ISBN: 978-81-974990-7-4

6. Bitcoin: Economics, Technology, and Governance

Dr. Sushil kumar

Assistant Professor,
Gargi College, University of Delhi.

Abstract:

Bitcoin is a virtual money that can be used for electronic payments and other internet communication protocols. Engineers created the regulations governing Bitcoin, with no apparent input from lawyers or regulators. The foundation of Bitcoin is a transaction log that is shared by all of the computers in the network. Tens of millions of transactions totaling billions of dollars have been completed with Bitcoin.

Bitcoin's decentralization has lured users in because it purposefully avoids depending on a single server or group of servers to store transactions or on a single entity that may restrict specific users or categories of transactions. Economists are interested in Bitcoin because of its potential to upend established payment and possibly monetary systems, as well as the abundance of information it offers regarding the behavior of agents and the Bitcoin system itself. We will talk about in this essay. Bitcoin: Technology, Governance, and Economics.

Keywords:

Bitcoin, Economics, Technology, Governance, Communication Protocol, Electronic Payments, Dollar, Cryptocurrency, Transactions, Blockchain, Cross-Border Payments, Community, Bitcoin Cash, Scarcity

6.1 Introduction:

Under the pseudonym Satoshi Nakamoto, an anonymous developer mined Bitcoin, the most well-known cryptocurrency, for the first time in 2009. It appears that neither authorities nor attorneys had any input when the regulations governing bitcoin were developed. The virtual currency market was completely transformed by the removal of third parties from transactions.

The foundation of Bitcoin is a decentralized transaction protocol that is run on a network of involved computers. It contains an element that deters power monopolies, invites early adopters to embrace it, and promotes genuine engagement. The design of Bitcoin allows for public transaction history, scheduled money generation, and irreversible transactions. Without having to disclose their true identity or go through a centralized verification process, anyone may sign up for a Bitcoin account for free.

When combined, these rules produce a system that is thought to be more flexible, private, and less regulated than conventional payment options. Because Bitcoin is a virtual money that has the potential to upend current payment and currency systems, economists are naturally interested in it. [1]

The blockchain is the name of the technology that permits digital currencies, among other things. The moniker Bitcoin itself is the most well-known cryptocurrency that helped make blockchain technology popular. Every peer-to-peer network transaction is documented on a distributed ledger called a blockchain. It enables users to transact without money movements being regulated by banks or other third parties. Bill payments, deal closing, voting, contract signing, and other things are examples of requests.

The development of virtual currencies like bitcoin offers scholars a distinctive setting in which to examine user behavior, financial system architecture, and the effects of regulation. Due to its widely available historical price and volume data, predefined rules, and publicly accessible transaction record, Bitcoin stands apart from other cryptocurrencies. Researchers will be able to watch the effects of these modifications when new rules, regulations, risk mitigation strategies, and technological advancements are included into the bitcoin environment in order to gain insights into how to better build it going forward. More generally, the use of bitcoin allows users to transfer digital property to one another. One possible use for this asset transfer mechanism is the purchase and sale of financial assets like bonds and stocks. Financial market participants may need to take virtual currency investments into account as part of their overall investment strategy if online currencies like bitcoin continue to grow and can effectively mitigate counterparty risk and regulatory risk. [2].

A. Bitcoin:

Bitcoin is an electronic money system (EMS) that was developed for exchanging so-called bitcoins, also known as BTC. While there have been several successful electronic money systems in the past, Bitcoin stands out as a novel and distinct cryptocurrency that incorporates features aimed at reducing the financial risks associated with EMSs. With a cryptocurrency, there is no need for a central authority to be involved in transactions, eliminating the possibility that they may limit the amount of money in circulation or feel obliged to arbitrate disputes. This is achieved through the application of cryptographic controls. In order to simulate a limited resource, like gold, the upper bound on the quantity of cryptocurrency units is well-known and restricted.

B. Economics of Bitcoin:

First and foremost, it's critical for understanding Bitcoin's economics. There is not a single central authority or point of trust supporting this virtual currency.

