability. One potential weakness is that the security of the network heavily relies on the price of its coin, and as a result, it's more susceptible to a 51% attack. As the price drops, it's easier for a malicious party to gain majority of the voting power, also known as the "Nothing-at-Stake" problem. Even though solutions to different angles of attack are being proposed [25][26][27], PoS is not as battle tested and is considered less secure than PoW [16].

There's no formal methodology to quantify the degree of decentralization in a network and therefore its security. The number of individual nodes, the distribution of processing power or staked amount in the network and how volatile those elements are over time, need to be taken into account [28]. Moreover, a methodology to determine the weakest point in the network is crucial, especially if there's a chance that a single point of failure exists. A popular metric for blockchains is the Nakamoto coefficient, which calculates the minimum number of entities needed to compromise the integrity of the network [29].

Some believe that the adoption of DLT will bring a new era for the World Wide Web, colloquially known as Web3.0, a term coined by Polkadot creator and Ethereum cofounder Gavin Wood [30]. Web1.0 is considered the period in which the vast majority of internet users were exclusively consumers of content on static webpages and Web2.0 is considered the period in which there was a shift to user-created content including blogs, forums and social media networks. Web3.0 is characterized by trustless, decentralized protocols, user-centric data models, censorship resistance and democratization of finance. Peer-to-peer communication will be the key enabler for the transition to this new generation of the internet.

Potential advantages of DLT such as security, immutability and inexpensive, near instant transactions, are lucrative to companies, institutions and governments that may be indifferent or even opposed to the ideas of user anonymity and decentralization. As a result, private and permissioned blockchains have been developed to increase efficiency. In private blockchains, only authorized participants can join and read, as opposed to public blockchains. In permissioned blockchains only authorized participants, determined by the network operator, can write or commit to it, in contrast with permissionless blockchains [31]. Without the need of a resource-intensive consensus mechanism that promotes decentralization, private and permissioned blockchains are being adopted in different industries, ultimately serving the same purpose as a centralized database.

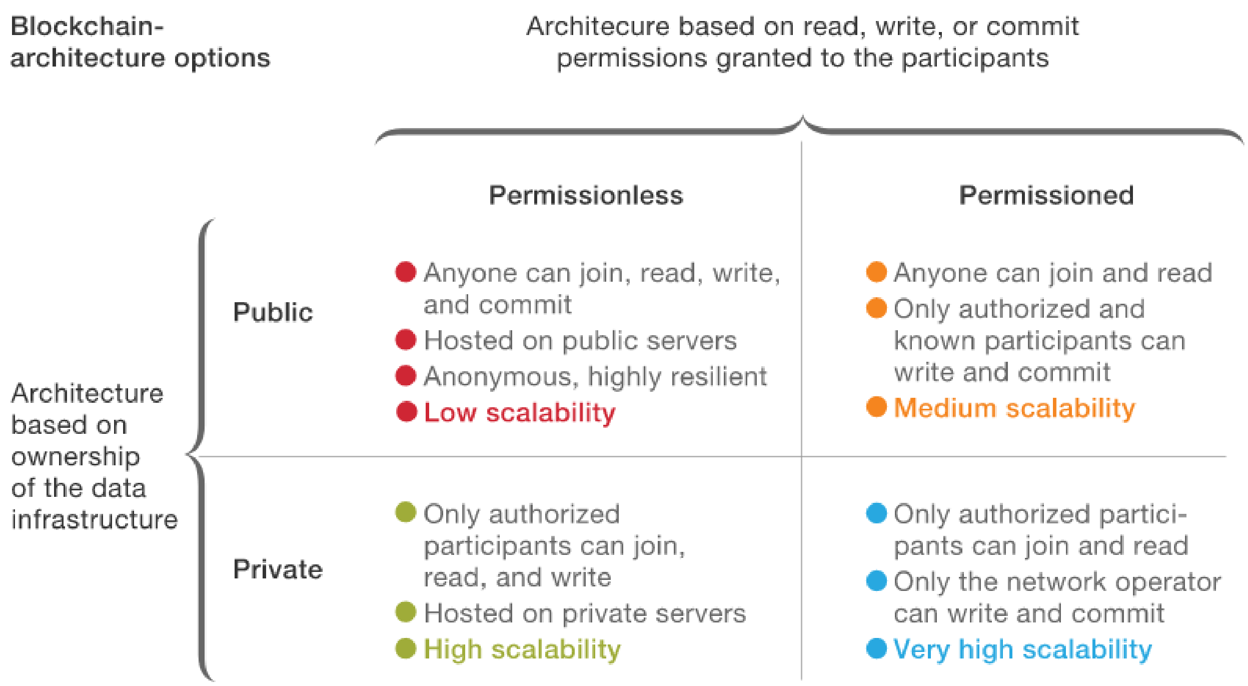


Figure 2: Blockchain-Architecture options [31]

DLT is also the inspiration for the creation of Central Bank Digital Currencies (CBDCs), which are digital representations of state issued sovereign currencies aiming to increase payment efficiency, promote financial inclusion, support financial digitalization and improve monetary policy effectiveness while combating corruption, crime and tax avoidance [32]. Antonopoulos disapproves of the idea, claiming that the removal of cash would turn money into a system of control and surveillance [33].

2. TOKEN DEFINITION AND CHARACTERISTICS

By design, the purpose of Bitcoin and its imitators is limited to that of currency or store of value. Blockchain platforms that support smart contracts, such as Ethereum, have a much broader spectrum of capabilities and an ever-expanding list of use cases. While the technological aspects of the blockchain are the foundations of all applications built on top of it, we need to make a connection with real world usages and traditional economic principles in order to grasp the disruptive potential of DLT.

Before we move forward, it's important to make the distinction between coins and tokens. Both represent value and can be traded for one another and often the terms are used interchangeably. The main difference is that coins operate on their own blockchain, while tokens operate on another coin's blockchain. Therefore, coins are used as currency within the network and their value reflects the value of their native blockchain. Tokens on the other hand, are not only a medium of exchange, but also represent digitalized value that is not limited to purely economic terms. They could represent ownership of a security or commodity, the right to access services or products, right to contribute work, copyright, governance functionality, voting rights, digital identities etc. [21][34].

As DLT is evolving at a fast pace and token use cases are expanding, it's not easy to give an exact definition that encompasses all the properties of tokens. Freni, Ferro and Moncada (2022) define tokens as *quantifiable representations of decentralized and disintermediated trust* [35].

Tokenomics, a portmanteau of "token" and "economics", can be described as the field that studies the value proposition of a project and how that value is captured in its respective tokens. It involves determining the token supply and demand drivers. Considerations include token emission and burning mechanisms[*], token distribution, vesting schedule and investor incentives. The nature of DLT allows for consistent alignment of investor behavior with the project's goals, through tokenomics utilization [35].

Over the last few years, many businesses and startups explored the value proposition of DLT and started building projects utilizing it. The team behind a blockchain based project usually designs a token to complement it, then releases it to the public through an Initial Coin Offering (ICO). An

---

[*] a burning mechanism involves sending tokens to a specified inactive address from which they are irretrievable, permanently removing them from circulation

ICO, similar to an Initial Public Offering (IPO), is a way for the team to raise capital through retail investors, in order to finance its operations. Investors are motivated by the potential value appreciation of the token, its exchange for services offered within its ecosystem and participation in governance. At the same time, the project experiences a network effect through a positive feedback loop where users, investors and developers increase along with the token's price.

The main difference between IPOs and ICOs is the regulatory environment in which they are issued. IPO is a lengthy and expensive legal and compliance process that includes, but is not limited to, a minimum earnings threshold, a good business track record and a prospectus that includes all IPO details that are relevant to an investor. In contrast, ICOs are mostly uncharted territory, regulatory wise. As a result, ICO is a fast and inexpensive process that requires minimal resources and exhibits low entry barriers. Those usually include a smaller team and a whitepaper loosely describing the project, targeted at the investor. Thus, IPOs are issued mainly by established private companies with large capital, while ICOs are issued mostly by startups aiming to reach investors worldwide, without any of the cross-border transaction frictions that normally apply. Another significant difference is that purchasing tokens does not grant ownership of the project or right to dividends. Lastly, IPOs are mostly targeted at institutional investors while ICOs are mainly targeted at retail investors and venture capitalists.

The lack of clearly defined legal and regulatory requirements, combined with its lower cost and simplicity, has led to many ICOs being used as a vehicle for fraud, posing a higher risk to investors. In the U.S., the Securities and Exchange Commission (S.E.C.) is assigned with the task of protecting investors from fraudulent ICOs and determining whether an ICO token should be considered a security, thus falling under the S.E.C.'s jurisdiction to enforce federal security laws. The S.E.C. applies the so-called Howey Test to determine whether an ICO should be considered a security offering. As per the Howey test an ICO token qualifies as a security if it is "*a contract, transaction, or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party.*" [36]. William H. Hinman, S.E.C. Director of the Division of Corporation Finance, stated that a digital asset may no longer represent a security "*if the network on which the token or coin is to function is sufficiently decentralized*", offering Bitcoin and Ethereum as examples. In that sense, a token could change is status of being treated as a security, once its network becomes large enough that there is no central third party whose efforts are a key determining factor in its success [37]. So far, the only token or coin that has been officially declared that it is not a security is Bitcoin, which is considered a commodity by the S.E.C. [38]. Currently, there is no robust definition for what decentralization means, what standards should be obtained for a project to be considered decentralized, what are the factors that affect it, how they are quantified and what the established threshold to regulate a token as a commodity, as opposed to a security, is. Acknowledging that decentralization exists on a spectrum, one could argue that the decisive question is: "Are there specific people or groups of people who, if they suddenly stopped their involvement with the project, the project would no longer be able to function?".

Ideally, the token’s properties are determined in a way that aligns with the team’s vision for the project and its goals. Listed below, are some of the factors that need to be taken into consideration while designing a token:

- Economics: What will the funding of the project look like? What is the initial and total supply of the token? What is the token issuance and burning mechanism? Will it follow an inflationary or deflationary model?
- Incentives: What incentivizes users to hold, spend or use the token? Those include potential for value appreciation, staking rewards, services that can be exchanged or accessed with the token, participation in governance etc.
- Use cases: What are the use cases of the token?
- Initial distribution: How are tokens allocated between the team, private and public investors? Will there be a vesting schedule to ensure gradual token release promoting commitment to the project and discourage immediate selloff after ICO?
- Technical considerations: Will the token be fungible? Is it going to be released in one or more blockchains?

The definition of a token remains somewhat abstract, so classifying them is a complex task that depends on the scope. Adding on the differences of each blockchain, tokens have distinct characteristics related to their technology, use cases, economics, governance, underlying value etc. Even though commonly agreed standards do not exist, previous works have contributed on creating token taxonomy frameworks [34][35][39][40][41][42][43].

3. COMMON CRITICISMS OF DISTRIBUTED LEDGER TECHNOLOGY

Despite potential benefits of DLT, cryptocurrencies are often subject to criticism, related to their environmental impact, unclear regulatory status and dubious economic premise.

3.1 Environmental concerns

As adoption increases, the energy consumption and carbon footprint of the crypto industry are also rising. While reliable and accurate estimations are not easy to make, it is generally accepted that the energy expenditure and carbon dioxide emissions of the Bitcoin network are comparable to those of medium-sized countries. As of October 2022, the Cambridge Center for Alternative Finance estimates that Bitcoin network's energy consumption is approximately 96.6TWh yearly, which amounts to 0.15% of the world's energy consumption. According to the same source, the gold mining industry, Bitcoin's closest physical analogue, consumes 131TWh yearly [44]. Bitcoin, specifically, is considered the least energy-efficient DLT network in terms of energy spent per transaction. At the same time, latest studies show Bitcoin network's yearly emissions of CO_2 ranging between 1.2-5.2 Mt to 130.50 Mt [45]. This broad range is a result of differences in the underlying assumptions and time frames. In addition, there's significant electronic waste coming from the frequent replacement of the hardware used for mining, as soon as its profitability drops. Use of renewable sources of energy and the transition from PoW to more environmental-friendly consensus mechanisms such as PoS, help to alleviate some of the criticism.

3.2 Law and regulations

Critics claim that as long as there is no defined regulatory and legal framework for cryptocurrencies, they can be more easily used for illicit activities, including money laundering, terrorism financing, frauds, hacks, theft, as a medium of exchange on online black markets or as a tool to avoid sanctions. Malicious actors often ask ransom in cryptocurrencies, which provide them a much safer option than cash. Even if an activity is legal, the transaction can be illicit if it involves tax evasion. Much like cash, if a large part of transactions is taking place in the shadow economy, the state's ability to collect taxes is hindered.

Investor protection is also cited, with increasing market capitalization of cryptocurrencies bringing more attention to the industry. Blockchain projects do not undergo the heavy scrutiny of equities and inexperienced investors can fall victim to misleading claims of unrealistic yields. Lack of regulation makes market manipulation in cryptocurrencies easier than in the stock market. Crypto industry's low market capitalization also allows for relatively low transaction volumes causing large market moves. Moreover, even centralized exchanges and platforms are not FDIC insured, so in the case of bankruptcy investors are not protected.

A popular catchphrase, "Code is Law" highlights another gray area of regulation. Smart contracts execute the code exactly as it was written, allowing no room for misinterpretation. This can be a double-edged sword, as any weaknesses in the code can be exploited by malicious actors. Issues arise, such as the relationship between smart contracts and legal contracts and the lack of legal compliance mechanism on DLT [46]. Irreversibility of transactions means that hacks can be detrimental to a platform and imposes certain limits on DLT. Notable examples include the security breach of the Mt. Gox exchange, where hundreds of thousands of Bitcoins were stolen and the infamous DAO hack, which was a defining moment for the Ethereum blockchain. In the case of the DAO hack, the community essentially voted for the restoration of the blockchain in a previous state, before the hack, in order to return the 3.6 million stolen ETH (10% of supply at that time) to the DAO. Those who did not agree with the decision on moral grounds, citing censorship, continued building blocks on the original blockchain. This caused the hard fork of the blockchain and the creation of a sister blockchain, called Ethereum Classic. In order to solve legal complications, efforts are being made by legal scholars and computer scientists to create smart legal contracts, which are smart contracts that are legally enforceable [47].

