



Blockchain Technology and Cryptocurrency: How Decentralization is Disrupting Traditional Finance

Apurba Ghosh¹, Payel Mondal², Amit Kumar Prajapati³ and Fazeel Ibtesam⁴

Faculty, Department of Basic Science and Humanities, Narula Institute of Technology, Kolkata, India^{1,2}

Student, Department of Artificial Intelligence and Machine Learning, Narula Institute of Technology, Kolkata, India^{3,4}

Abstract: In this era of digital evolution, we cannot think currency only as a piece of paper only while we are sharing our emotions through emojis. Though we use digital transaction for our entertainment it will remain a matter of strain when an announcement of demonetization is there. We need an alternative form of currency under my control, secure to use and has a broader aspect. Here cryptocurrency comes into the role termed as digital or virtual currencies underpinned by cryptographic systems. Cryptocurrencies operate on a decentralized network, meaning they are not controlled by a single entity such as a government or financial institution. Instead, they rely on a network of nodes, or computers, to verify and process transactions. These nodes work together to ensure the accuracy and security of the transactions, making it difficult for anyone to manipulate the system. Blockchain is a decentralized, distributed ledger technology that allows for secure, transparent, and tamper-proof transactions. Each block in a blockchain contains a cryptographic hash of the previous block, along with a timestamp and transaction data. Cryptocurrencies like Bitcoin and Ethereum use blockchain technology to facilitate peer-to-peer transactions without the need for intermediaries such as banks or financial institutions. In this paper we will discuss about cryptocurrency and its mining together with how it works as decentralized system. Also, we will focus on the effectiveness of cryptocurrency on our traditional finance system and its constraints to use.

Keywords: Cryptographic Algorithms, Stablecoin, Bitcoin, Money Laundering

I. INTRODUCTION

Over the recent years, there has been a notable surge in technological advancements on a global scale. These innovations have sparked significant changes in various sectors, particularly in finance and governance. The rise of cryptocurrencies and blockchain technologies is just one facet of the larger trend of technologies enabling peer-to-peer (P2P) transactions, personalized product experiences, and adaptable production methods. This trend gained momentum in the aftermath of the worldwide financial crisis about a decade ago. Major digital platforms like Alibaba, Amazon, Uber, and Airbnb are displacing traditional brick-and-mortar stores, service providers, and conventional employment models. Blockchain technologies aspire to push the envelope even further by orchestrating P2P transactions and information exchanges without relying on the presence of intermediary companies. The question of whether these technologies will entirely supplant intermediaries, or if new forms of trustworthy middlemen will emerge, remains unanswered.

Cryptocurrencies stand as the pioneering, and consequently, the most mature manifestation of blockchain technologies. They establish currency independently of central banks and streamline transactions outside the realm of financial establishments. The achievements of numerous cryptocurrencies exert competitive force on the transaction modalities employed by established financial bodies. Nevertheless, significant constraints have come into view. The decentralized structuring of markets without dependable intermediaries can incur substantial expenses, and the instability in the valuation of cryptocurrencies poses a significant hindrance to their potential as a substitute for official legal tender.

A decade after a groundbreaking experiment aimed at establishing a cryptocurrency for secure and confidential digital transactions without relying on central or commercial banks, cryptocurrencies have evolved into a multi-billion-dollar industry. By December 2017, the average value of a single bitcoin (the inaugural cryptocurrency) had surged from mere cents in 2009 to \$15,000, doubling in value within a single month.

These impressive gains captured the attention of global investors. On December 1, 2017, the U.S. Commodity Futures Trading Commission granted approval for the trading of bitcoin futures. Despite the bitcoin's price dipping to around \$8,000 in April 2018, the collective value of circulating bitcoins reached approximately \$150 billion by April 10, 2018. Prominent corporations and collaborative groups of individuals are engaged in a competition for the privilege of appending new transactions to the existing chain. Their earnings, in the form of newly minted bitcoins and transactional charges, amass to nearly \$20 million daily.



