Proceedings of the 2nd International Conference on Management Research and Economic Development
DOI: 10.54254/2754-1169/86/20240942

Research on the Features and Functions of Bitcoin and Digital Currencies

Boyan Yu[1,a,*]

[1]*SWUFE-UD Institute of Data Science Southwestern University of Finance and Economics Chengdu, 610000*
a. yuboyan@udel.edu
**corresponding author*

Abstract: Since the creation of Bitcoin in 2008, these digital currencies have not only attracted widespread attention from the public and economists, but have also triggered a rethinking of the nature of money, the store of value, and the modes of exchange. This paper explores the transformative impact of Bitcoin and digital currencies on global finance, emphasizing their emergence as a challenge to the traditional concept of money and a paradigm shift. Furthermore, the paper delves into the birth of Bitcoin, its decentralized nature and its pioneering role in the field of digital currencies, discusses the historical background, technological underpinnings, and monetary functions of digital currencies, and highlights the potential and challenges of their integration into the financial system. It aims to examine the characteristics and functions of bitcoin and digital currencies in the contemporary financial landscape, focusing on how they can challenge traditional monetary policy as an emerging financial asset, as well as their potential impact and integration challenges in the global economic system.

Keywords: Bitcoin, digital currencies, global finance, paradigm shift, financial system integration

1. Introduction

In the ever-evolving landscape of global finance, the emergence and integration of Bitcoin and other digital currencies represent a paradigm shift, challenging traditional conceptions of money and monetary transactions. This study seeks to offer an overview of digital currencies, with a special emphasis on Bitcoin, as it stands as the forerunner and the most influential of these digital assets. Bitcoin, since its inception, has not only captured the public imagination but also sparked significant interest and debate among economists, policymakers, and financial experts. Some economists regarded Bitcoin, along with other cryptocurrencies as an economic bubble.

The concept of digital currencies dates back to the late 20th century, but it wasn't until the creation of Bitcoin in 2008 by an individual (or group) known as Satoshi Nakamoto [1] that this idea truly came to fruition. Bitcoin (abbreviation: BTC or XBT; sign:B) introduced a decentralized system, fundamentally different from the centralized control of traditional fiat currencies managed by governments and central banks. The evolution of digital currencies can be traced through various phases, starting as a niche interest among tech enthusiasts, evolving into a speculative investment, and increasingly being considered a legitimate form of financial asset (which is of highly volatility

DOI: 10.54254/2754-1169/86/20240942

and does not resemble any other conventional ones). They challenge conventional banking systems and monetary policies, introducing a new paradigm in the way we understand money, and also raises questions about the future of monetary transactions and policies.

The thrust of this study is to discuss the features and Functions of Bitcoin and similar digital currencies in the contemporary financial landscape. It starts with the historical context and technology behind Bitcoin. Further, it seeks to reveal how digital currencies fulfill or diverge from the basic functions of money and understand their impact on traditional monetary policies. This case study exploration is meaningful in an era where digital currencies are not just technological novelties but are becoming significant players in the global financial system, where digital currencies posing both opportunities and challenges for existing monetary and financial structures.

2. Historical Context of Bitcoin and Other Digital Currencies

The development of digital currencies from theoretical conception to mainstream financial assets has been a process of technological innovation and evolving economic paradigms. The concept of digital money predates Bitcoin, with early iterations in the 1980s and 1990s, such as David Chaum's DigiCash [2] and Wei Dai's b-money. However, it was the introduction of Bitcoin in 2009 by an individual or group under the pseudonym Specifically, in Satoshi Nakamoto's paper "Bitcoin: A Peer-to-Peer Electronic Cash System," a decentralized system is proposed that uses blockchain technology to enable secure, transparent transactions without the need for a central authority.