People who prefer a "freely traded currency" and avoid intermediaries like banks and governments are drawn to it because of its decentralized nature (Barber et al., 2012 and Bohme et al., 2015). A few other similarities between these two articles are listed, including the fixed or predictable supply, secrecy, and incentive structure of Bitcoin.

As previously mentioned, the limited supply of Bitcoin stems from its generation via mathematical processes. However, fixed supply presents certain significant issues that, if the volume of transactions keeps growing, could lead to an imbalance in the macroeconomy. Furthermore, while the quantity of Bitcoin may be set, the broader market for digital currencies is not. As of right now, there are over 2,000 different digital currencies available, and more are constantly being introduced.

The decentralized nature of Bitcoin and its limited supply are the foundation of its economics. In contrast to conventional currencies, Bitcoin is limited to a maximum of 21 million coins, guaranteeing scarcity and safeguarding against inflation. Mining is the process of producing new Bitcoins by figuring out intricate mathematical puzzles and validating network transactions.

The Proof of Work (PoW) consensus process, which gives miners new Bitcoins in exchange for their computer labor, is the foundation of the Bitcoin economic model. Miners are encouraged to protect the network and uphold its integrity as a result. [3]

C. Technology behind Bitcoin:

The distributed ledger at the heart of Bitcoin, or blockchain, is a visible, unchangeable record of every transaction. Transactions are safe and impervious to change or tampering thanks to the blockchain. Outside of the finance industry, this characteristic has attracted a lot of attention due to its possible uses in voting systems, supply chain management, and other areas.

Peer-to-peer transactions are also made possible by Bitcoin's technology without the use of middlemen. In particular for cross-border payments, this removes the need for reliable third parties, lowers transaction costs, and speeds up transactions.

D. Governance of Bitcoin:

Decentralized governance underpins Bitcoin, with a consensus-based decision-making process. Through open dialogue and suggestions, the community of Bitcoin users and stakeholders takes part in the decision-making process.

However, because different people in the community have different interests and points of view, coming to a consensus might be difficult.

Proposals pertaining to the future evolution of Bitcoin, including changes to the protocol and scaling strategies, have generated discussions and forced hard forks that have given rise to new cryptocurrencies names like Bitcoin Cash and Bitcoin SV. [4]

E. Review of Literature:

The idea of scarcity serves as the foundation for the Bitcoin design. In my opinion, as does the opinion of many economists, virtual currencies, such as Bitcoin, should be treated like any other type of money because it is the functions of money that define it, not its form. Additionally, virtual currencies fulfill all the purposes of physical money, acting "as a unit of account, a store of value, and a means of exchange" (Böhme et al.). Virtual currencies should also be seen in terms of scarcity, much like any other type of currency. Money gets its value (at least in part) from scarcity. It stops the creation of counterfeit money in the first place since it forbids arbitrary money creation. Secondly, in a broader sense, it also establishes rigorous limitations on the growth of the monetary base and upholds and ensures price stability (Böhme et al., "Bitcoin: Economics, Technology, and Governance" 215). The writers discuss many sources of money while demonstrating its shortage. [5]

"An electronic payment system based on cryptographic proof instead of trust [emphasis added], allowing any two willing parties to transact directly with each other without the need for a trusted third party [was developed by Satoshi Nakamoto [Citation2008, 1]." Peer-to-peer networks in this system timestamp transactions by cryptographically hashing them into a blockchain. Public blockchains are said to avoid extractive external parties and stop cheating. As so, one could think of the network as a self-governing entity. The idea that computer networks can provide order in society without raising transaction costs and so limiting human control aligns with the libertarian ideal of Silicon Valley. [6]

How closely the Bitcoin market adheres to fundamental economic concepts will decide how effective it is. The majority of the literature has shown that the reason for the volatility of the Bitcoin market is its relative youth. Over time, the price stabilizes, volatility decreases, and the likelihood of a bubble lowers. Blockchain technology is the foundation of the entire Bitcoin transaction system, and almost all forms of technology improve with time. Houy pointed out a direct consequence of this, which is that as mining technology advances over time, the difficulty of mining decreases and the process becomes more efficient overall. An earlier study by Houy (2014) examines the economics of Bitcoin transaction fees and concludes that imposing a transaction fee and limiting block size during mining improves efficiency. [7]

Objectives:

- To Study the Economics of Bitcoin.
- To Study the Technology of Bitcoin.