II. CRYPTOCURRENCY AND ITS MINING

Cryptocurrency, a variant of digital currency operating on an open and decentralized framework, leverages cryptography to heighten security and govern the creation of new units. It is hailed as the evolutionary progression beyond traditional monetary transactions. A diverse array of cryptocurrencies exists today, with Bitcoin reigning as the most eminent among them. The genesis of cryptocurrencies is rooted in the process of mining, serving as compensation for validating transactions. The velocity at which hashing functions are computed to validate transactions has surged using specialized devices such as FPGAs and ASICs, executing intricate hashing algorithms like SHA-256 and Scrypt. This advancement has expedited the production of cryptocurrencies. This pursuit to develop more economical yet effective machines has been relentless since the inception of the first cryptocurrency, Bitcoin, in 2009. However, as an increasing number of individuals venture into the realm of virtual currency, the computational complexity of generating hashes for validation has markedly escalated over time.[1], [2]

Mining is the integral process wherein generation, transmission, and validation of transactions of cryptocurrencies is done. It ensures stable, secure and safe propagation of the currency from the payer to payee. Unlike fiat currency, where a centralized authority controls and regulates the transactions, cryptocurrencies are decentralized and work on a peer-to-peer system. Banks that generate physical currency and monitor the transactions require huge infrastructure to function and operate. Cryptocurrencies overcome this need by implementing a mining system where people in the network, called 'miners' or 'nodes', monitor and validate transactions which generates currency.

The main purpose of mining is to generate and release coins into its coin economy. Whenever a transaction takes place and is validated, miners collect these transactions and include them into the block they are currently solving. Every block must be solved before being broadcasted and put in the block chain. Solving of a block involves mathematical puzzles which are difficult to unlock and crack provided there will be some constraints on the output generated.[3] Only on solving the mathematical puzzle is one allowed to add the block to the ledger and a reward of coins is given in return. Thus, mining eventually boils down to a competition of mathematical puzzles to solve for the reward of coins. This mechanism prevents miners from easily procuring coins and thus maintains the fairness of the system.[4]

III. DECENTRALIZATION ILLUSION

Voting privileges within decentralized autonomous organizations and the accumulation of wealth exhibit a tendency toward even greater concentration in the realm of cryptocurrencies, surpassing the levels observed in traditional financial systems. Additionally, the capacity of decentralized blockchain technology to handle substantial transaction volumes is limited, and it lacks the provision for transaction reversals.

Consequently, it appears inevitable that intermediaries will arise to streamline the operation of unwieldy decentralized services for users. This prospect gains traction given the potential profits associated with such intermediation. Candidly stated, economists at the Bank for International Settlements have reached the conclusion that a "decentralization illusion" prevails, stemming from the essential requirement for centralized governance and the inclination of blockchain consensus mechanisms to centralize power. Indeed, a multitude of crypto businesses that have emerged over the past decade make no attempt to feign decentralization. Centralized exchanges, wallet providers, and stablecoin issuers, for instance, assume pivotal roles within the crypto ecosystem. Many of these intermediaries essentially constitute novel (and often unregulated) equivalents of their counterparts in traditional finance.

Thus, users of cryptocurrencies will invariably find themselves compelled to place trust in individuals. These individuals are no less driven by greed or biases than others, but they often operate with minimal regulation (occasionally even without identification). In the absence of consumer protection regulations, the crypto industry's assertions of advancing financial inclusion adopt a more disconcerting demeanour. The realm of crypto is undeniably fraught with breaches and fraudulent schemes that target users. However, at a more fundamental level, the valuation of crypto assets rests entirely upon demand, as there is no inherent productive capacity underpinning them. Consequently, founders and initial investors can reap profits only by locating new investors to whom they can sell. Should these entrepreneurs rely on historically underserved populations to constitute that market, the most vulnerable segments of society—both in developed and developing economies—might bear the brunt of adverse consequences.

Even if the market for crypto assets were hypothetically sustainable, scepticism abounds regarding crypto's potential to democratize finance. For instance, crypto lending platforms mandate substantial amounts of crypto collateral before granting loans, thereby excluding those without preexisting financial assets. Despite the frequent promotion of stablecoins as superior payment mechanisms for underserved populations, the World Economic Forum's evaluation concludes that "stablecoins as currently implemented would not yield compelling new advantages for financial inclusion beyond those already provided by existing options."



IV. FIXING FINANCE'S FLAWS

To clarify, the issue of financial inclusion is an authentic and pressing concern, and there are numerous other issues within traditional finance that necessitate resolution. Part of the rationale behind the remarkable success of crypto firms, venture capitalists, and lobbyists lies in their articulate and compelling indictment of the prevailing financial system. The major banks performed dismally in the lead-up to 2008 (with some still continuing such behaviour), and a substantial portion of the population remains underserved by the current financial structure. Particularly in the United States, the speed of payment processing is insufficient. Yet, these issues are predominantly political rather than technological in nature. Unless the underlying political challenges are addressed, the emergent crypto intermediaries will merely perpetuate the existing predicaments. While technological enhancements to our present systems might indeed be warranted, frequently there already exist simpler, centralized technological remedies (as is the case with real-time payments). The absence often lies in the political determination to implement these solutions.

