

Analysis the Principle, Applications and Future for Cryptocurrency

Zhejia Hu^{1,a,*}

¹Century College, Beijing University of Posts and Telecommunications, Beijing, China

a. huzhejia@ldy.edu.rs

*corresponding author

Abstract: Cryptocurrencies, powered by blockchain technology, have revolutionized the financial landscape by offering decentralized, secure, and transparent alternatives to traditional currencies since it was very first proposed. This study explores the key principles of cryptocurrency, including its underlying cryptographic mechanisms, and evaluates its current market status, applications, and the challenges it faces, e.g., volatility, regulatory uncertainty, and scalability issues. According to the analysis, while cryptocurrencies have made significant strides in adoption and innovation, they still face substantial barriers to widespread use, particularly in comparison to traditional digital payment systems like Alipay. Addressing these limitations through technological advancements and regulatory clarity will be crucial for cryptocurrencies to achieve broader mainstream integration. This research highlights the transformative potential of cryptocurrencies while identifying the areas that require development for them to realize their full promise in the global financial system and how to make cryptocurrencies market popularize while maintaining its unique features and advantages.

Keywords: Cryptocurrencies, mainstream, potential.

1. Introduction

Blockchain, the underlying technology behind cryptocurrencies, has evolved remarkably since its inception. Originally conceptualized in 1976, the paper "New Directions in Cryptography" introduced the concept of distributed ledgers. Stuart Haber and Scott Stornetta's work further developed the idea of timestamping data. David Chaum's model for "Electronic Cash" also contributed to the foundation of blockchain, followed by e-cash protocols addressing double-spending. In 1997, Adam Back's "hashcash" provided a spam control solution, inspiring Wei Dai's "b-money," a peer-to-peer digital currency concept [1], blockchain technology remained underdeveloped until the release of Bitcoin by Satoshi Nakamoto who is also considered as the inventor of blockchain technology in 2008. This breakthrough in decentralized technology allowed for the secure, peer-to-peer transfer of digital assets without the need for intermediaries like banks. It enables parties who may not have reason to trust each other to agree on the current assets and who has those assets, so that they may conduct new business [2]. The development of blockchain technology did not stop with the birth of the Bitcoin. Over time, blockchain technology has revolutionized the management of contracts, transactions, and records, transforming the fundamental structures of global economic, political, social, and legal systems [3] and blockchain technology also has come a long way, breaking free from a niche concept

for time-stamping documents to a transformative technology with the potential to revolutionize multiple industries. Its continued development will likely shape the future of digital economies, governance, and beyond.

Blockchain, the decentralized framework and distributed computing model behind Bitcoin and other cryptocurrencies, has attracted considerable attention in recent years, both in academic research and practical applications [4]. A 2016 report from the European Commission estimated the global market value of cryptocurrency to exceed 7 billion euros. By 2018, the total market capitalization of cryptocurrencies had surged to USD 128 billion, further increasing to more than USD 237 billion by 2020. Remarkably, during the third quarter of 2020, Ethereum alone averaged over 1,100 transactions per day [5]. As of 2024, the global cryptocurrency market has expanded significantly, reaching a market capitalization of over USD 2 trillion. Bitcoin, Ethereum, and numerous altcoins have gained popularity, and institutional investors, including Tesla and MicroStrategy, have incorporated cryptocurrencies into their portfolios. This rapid expansion is attributed to the factors like increased interest from institutional investors, the rise of decentralized finance (DeFi), and a growing global recognition of cryptocurrencies as legitimate financial assets. decentralized finance (DeFi), NFTs, and the increasing need for financial sovereignty. As an emerging interdisciplinary field, the analysis and mining of cryptocurrency transactions from a network perspective have garnered growing interest. Researchers are increasingly focusing on exploring the complex interactions and structures within cryptocurrency networks, aiming to understand transaction patterns, network security, and scalability [6]. These efforts are crucial for enhancing the efficiency, transparency, and trustworthiness of blockchain systems, as well as for developing more robust applications in financial and non-financial domains. However, regulatory uncertainty and market volatility continue to affect the industry, despite the significant growth, cryptocurrencies remain subject to market volatility and regulatory uncertainties. This highlights both the transformative potential of cryptocurrencies and the challenges they present to conventional financial systems.