Furthermore, numerous scams or mistakes of smaller magnitude cause individuals to lose their tokens on a daily basis. Irreversibility of transactions makes this loss of funds permanent. This means that the computer literacy entry barrier of the crypto industry is quite high. In the case of mainstream adoption, one would expect most users to continue to rely on intermediaries, in order to keep their funds safe. Moreover, one cannot expect to tokenize the ownership of an asset, such as a car or real estate, without any authority that he can appeal to, in case of theft or loss of the respective tokens.

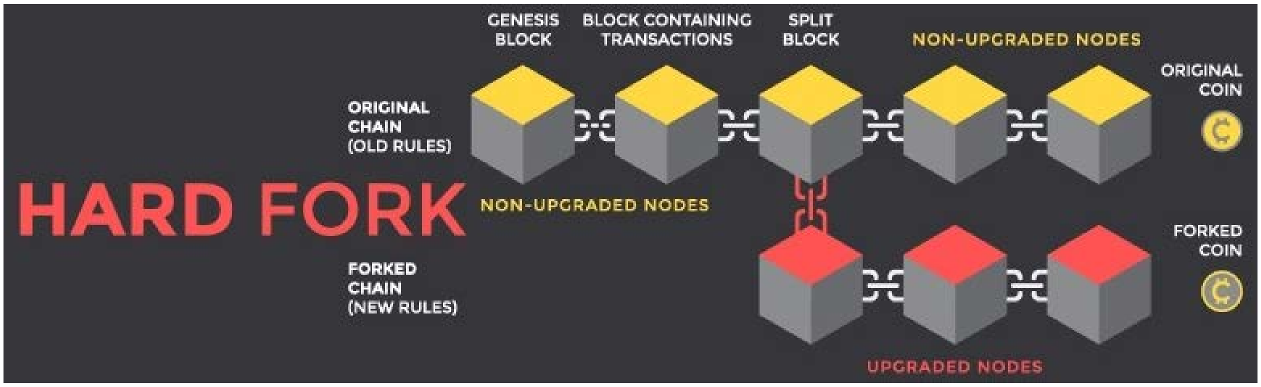


Figure 3: A blockchain hard fork (source: financemagnates.com)

Regulatory implications of cryptocurrencies include restrictions on ownership, mining and trading, taxation frameworks, Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) procedures. Compliance efforts focus on centralized exchanges which operate as on-ramps and off-ramps for fiat currencies and cryptocurrencies. These exchanges cooperate with authorities and flag transactions depending on their source and size. Countries, depending on their economic policy and system of government, impose restrictive, endorsing or neutral regulations to cryptocurrencies. Notable examples include a complete cryptocurrency mining and trading ban in China and Bitcoin's acceptance as legal tender in El Salvador and the Central African Republic. As discussed earlier, token classification as currency, security or commodity will be required in order to create a regulation and taxation framework to tackle the complications that DLT brings.

3.3 Economic premise and intrinsic value in cryptocurrencies

Skeptics, often refer to the cryptocurrency industry as a speculative bubble [48][49][50], comparable to the dot-com bubble, citing its extreme volatility, scams (Ponzi schemes, pump and dump schemes, project rug pulls), unsustainable yields and documented cases of projects failing to live up to expectations. They suggest that prices are primarily driven by greed or fear, not by a project's fundamentals. Ultimately, at the core of this debate lies the question: "Do tokens have intrinsic value, and if so, how can this value be assessed?"

The heated debate on the intrinsic value of tokens is no coincidence. The nature of cryptocurrencies challenges well established economic concepts and the definitions of money, intrinsic and extrinsic value. These definitions were neither written in stone nor are they universally agreed upon. Over the centuries, they gradually adapted, maintaining an equilibrium at all times, rendering any debate over the semantics more philosophical than practical. The invention of Bitcoin, shook the established financial system in a way that cannot be ignored, provoking declarations of condemnation or worship.

The Oxford Handbook of Value Theory defines intrinsic value by contrasting it to extrinsic value: "*The concept of intrinsic value has been glossed variously as what is valuable for its own sake, in itself, on its own, in its own right, as an end, or as such. By contrast, extrinsic value has been characterized mainly as what is valuable as a means, or for something else's sake*"[51]. In a more finance-specific approach, intrinsic or fundamental value could be defined as the measure of what an asset, in this case a token, is worth. The distinction between intrinsic and extrinsic value is not always obvious. Treiblmaier, citing pragmatist John Dewey, argues that intrinsic value is not an absolute, but rather a relative property that is contingent on a specific situation [52][53]. No matter what the methods, financial models and underlying assumptions behind the intrinsic value estimate are, it is likely that the intrinsic value is nowhere near the market value at any given time.

At the moment, there is no agreed upon framework for token valuation. Moreover, until the complications and obstacles DLT encounters are straightened out, the majority of cryptocurrency projects will be far from offering an end product that can achieve mainstream adoption. Typically, the team behind a project publishes a roadmap containing upcoming milestones for the following months or years[*]. As a result, any estimation for a token's intrinsic value heavily relies on the project delivering on its promises. On top of that, crypto market sentiment is often dictated by FOMO (Fear Of Missing Out) or FUD (Fear, Uncertainty, Doubt). While estimating the intrinsic value of a stock is a challenging task in itself, the nature of the crypto industry makes it even harder to perform fundamental analysis on a token.

Going one step further, numerous prominent figures in the finance world, including Nobel laureates and scholars, have questioned the existence of intrinsic value in tokens and if they have actual use

[*]Interestingly, there are project teams that refrain from publishing a roadmap, to avoid taking responsibility of the project's fate in the eyes of investors, which could cause their token to be labeled as security by the S.E.C.

cases. Criticism is often directed towards Bitcoin, since it is the most recognizable cryptocurrency, however, many of the concerns are extrapolated towards other tokens as well.

Nobel laureate Nouriel Roubini, suggests that: "*As a currency, bitcoin should be a serviceable unit of account, means of payments, and a stable store of value. It is none of those things. No one prices anything in bitcoin. Few retailers accept it. And it is a poor store of value, because its price can fluctuate by 20% to 30% in a single day*". Nobel laureate Robert Merton, mentions that: "*The only possible legal tender currency is one controlled by government. Fiat but legal tender currencies actually have intrinsic value because by law they can be used to settle all tax and other payments to the government and they MUST be accepted as payment for obligations denominated in that currency*", adding that: "*Bitcoin is not a government-controlled currency. Who is responsible for the value of our currency if tomorrow morning all the bitcoin screens go dark?*". Warren Buffett, chairman and CEO of Berkshire Hathaway, concluded that: "*Cryptocurrencies basically have no value. You can't do anything with it except sell it to somebody else*", a belief shared by Microsoft co-founder Bill Gates that considers cryptocurrencies a phenomenon "*100% based on greater fool theory*". Charlie Munger, vice chairman of Berkshire Hathaway, has been extremely critical on Bitcoin noting that "*It's like somebody else is trading turds and you decide you can't be left out.*" and labeling it "*worthless artificial gold*". Nobel laureate Joseph Stiglitz, considers Bitcoin "*successful only because of its potential for circumvention [and] lack of oversight*", suggested that: "*There is no need for anybody to go to a cryptocurrency*" and asked for cryptocurrencies to be shut down [54]. Bank of England governor Andrew Bailey, made the distinction between intrinsic and extrinsic value arguing that cryptocurrencies "*have no intrinsic value.*" Before adding: "*That doesn't mean to say people don't put value on them, because they can have extrinsic value. But they have no intrinsic value*" [55].

4. THE CASE FOR INTRINSIC VALUE IN CRYPTOCURRENCIES

Previous works have made the case for the existence of intrinsic value in cryptocurrencies [5][56] and others have attempted to create a valuation framework [57][58].

Before making my case on the intrinsic value debate, it would be helpful to classify tokens in different categories. For the purposes of determining the existence of intrinsic value, I classify tokens in 3 categories, taking into consideration what the underlying value of the token in each case is. This classification also includes coins, according to the definition mentioned earlier, as the distinction between coins and tokens is a rather technical one.

1) *Asset tokens*: They represent ownership of an underlying physical, digital or legal asset. Examples of those tokens are tokens pegged to fiat currencies like USD, commodities like gold, wrapped Bitcoins (tokens whose price is pegged to the price of Bitcoin, native to a blockchain in which Bitcoin is not native) and certain NFTs.
2) *Utility tokens*: They are used in exchange for goods and services (i.e., utility), within an ecosystem. They can give the right to work, vote or access services, they can be used as a means of payments within a network, be a part of the consensus mechanism or play a role in governance. They usually serve a significant role in the funding of a project through ICOs, that's why they are often called ICO tokens.
3) *Currency coins*: They are the native assets of a blockchain and their main purpose is to serve as means of exchange.

Clarification: Depending on the definition, the native assets of blockchains are coins, usually called cryptocurrencies. However, in the case of blockchains that have smart contract capabilities such as Ethereum and Cardano, the respective coins, in this case Ether and Ada, have utility that goes beyond that of a currency within their network. As a result, their intrinsic value is based on the same elements as that of a utility token.

4.1 Asset tokens

The most recognizable tokens in this category are those whose price is pegged to that of a fiat currency or commodity, called stablecoins. The most popular stablecoins are pegged to the U.S. Dollar. Other notable stablecoins include tokens pegged to the Mexican Peso, the Euro or gold-backed tokens such as PAXG. As mentioned before, some of the use cases of DLT are as simple as peer-to-peer transactions, whether that is remittances, micropayments or service fees. As DLT grew in popularity, the need for a token that does not experience the volatility of Bitcoin or similar cryptocurrencies grew larger.

The premise is simple: An organization mints tokens that are digital representations of the USD on the blockchain. At any moment, that organization holds reserves of at least equal total value denominated in USD, as the total value of tokens in circulation. Whenever someone wants to convert the token to USD or vice versa, the institution makes the conversion for a small fee. That organization is usually centralized, as is the case with USD Coin (USDC), Tether USD (USDT) and Binance USD (BUSD). There are also cases of decentralized stablecoins such as DAI, which is minted by the Maker DAO and is over-collateralized by other cryptocurrencies in the DAO's vault. In the case of the collateral value dropping between a minimum ratio, the collateral is liquidated in order to keep the peg. Algorithmic stablecoins are a unique case of stablecoins, that are not backed by anything, but hold their peg through an arbitrage mechanism. So far, algorithmic stablecoins have been proven unreliable, with the notable case of Terra USD (UST) where around 45 billion USD in market capitalization were wiped within a week after UST lost its peg, causing a death spiral to its ecosystem's tokens.

Wrapped crypto tokens are tokens pegged to the price of another token, that exist in a blockchain in which the second token is not native to. This allows the wrapped token to be traded, borrowed or lent in a different blockchain than its underlying token. Wrapped assets are useful, as interoperability between different blockchains is still at its infancy.

Non-Fungible-Tokens (NFTs) are often used to denote ownership of assets that are not fungible. Fungibility refers to the ability of a token to be interchanged with another token in reference to its value, so it implies that the value between the tokens is equal. Bitcoin is fungible, which means that it can be interchanged with another Bitcoin. The same principle would apply if we intended to interchange two 10 USD notes. NFTs cannot be interchanged based on their value. A real-world example are diamonds, where the presence of miniscule differences in quality, even if two are almost identical, means it's practically impossible to find two diamonds of equal value. NFTs represent ownership of assets that are unique or have limited quantity, such as art (physical or digital), tickets, collectibles, intellectual property and legal contracts. NFTs do not necessarily represent ownership, but they can also have use cases in supply chains, healthcare, digital identification, voting platforms and the gaming industry. Fungibility is a technical, not economical, property of a token, therefore NFTs that are not asset tokens, can be considered utility tokens as described below.

Practically, anything of value such as commodities, securities, real estate, intellectual property etc. can have a digitalized representation that denotes its ownership. I claim that, as long as the underlying asset has intrinsic value, then the token that represents ownership of that asset has intrinsic value.

4.2 Utility tokens

Utility tokens possess diverse properties and perform a wide range of functions within their ecosystem. If DLT is the backbone of a dApp, utility tokens are the driving force that brings dApps to life. If blockchain applications have intrinsic value, then the respective utility tokens must also have intrinsic value. It is impossible to list all potential utility token usages; capabilities are endless. It's the never-ending human creativity and inventiveness that will shape Web3.0 as DLT pioneers envisioned it.

The following is a non-exhaustive list of existing and potential decentralized applications:

- DeFi applications: non-custodial asset management dApps (wallets), financial derivatives, decentralized marketplaces which utilize automated market maker (AMM) protocols, data marketplaces, insurance services, token mixing services, cross-chain swaps through the use of bridges etc. [59][60][61].
- DAOs: Organizations which operate through a decentralized government system and perform actions automatically. Just a few of its use cases are: investing, (crowd)funding, dApp governance, lending services, lobbying and activism [62][63].
- Compliance applications: Those include KYC, KYT (Know-Your-Transactions), AML and CFT (Combating-the-Financing-of-Terrorism) applications that achieve increased security through cryptography.
- Identity management: Using non-transferable "soulbound" tokens in order to store credentials, academic records, employment history etc., bound to a pseudonym, without revealing the user's true identity [64].

- Decentralized file storage: Cryptography minimizes the risk of security breaches and ensures data privacy.
- Distributed computing: Horizontal scalability offers low cost, efficient computing with no single point of failure.
- Gaming: Decentralized videogames that can utilize NFTs in the form of collectibles.

In cases where decentralization is not desired, industries that can benefit from DLT, using private and/or permissioned blockchains include:

- Banking & fintech: Immutable data storage deters corruption and fraud, increasing transparency. DLT networks allow for efficient and fast cross-border transactions, with near instant settlement [65].
- Healthcare industry: Storing patient records with improved security and data privacy.
- Supply chains: Improving transparency and traceability while alleviating information asymmetry [66][67].
- Other industries include: Transport, logistics, media, telecommunications, insurance, manufacturing, art, retail etc.