- To Study the Governance of Bitcoin

F. Research Methodology:

The overall design of this study was exploratory. The research paper is an effort that is based on secondary data that was gathered from credible publications, the internet, articles, textbooks, and newspapers. The study's research design is primarily descriptive in nature.

6.2 Result and Discussion:

6.2.1 The Governance of Bitcoin:

Bitcoin uses a Proof-of-Work (Pow) consensus mechanism as its governance protocol. PoW generally involves Bitcoin miners competing to solve a cryptographic problem, with the winner receiving both transaction fees and newly mined bitcoins.

Because it is impossible to game the Bitcoin blockchain system due to the associated costs, the proof-of-work consensus mechanism of the cryptocurrency ensures effective governance.

Additionally, because Bitcoin offers intrinsic economic incentives, it guarantees honesty and allows anyone to participate, regardless of gender, age, or race. Although the PoW consensus technique was created in 1993, it gained widespread recognition when Satoshi Nakamoto used it to power Bitcoin in 2009. [8]

6.2.2 Economics of Bitcoin:

A. Incentive:

The possible reward for their labor is the reason the nodes execute the transactions and expand the block chain rather than branching off. A node can add a generation or coin base transaction, which is a separate transaction, to a block before it starts working on it (seen inside Block on Figure 7.1).

The Bitcoin Network's quantity of bitcoin is increased by this unique transaction, but the protocol is designed to exponentially reduce its value. The Bitcoin Network was sparked by the possibility of reward, which continues to serve as motivation until the network is developed to the point that transaction fees are feasible.

To increase the likelihood that a node would include a particular transaction in a block, the transaction fee may be added to the transaction. Over time, the strategy shifts network funding from inflation to transaction fees.

B. Transaction Value:

Because the value of bitcoins has increased disproportionately to the number of transactions, the cost per transaction has climbed dramatically over time. There are many who argue that there is an innate inefficiency in Bitcoin, while others anticipate that market forces will eventually bring this into equilibrium at the agreed-upon market value of a transaction. Figure 5 illustrates the relationship between the determined technical requirements and the high-level objectives of different types of researched users.

Although user requirements may overlap, the Central Authority Concerned user's concerns will take precedence over those of the General Consumer in terms of overhead. Likewise, the Central Authority A concerned user might value anonymity more than the average user would, which would raise the transaction cost. [9]

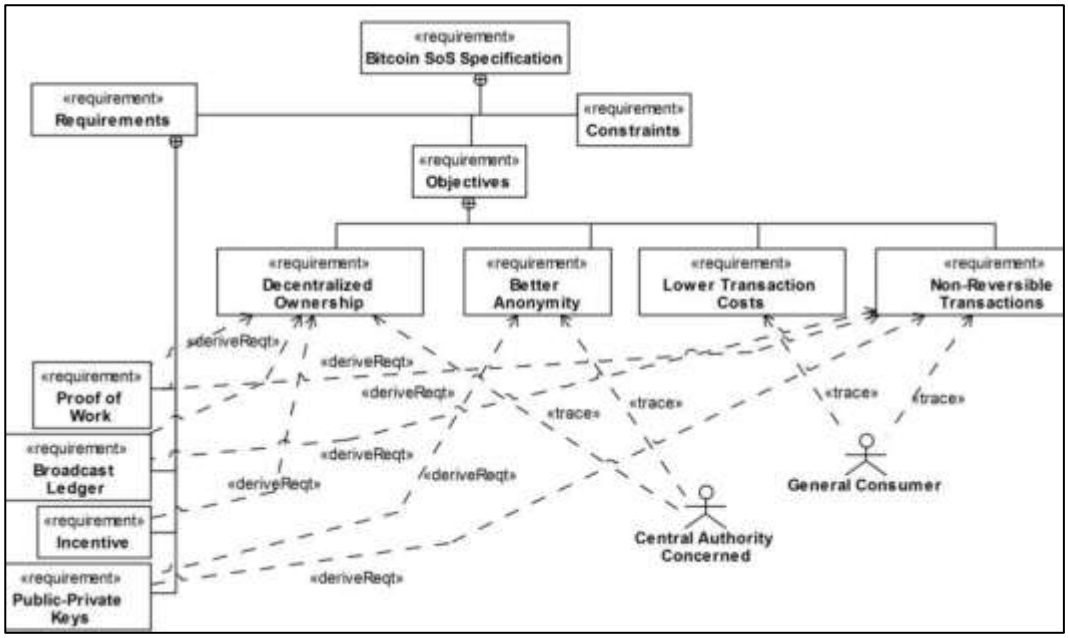

Figure 6.1: User Objective [10]