Aiming at analyzing the key principles, applications, limitations, and prospects of cryptocurrency, this paper will explain basic Descriptions of blockchain techniques, describes the principles governing cryptocurrency, focusing on cryptography and transaction mechanisms, Provides an analysis of the current status of cryptocurrency, examining market trends and real-world applications, discusses limitations and future outlooks, considering regulatory challenges and technological advancements and summarizes findings, discusses the significance of the research, and provides concluding remarks.

2. Basic Descriptions of Blockchain Technique

A blockchain is a decentralized digital ledger, continuously maintained by multiple nodes using distributed cryptographic technology, eliminating the need for a central authority. Its decentralized structure also leads to its designation as distributed ledger technology (DLT) [7]. Due to this characteristic, blockchain facilitates secure, transparent, and tamper-proof record-keeping within a decentralized network. Each block in the chain holds a set of transactions that, once verified by a consensus mechanism, are irreversibly incorporated into the blockchain. This immutability is maintained through cryptographic hashing, making it nearly impossible to alter the data once recorded. Blockchain technology's evolution started with the creation of Bitcoin by the pseudonymous Satoshi Nakamoto in 2008, which introduced the foundational concept of blockchain and represented the first use of cryptocurrencies in financial systems, particularly for digital transactions—this phase is often referred to as Blockchain 1.0. The second stage of blockchain development brought smart contracts, expanding its utility beyond mere monetary exchanges to cover assets such as stocks, loans, and smart properties. The third generation of blockchain technology improves on security compared to both Blockchain 1.0 and 2.0, offering greater scalability, adaptability, and sustainability. It's also expanded

blockchain's use cases even further, applying the technology in fields such as healthcare, government, and scientific research, moving beyond its initial focus on finance. In just under a decade, blockchain has rapidly evolved through these three stages and is now progressing into a fourth generation, which integrates Artificial Intelligence (AI) and advanced digital intelligence solutions. The smart contracts, proof-of-work, mining, and digital signatures plus hash techniques are base for blockchain technologies [8]. smart contracts, which are self-executing contracts coded on platforms like Ethereum, allow for the automation of complex agreements without intermediaries. Proof-of-work, a broader term is called consensus protocols is ensuring agreement across decentralized nodes. Mining is a critical process in blockchain technology that ensures the validation and security of transactions by using computational power to solve complex cryptographic puzzles, enabling the addition of new blocks to the blockchain and maintaining the integrity of the decentralized network and hashing algorithms, which secure transaction data.