DLT is by no means a be-all and end-all solution for any problem that arises in these industries. For example, high remittance fees and delays are not caused by technological limitations, but they are a result of regulatory compliance and other socioeconomic factors. If anything, DLT maximalists allow level-headed, balanced perspectives to give way to fanatic, reactionary opposition.

In any case, it cannot be denied that blockchain offers advantages in certain areas, even if it is inefficient in others. The fact that it has unique use cases and potential to improve on existing technology, in numerous industries that constitute a large part of today's economy, shows that there is value in DLT networks. Consequently, I conclude that utility tokens have intrinsic value.

4.3 Currency coins

The initial purpose of Bitcoin was to serve as currency, even though the narrative has slowly shifted towards it having better use as a store of value. Numerous tokens have appeared in the last years, aspiring to become the dominant cryptocurrency and promising fast, cheap, secure, frictionless and borderless transactions. Their supporters claim potential adoption that ranges from a parallel digital cash economy to replacing sovereign currencies, on a global scale. Even if the latter scenario seems far-fetched, the main question that arises is: “Can a token be used as a form of currency?”.

Mankiw describes the main functions of money [68] (and therefore currency) as:

- Store of value: One expects to be able to trade it for goods and services at any time in the future.
- Unit of account: A measure of market value of goods, services and debt.
- Medium of exchange: It is generally accepted for buying goods and services or servicing a debt, one can be confident that he can easily exchange money for an asset or vice versa.

It’s safe to say all tokens, Bitcoin included, have failed to perform these functions. Their extremely high volatility, compared to that of fiat currencies, means that prices of assets denominated in cryptocurrencies fluctuate daily by a significant amount. On the contrary, the purchasing power of fiat currencies is orders of magnitude more predictable than that of cryptocurrencies [69]. This means that no token, at least for now, can be considered a store of value.

It is also evident that cryptocurrencies are very far from being widely accepted as a unit of account or medium of exchange. On that note, Paul Krugman points out that “*the value of a dollar doesn’t come entirely from self-fulfilling expectations: ultimately, it’s backstopped by the fact that the U.S. government will accept dollars as payment of tax liabilities—liabilities it’s able to enforce because it’s a government. If you like, fiat currencies have underlying value because men with guns say they do*”. Inadvertently, Krugman highlights the fact that citizens, essentially, do not have a choice on which currency to use in their daily lives and it is up to the jurisdiction of their government to decide on which currency to adopt as legal tender [52]. Such examples are El Salvador and Central African Republic, which recently determined Bitcoin as legal tender [70][71], a decision that was not unanimously well received [72][73].

Geoffrey Ingham emphasizes the existence of social conventions implied in the use of money, suggesting that: “*All money is constituted by credit-debt relations - that is, social relations*” [74]. On a similar note, Lippert argues that “*Value is a social relationship that is formed on the social level between exchange partners*” [75]. This suggests the possibility of a socially backed currency, that holds value as long as a sufficient number of people believe that it holds value. As the adoption as a means of payment grows, the impact of speculators will drop and the price volatility will be small enough to allow for it to be used as medium of exchange and store of value [76].

The common element in these approaches is trust. Money is not just gold, paper or lines of code, it is ultimately trust in a system. Fiat currencies that are legal tender have intrinsic value because governments are trusted to keep accepting them for taxes. In the same vein, cryptocurrencies have value because people are trusted to keep using them for transactions. That trust is reinforced by game theory incentives that prevent bad actors from emerging, their open-source code that greatly reduces the possibility of a backdoor exploit compromising the network's integrity and the fact that no centralized entity can shut down the network.

Another case for the existence of intrinsic value could be provided if Merton's argument for Bitcoin losing its value "*when all bitcoin screens go dark*" gets flipped. The network requires hardware to run on and energy to be powered by. Consequently, their intrinsic value is indication of intrinsic value in the respective token. If miners stop providing value through their efforts and production costs, the network stops and transactions are no longer possible. Therefore, I conclude that a decentralized peer-to-peer network of transactions, that uses a currency that does not rely on trusting a third party to prevent its debasement, must have non-zero intrinsic value.

5. TOKEN VALUATION FRAMEWORK

Once the existence of intrinsic value is asserted, a framework for its evaluation can be designed. The same taxonomy will be used and different valuation methods will be applied for each token category.

I will refrain from using market capitalization for comparative analysis between cryptocurrencies, as I consider it an inaccurate metric for their true value. Market prices are driven by speculation and sentiment. Studies have shown positive correlation between the stock market and the crypto market [77] and as is the case with equities, market value does not equal intrinsic value. Studies have also found positive correlation of price movement between cryptocurrencies [78].

Moreover, the price of a token is affected by its liquidity. Market capitalization is calculated using the last transaction price, but there is often not enough market depth to facilitate large transactions in that price. In cases of low liquidity, market capitalization can be inflated and does not reflect the market price that a large quantity of tokens could be sold at. It's also common for project teams to hold a percentage of token supply, essentially removing it from circulation. Finally, lost tokens or tokens kept as long-term savings also affect liquidity and need to be accounted for.

5.1 Asset tokens

Asset tokens are fully collateralized by physical, digital or legal assets. In this case, the value of the token is practically equal to the value of the underlying asset. Traditional valuation methods could be applied to estimate the intrinsic value of those assets and their respective tokens.

In the case of NFTs that represent ownership the same method can be applied, even in the cases where value is difficult to quantify, such as collectibles or art. NFTs that do not represent ownership have different use cases and can be considered utility tokens.

It should be noted that until a regulatory authority imposes strict rules and requirements on the issuance of asset tokens, there is a certain counterparty risk involved in holding them. As an example, we can examine a cross-chain bridge whose purpose is to allow usage of a token on a different blockchain than its native. The bridge locks the tokens in a smart contract in their native blockchain and mints and the same amount of tokens on the destination blockchain. When the user wants to use the tokens in the native blockchain, he burns the newly minted tokens and the original tokens get released, essentially not affecting the circulating supply. Unfortunately, there have been occurrences where a hacker found vulnerabilities in the bridge code, essentially allowing them to steal all underlying assets. A recent example was the Wormhole bridge hack on the Solana network, in which at least 93,750 ETH were stolen [79].

Similar risks can be found whenever there are smart contracts involved, as code cannot be infallible. Risk magnitude depends on the developer team and code complexity and can be assessed by a certified security auditor. Additionally, whenever there is a company issuing asset tokens, there is an added business risk compared to holding the asset itself. Business risk can be evaluated using traditional methods. Therefore, I propose a discount on the asset token's intrinsic value compared to the asset itself.

5.2 Currency coins

A currency token, past its early adoption stages, is no longer a speculative asset and its price volatility is similar to that of fiat currencies. As a form of money, it is subject to the Quantity Theory of Money (QTM) and the intrinsic value of the token can be approximated with the equation of exchange. Existing literature has been both in favor [80][81] and against [82][83] this approach.

Equation of Exchange

Based on the QTM, the equation of exchange can be written as:

$$M \cdot V = P \cdot Q \quad (1)$$

where:

- M is the total money supply in circulation, on average, within a specific time frame,
- V is the average money velocity in that time frame,
- P is the average price level in that time frame,
- Q is the total volume of goods and services transacted in that time frame.

Moreover, the fair price of a token p could be calculated as:

$$p = \frac{1}{P} \quad (2)$$

And from equations (1) and (2) we derive:

$$p = \frac{Q}{M \cdot V}$$

As discussed earlier, usually, not all tokens are issued from the beginning, with a percentage being hold in reserves by the team. Taking into account the percentage of tokens in circulation compared to the total token supply we get:

$$p = \frac{Q}{M_{max} \cdot f \cdot V}$$

where:

- M_{max} is the maximum token supply as determined in the protocol,
- f is the number of tokens in circulation M divided by the maximum token supply M_{max}.

Percentage of tokens in circulation f: Tokenomics, such as issuance rate, vesting schedule, burning mechanisms etc. are usually known in advance, either being public on the blockchain or published by the project team. This means that f can be estimated with a fairly good accuracy. In order for a currency to achieve low volatility, f ratio should not fluctuate vastly.

Money velocity V: Money velocity denotes the average number of transactions in a specified period of time. A token being used as a currency implies that volatility in the daily transaction number is relatively low, so a one-year time frame would be a logical choice.

Total Volume of Goods & Services: Estimating total expenditure is a very problematic task. Sending tokens from one address to another does not necessarily imply that goods and services were exchanged for them, and even if they were, it would be impossible to measure their total volume. Alternatively, one could estimate the total transaction volume of a cryptocurrency as a share of the total economic demand. Finally, the formula is:

$$p = \frac{D \cdot r}{M_{max} \cdot f \cdot V}$$

where:

- p is the fair price of a token,
- D is the total economic demand, namely global GDP, in a specified time frame,
- r is the share of the total demand met by a specific cryptocurrency compared to all available currencies in the specified time frame,
- M_{max} is the maximum token supply as determined in the protocol,
- f is the average number of tokens in circulation in the specified time frame M divided by the maximum token supply M_{max},
- V is the average money velocity in the specified time frame.

A cryptocurrency's market share r is a measure of its adoption. One would first estimate the percentage of demand met by cryptocurrencies, out of the total demand met by currencies. Then he would estimate the market share of a specific cryptocurrency, out of the total demand met by cryptocurrencies. Essentially, he would have to estimate, both the adoption of cryptocurrencies in general and the competition within the industry. Predicting either of them involves a significant margin of error, as it requires intuitively quantifying adoption parameters.

Applying time and risk: The model above calculates the value of a token at a given time. As there is no token at the moment that functions as currency at a large scale, it would make sense to calculate the present value of a token at a future time. A discount would be made, taking into account the time value of money, using the risk-free interest rate. A second discount should also be made, in order to quantify the risks mentioned above, both for the crypto industry and the specific token. Entering this uncharted territory, any quantification should be approached very cautiously and be continuously realigned to reflect newer data. Sensitivity analysis is essential for all possible scenarios.

Effective circulating supply: Tokens in long-term savings or tokens lost are effectively removed from the circulating supply. This includes tokens owned by retail or institutional investors who speculate on the price of the token over a long-term horizon and tokens that are forever inaccessible, because of lost wallets or keys. While the percentage of these tokens cannot be precisely calculated, on-chain analysis of long-time inactive addresses could help in creating probability scenarios. Staked tokens, depending on the lockup period, are also not a part of the circulating supply. Following up, sensitivity analysis could be applied to quantify the effect of tokens removed from circulation on the value of the token.

5.3 Utility tokens

The same valuation framework can be applied both for utility tokens and coins native to blockchains that have utility, by supporting smart contracts. NFTs that do not represent ownership of an underlying asset, but have some kind of utility are also included in this category.

The value of a network consists of two parts:

1) *Value derived from current utility* V_u: This value reflects the current state of the network.
2) *Value derived from expected growth* V_g: This value reflects expected future growth of the network.

The value of the network is simply:

$$V = V_u + V_g$$

Respectively, the fair price of a utility token can be derived:

$$p = p_u + p_g$$

where:

- p is the fair price of the utility token,
- p_u is the part of the fair price of the utility token that can be attributed to its current utility,
- p_g is the part of the fair price of the utility token that can be attributed to the network's expected growth.

On first glance, valuating a token based on an increasing number of its buyers might seem to reinforce Bill Gates' greater fool theory. A stock's intrinsic value is estimated, based on the goods and services the company expects to sell. Tokens have intrinsic value because they can be directly exchanged for goods and services within their ecosystem. Increased demand for the token leads to lower price level in the ecosystem, which means that more goods and services can be exchanged for the same number of tokens. Value attributed to growth does not come from expecting to sell the token to a "greater fool", but from the expectation that utility "gained" per token will be increased. Unlike stocks, if the expected future cash flows are zero, there is still intrinsic value in the token, as long as the network is active.

Depending on the stage of a network's lifecycle, value attributed to expected growth can be positive, zero, if the network has reached equilibrium, or even negative if its user base is expected to decline. In the latter case, a subtraction from the value attributed to current utility must be made.

5.3.1 Current utility

Below are shown two different methods to approach the fair price of the token that can be attributed to its current utility p_u.

<u>*Implicit value*</u>

All the benefits acquired by holding, staking, spending or burning the token can be named utilities of the token. A token's value is equal to the intrinsic value of these utilities. Utility tokens can be either fungible or non-fungible.

A simple approach suggested by crypto.com is based on quantifying the intrinsic value of utilities that can be exchanged through a token [84]. Using this approach, we derive:

$$p_u = \frac{U_1 + U_2 + \cdots + U_n}{N}$$

where:

- p_u is the fair price of the token that can be attributed to its current utility,
- U_i is the intrinsic value of utilities in exchange for holding, staking, spending or burning tokens,
- N is the number of tokens required to gain access to these utilities.

Applying time: Those utilities may be accessible anytime, may be unlocked in some future time or may last a certain period of time. If a certain utility is not accessible in the present, the time value of money needs to be accounted for, a discount is required.

<u>*Equation of Exchange*</u>

All utilities in an ecosystem can be denominated in its native token, thus we can say that a utility token acts as currency within its ecosystem [85]. Similar to currency tokens we can use the equation of exchange:

$$p_u = \frac{D \cdot r}{M_{max} \cdot f \cdot V}$$

where:

- p_u is the fair price of a token that can be attributed to its current utility,
- D is the total economic demand for a particular market in a specified time frame,
- r is the share of the total demand met by the token compared to all available tokens in the particular market in the specified time frame,
- M_{max} is the maximum token supply as determined in the protocol,
- f is the average number of tokens in circulation in the specified time frame M divided by the maximum token supply M_{max},
- V is the average money velocity in the specified time frame.

The economic demand for a particular market D depends on the platform's or application's utility. One example are oracles, entities which allow for communication between the blockchain and external systems. We would first need to estimate the total demand for oracles in the market, then find a specific oracle's market share e.g. Chainlink's. In the case of a blockchain that supports smart contracts, as Ethereum, competitors for the market share are blockchains that have dApp capabilities, like Cardano, Solana and Algorand.