Initially perceived as a technical novelty among computer enthusiasts, Bitcoin gradually gained recognition as a potential financial asset. Its decentralized nature and limited supply, capped at 21 million coins, appealed to those skeptical of government-controlled monetary systems and those seeking alternative investment avenues. Notably, the so-called Silk Road, a notorious darknet marketplace, which was active between 2011 and 2013, processed approximately 9.9 million bitcoins worth of transactions using primarily bitcoin operations, equivalent to approximately $214 million at the time.

In March 2013, the U.S. Financial Crimes Enforcement Network (FinCEN) issued guidelines for decentralized digital currencies. These guidelines categorized U.S. bitcoin miners that sell the bitcoins they mine as money service businesses, subjecting them to regulatory scrutiny and legal requirements.In December 2013, the People's Bank of China (PBOC) banned the use of bitcoin by financial institutions in China.This regulatory stance intensified in February 2018 when China imposed a total ban on bitcoin trading, leading to a significant drop in the price of bitcoin..

However, the narrative around Bitcoin began to shift by 2020, as it began to attract the attention of major companies and institutions, marking a shift in its perception and utility. This growing acceptance culminated in February 2021 when Bitcoin's market capitalization hit the historic milestone of $ 1 trillion, showcasing its growing prominence in the financial world. Over these years, other digital currencies like Ethereum, Ripple, and Litecoin have emerged, each with unique features, but generally following the decentralized model introduced by Bitcoin.

3. Technology behind Bitcoin: Decentralization and Blockchain

The advent of digital currencies brought forth a new realm of financial transactions, one that operates independently of traditional, centralized monetary systems. This paradigm shift posed unique challenges, chief among them being the assurance of transaction integrity in a decentralized network. The need for a robust system to validate and secure transactions without central oversight set the stage for the development of Bitcoin's distinctive features. This backdrop is crucial for appreciating the significance of Bitcoin's approach to resolving the double-spending issue and its reliance on blockchain technology as a fundamental tool in achieving this.

DOI: 10.54254/2754-1169/86/20240942

Bitcoin's most significant contribution lies in its innovative solution to the double-spending problem [3], a fundamental challenge in digital financial transactions, without involving centralized authority to distribute coins or to track who holds which coins. The double-spending issue arises when a unit of digital currency is used more than once, undermining the integrity of the transaction system. Formally, a payment system is not vulnerable to the double-spending problem if the probability of a successful double spend can be made arbitrarily close to zero. In a traditional, centralized financial system, this problem is easily managed by the central authority, which validates transactions and ensures that each unit of currency can only be spent once. However, in decentralized systems, where there is no central authority to oversee transactions, preventing double-spending becomes a complex issue. Bitcoin addresses this challenge through a novel consensus mechanism, which is called blockchain technology, in a decentralized environment [4].

The blockchain is the foundational technology of Bitcoin. Essentially, it's a public ledger that records all confirmed transactions in a chain of blocks. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.

The mechanism can be summarized in the following steps:

●Transaction Data: When a Bitcoin transaction is made, it's broadcasted to the network.

●Block Creation: Transactions are grouped into a block by miners (nodes in the network that validate transactions).

●Validation Process: Miners solve a computational puzzle, known as Proof of Work][5] (PoW), to validate a block. The PoW involves finding a number (nonce) that, when hashed with the block content, produces a result within a specific range. This process is computationally intensive and serves as the cornerstone of Bitcoin's security. The simplified version of the PoW equation is: Hash (block contents+nonce)¡target Here, the "Hash" is a cryptographic function, the "nonce" is a variable number miners are solving for, and the "target" is a threshold that determines the difficulty level of the puzzle.

●Adding to the Blockchain: Once the PoW puzzle is solved, the block is added to the blockchain. This block, now containing a unique hash and the previous block's hash, links back to the previous block, forming a chain.

●Consensus and Verification: Other nodes in the network verify the solution to the PoW and, once verified, accept the new block. This consensus mechanism [6] ensures that all nodes have an identical copy of the ledger, maintaining the integrity and chronological order of the blockchain.