Sys ML parametric diagrams can be used to show the possible relationships between attributes of various system aspects using a system of equations. Figure 7.2 is a simple example of a more comprehensive cost of the transaction. Complete compute costs, transaction fees, any flat transaction fees, and the cost of converting bitcoins back into the original currency all contribute to the total transaction cost. The cost can be specified, but it is up to each user class to decide if the benefits of the system that are important to them warrant the extra expense. In the same manner that there is no intrinsic guarantee that a transaction will be non-reversible, there is also no inherent guarantee that the cost will be less than that of a traditional system. [11]

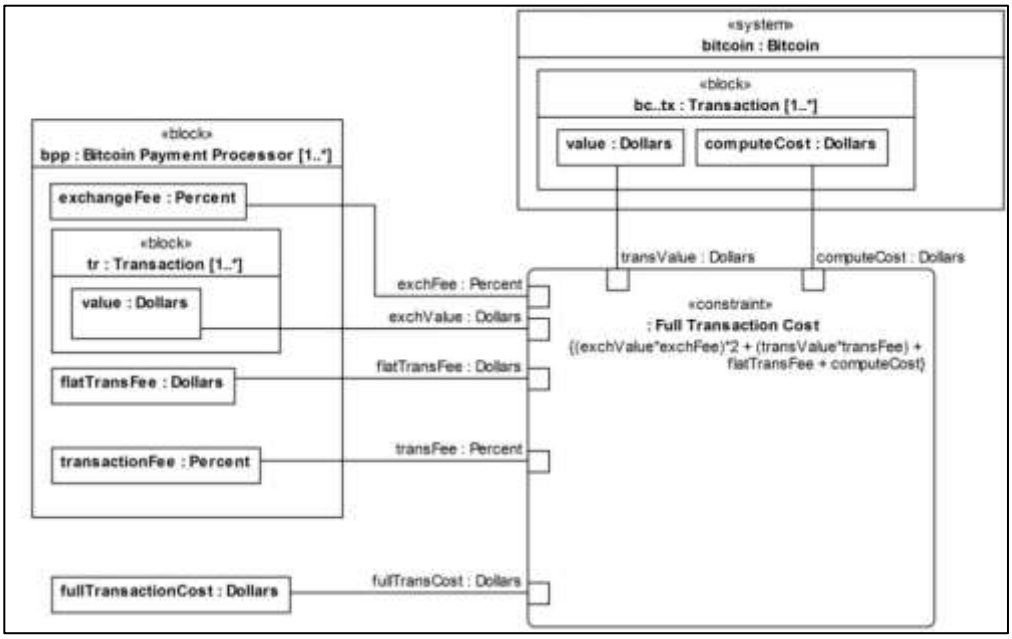

Figure 6.2: Transaction Cost Parametric Model [12]

6.2.3 Technologies and Processes:

You can get the "Bitcoin core" software for free at https://bitcoin.org/en/choose-your-wallet. Numerous functionalities are present in the basic Bitcoin implementation. Generally, it generates a unique node for the user in the peer-to-peer Bitcoin network that can be used with a regular Internet connection; it creates a "wallet" file for the user to store bitcoins (without revealing a name or identity proof); and it grants access to the "block chain" data structure that validates all previous Bitcoin activity.