Utility tokens, being in a stage of growth, may exhibit higher volatility than currency coins. Consequently, the time frame for estimating money velocity V, economic demand D etc, ratio f and market share r could be much shorter than a year, depending on project specific and macroeconomic factors.

As detailed before, tokens lost, staked, kept in a platform's treasury or in long-term savings, are effectively removed from circulation and need to be accounted for.

5.3.2 Expected growth

A network in its early stages will keep growing, until adoption peaks and the user base is relatively stable. The evaluation of expected network growth could be performed using a DCF model, similarly to a company. A typical company estimates revenue and future cash flows in order to get a fair valuation of its stock. In the context of a blockchain project, flow of capital comes both from new users of the network and from investors speculating on the token's price. This leads to increased market capitalization and token price appreciation. While the approaches are similar, it is evident that the novelty of cryptocurrencies does not allow for as confident results as traditional company valuations. Existing literature highlights the difficulties of applying DCF valuation to cryptocurrencies [86][87][88].

The discounted cash flow of year t DCF_t is estimated as:

$$DCF_t = \frac{CF_t}{(1+i)^t}$$

where:

- CF_t is the cash flow to the project for year t,
- i is the discount rate, equal to the risk-free interest rate.

The present value PV of the project can be estimated by aggregating all DCF for n years.

$$PV = \sum_{t=1}^{n} \frac{CF_t}{(1+i)^t}$$

We cannot get the token price simply be dividing PV by the token supply, because supply is time-dependent. However, we could write:

$$p_g = \sum_{t=1}^{n} \frac{CF_t}{(1+i)^t \cdot M_t}$$

where:

- p_g is the part of the fair price of the utility token that can be attributed to the network's expected growth,
- M_t is the average token supply in circulation in year t.

In the case of a PoS network, staking tokens earns yield so we get:

$$p_g = \sum_{t=1}^{n} \frac{(1+y)^t \cdot CF_t}{(1+i)^t \cdot M_t}$$

where y is the annual percentage yield (APY) that token holders earn as a reward from staking.

At any time, only a fraction of total supply is being staked. Along with a possible burning mechanism, that means that APY should not necessarily equal the inflation rate. For more accuracy, we could consider the cost of energy and hardware maintenance required for staking or the commission earned by a staking pool or centralized platform that provides staking services. That cost or commission should be then subtracted from the APY.

$$y^* = y - c$$

where:

- y^* is the effective APY,
- c is either the cost of energy and hardware required or the commission earned by an intermediary.

Token circulating supply at a given time depends on the network's tokenomics. As discussed above, issuance mechanisms and vesting schedules are usually public. However, unlike Bitcoin, not all networks have entirely predictable issuance rate. PoS blockchains issue tokens as a reward for staking, but the percentage of tokens staked is not constant. In any case, issuance rate can be estimated with sufficient accuracy. Token burning is usually proportionate to the number of transactions, which gets increasingly difficult to predict, the more distant the time frame gets. Moreover, developers or community can, at any time, decide on a change in tokenomics. One example is Ethereum's EIP 1559, a proposal which passed in August 2021, which introduced token burns in the network's transaction fee mechanism [89]. Another radical change in Ethereum's tokenomics was its transition from PoW to PoS consensus mechanism on 15 September 2022.

Estimating cash flows for the following years is the most daunting part of this evaluation process. Crypto industry is heavily affected by macroeconomics and its market capitalization shows strong correlation with the stock market. Updates, unexpected setbacks and new project launches play an important role in competing platforms and may drive cash flows from one chain to another. Crypto investors are willing to take more risks than traditional investors and certain market moves have been result of social media trends and hype [90][91]. Regulatory frameworks in different jurisdictions are constantly evolving. All those parameters make forecasting future cash flows extremely challenging.

In order to arrive at an adequate approximation on a project's value, thorough analysis should be conducted on three levels.

1. Crypto industry's position in the global economy should be assessed. What will the consensus about cryptocurrencies in the upcoming years be? How substantial will crypto adoption be in the long term? What will the regulatory and taxation framework look like?
2. Blockchain's potential in a specific market should be examined. Do the advantages of using DLT in a specific case outweigh the disadvantages, and if so, can the effect be quantified? Is there an actual use case in a field or is DLT or does existing technology function better? How will blockchain affect in the industry be in the future? What is the current state of competition in the industry?
3. Project specifics should be considered. What is the team behind the project, what are their background and past ventures, how committed are they? Will more funding rounds be required? If so, under what circumstances? What is the degree of decentralization in the present, and how is it expected to change in the future? What are the project's strong points, what problems does it solve? What are its weaknesses?

As discussed previously, holding tokens does not grant a share in the project. This is why the token's value does not include any parameters related to the developing team's assets and infrastructure. However, it is evident that all projects in their early stages are fairly centralized, both in terms of token allocation and in terms of dependence on a specific group of people. Thus, I propose a discount, to take into account this increased counterparty risk. Once the network is sufficiently decentralized, this risk is minimized. I argue that, at the moment, only Bitcoin network is decentralized enough to render this risk insignificant.

5.4 The unique case of Bitcoin as store of value

Bitcoin was originally invented as a currency. The Lightning Network (LN), a second layer protocol that enables micropayment channels, was invented as a Bitcoin network scaling solution that enables fast transactions [92]. LN's first large scale implementation was in El Salvador, when Bitcoin was made legal tender.

However, Bitcoin's main utility has, for the most part, moved from being a medium of exchange to being a store of value. Reasons are its non-negligible transaction costs, inconveniently long settlement time and its non-inflationary nature.

Comparative Analysis

As a possible inflation hedge, a safe-haven in turbulent times, it is often compared to gold. An intrinsic value for Bitcoin could be derived if we used comparative analysis for Bitcoin and gold. According to the World Gold Council the total amount of gold mined is approximately 205,238 tonnes [93]. With gold price at around 1,735 USD per ounce, gold's market capitalization is approximately 12.5 trillion USD. Assuming that Bitcoin reaches the same market capitalization and dividing by Bitcoin's maximum supply we reach a price of around 600,000 USD for each Bitcoin.

This estimation is extremely speculative and certain considerations need to be made:

- The assumption that Bitcoin's market capitalization will equal that of gold is completely arbitrary. Gold place in the global economy is unique and has deep historic roots. Gold's intrinsic value is still unclear, with the majority of demand coming from the jewelry industry, investments and central banks, with a small percentage coming from its application in technology [94].
- Bitcoin's adoption as a safe-haven will be largely determined by the degree of adoption of DLT. Even so, the fact that Bitcoin does not have everyday use cases, as utility tokens do, means that its adoption will be mostly driven by sentiment.
- Bitcoin is considered a risk-on asset and exhibits positive correlation with the stock market [95] and no correlation with gold [96], thus, at the moment, it cannot be considered an inflation hedge.

Stock to Flow Model

Stock to flow (S2F) model aspires to make a connection between the value of commodities and the growth rate of their total supply. S2F ratio is calculated by dividing a commodity's total supply with the new annual supply flowing in the market.

$$S2F\ ratio = \frac{total\ supply}{annual\ flow} = \frac{1}{supply\ growth\ rate}$$

High S2F ratio implies a lower supply growth rate in relative to the existing supply and vice versa. Consumable goods have low S2F ratio because the existing supply is constantly consumed. Moreover, they have volatile market value, because their supply and demand are also volatile. In contrast, commodities such as gold and silver have high S2F ratio, as the supply constantly grows and should, theoretically, retain their value as their supply growth rate slowly drops. Applying regression analysis to model such an asset's market capitalization based on its S2F ratio, one could theoretically predict the asset's future price.

As an indestructible asset, a similar model could be applied to Bitcoin [97], with the added benefit that its S2F ratio is known, not only for the past, but also for the present and the future. Morillon and Chacon showed evidence that there is a relation between Bitcoin's price and its S2F ratio and that the model's accuracy increases over time [98].

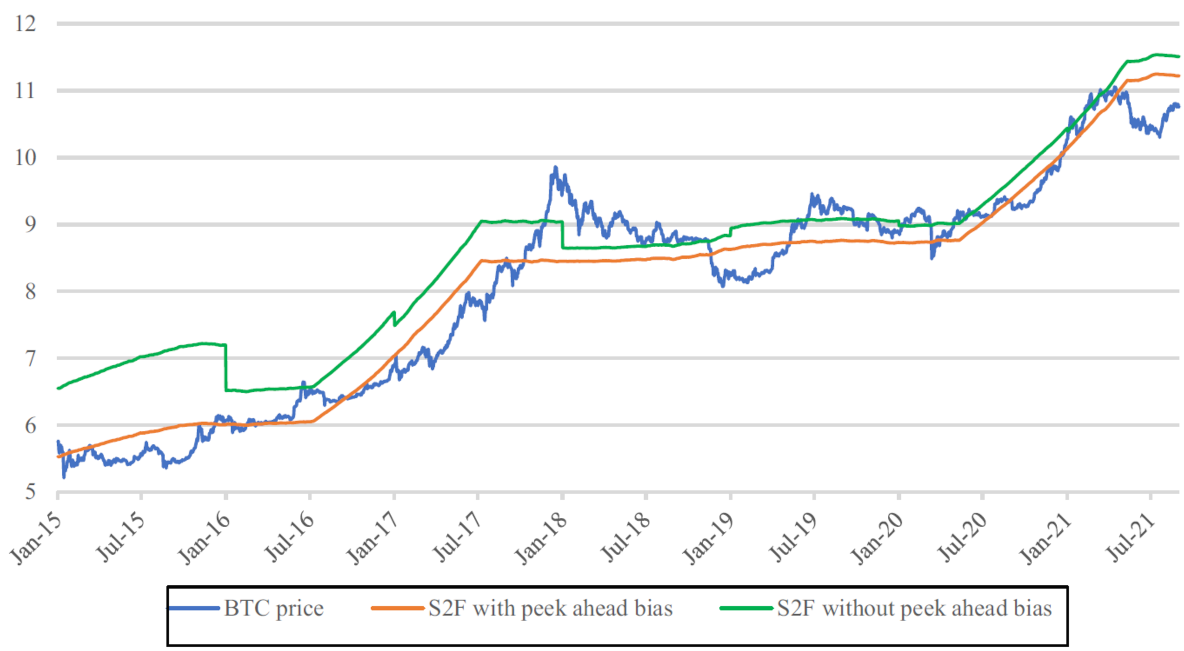


Figure 4: Comparison of the price prediction of the original S2F model with the peek-ahead bias (orange) to the prediction of the S2F model without peek-ahead bias (green) and the actual Bitcoin price (blue) [98]].

However, there is significant skepticism about the model's assumptions:

- Model estimates 100 trillion USD market capitalization after the next two halvings (2028) and approximately 20,000 trillion USD market capitalization after the next four halvings

(2036). Even accounting for fiat currencies' inflation, these projections are unrealistic. Bitcoin's exponential price appreciation is not sustainable.

- As Morillon and Chacon point out, the model takes into account supply, but not demand. It is reasonable to assume that demand is the main driver behind Bitcoin's appreciation. As the market matures, one would expect slower demand growth, as predicted by an innovation's adoption lifecycle [99].
- Efficient market hypothesis suggests that all currently known information is reflected on the price. Considering that the S2F model uses precise, not hypothesized, supply and flow numbers, Bitcoin's price should remain stable, adjusted to inflation, as no new information is released.

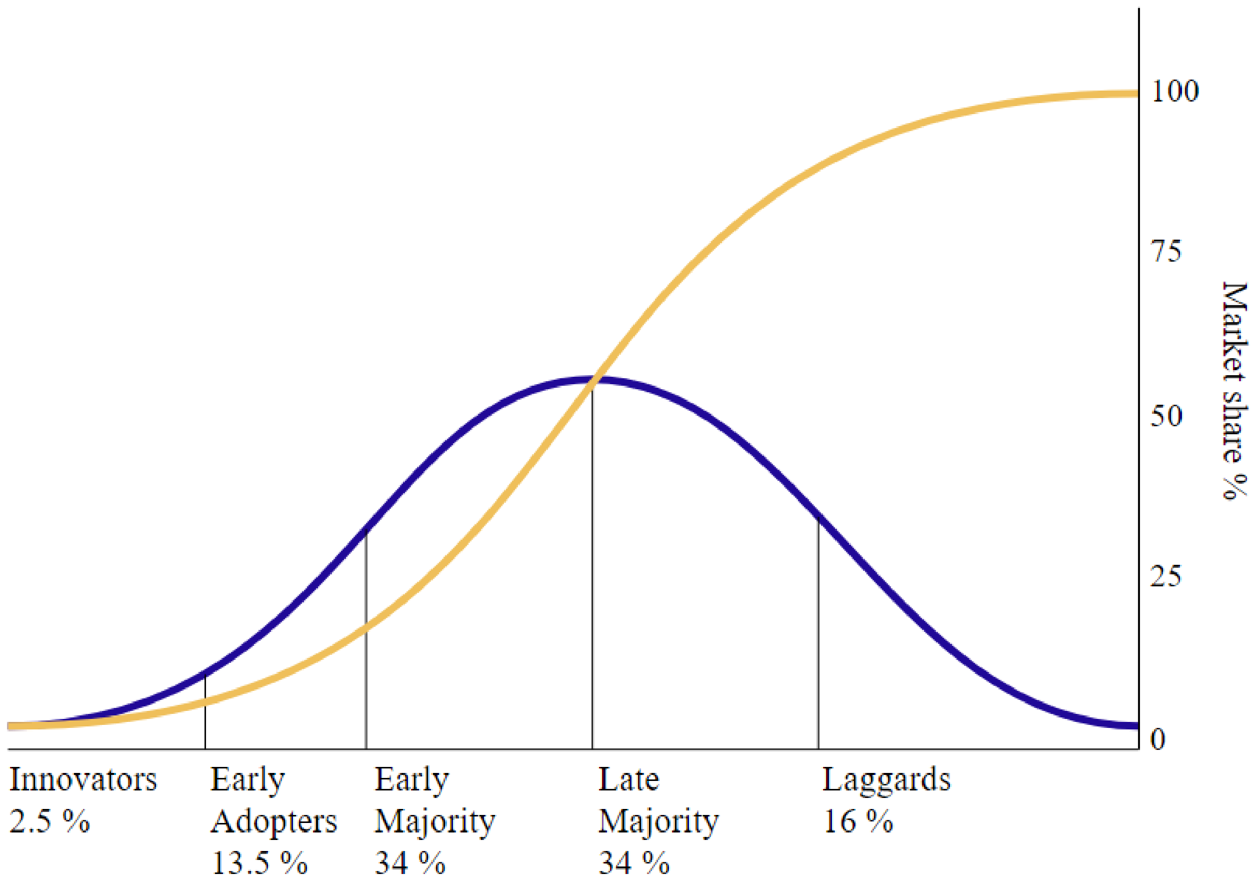


Figure 5: The "S"-curve (yellow) depicts the cumulative rate of innovation adoption. The bell curve (blue) depicts the ratio of new adopters in the same time frame [99].