3. Principle of the Cryptocurrency

Cryptocurrency, a technology built on blockchain, is commonly utilized as digital currency. Unlike traditional forms of money, digital currency does not exist in a physical form; instead, it consists of data blocks that are validated through a hash function [9]. Cryptocurrencies operate on the principles of cryptographic security, decentralized control, and peer-to-peer transactions. At the core of any cryptocurrency is its reliance on cryptographic algorithms that secure transactions and protect the privacy of users. A currency lacking intrinsic value can function efficiently only when there is adequate trust among its users. For traditional fiat currencies, this trust is directed towards the central bank, or the state mandates its use through legal means, irrespective of public confidence. On the other hand, cryptocurrencies differ in that new issuances and transactions are authenticated by the most network participants. These participants operate within a system designed to be trustless, where they collectively monitor and verify transactions to ensure transparency and security [10]. In this system, the decentralized nature of the network ensures that the trust required in traditional fiat systems is replaced by cryptographic proof, making it a trustless environment. Participants verify each other's actions, eliminating the need for intermediaries like banks or government institutions, which are typically required to enforce trust in conventional financial systems. Cryptocurrency transactions are governed by protocols encoded within the blockchain, allowing for rules like transaction limits, fees, and rewards for miners to be enforced automatically. In many cryptocurrency networks, there are inherent transaction limits based on the size of the blockchain's blocks or the protocol itself. The transaction limit also serves as a mechanism to maintain security and ensure that the network remains decentralized. Transaction fees play a crucial role in the functioning of cryptocurrency networks. To prevent overload attacks (e.g., denial of service attacks) that could disrupt cryptocurrency operations, crypto exchanges implement transaction fees. These fees help to deter the transfer of insignificant amounts, thereby reducing unnecessary transactions that could burden the network [10]. These fees incentivize miners or validators to prioritize certain transactions over others, especially during periods of high network activity. Mining rewards are another crucial aspect of cryptocurrency transaction rules. This dual reward system ensures that miners have an ongoing incentive to maintain the network's security and verify transactions. Cryptocurrency transactions are regulated through a combination of limits that prevent congestion, fees that prioritize transactions and reward validators, and mining rewards that incentivize network security. These mechanisms ensure the efficient and decentralized functioning of cryptocurrency networks.

4. Current Status

Since 2020, cryptocurrencies have experienced rapid growth, with increased adoption by both individuals and institutions (seen from Fig. 1). Bitcoin has solidified its position as a "store of value" like digital gold, while Ethereum has become the foundation for a thriving decentralized finance (DeFi) ecosystem, hosting thousands of decentralized applications (dApps). In the early 2010, Laszlo Hanyecz purchased two pizzas from Papa John's for around USD 30, paying with 10,000 bitcoins. By 2018, the value of those bitcoins had soared to over USD 80 million [3]. As of 2024, the cryptocurrency market has a market cap of over \$2 trillion, with the adoption of stablecoins like Tether (USDT) and USD Coin (USDC) accelerating as people seek alternatives to volatile assets. Beyond financial speculation, cryptocurrencies have found practical applications in areas such as cross-border remittances, digital identity verification, and even government-backed central bank digital currencies (CBDCs). The People's Bank of China (PBOC) has conducted one of the most extensive real-world trials for cryptocurrency globally by issuing digital currency in several test cities. In Shenzhen, for instance, nearly 50,000 people were issued digital currency through a public lottery system, which could be used in over 3,000 stores within the city [5]. At one point, cryptocurrencies were declared illegal and banned in Zimbabwe, significantly hindering the sector's growth. However, the Minister of Finance (2018-2021) has shown great interest in digital currencies, advocating that Zimbabwe should leverage the knowledge of young people about cryptocurrencies and establish favorable regulations to enable the sector to flourish [11]. The current state of cryptocurrencies shows rapid growth and increasing integration into mainstream financial markets. Cryptocurrencies are now seen by many individuals and institutions as both an investment vehicle and a store of value. Moreover, their application continues to expand, especially in areas like decentralized finance (DeFi), cross-border payments, and smart contracts, showcasing significant potential. The rise of stablecoins has provided a buffer against the volatility of the cryptocurrency market, making them more practical for everyday transactions.

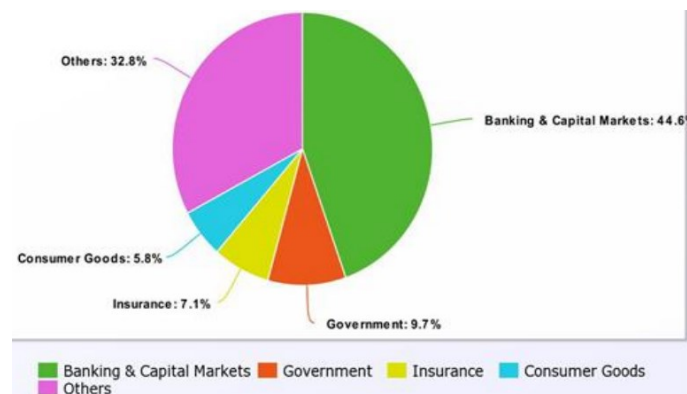


Figure 1: Industry using blockchain [1].