Foremost, banks should be proscribed from issuing or trading any form of crypto asset, encompassing stablecoins (which are infrequently employed for tangible-world transactions; their primary function is to facilitate crypto investments). Implementing such measures could be executed within existing frameworks of banking laws, often necessitating no new regulations or statutes. However, policymakers might contemplate enacting new regulations or statutes targeted more directly at the crypto industry. Given the absence of benefits and the presence of adverse impacts associated with crypto, a total ban might be apt. If policymakers opt against an outright ban, they should manage crypto's detrimental effects through more targeted regulations or rules. Imposing regulations and rules on centralized crypto intermediaries would be relatively straightforward (although jurisdictional complications could arise); extending these to ostensibly decentralized entities might encounter additional obstacles. Nevertheless, these challenges aren't insurmountable, as no facet of crypto is truly decentralized. For instance, individuals could be barred from holding governance tokens within noncompliant decentralized autonomous organizations—an enforcement relatively easy to execute against founders, venture capital firms, and major holders.

Ultimately, policymakers should remain impervious to questionable promises of decentralization and democratization; instead, they should be proactive in curtailing the adverse repercussions of crypto. The architects shaping the future of finance must address an array of predicaments and devise the most straightforward and direct solutions. Attempting to retrofit crypto assets and blockchains as remedies for these predicaments is liable to exacerbate the situation further.

V. DISCREPANCY BETWEEN BITCOIN AND TRADITIONAL FINANCE

The subsequent illustration illustrates a time series plot showcasing the unprocessed data for spot Bitcoin prices, the S&P 500 Stock Index, the S&P 500 Bond Index, the USD Broad Exchange Rate, Gold, the WTI Oil Price, the VIX, the US Economic Policy Uncertainty (US_EPU) index, and the Twitter-based economic uncertainty (TEU) index. The timeline spans from April 29, 2013, to June 30, 2020. Notably, conspicuous fluctuations emerge beginning January 1, 2020. During this period, the value of gold surged to an all-time high, while the WTI Crude Oil price plummeted to its nadir (as evident in the highlighted segment in Figure 1). [5-8] Moreover, it's discernible that all measures of uncertainty exhibited a marked ascent during the initial wave of the COVID-19 pandemic.

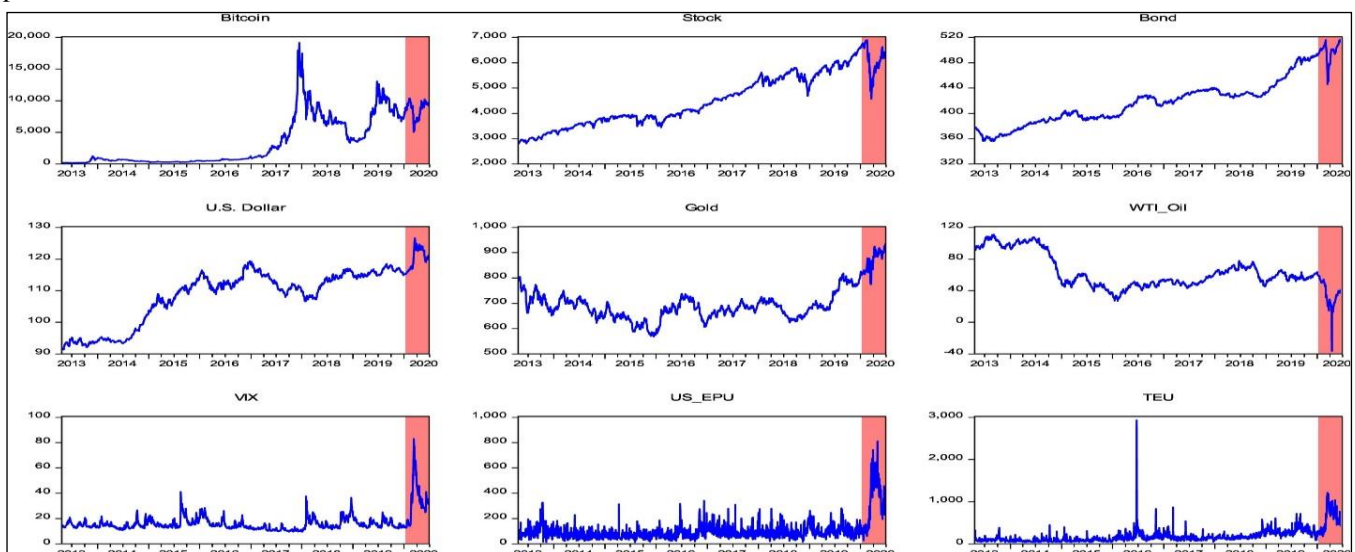


Fig.1 Daily time evolution of bitcoin, traditional financial assets and major global uncertainty measures.