The unique position of Bitcoin is a result of its tokenomics, but more importantly of its first-mover advantage. This highlights a potential issue of valuation models: as long as cryptocurrencies continue to evolve, not only is their evaluation complicated, but the taxonomy on which it is based is potentially fluid.

6 BITCOIN INTRINSIC VALUE SENSITIVITY ANALYSIS

In the previous chapter I created a theoretical token valuation framework. In order to get a better understanding on the accuracy and limitations of such a framework, I will perform sensitivity analysis to determine the fair price of a coin designed to serve as currency, in this case Bitcoin.

6.1 Bitcoin intrinsic value as a currency

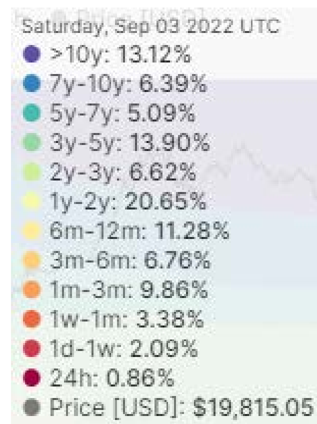
The fair price of Bitcoin, according to the equation of exchange, is a function of the total economic demand D, the share of the total demand met by Bitcoin r, the token supply M and the average money velocity V. I will attempt to assess a possible range for these parameters and intuitively attempt a rough estimation of Bitcoin's intrinsic value.

$$p = \frac{D \cdot r}{M \cdot V} = \frac{Q}{M \cdot V}$$

The product $D \cdot r$ is the share of the total demand met by Bitcoin compared to all available currencies, denominated in fiat currency. This product is the total volume of Bitcoins transacted denominated in fiat and it will be denoted Q. There is no direct way of finding the ratio r, for practical applications finding Q first is easier. Estimation of Q can be derived using the Bitcoin daily transaction volume. However, two factors need to be taken into account. Firstly, a transaction between two Bitcoin addresses is not necessarily the result of the exchange of goods and services. Currently, Bitcoin is mostly considered an investment, so it's fair to assume that the majority of transactions belong to individuals moving Bitcoin through exchanges, centralized platforms, decentralized protocols and different wallets. Secondly, transaction volume is volatile, since it depends on cryptocurrency industry trends, macroeconomic trends and the price of Bitcoin by itself. One would have to use some kind of moving average to get an estimation of transaction volume, however choosing the most suitable time frame and weighting factors is not easy in such a volatile market.

Using on-chain historical data from Messari.io, we can calculate Bitcoin transaction volume denominated in USD [100]. Messari attempts to disregard artificially inflated transaction volume, a common practice used by centralized exchanges. I will be using one-year data (September 4th 2021 to September 3rd 2022), long enough to smooth out short term fluctuations. During that period, average daily transaction volume was 15,127,397,300USD, with total transaction volume being 5.522 trillion USD (148,316,782 Bitcoins).

Bitcoin's circulating supply as of September 3rd 2022 is 19,139,575 Bitcoins, with a growth rate of approximately 850 Bitcoins daily, until the next halving in 2024 [101]. As mentioned before a fraction of the supply exists in wallets, for which the access is forever lost. It is impossible to know which addresses are forever inaccessible, but dormancy might be an indicator, since one would assume that the enormous price appreciation over the last decade would drive most of the long term holders to exchange some of their returns into fiat currencies.



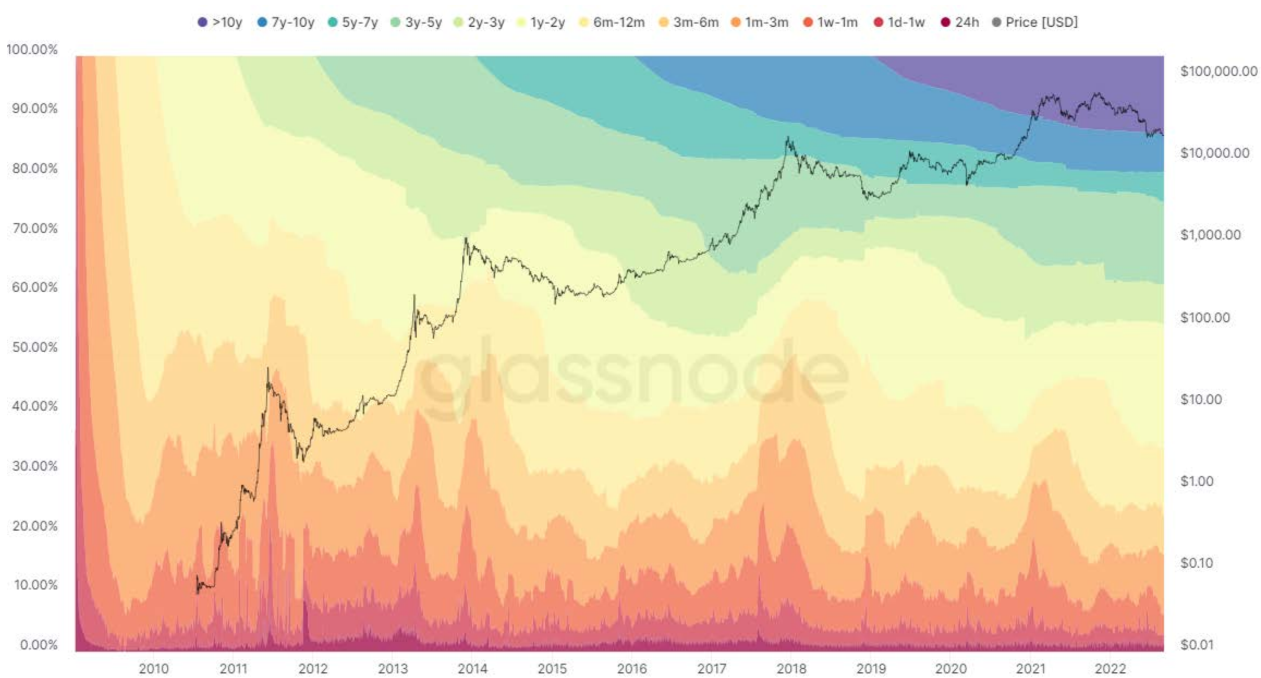


Figure 6: Bitcoin dormant addresses (source: Glassnode)

In the case of a holder's unexpected demise, it is likely that non-custodial Bitcoins will be lost, unless arrangements were previously made. It is evident that dormancy duration is strongly correlated with the chance that the coins cannot be retrieved. According to Glassnode, 24.6% of Bitcoin is dormant for more than 5 years and 13.12% is dormant for more than 10 years [102]. By the time Bitcoin price reached 1 USD for the first time, in April 2011, 6 million Bitcoins had already been minted. In September 2012, the circulating supply was 10 million Bitcoins and its price was around 10 USD. This suggests that early adopters held significant amounts of Bitcoin. However, its low price at the time, means that they would probably be less cautious when storing their coins and securing their password or network. One notable, but not unique, case, is that of James Howells, who reluctantly threw away a hard drive, causing him to lose access to 8,000 Bitcoins, worth approximately 160 million USD in today's prices [103]. For calculation purposes, I will, arbitrarily, assume 10% of total Bitcoin supply is forever lost.

Money velocity V denotes how often each Bitcoin is transferred between addresses in exchange for goods and services, so we'll attempt to include only the actual circulating supply, Bitcoins that are used as a medium of exchange. As a result, multiple addresses belonging to the same person should not be taken into account, although identifying them is often impossible. Bitcoins held as store of wealth, essentially used as a vehicle for speculative investment are excluded. Due to technological and economical limitations, Bitcoins used as medium of exchange are not strictly defined, a formal definition does not exist. However, we can assume that Bitcoins dormant for more than a month should be considered an investment, an approach supported by existing literature [50][104][105]. Using Glassnode data, we can derive that approximately 6.3% of total Bitcoin supply is dormant for less than a month. Even so, only a fraction of that is, at any time, used as medium of exchange. I, arbitrarily, suggest that this accounts for 1% of total Bitcoin supply.

According to Athey et. al. [105] Bitcoin velocity can be calculated as:

$$V = \frac{T}{M^*}$$

where:

- T is the total number of Bitcoins transacted in one year,
- M* is the number of Bitcoins used as medium of exchange in one year.

Our time frame for T and M* is long enough to smooth out any short term volatility, but not long enough to misrepresent the current state of the network.

Ultimately, the Bitcoin intrinsic value can be calculated as:

$$p = \frac{Q \cdot M^*}{M \cdot T}$$

where

$$Q = 5{,}522{,}000{,}000{,}000 \text{ USD/year}$$

$$M^* = 19{,}139{,}575 \cdot 2\% = 382{,}800 \text{ Bitcoins}$$

$$M = 19{,}139{,}575 \cdot 90\% = 17{,}225{,}600 \text{ Bitcoins}$$

$$T = 148{,}316{,}782 \text{ Bitcoins/year}$$

Which gives us an intrinsic value of 830USD/Bitcoin.

This value is significantly lower than the market price of approximately 20,000USD/Bitcoin on September 4th 2022, even accounting for significant deviations between our assumptions and real numbers. This was expected, as the biggest part of Bitcoin supply is held for speculation. As mentioned earlier, Bitcoin’s labeling as digital gold, due to its scarcity, and its non-negligible transactions fees make it a better store of value, than a medium of exchange. It is evident that Bitcoin’s price is mainly determined by the size of the speculative position. In predicting Bitcoin’s market price, one should focus on macroeconomic factors, sentiment around cryptocurrencies and Bitcoin specifically and utilize technical analysis. Miner costs, Bitcoin futures and network hash rate are also known to affect the price.

6.2 Sensitivity Analysis

In our effort to find Bitcoin’s intrinsic value, we used the actual circulating supply M and the number of Bitcoins used as medium of exchange M*. These variables can be estimated using on-chain metrics. However, calculation of p can be further simplified since both variables, M and M* represent a fraction of the total supply. They can be rewritten as:

$$M = r_{circ} \cdot M_{max} \qquad and \qquad M^* = r_{med} \cdot M_{max}$$

where:

- M_{max} is the total supply,
- r_{circ} is the ratio of actual circulating supply (subtracting Bitcoins that are forever lost) to the total circulating supply,
- r_{med} is the ratio of Bitcoins used as medium of exchange to the total Bitcoin circulating supply.

Intrinsic value p can be rewritten as:

$$p = \frac{Q \cdot r_{med} \cdot M_{max}}{r_{circ} \cdot M_{max} \cdot T} = \frac{Q \cdot r_{med}}{r_{circ} \cdot T}$$

and finally:

$$p = \frac{Q \cdot r^*}{T}$$

where

- Q is the total transaction volume of Bitcoin in a year, denominated in USD
- r^* is the ratio of Bitcoins used as medium of exchange to the actual circulating supply,
- T is the total number of Bitcoins transacted in one year.

Ultimately, intrinsic value p can be described as a function of three independent variables. I will perform sensitivity analysis to estimate the impact of each independent variable on Bitcoin's intrinsic value. Each time, I will be using the initial assumptions for the other two independent variables.

6.2.1. Intrinsic Value Sensitivity to Bitcoin transaction volume

We examine Bitcoin's intrinsic value sensitivity using a Bitcoin transaction volume range of zero to 100 trillion USD, while keeping r* and T constant. Intrinsic value p is a linear function of Q. With Bitcoin transaction volume equal to 100 trillion USD (slightly bigger than the current world GDP), Bitcoin's intrinsic value is approximately 15,000USD.