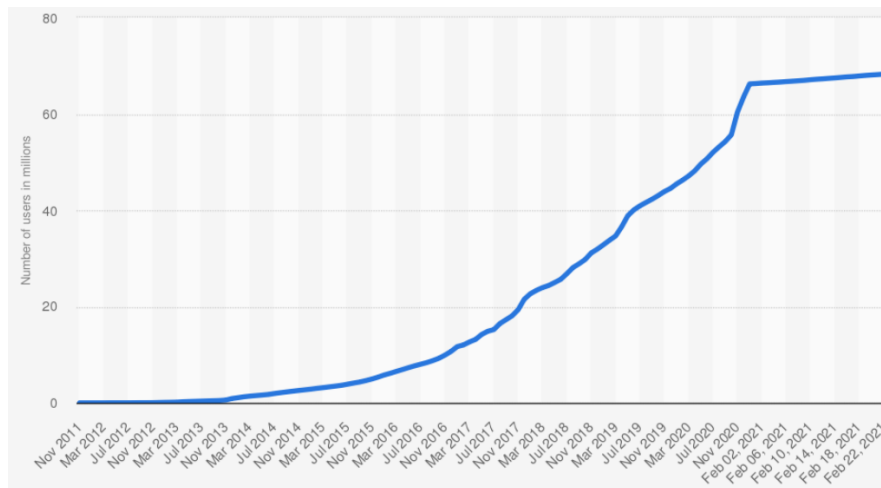


Figure 2: Number of Blockchain wallet users worldwide from November 2011 to February 22, 2021 (in millions) [4].

5. Limitations and Prospects

Cryptocurrency has gained popularity and become famous due to its unique non-regulated form and its potential to disrupt and challenge the traditional financial systems [12]. Despite their advantages, cryptocurrencies face significant limitations. One major issue is security, it is precisely because of its non-regulatory that the cryptocurrency market has more risks than the traditional, regulatory challenges also pose a hurdle. Governments worldwide have responded to cryptocurrencies with varying degrees of skepticism, often citing concerns around illicit activities, market manipulation, and the potential for destabilizing traditional financial systems. The Federal Trade Commission reports a significant rise in cryptocurrency scams between October 2020 and March 2021, with close to 7,000 individuals reporting losses exceeding \$80 million [12]. Obviously, this is not the first incident, nor will it be the last. For this reason, governments worldwide have responded to cryptocurrencies with varying degrees of skepticism, often citing concerns around illicit activities, market manipulation, and the potential for destabilizing traditional financial systems, each country struggle to handle it and introduce various legal systems for regulating cryptocurrency, some of them even have more specific and detailed measures, laws and regulations. For instance, Australia and Canada have recently passed legislation to regulate cryptocurrency transactions and the institutions that facilitate them, bringing them under the scope of anti-money laundering and counter-terrorist financing laws [5]. but questions about the security remain, countries including Algeria, Bolivia, Morocco, Nepal, Pakistan, and Vi have even issued explicit bans for all the cryptocurrencies [5].

Scalability challenges also pose a hurdle, greatly affected the progress and efficiency of transaction, as existing blockchains (e.g., Bitcoin and Ethereum) aims to mitigate this issue, but questions about the long-term scalability of decentralized systems remain large volumes of transactions due to their reliance on computationally expensive consensus mechanisms, until blockchain technology can scale effectively, it cannot compete with the transaction speeds and efficiency of centralized payment systems. Cryptocurrencies like Bitcoin and Ethereum are known for their high volatility. Unlike traditional digital payment systems that are linked to stable fiat currencies, the value of cryptocurrencies can fluctuate dramatically within short periods. This makes them less reliable for everyday transactions, where consumers and merchants expect stability in purchasing power. Moreover, cryptocurrencies require significant computational power and energy. This has raised environmental concerns, making them less appealing for widespread, everyday use. Besides, the process of acquiring, storing, and using cryptocurrencies remains complex for the average user.