The security of Bitcoin against double-spending is maintained as long as the cumulative computational power employed by honest miners is greater than that of any potential attacker. This ensures that the honest blockchain grows at a faster rate, preventing attackers from overtaking it with fraudulent transactions.

By leveraging blockchain technology, Bitcoin creates an immutable ledger of transactions. Each transaction is verified and added to the blockchain, ensuring that once a unit of Bitcoin is spent, it cannot be used again. This mechanism effectively resolves the double-spending problem without the need for a centralized governing body, marking a groundbreaking development in the realm of digital currencies and their potential for secure, autonomous transactions.

4. Monetary Functions of Digital Currencies

Digital currencies, especially Bitcoin, have introduced a new paradigm in the financial world, challenging traditional notions of monetary functions. This section examines how digital currencies fulfill or diverge from the basic functions of money: as a medium of exchange, a store of value, and a unit of account, and explores the underlying reasons for their performance in these roles.

DOI: 10.54254/2754-1169/86/20240942

4.1. Medium of Exchange

Bitcoin and its counterparts have made significant strides as mediums of exchange [7]. They enable the transfer of value across borders swiftly and with relatively low fees, particularly for online transactions.

Their digital nature allows for innovative payment solutions, such as micropayments and smart contracts, that traditional currencies cannot feasibly support due to the higher costs and complexity of managing small transactions. However, the extent to which digital currencies are used for everyday transactions remains limited compared to fiat currencies, partly due to volatility and regulatory uncertainty that affect their acceptance by merchants and consumers. Its effectiveness is undermined by significant price fluctuations, which can discourage merchants and consumers from using it for daily transactions. The hesitation is further exacerbated by the potential for sudden regulatory changes, which can swiftly alter the currency's legality and usability across borders.

4.2. Store of Value

A stable store of value is one that maintains its worth over time, allowing holders to preserve capital. The function of digital currencies as a store of value is arguably the most debated, struggle to perform this function reliably due to their high price volatility. Supporters claim that attributes such as the fixed supply of Bitcoin can protect against inflation, a common issue for fiat currencies subject to central bank policies. Yet, the price volatility witnessed in cryptocurrency markets can undermine their reliability as a store of value. Frequent and unpredictable price swings can lead to substantial losses in purchasing power in short periods, counteracting the very principle of a store of value. This volatility stems from a variety of factors, including speculative trading and evolving regulatory landscapes, which can lead to dramatic price fluctuations over short periods.

4.3. Unit of Account

A unit of account is an essential attribute of money that allows it to represent the value of goods and services, enabling it to serve as a standard measurement of value within an economy. Digital currencies face challenges in this area due to the same volatility that affects their role as a store of value. The widespread fluctuation in their value, when expressed in fiat terms, makes pricing goods or services in cryptocurrencies impractical for many businesses. Furthermore, the tendency to revert to fiat currency values when assessing the worth of cryptocurrencies indicates that they have not yet fully established themselves as independent units of account.

While digital currencies have shown potential to fulfill some of the traditional functions of money, they have not yet achieved these functions to the same extent as fiat currencies. The primary reason behind these challenges is the speculative nature of digital currency markets, which are relatively new and lack the depth and stability of traditional financial systems. Furthermore, the nascent regulatory environment contributes to market uncertainty, affecting their ability to function as a consistent store of value and unit of account. With their continued evolution, adoption, and integration into the global economy, these roles may become more defined and potentially more stable, aligning more closely with the established functions of money. The effectiveness of digital currencies in fulfilling these monetary functions will significantly influence their role in financial markets and the formulation of monetary policy. However, for the present, the adoption of digital currencies in these monetary roles remains limited.

DOI: 10.54254/2754-1169/86/20240942

5. Monetary Policy of Bitcoin

Digital currencies, especially Bitcoin, have brought to life a form of monetary policy that resembles the "k-percent rule" advocated by Milton Friedman [8], which calls for a fixed growth rate of the money supply. Bitcoin's protocol envisions a future where the creation of new bitcoins will cease, potentially reaching a point where the growth rate becomes zero or even negative, as coins are permanently lost when private keys are forgotten. This fixed supply cap means that Bitcoin's money supply is inelastic and not responsive to demand fluctuations, potentially leading to deflationary pressures in an economy if adopted widely. The demand for digital currencies is influenced by factors such as technological adoption, market sentiment, and the regulatory environment, rather than the economic indicators that typically influence fiat currencies.