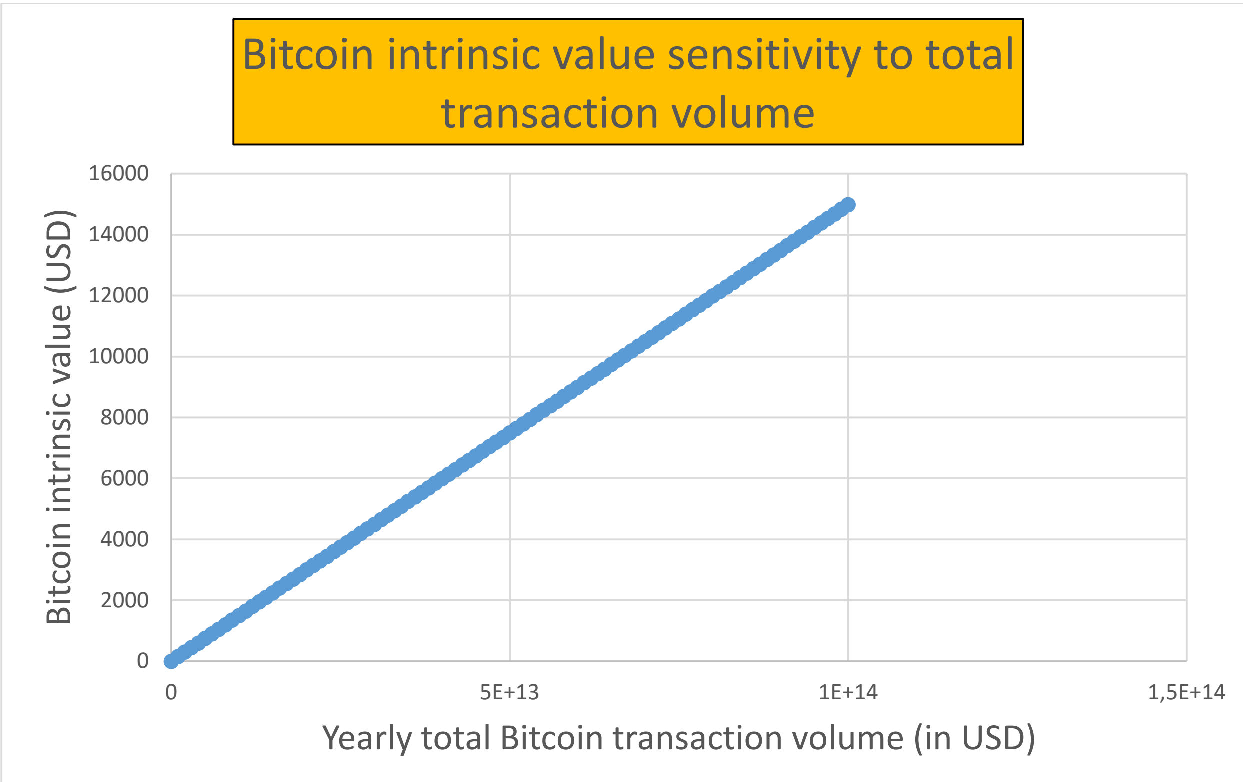


Figure 7: Bitcoin price sensitivity to total transaction volume

6.2.2 Intrinsic Value Sensitivity to the ratio of Bitcoins used as medium of exchange to the total Bitcoin circulating supply

We examine Bitcoin's intrinsic value sensitivity using a ratio r* range of zero to one, while keeping Q and T constant. A ratio of 0 means that all circulating supply is used for speculation purposes, while a ratio of 1 means that all circulating supply is used as a medium of exchange. Intrinsic value p is a linear function of r*. With a ratio equal to one, Bitcoin's intrinsic value is estimated at approximately 37,200USD.

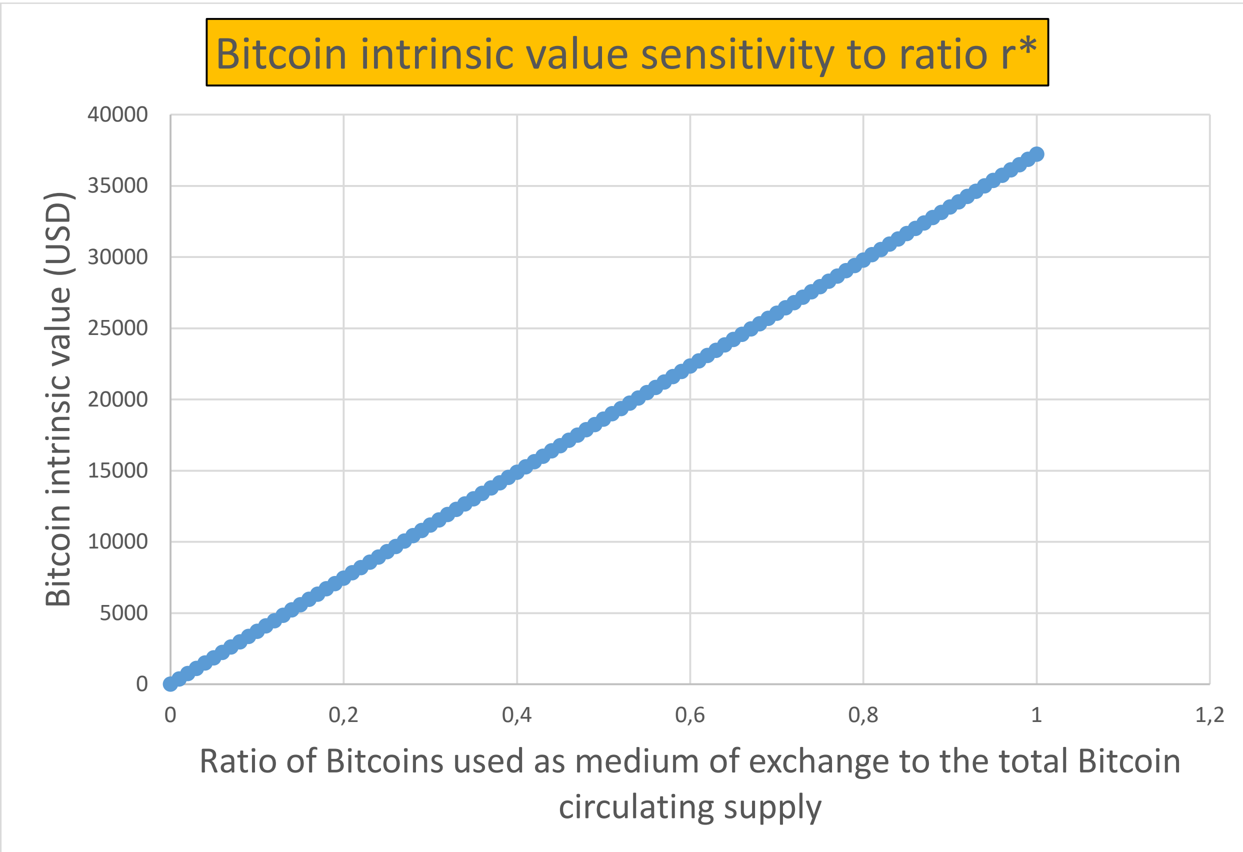


Figure 8: Bitcoin price sensitivity to ratio r

6.2.3 Intrinsic Value Sensitivity to the number of Bitcoins transacted

We examine Bitcoin's intrinsic value sensitivity to the number of Bitcoins transacted, while keeping Q and r* constant. The number of Bitcoins transacted, is an on-chain metric whose value range is not obvious. However, it is evident that if goods and services, of the same value, can be bought are exchanged with a lower amount of Bitcoins, that means that Bitcoin's intrinsic value is higher. Intrinsic value p is an inverse function of T. Assuming a range of 10 million to 1 billion Bitcoins transacted per year, the maximum intrinsic value is approximately 12,300USD/Bitcoin.

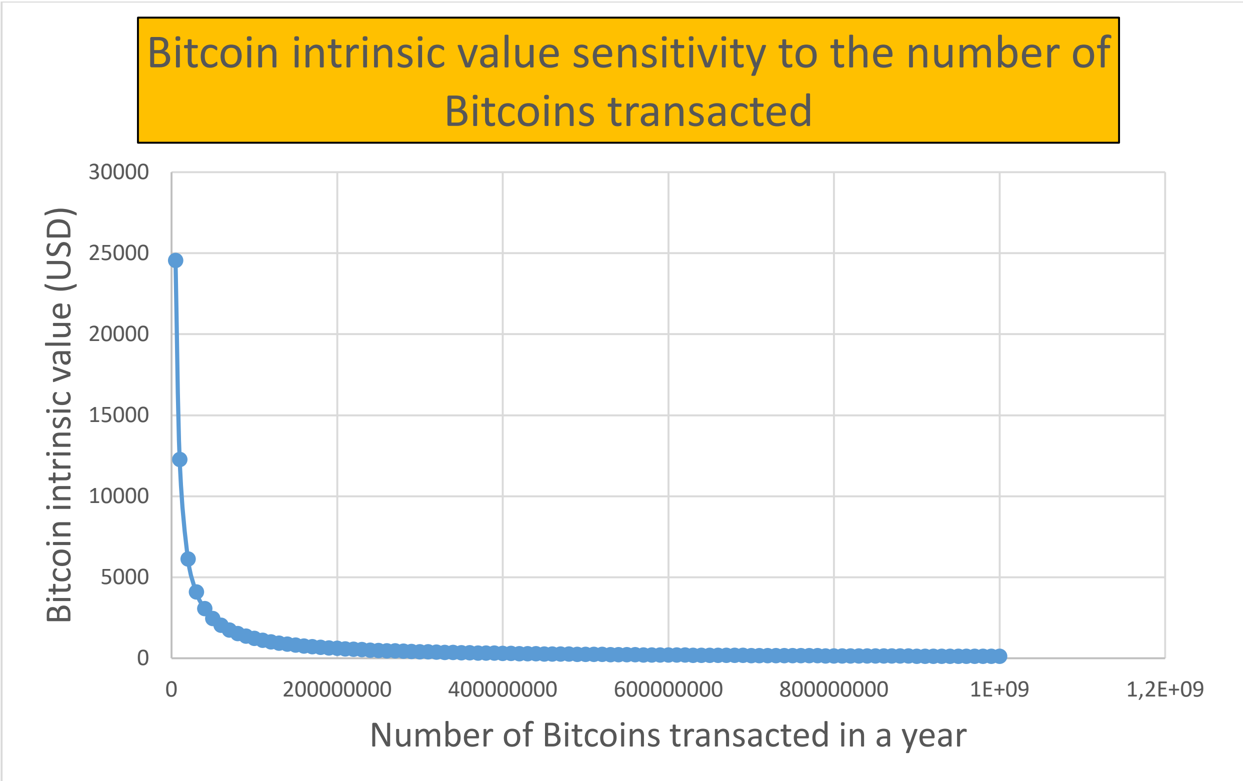


Figure 9: Bitcoin intrinsic value sensitivity to the number of Bitcoins transacted

6.3 Limitations and considerations

While sensitivity analysis gives us better perspective on how certain parameters affect a token's intrinsic value, some considerations need to be made.

As Pernice, Gentzen and Elendner discuss, money velocity in cryptocurrencies does not have a single definition, thus different approaches can be used, yielding different results [106]. Moreover, the way money velocity is measured depends on the blockchain's bookkeeping model, essentially the manner in which the state of the network is recorded. UTXO and account model being the most common bookkeeping models, utilized by Bitcoin and Ethereum respectively [107]. These models also have an effect on how transaction volume is calculated.

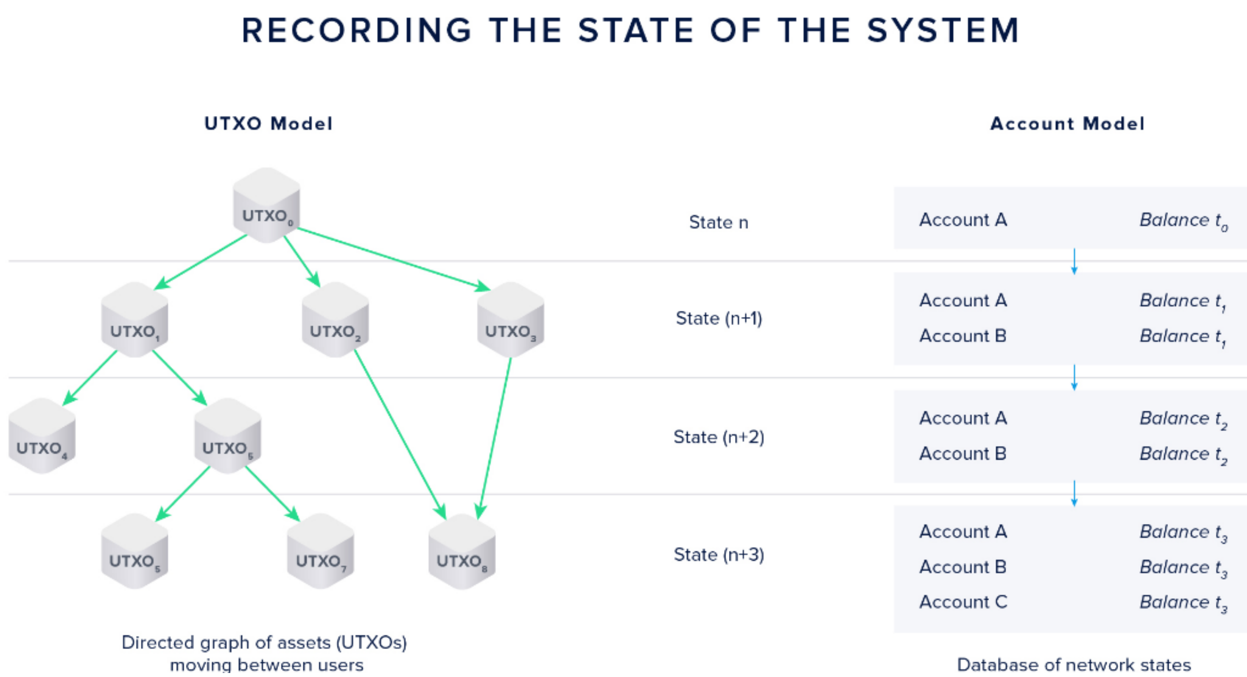


Figure 10: UTXO vs Account model [107]

In our calculations inflation is not taken into account. However, assuming modest money supply increases, both for the fiat currency and the cryptocurrency, over a year period, there should not be a significant effect on the exchange rate due to inflation. As a result, the volume of goods and services transacted within that time period should not be affected by it. Inflation, caused by increase in money supply, should play a significant role in a long term perspective.

The most significant limitation stems from the fact that the majority of transactions is a result of speculation. The consequence is that a small change in our initial, arbitrary, assumptions cause a large deviation on the outcome. This is in line with the framework proposed by Bolt and Van Oordt, which suggests that a lower volume of real transactions indicates higher exchange rate sensitivity to the size of the speculative position [80]. Concluding, it's apparent that Bitcoin's intrinsic value is extremely sensitive to the ratio of Bitcoins used as medium of exchange to the actual circulating supply r*.

Future research could focus on attempting to identify the volume of tokens used as a medium of exchange in a more consistent manner. A potential approach can be based on the fact that the size of the speculative position changes through market cycles. In a bear market, investors are more risk averse, and are less likely to allocate a significant part of their portfolio in volatile assets, such as cryptocurrencies. At the same time, the volume of tokens used as a medium of exchange, is not expected to fluctuate as much due to macroeconomic factors. A comparison between bull and bear cycle transaction volumes, could reveal to what extend daily activity is based on speculation or actual utility. Lastly, such a distinction could provide the basis for comparative analysis between different cryptocurrencies.