A. Transactions and the Block Chain:

Bitcoin transactions are tracked. Charlie, for example, is not just a user who "holds" three bitcoins. Instead, Charlie takes part in a publicly verifiable transaction demonstrating that Bob gave him three bitcoins. Due to a previous transaction in which Bob got three bitcoins from Alice and no previous transaction in which Bob spent these three bitcoins, Charlie was able to confirm that Bob could make that payment. Figure 3 depicts these exchanges. In fact, every single bitcoin can be easily tracked back to the beginning of its circulation by looking through all of the transactions in which it was utilized. Everybody can access records of every Bitcoin transaction because they are kept in a data structure that is extensively copied. Recursive ordering of transactions typically occurs when a transaction's input, or more specifically, its funding source, is referred to by the output of a prior transaction. (For instance, the transaction might show that Bob uses the bitcoin he got from Alice to pay Charlie.) [13]

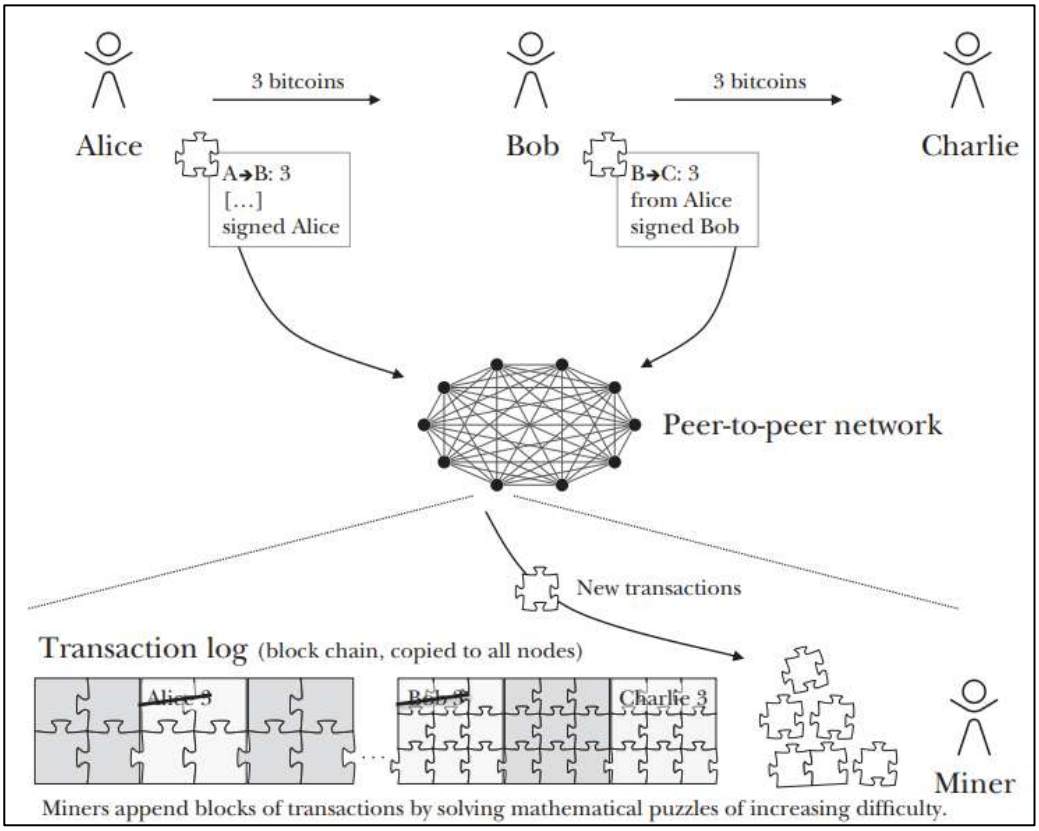

Figure 6.3: Bitcoin's Approach to Transaction Flow and Validation

Bitcoin is based on two core cryptographic technologies: transaction validation using cryptography and public private key cryptography for money storage and spending. Anyone can generate a public key and a corresponding private key using standard public-private key cryptography. As implied by the name, public keys are intended to be widely distributed.

Anyone can encrypt a message that only the designated recipient can read, but messages encrypted with a public key can only be decrypted by someone who has the matching private key. Similar to this, only the matching public key can be used to decrypt messages encrypted with a private key, enabling a designated sender to produce a message whose authenticity can be verified.

The technology known as blockchain makes cryptocurrency possible, among other things. The most well-known cryptocurrency is called Bitcoin, and it is this one that gave rise to blockchain technology as it exists today.