This raises pivotal questions within monetary policy: the effects on an economy when its growth outpaces the growth of its money supply. Observing the Bitcoin economy offers a glimpse into what might happen in such a scenario. Meanwhile, this fixed supply cap means that Bitcoin's money supply is inelastic, and not responsive to demand fluctuations. Theoretically, if Bitcoin were to be widely adopted, its limited, predetermined supply could lead to deflation, much like the gold standard's impact has historically been noted by economists like Krugman. It's also worth mentioning that the demand for digital currencies is influenced by factors such as technological adoption, market sentiment, and regulatory environment, rather than the economic indicators that typically influence fiat currency. Acknowledging these deflationary risks, some developers have proposed cryptocurrencies with alternative rules. Primecoin and Peercoin, for instance, have modified the Bitcoin protocol to allow an expanding money supply, with Peercoin aiming for a growth rate around 1 percent, thereby sidestepping Bitcoin's fixed supply's deflationary constraints. Yet, whether decentralized cryptocurrencies can incorporate monetary policies that adapt to economic conditions remains uncertain. Bitcoin's current monetary policy does not account for real-world economic activity, it is a system based on a rigid supply schedule irrespective of economic demand. While the blockchain provides some nominal data, like transaction volumes and amounts, it lacks the ability to assess the real value exchanged, limiting the potential for an automatic, data-driven monetary policy.

6. Conclusion

In conclusion, digital currencies, led by Bitcoin, have sparked significant discourse in monetary finance, probing the boundaries of money's traditional roles and prompting a re-examination of monetary policy in the digital age. Despite the innovative solutions they offer and the promise of decentralization, instability and the current regulatory environment have prevented their full acceptance as the equivalent of traditional fiat currencies. These currencies are at a critical juncture in their development.; as the market matures and regulatory frameworks evolve, they have the potential to become more stable and integrated into the global financial system. The ongoing development and acceptance of digital currencies will be a key area to watch, with the possibility of reshaping monetary theory and practice in profound ways. Although this study provides a preliminary study on Bitcoin and digital currencies in the global financial system, it lacks a certain breadth in terms of data acquisition and should include analysis related to data. For future research directions, the acceptance of digital currencies in different countries and regions should be considered, as well as the user experience and market acceptance in different regions.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Decentralized business review, 2008.

DOI: 10.54254/2754-1169/86/20240942

[2] *Arvind Narayanan and Jeremy Clark. Bitcoin's academic pedigree. Communications of the ACM, 60 (12):36-45, 2017.*
[3] *Usman W Chohan. The double spending problem and cryptocurrencies. Available at SSRN 3090174, 2021.*
[4] *Laurie Hughes, Yogesh K Dwivedi, Santosh K Misra, Nripendra P Rana, Vishnupriya Raghavan, and Viswanadh Akella. Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. International journal of information management, 49:114-129, 2019.*
[5] *Bahman Zohuri, Hang T Nguyen, and Masoud Moghaddam. What is the cryptocurrency. Is it a Threat to Our National Security, Domestically and Globally, pages 1-14, 2022.*
[6] *Rainer Bohme, Nicolas Christin, Benjamin Edelman, and Tyler Moore. Bitcoin: Economics, technology, and governance. Journal of economic Perspectives, 29(2):213-238, 2015.*
[7] *Dirk G Baur, Kihoon Hong, and Adrian D Lee. Bitcoin: Medium of exchange or speculative assets? Journal of International Financial Markets, Institutions and Money, 54:177-189, 2018.*
[8] *Milton Friedman. A program for monetary stability. Number 3. Ravenio Books, 1960.*