7. CONCLUSIONS

The concepts of digital currency, smart contracts and blockchain preceded Satoshi Nakamoto, but Bitcoin proved to be the catalyst for a new industry to emerge. Bitcoin, utilizing carefully thought out incentives, delivered on its premise: A secure, trustless, censorship resistant, peer-to-peer transaction network. Bitcoin's ingenuity sparked the appearance of numerous cryptocurrencies. Arguably, the most significant addition to the original inception was the introduction of 2nd generation blockchains, supporting smart contracts, enabling the development of decentralized applications.

The emergence of cryptocurrencies has been met with a great degree of skepticism, with many prominent figures dismissing it as nothing more than a speculative bubble. Blockchain and Web3.0 are criticized as being little more than a buzzword, a solution looking for a problem. Cryptocurrencies often appear in sensationalist headlines, owing to high volatility and investors suffering heavy financial losses. Investors are unprotected against malicious actors, due to lack of regulation.

At the same time, developers are working ceaselessly to create the infrastructure for Web3.0, a new internet era, in which security, privacy and decentralization will play a major role. Slowly, but surely, technological advancement will be separated from the hype and the disruptive potential of DLT will be evident. Once the bubble inevitably bursts and the misconception that DLT is suited for just about every purpose diminishes, the focus will shift more towards projects with actual use cases.

I listed common arguments against cryptocurrencies' economic premises, then proceeded to make the case for the existence of intrinsic value. I classified tokens in three categories, in order to identify the source of intrinsic value in each case. This classification was also used in the creation of a valuation framework.

This valuation model is not focused on precision; such expectations would be unrealistic. Instead, I attempted to identify the fundamental parameters that determine a token's value and provide an elementary valuation framework based on them. Estimation of most parameters contains a substantial safety margin.

There are certain factors that impose limitations in the model's predictive strength:

- DLT's value is still debated. While maximalist arguments from both sides tend to simplify the topic, predicting DLT's adoption in the long-term is a complicated task.

- Cryptocurrencies are a new asset class that has unique technological and economical characteristics. Traditional valuation methods are not directly applicable.

- Regulations will undoubtedly reform the crypto space, making it much safer for investors. So far, institutions have been hesitant to dip their toes in the uncertain waters of cryptocurrencies, as high volatility deters risk-averse investors.

- The extent of regulatory implications is yet unclear. Various jurisdictions may approach DLT in different manner, creating an uneven playing field.

- The impact of DLT on various industries is not yet clear. At the moment, large scale applications of DLT are limited. As the technology evolves, more use cases will emerge.

- It is unknown to what extend decentralized public blockchains will be used over private, permissioned ones. Businesses may use blockchain infrastructure, focusing on the immutability and security it brings and not on the economic premises of public, permissionless blockchains, such as ICOs.

- Arguably, the biggest limitation is quantifying the size of the speculative position, in comparison to intrinsic network value. This also makes present intrinsic value estimation a demanding task.

At the moment, market value deviates significantly from the intrinsic value due to speculation, but we expect that gap to be slowly bridged as the market matures. Constant reevaluation of up to date information is required. Valuation models will inevitably be more precise as the industry's position becomes clearer. Scenario probability distributions and sensitivity analysis is essential, in order to arrive at a useful conclusion.

I chose to perform sensitivity analysis on Bitcoin's present intrinsic value, as the most recognizable cryptocurrency. The public nature of its distributed ledger allowed me to use on-chain analysis to get access to extremely precise metrics. However, it quickly became apparent that the manner in which these metrics are interpreted can cause large discrepancies in the final estimation. Initial assumptions of the size of the speculative position proved to be the parameter in which Bitcoin's intrinsic value is the most sensitive, considering the complexity of estimating it.

It is very challenging to foresee what Web3.0 will look like. All major internet innovations in the last decades, such as search engines or social media, emerged unpredictably, gained traction very rapidly but their enormous impact was not immediately obvious. It is my belief that, sooner or later, decentralization maximalists will have to give way to regulations and transparency which are necessary for mainstream adoption.

Potential future research questions include:

- How can decentralization be measured consistently? How can factors such as mining, token distribution, governance and developer impact be quantified?

- What are the drivers of a project's success? How important are metrics such as decentralization, security, developer activity, growth rate of active participants in the network, total value locked within the network? How can their impact be quantified?

- What role do VCs play in a project's success? How does VC funding affect the performance of an ICO token? How does VC funding affect a project's decentralization?

- How can we estimate the size of the speculative position in a more confident manner?

No single valuation model can aspire to accurately estimate a token's intrinsic value. One should apply different techniques to gauge its value as efficiently as possible. Any model will exhibit a significant margin of error and should be used alongside different qualitative and quantitative metrics. Due to the novelty of cryptocurrencies, such models are better suited to establish comparability across different tokens, rather than attempting to precisely measure intrinsic value. Future research could focus on on-chain metrics and their efficient interpretation to derive more accurate results.

REFERENCES

[1] Chohan, U. W. (2021), "The Double Spending Problem and Cryptocurrencies", Available at: https://ssrn.com/abstract=3090174

[2] Nakamoto, S. (2008), "Bitcoin: a peer-to-peer electronic cash system", Available online at: http://www.bitcoin.org/bitcoin.pdf

[3] Benos, E., Garratt, R. and Gurrola-Perez, P. (2017), "The economics of distributed ledger technology for securities settlement", *Bank of England*, Available at: https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2017/the-economics-of-distributed-ledger-technology-for-securities-settlement

[4] Eyal, I. and Sirer, E.G. (2014). "Majority Is Not Enough: Bitcoin Mining Is Vulnerable", *FC 2014: Financial Cryptography and Data Security*, pp. 436-454, Available at: https://doi.org/10.1007/978-3-662-45472-5_28

[5] Böhme, R., Christin, N., Edelman, B. and Moore, T. (2015), "Bitcoin: Economics, Technology, and Governance", *Journal of Economic Perspectives*, Vol. 29, pp. 213–238, Available at: https://www.aeaweb.org/articles?id=10.1257/jep.29.2.213

[6] Meynkhard, A. (2019), "Fair market value of bitcoin: halving effect", *Journal of Investment Management and Financial Innovations*, Issue 4, pp. 72-85, Available at: https://www.businessperspectives.org/journals/investment-management-and-financial-innovations/issue-334/fair-market-value-of-bitcoin-halving-effect

[7] Antonopoulos, A. (2017), "Mastering Bitcoin (2nd edition)", O'Reilly, p73

[8] Zhang, R., Xue, R., Liu, L. (2019), "Security and Privacy on Blockchain", *ACM Computing Surveys*, Volume 52, Issue 3 Article No.: 51, pp. 1–34, Available at: https://doi.org/10.1145/3316481

[9] (2013, October 2), "FBI claims largest Bitcoin seizure after arrest of alleged Silk Road founder", *The Guardian*, https://www.theguardian.com/technology/2013/oct/02/alleged-silk-road-website-founder-arrested-bitcoin

[10] Woo, D., Gordon, I., Iaralov, V. (2013), "Bitcoin: A first assessment", *Bank of America Merrill Lynch*, Available online at: https://files.static-chmedia.ch/extfile/127c0c3b1fca5320245d73f9921413f2f10b4d08

[11] Szabo, N., Smart Contracts: Building Blocks for Digital Markets, Available online at: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[12] Buterin, V. (2014), "Ethereum Whitepaper", Available online at: https://ethereum.org/en/whitepaper/

[13] "The challenge of decentralized scaling", Ethereum.org, Available online at: https://ethereum.org/en/upgrades/vision/

[14] "Potential for increased sales", Visa.com, Available online at: https://usa.visa.com/run-your-business/small-business-tools/retail.html

[15] Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S. (2016), "On the Security and Performance of Proof of Work Blockchains", *CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 3-16, Available at: https://dl.acm.org/doi/abs/10.1145/2976749.2978341

[16] Lepore, C., Ceria, M., Visconti, A., Rao, U. P., Shah, K. A., Zanolini, L. (2020), "A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS", *Special Issue "The Cryptography of Cryptocurrency"*, Available at: https://www.mdpi.com/2227-7390/8/10/1782

[17] Aiyar, K., Halgamuge, M., Mohammad, A. (2021), "Probability Distribution Model to Analyze the Trade-off between Scalability and Security of Sharding-Based Blockchain Networks", *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, Available at: https://ieeexplore.ieee.org/abstract/document/9369563

[18] Zhou, Q., Huang, H., Zheng, Z., Bian, J. (2020), "Solutions to Scalability of Blockchain: A Survey", *IEEE Access (Volume: 8)*, pp. 16440-16455, Available at: https://ieeexplore.ieee.org/abstract/document/8962150

[19] Hafid, A., Hafid, A. S., Samih, M. (2020), *IEEE Access PP(99)*, Available at: https://www.researchgate.net/publication/342639281_Scaling_Blockchains_A_Comprehensive_Survey

[20] Li, W., Feng, C., Zhang, L., Xu, H., Cao, B., Imran, M. A. (2021), "A Scalable Multi-Layer PBFT Consensus for Blockchain", *A Scalable Multi-Layer PBFT Consensus for Blockchain*, Available at: https://ieeexplore.ieee.org/abstract/document/9279277

[21] Dhaliwal, E., Gurguc, Z. (2019), "Token Ecosystem Creation", *Outlier Ventures*, Available at: https://outlierventures.io/wp-content/uploads/2019/05/Token-Ecosystem-Creation-Outlier-Ventures-PDF.pdf

[22] "Ethereum Average Transaction Fee", *ycharts.com*, Available online at: https://ycharts.com/indicators/ethereum_average_transaction_fee

[23] (2022, May 1), "Solana Suffers Seven-Hour Outage as NFT Demand Spills Over", *Bloomberg US Edition*, Available online at: https://www.bloomberg.com/news/articles/2022-05-01/solana-suffers-seven-hour-outage-as-nft-demand-spills-over

[24] Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D, Nguyen, H. T., Dutkiewicz, E. (2019), "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities", *IEEE Access*, *vol. 7*, pp. 85727-85745, Available at: https://ieeexplore.ieee.org/abstract/document/8746079

[25] Li, W., Andreina, S., Bohli, JM., Karame, G. (2017), "Securing Proof-of-Stake Blockchain Protocols", *Data Privacy Management, Cryptocurrencies and Blockchain Technology. DPM CBT 2017 2017. Lecture Notes in Computer Science, vol 10436. Springer, Cham.*, pp. 297-315, Available at: https://doi.org/10.1007/978-3-319-67816-0_17

[26] Kiayias, A., Russell, A., David, B., Oliynykov, R. (2017), "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol", *Advances in Cryptology – CRYPTO 2017*, pp. 357-388, Available at: https://doi.org/10.1007/978-3-319-63688-7_12

[27] Gaži, P., Kiayias, A., Russell, A. (2018), "Stake-Bleeding Attacks on Proof-of-Stake Blockchains", *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 85-92, Available at: https://ieeexplore.ieee.org/abstract/document/8525396

[28] Lin, Q., Li, C., Zhao, X., Chen, X. (2021), "Measuring Decentralization in Bitcoin and Ethereum using Multiple Metrics and Granularities", *2021 IEEE 37th International Conference on Data Engineering Workshops (ICDEW)*, pp. 80-87, Available at: https://ieeexplore.ieee.org/abstract/document/9438771

[29] Srinivasan B. S. (2017), "Quantifying Decentralization", Available online at: https://news.earn.com/quantifying-decentralization-e39db233c28e

[30] (2014, April 17), "DApps: What Web 3.0 Looks Like", *gavwood.com*, Available at: https://gavwood.com/dappsweb3.html

[31] (2018, June 19), “Blockchain beyond the hype: What is the strategic business value?”, *mckinsey.com*, Available at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value

[32] Kiff, J., Alwazir, J., Davidovic, S., Farias, A., Khan, A., Khiaonarong, T., Malaika, M., Monroe, H., Sugimoto, N., Tourpe, H., Zhou, Z. (2020), “A Survey of Research on Retail Central Bank Digital Currency”. Available at SSRN: https://ssrn.com/abstract=3639760

[33] Antonopoulos, A. M. (2019), "The internet of money three: A collection of talks by Andreas M. Antonopoulos", Merkle Bloom LLC

[34] Oliveira, L., Zavolokina, L., Bauer, I., Schwabe, G. (2018), “To Token or not to Token: Tools for Understanding Blockchain Tokens,” Available at: https://www.zora.uzh.ch/id/eprint/157908/1/To%20Token%20or%20not%20to%20Token_%20Tools%20for%20Understanding%20Blockchain%20Toke.pdf

[35] Freni, P., Ferro E., Moncada, R. (2022), “Tokenomics and blockchain tokens: A design-oriented morphological framework”, Available at: https://www.sciencedirect.com/science/article/pii/S2096720922000094

[36] “Framework for “Investment Contract” Analysis of Digital Assets”, *sec.gov*, Available online at: https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets

[37] “Digital Asset Transactions: When Howey Met Gary (Plastic)”, *sec.gov*, Available online at: https://www.sec.gov/news/speech/speech-hinman-061418

[38] “Funds Trading in Bitcoin Futures – Investor Bulletin”, *sec.gov*, Available online at: https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_fundstrading

[39] Jens, L. (2019), “Regulating Initial Coin Offerings? A Taxonomy of Crypto-Assets”, Proceedings of the 27th European Conference on Information Systems (ECIS), Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3391764

[40] Ankenbrand, T. Bieri, D., Cortivo, R., Hoehener, J. Hardjono, T. (2020), “Proposal for a Comprehensive (Crypto) Asset Taxonomy”, 2020 Crypto Valley Conference on Blockchain Technology (CVCBT), Available at: https://ieeexplore.ieee.org/abstract/document/9150184

[41] Euler, T. (2018), “The Token Classification Framework: A Multi-Dimensional Tool for Understanding and Classifying Crypto Tokens, Untitled INC”, *untitled-inc.com*, Available online at: http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/