A cryptocurrency is a digital medium of exchange similar to the US dollar that controls the production of new monetary units and verifies the movement of funds using cryptographic techniques and protocol. [14]

B. Blockchain Technology:

A peer-to-peer network's decentralized ledger of all transactions is called a blockchain. Participants can confirm transactions using this method without requiring a central clearing body. Enterprise blockchain applications, sustainability, tokenization, fund transfers, supply chain tracking, and many other sectors are examples of potential applications.

C. Cryptocurrency:

Using cryptographic techniques to confirm the transfer of funds and an algorithm to regulate the production of monetary units, cryptocurrency is a medium of exchange that is created and kept electronically on the blockchain. The most well-known example is Bitcoin.

a. Is not redeemable for another good, like gold, hence it has no intrinsic worth.
b. Resides only within the network and lacks a physical form.
c. The protocol, not a central bank, controls its supply, and the network is entirely decentralized.

D. Blockchain technology also has potential uses outside of digital assets like cryptocurrencies and bitcoin:

Blockchain technology can be viewed as a sort of next-generation software for business process improvement from a business standpoint. Blockchain technology is one example of collaborative technology that claims to be able to enhance commercial operations between organizations, drastically reducing the "cost of trust." Because of this, compared to the majority of conventional internal investments, it might deliver noticeably better returns for each dollar invested. [14]

6.3 Conclusion:

Existing payment methods may be disrupted by the bitcoin system, but not before it resolves unresolved concerns such market, counterparty, transaction, operational, privacy, and regulatory risks.

6.4 References:

1. Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. "Bitcoin: Economics, Technology, and Governance." Journal of Economic Perspectives 29, no. 2 (Spring 2015): 213–238.
2. Baur, D. G., & Lucey, B. M. (2010). Is gold a hedge or a safe haven? An analysis of stocks, bonds and gold. Financial Review, 45(2), 217-229.

3. Lipton, A., Shrier, D., & Pentland, A. (2016). Digital banking manifesto: the end of banks. USA: Massachusetts Institute of Technology.
4. Bhutoria, R. (2020). Addressing persistent Bitcoin criticisms. Fidelity Digital Assets.
5. Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. "Bitcoin: Economics, Technology, and Governance." Journal of Economic Perspectives 29.2 (2015): 213-238. Print.
6. Nakamoto, Satoshi 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." (October 31, 2008). http://nakamotoinstitute.org/bitcoin/. Accessed May 7, 2018.
7. Houy, N. (2014). The economics of Bitcoin transaction fees. GATE WP, 1407.
8. Kim, Y. B., Lee, J., Park, N., Choo, J., Kim, J. H., & Kim, C. H. (2017). When Bitcoin encounters information in an online forum: Using text mining to analyze user opinions and predict value fluctuation. PloS one, 12(5), e0177630.
9. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013, October). A fistful of Bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference (pp. 127-140). ACM.
10. Huang, Jon; O'Neill, Claire; Tabuchi, Hiroko (3 September 2021). "Bitcoin Uses More Electricity Than Many Countries. How Is That Possible?". The New York Times. ISSN 0362-4331. Archived from the original on 17 February 2023. Retrieved 26 October 2022.
11. S., L. (2 November 2015). "Who is Satoshi Nakamoto?". The Economist. Archived from the original on 22 November 2020. Retrieved 21 November 2023.
12. Davis, Joshua (10 October 2011). "The Crypto-Currency: Bitcoin and its mysterious inventor". The New Yorker. Archived from the original on 1 November 2014. Retrieved 31 October 2014.
13. Serwer, Adam; Liebel son, Dana (10 April 2013). "Bitcoin, Explained". Mother Jones. Archived from the original on 27 April 2014. Retrieved 26 April 2014.
14. Vigna, Paul (17 January 2016). "Is Bitcoin Breaking Up?". The Wall Street Journal. Archived from the original on 20 August 2016. Retrieved 8 November 2016.
15. P. Surda and P. R. Haiss, "Economics of Bitcoin: is Bitcoin an alternative to at currencies and gold? by Peter urda Advisor: Univ. Dos. Mag. Dr. Peter R. Haiss.