Wallet management, private keys, and the risk of losing access to funds can deter people from using cryptocurrencies. These limitations highlight why cryptocurrencies, while innovative, currently cannot match the level of widespread usage and integration that digital payment platforms like Alipay have achieved. For cryptocurrencies to become more mainstream, solutions to volatility, scalability, regulatory clarity, and ease of use must be addressed. Looking ahead, the future of cryptocurrencies could involve greater regulatory clarity, broader institutional adoption, and the integration of blockchain into everyday digital systems. For cryptocurrencies to become more mainstream, solutions to volatility, scalability, regulatory clarity, and ease of use must be addressed.

6. Conclusion

To sum up, cryptocurrency, driven by blockchain technology, represents a revolutionary shift in how financial transactions are conducted. This research has explored the origins of blockchain, the cryptographic principles underlying cryptocurrencies, and the current market landscape, providing insights into both the opportunities and challenges that lie ahead. Despite their significant potential, cryptocurrencies face several challenges that hinder their widespread adoption. Issues such as regulatory uncertainty, high volatility, scalability limitations, and energy consumption remain major hurdles that must be addressed for cryptocurrencies to move beyond speculative assets and achieve broader acceptance in everyday transactions. As explored, cryptocurrencies have yet to reach the level of integration and convenience offered by traditional digital payment platforms, e.g., Alipay, largely due to these limitations. The significance of this research lies in its examination of both the opportunities and obstacles that lie ahead for the cryptocurrency industry. While there are significant barriers to overcome, the continuous evolution of blockchain technology and the growing interest from both individuals and institutions suggest that cryptocurrencies will continue to play a major role in shaping the future of global finance.

References

- [1] Sarmah, S.S. (2018) *Understanding blockchain technology*. *Computer Science and Engineering*, 8(2), 23–29.
- [2] Jaikaran, C. (2018) *Blockchain: Background and policy issues* (CRS Report No. R45116) Congressional Research Service.
- [3] Casalino, G. (2023) *A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges*. *Decision Analytics Journal*, 9, 100344.
- [4] Wisetsri, W., Vijai, C., Kasidit, C. and Jirayus, P. (2022) *Cryptocurrency – An overview*. *Journal of Positive School Psychology*, 6(2), 2694–2704.
- [5] Riley, J. (2021) *The current status of cryptocurrency regulation in China and its effect around the world*. *China & WTO Review*, 7(1), 135–152.
- [6] Wu, J., Liu, J., Zhao, Y. and Zheng, Z. (2021) *Analysis of cryptocurrency transactions from a network perspective: An overview*. *Journal of Network and Computer Applications*, 190, 103139.
- [7] Verma, S., Yadav, D. and Chandra, G. (2022) *Introduction of formal methods in blockchain consensus mechanism and its associated protocols*. *IEEE Access*, 10, 66611–66624.
- [8] Madakam, S. and Kolli, S. (2020) *Blockchain technologies fundamentals – Perceptions, principles, procedures and practices*. *Prajnan*, 48(4), 2019-2020.
- [9] Astuti, I.D., Rajab, S. and Setiyoudi, D. (2022) *Cryptocurrency blockchain technology in the digital revolution era*. *University of Raharja*.
- [10] Péter, P.G. and Zoltán, Z. (2023) *Cryptocurrency operating principle, market and risks*. *Acta Carolus Robertus*, 13(1), 62–75.
- [11] Mazorodze, T., Sibanda, V. and Tadu, R. (2022) *Towards a regulatory framework for the adoption and use of cryptocurrencies in Zimbabwe*. In *Blockchain technology*, 22.
- [12] Weichbroth, P., Wereszko, K., Anacka, H. and Kowal, J. (2023) *Security of cryptocurrencies: A view on the state-of-the-art research and current developments*. *Sensors*, 23(6), 3155.