[42] Marshall, L. (2018), “Cryptoasset Taxonomy Report”, *cryptocompare.com*, Available online at: https://www.cryptocompare.com/media/34478555/cryptocompare-cryptoasset-taxonomy-report-2018.pdf

[43] “Token Taxonomy Framework Overview, 2019”, Available online at: https://f.hubspotusercontent10.net/hubfs/6102067/pdfs/TTF-Overview-1.pdf

[44] “Bitcoin network power demand”, Cambridge Center for Alternative Finance, Available online at: https://ccaf.io/cbeci/index

[45] Baur, D. G., Oll, J. (2021), "Bitcoin investments and climate change: A financial and carbon intensity perspective", *Finance Research Letters*: 102575. Available at: https://doi.org/10.1016/j.frl.2021.102575

[46] Durovic, M., Lech, F. (2019), “The Enforceability of Smart Contracts”, *5 Italian L.J. 493*, Available online at: https://theitalianlawjournal.it/data/uploads/5-italj-2-2019/493-durovic-lech.pdf

[47] “Smart legal contracts: Summary”, lawcom.gov.uk, Available online at: https://www.lawcom.gov.uk/project/smart-contracts/

[48] Hanley, B.P. (2015), “The False Premises and Promises of Bitcoin”, *Cornell University Library*, Available at: https://arxiv.org/abs/1312.2048

[49] Williams, M.T. (2014), “Virtual currencies - Bitcoin risk”, World Bank Conference, Washington, D.C., Available at: https://www.bu.edu/questrom/files/2014/10/Wlliams-World-Bank-10-21-2014.pdf

[50] Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M.C., Siering, M. (2014), “Bitcoin - Asset or Currency? Revealing Users’ Hidden Intentions”, Twenty Second European Conference on Information Systems, Tel Aviv, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425247

[51] Hirose, I., Olson J. (2015), “The Oxford Handbook of Value Theory”, Oxford University Press, pp. 29–43 https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199959303.001.0001/oxfordhb-9780199959303

[52] Treiblmaier, H. (2021), “Do cryptocurrencies really have (no) intrinsic value?”, *Electron Markets (2021)*, Available at: https://doi.org/10.1007/s12525-021-00491-2

[53] Dewey, J. (1939), “Theory of valuation”, University of Chicago Press

[54] (2019, May 6), “Joseph Stiglitz, Nobel Prize Economist, Says Cryptocurrencies Go Against Financial Transparency and Should Be Shut Down”, *crowdfundinsider.com*, https://www.crowdfundinsider.com/2019/05/147129-nobel-prize-economist-and-professor-joseph-stiglitz-says-cryptocurrencies-should-be-shut-down/

[55] (2021, May 9), “ECB Chief Lagarde: Cryptocurrencies Prone to Money Laundering, No Intrinsic Value, Buy if Prepared to Lose all Money”, *news.bitcoin.com*, https://news.bitcoin.com/ecb-chief-lagarde-cryptocurrencies-money-laundering-no-intrinsic-value-buy-prepared-to-lose-all-money/

[56] Adhami, S., Giudici, G., Martinazzi, S. (2018), “Why do businesses go crypto? An empirical analysis of initial coin offerings”, Journal of Economics and Business, Volume 100, pp. 64–75, Available at: https://www.sciencedirect.com/science/article/pii/S0148619517302308

[57] Nadler, P., Guo, Y. (2020), “The fair value of a token: How do markets price cryptocurrencies?”, Research in International Business and Finance 52, Available at: https://www.sciencedirect.com/science/article/pii/S0275531919300601

[58] García-Monleón, F., Danvila-del-Valle, I., Lara, F.J. (2021), “Intrinsic value in crypto currencies”, Technological Forecasting and Social Change, Volume 162, Available at: https://www.sciencedirect.com/science/article/pii/S0040162520312191

[59] Subramanian, H. (2018), “Decentralized blockchain-based electronic marketplaces”, Communications of the ACM, Volume 61, Issue 1, pp. 78–84, Available at: https://doi.org/10.1145/3158333

[60] Lawrenz, S., Sharma, P., Rausch, A. (2019), “Blockchain Technology as an Approach for Data Marketplaces”, *ICBCT 2019: Proceedings of the 2019 International Conference on Blockchain Technology*, pp. 55–59, Available at: https://doi.org/10.1145/3320154.3320165

[61] Qin, K., Zhou, L., Afonin Y., Lazzaretti, L., Gervais, A. (2021), “CeFi vs. DeFi -- Comparing Centralized to Decentralized Finance”, Available at: https://doi.org/10.48550/arXiv.2106.08157

[62] Jentzsch, C. (2016), “Decentralized Autonomous Organization to Automate Governance” Available online at: https://lawofthelevel.lexblogplatformthree.com/wp-content/uploads/sites/187/2017/07/WhitePaper-1.pdf

[63] Fenwick, M., Vermeulen, E. (2018), “Technology and corporate governance: Blockchain, crypto, and artificial intelligence”, Lex Research Topics in Corporate Law & Economics

Working Paper No. 424/2018, *European Corporate Governance Institute (ECGI)*, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3263222

[64] Weyl, E. G., Ohlhaver, P. Buterin, V. (2022), "Decentralized Society: Finding Web3's Soul" Available at: https://ssrn.com/abstract=4105763

[65] Nelaturu, K., Du, H., Le, D.-P. (2022), "A Review of Blockchain in Fintech: Taxonomy, Challenges, and Future Directions", *Cryptography 2022*, 6, 18, Available at: https://doi.org/10.3390/cryptography6020018

[66] Roeck, D., Sternberg, H., Hofmann, E. (2020), "Distributed ledger technology in supply chains: a transaction cost perspective", *International Journal of Production Research*, 58:7, 2124-2141, Available at: https://doi.org/10.1080/00207543.2019.1657247

[67] Wang, R., Wu, Y. (2021), "Application of Blockchain Technology in Supply Chain Finance of Beibu Gulf Region", *Mathematical Problems in Engineering*, vol. 2021, Article ID 5556424, Available at: https://doi.org/10.1155/2021/5556424

[68] Mankiw, N. G. (2019), "Macroeconomics (10th edition)", Macmillan Higher Education, p. 127

[69] Krugman, P. (2020), "Arguing with Zombies: Economics, Politics, and the fight for a better Future", W. W. Norton & Company, pp. 413-414

[70] (2021, September 7), "El Salvador Just Became The First Country To Accept Bitcoin As Legal Tender", *npr.org*, https://www.npr.org/2021/09/07/1034838909/bitcoin-el-salvador-legal-tender-official-currency-cryptocurrency?t=1657112405411

[71] (2022, April 28), "Central African Republic becomes second country to adopt bitcoin as legal tender", *cnbc.com*, https://www.cnbc.com/2022/04/28/central-african-republic-adopts-bitcoin-as-legal-tender.html

[72] (2022, January 26), "IMF urges El Salvador to remove Bitcoin as legal tender", *bbc.com*, https://www.bbc.com/news/world-latin-america-60135552

[73] (2022, April 3), "El Salvador's bitcoin experiment makes tech tourists happy but the locals are not convinced", *abc.net*, https://www.abc.net.au/news/2022-04-04/el-salvador-bitcoin-experiment-cryptocurrency-legal-tender/100928650

[74] Ingham, G. (2004), "The Nature of Money", Polity Press Ltd, p. 72

[75] Lippert, R. (2019), "Was ist falsch an der Arbeitswerttheorie? Wie Wert wirklich gebildet wird [What is wrong with the labor value theory? How value is really made]", MPRA Paper

(No. 91189), *University Library of Munich, Germany*, Available at: https://ideas.repec.org/p/pra/mprapa/91189.html

[76] Bolt, W., van Oordt, M. R.C (2016), "On the Value of Virtual Currencies", *Bank of Canada*, Working Paper No. 2016-42, Available at: https://ssrn.com/abstract=2767609

[77] Klein, T., Thu, H.P., Walther, T. (2018), "Bitcoin is not the New Gold – A comparison of volatility, correlation, and portfolio performance", *International Review of Financial Analysis*, Volume 59, pp. 105-116, Available at: https://www.sciencedirect.com/science/article/abs/pii/S105752191830187X

[78] Gkillas, K., Bekiros, S., Siriopoulos, C. (2018), "Extreme Correlation in Cryptocurrency Markets", Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3180934

[79] (2022, February 2), "More than $320 million stolen in latest apparent crypto hack", *cnbc.com*, https://www.cnbc.com/2022/02/02/320-million-stolen-from-wormhole-bridge-linking-solana-and-ethereum.html

[80] Bolt, W., Van Oordt M.R.C (2019), "On the Value of Virtual Currencies", *Journal of Money, Credit and Banking*, Vol. 52, No. 4 (June 2020), Available at: https://doi.org/10.1111/jmcb.12619

[81] Wang, J.C-Y (2014), "A Simple Macroeconomic Model of Bitcoin", Bitquant Research Laboratories, *Working Paper No. 1*, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2394024

[82] Senner, R., Sornette, D. (2019), "The Holy Grail of Crypto Currencies: Ready to Replace Fiat Money?", *Journal of Economic Issues*, 53(4), 966–1000, Available at: https://doi.org/10.1080/00213624.2019.1664235

[83] Cachanosky, N. (2019), "Can Bitcoin become money? The monetary rule problem", *Australian Economic Papers*. Available at: https://doi.org/10.1111/1467-8454.12158

[84] "Introduction to Crypto Assets Valuation, *crypto.com*, Available online at: https://crypto.com/university/introduction-to-crypto-assets-valuation

[85] (2019, March 7), "The valuation of crypto-assets", *Ernst & Young*, Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/emeia-financial-services/ey-the-valuation-of-crypto-assets.pdf

[86] Cong, L.W., Li, Y., Wang, N. (2022), "Tokenomics: Dynamic Adoption and Valuation", *The Review of Financial Studies, Volume 34, Issue 3*, March 2021, Pages 1105–1155, Available at: https://doi.org/10.1093/rfs/hhaa089

[87] Chaim, P., Laurini, M. P. (2019), "Is Bitcoin a bubble?", *Physica A: Statistical Mechanics and its Applications*, Volume 517, 1 March 2019, Pages 222-232, Available at: https://doi.org/10.1016/j.physa.2018.11.031

[88] Bheemaiah, K., Collomb, A (2018), "Cryptoasset Valuation: Identifying the variable of analysis", Working Report v1.0, Available online at: http://proof.certisio.com/wp-content/uploads/2019/01/stratumn_cryptovaluationreport-v20181016-fv.pdf

[89] "EIP 1559 FAQ", *notes.ethereum.org*, Available online at: https://notes.ethereum.org/@vbuterin/eip-1559-faq

[90] Lammer, D.M., Hanspal, T., Hackethal, A. (2020), "Who are the Bitcoin investors? Evidence from indirect cryptocurrency investments", SAFE Working Paper, No. 277, *Leibniz Institute for Financial Research SAFE, Frankfurt a. M.*, Available at: https://doi.org/10.2139/ssrn.3501549

[91] Chohan, U. W. (2021), "A History of Dogecoin", Discussion Series: Notes on the 21st Century, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091219

[92] Poon, J., Dryja, T. (2016), "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments", Available at: https://lightning.network/lightning-network-paper.pdf

[93] (2022, January 28), "Above-ground stocks", *World Gold Council*, https://www.gold.org/goldhub/data/how-much-gold

[94] (2022, May 23), "Distribution of gold demand worldwide by sector in 2021", *statista.com*, https://www.statista.com/statistics/299609/gold-demand-by-industry-sector-share/

[95] Shahzad, S. J. H., Bouri, E., Rehman, M.U., Roubaud, D. (2021), "The hedge asset for BRICS stock markets: Bitcoin, gold or VIX", *World Economy*, 2022;45, pp. 292-316, Available at: https://onlinelibrary.wiley.com/doi/abs/10.1111/twec.13138

[96] Baur, D. G., Hoang, L. (2021), "The Bitcoin gold correlation puzzle", *Journal of Behavioral and Experimental Finance*, Volume 32, Available at: https://doi.org/10.1016/j.jbef.2021.100561

[97] (2019, March 22), "Modeling Bitcoin Value with Scarcity", PlanB, Available online at: https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25

[98] Morillon, T.G., Chacon, R.G. (2022), "Dissecting the stock to flow model for Bitcoin", *Studies in Economics and Finance*, Vol. 39 No. 3, pp. 506-523. Available at https://doi.org/10.1108/SEF-10-2021-0409

[99] Rogers, E. M. (2003), "Diffusion of Innovations (5th edition)", Simon & Schuster

[100] "Bitcoin Historical Data", *messari.io*, Available online at: https://messari.io/asset/bitcoin/historical

[101] "Bitcoin Circulating Supply", *messari.io*, Available online at: https://messari.io/charts/bitcoin/sply-circ

[102] "Bitcoin: HODL Waves", *glassnode.com*, Available online at: https://studio.glassnode.com/metrics?a=BTC&category=Lifespan&ema=0&m=supply.HodlWaves&mAvg=0&mMedian=0&s=1504625678&u=1662305678&zoom=1825

[103] (2021, December 6), "Half a billion in Bitcoin, lost in the dump", *newyorker.com*, Available online at: https://www.newyorker.com/magazine/2021/12/13/half-a-billion-in-bitcoin-lost-in-the-dump

[104] Kalodner, H., Goldfeder, S., Chator, A., Möser, M., Narayaman, A. (2017), "BlockSci: Design and applications of a blockchain analysis platform", Available at: https://arxiv.org/abs/1709.02489

[105] Athey, S., Parashkevov, I., Sarukkai, V., Xia, J. (2016), "Bitcoin Pricing, Adoption, and Usage: Theory and Evidence", *Stanford University Graduate School of Business Research*, Paper No. 16-42, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2826674

[106] Pernice, I.G.A., Gentzen, G., Elendner, H. (2019), "Cryptocurrencies and the Velocity of Money", Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3499500

[107] "UTXO VS. ACCOUNT MODEL", *horizon.io*, Available online at: https://www.horizen.io/blockchain-academy/technology/expert/utxo-vs-account-model/