The aforementioned visual representations depict the fluctuation in daily data series encompassing Bitcoin price, the S&P 500 stock index, the S&P bond index, the USD Broad Exchange Rate, Gold price, the WTI Crude Oil price (WTI_Oil), the VIX, the US economic policy uncertainty index (US_EPU), and the Twitter-based economic uncertainty index (TEU). The timeline spans from April 29, 2013, to June 30, 2020. The highlighted red region corresponds to the period marked by the advent of the COVID-19 pandemic. Additionally, the subsequent visual representation portrays the transformed data series under examination. This includes returns on Bitcoin and other asset classes (namely the USD, Bonds, Stocks, Gold, and Crude Oil Returns), the VIX, the US EPU index, and the Twitter-based economic uncertainty (TEU) index, presented in logarithmic form.

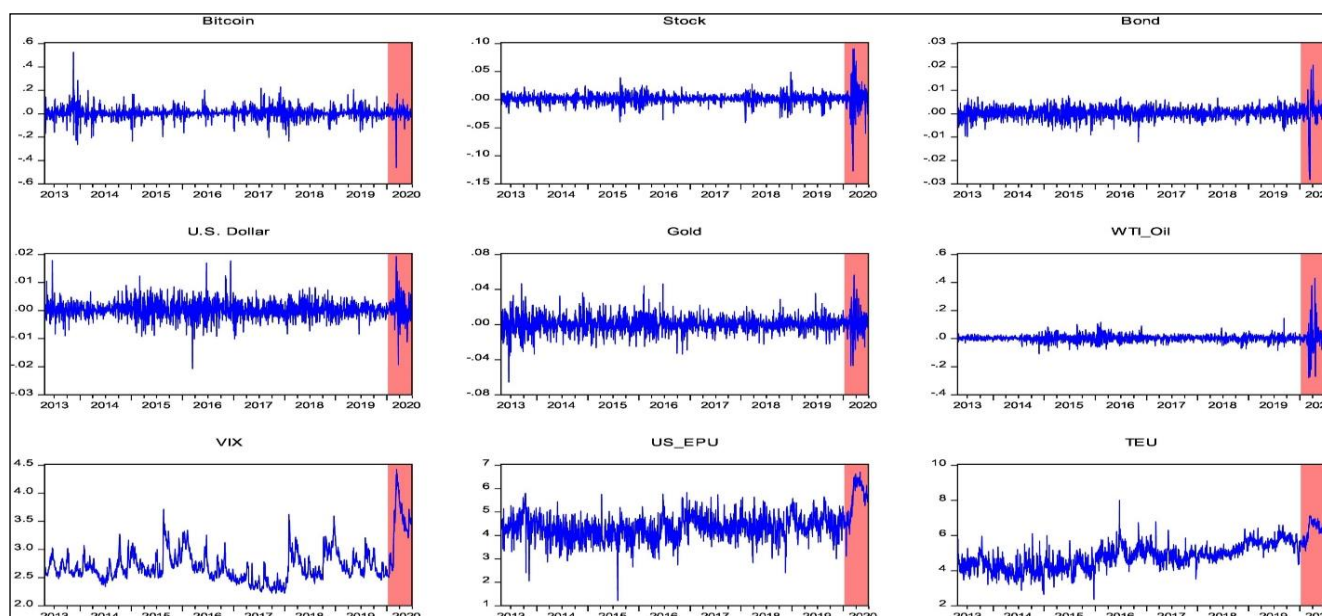


Fig. 2 Daily returns of bitcoin, traditional financial assets and major global uncertainty measures

Fig2 further presents the returns within the daily data series, encompassing Bitcoin price, the S&P 500 stock index, the S&P bond index, the USD Broad Exchange Rate, Gold price, the WTI Crude Oil price (WTI_Oil), the VIX, the US economic policy uncertainty index (US_EPU), and the Twitter-based economic uncertainty index (TEU).[9-11] The depicted red region demarcates the phase coinciding with the advent of the COVID-19 era.

VI. TRADITIONAL BANKING EFFECTED BY CRYPTOCURRENCY

Cryptocurrency's influence on traditional banking is perhaps most pronounced in the realm of disruption it has engendered. By providing an alternative avenue for executing financial transactions, cryptocurrency has presented a direct challenge to the established banking paradigm. This transformative impact has precipitated a redistribution of influence, effectively diverting power from conventional banks toward cryptocurrency exchanges. Cryptocurrency exchanges have emerged as pivotal players in this shifting landscape, offering users an avenue to engage in the purchase and sale of digital currencies sans the requirement of a traditional bank. This autonomy translates to the ability to effectuate fund transfers without intermediation by a bank, often resulting in swifter and more cost-effective transactions. Moreover, cryptocurrency exchanges augment transparency by recording all transactions on a publicly accessible ledger. With this foundation established, we now delve into the subsequent subjects.

Regulatory Challenges: The advent of cryptocurrency has indeed caused significant disruption within the traditional banking landscape, but it has also ushered in a complex array of regulatory challenges. Cryptocurrency functions autonomously, detached from the oversight of central banks, thus posing a formidable obstacle for governments striving to establish effective regulation. Consequently, apprehensions have arisen, primarily centered around issues such as money laundering and illicit activities. Governments across the globe grapple with the task of devising regulatory frameworks to govern cryptocurrency. While some nations have opted for an outright ban on cryptocurrency, others have opted for stringent regulatory measures. The dearth of standardized regulations has engendered an atmosphere of uncertainty, casting shadows over the market and impeding the entrance of traditional banks into the cryptocurrency domain.

Security Concerns: Cryptocurrency's influence on traditional banking extends to the realm of heightened security concerns it has brought to the forefront. Cryptocurrency transactions rely on the application of intricate cryptographic algorithms for safeguarding, a measure that imparts robust security.



However, this very reliance on cryptography renders cryptocurrency transactions susceptible to hacking. Spanning back centuries, traditional banks boast an extensive history and have formulated rigorous security protocols to fortify the protection of customer assets. In stark contrast, cryptocurrency exchanges are relatively recent additions and have not yet attained the same level of security maturity. Consequently, several instances of high-profile breaches targeting cryptocurrency exchanges have emerged, compromising consumer confidence in the market's integrity.

VII. CONCLUSION

In summary, the influence of cryptocurrency on traditional banking stands as a marked and multifaceted phenomenon. Its disruptive force has reverberated through the conventional banking system by furnishing an alternative avenue for financial transactions. Moreover, its introduction has engendered heightened competition within the financial landscape, compelling traditional banks to recalibrate and cultivate innovation. Concurrently, cryptocurrency's advent has ushered in a realm of regulatory intricacies and security apprehensions. Governments worldwide grapple with the formulation of comprehensive regulations to address cryptocurrency's unique attributes, while the absence of standardized rules fuels market ambiguity. Additionally, the security integrity of cryptocurrency transactions has been cast into doubt following several noteworthy breaches. Collectively, the repercussions of cryptocurrency on traditional banking remain in a state of flux. While its disruptive impact on the industry is undeniable, the trajectory toward becoming a viable alternative to traditional banking in the long term remains an open question.

REFERENCES

- [1]. Peck M. E. (2013). The Bitcoin Arms Race is on! Spectrum, IEEE, 50 (6), 11-13.
- [2]. Allied Control – Analysis of Large-Scale Bitcoin Mining Operations (White Paper).
- [3]. Brito J. and Castillo A. (2013). Bitcoin: A Primer for Policymakers.
- [4]. Nakamoto S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, | URL: <https://bitcoin.org/bitcoin.pdf>, 2008.
- [5]. Nir Y. and Min T. C. (2017). End-to-End Verifiability in E-Voting Systems. In Handbook of eID Security (pp. 1-24). Springer, Cham.
- [6]. Raval S. (2016). Decentralized Applications: Harnessing Bitcoin's Blockchain Technology. O'Reilly Media.
- [7]. Thomas M. C., Ojha V. and Nadarajah N. (2020). Blockchain Technology in Public Administration and Governance: An Overview of the Indian Experience. In Public Administration and Information Technology (pp. 285-305). Springer, Singapore.
- [8]. Vasudevan A., Potnis D., Suthaharan P. and Prakash M. (2018). Blockchain-Based Decentralized Voting System. In Proceedings of the International Conference on Information Technology (ICIT) (pp. 55-60). IEEE.
- [9]. Nakamoto S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from <https://bitcoin.org/bitcoin.pdf>.
- [10]. Drescher D. (2017). Blockchain Basics: A Non-Technical Introduction in 25 Steps. Apress.
- [11]. Kosba A., Miller A., Shi E., Wen Z. and Papamanthou C. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In Proceedings of the IEEE Symposium on Security and Privacy (S&P) (pp. 839-858). IEEE.