THE PROMISING FUTURE OF BLOCKCHAIN TECHNOLOGY

Andrei BELII

Group TI-2310, Faculty of Computers, Informatics and Microelectronics
Technical University of Moldova, Chișinău, Republic of Moldova

Corresponding author: Andrei Belii, andrei.belii@isa.utm.md

Coordinator: **Corina TINTIUC,** university assistant, Department of Foreign Languages, TUM

Abstract: *Blockchain technology has been around for over a decade. The technology is primarily recognized as the backbone of cryptocurrencies like Bitcoin. This cutting-edge and secure information technology fosters innovation across business and industrial sector. However, existing limitations regarding scalability, flexibility, and cybersecurity constrain development of Blockchain. Emerging solutions are beginning to address these issues. The use of solar energy to power up the Blockchain network would highly reduce energy consumption. The given paper envisions the underlying technology behind cryptocurrency extremely promising. The number of live blockchains is rapidly increasing on a daily basis. There are four primary types of blockchain networks, which are private, public, hybrid and consortium. Future blockchains aim not only to serve as a means of storing wealth, but also to facilitate the storage of property rights, medical records, and various legal contracts. Undoubtedly, the impact of the transformative blockchain technology on a wide range of industries, including banking, healthcare, supply chains, e-commerce, education, and other fields, establishes it as one of the most innovative technologies of the twenty-first century.*

Keywords: *cryptocurrency, proof-of-work, decentralization, transactions, transparency, security.*

Introduction

When we think of Blockchain, the first thing that comes to mind is the popular Bitcoin cryptocurrency. Indeed, Blockchain technology began with the Bitcoin network and its creator is the mysterious Satoshi Nakamoto. As of February 2, 2024, Bitcoin makes up 48.6% of the total value of the crypto market [1].

Today blockchain technology is being used for smart contracts, digital identity management, supply chain oversight, and various other areas. The reason we have chosen to focus on this technology is its promising future. It holds the potential to revolutionize established business models and foster novel avenues for both growth and innovation.

What Is Blockchain?

In simple words, a blockchain is a series of blocks, where each block is securely connected to the next one using advanced cryptography formulas, forming an immutable chain. Each block typically contains a cryptographic hash of the previous block, a timestamp, and transaction data. Consequently, the whole chain is shared among many computers in a network, and each computer has its own copy. This setup makes sure that everyone sees the same information, and even if one computer fails, the others still have all the data. This makes blockchains very reliable and transparent, as no single entity controls the entire system.

Blockchains are divided into four main types: public, private, consortium and hybrid. Public blockchains, also known as permissionless blockchains, rely on cryptography and a consensus system like proof of work (PoW) for security. In contrast, private blockchains, or permissioned blockchains, require approval for each node to join. Hybrid blockchains blend features of both private and public blockchains. Consortium blockchains, meanwhile, are essentially private blockchains with restricted access to specific groups. This setup mitigates the risks associated with a single entity controlling the network in a private blockchain.

Safety Measures

To ensure safety, Blockchain uses different types of consensus mechanisms.

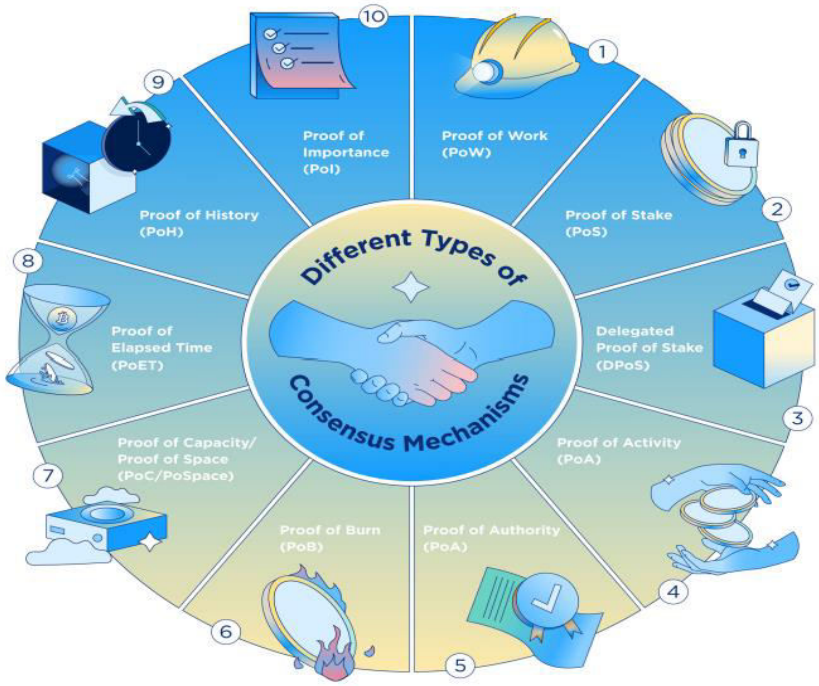

Figure 1. Types of Consensus Mechanisms [2]

Proof-of-work (PoW) describes a consensus mechanism that requires a significant amount of computing effort from a network of devices. Participants in the network broadcast their transactions to the entire network. Nodes in the network verify the validity of transactions by checking if the sender has the required funds and if the transaction follows the rules of the network. Information such as transaction amounts, wallet addresses, time, and date are recorded and encrypted into a block header — a hexadecimal number created through the blockchain's hashing function. Verified transactions are grouped into blocks. The newly added block becomes the latest link in the blockchain. The hash of this block is used as an input for the next block, creating a chain of blocks that is resistant to tampering.

In a Proof-of-Stake (PoS) system, the right to validate transactions and create new blocks is determined by the number of cryptocurrency tokens held by a participant. The more tokens someone has, the higher the chance they have to be chosen as the validator. Validators take turns proposing and validating new blocks in a deterministic manner, usually based on factors like the number of tokens they hold, the duration of their participation in the network, or a combination of such criteria. PoS systems aim to provide security by making it economically disadvantageous for validators to act maliciously. Validators have a financial stake in the network, and any malicious behavior could lead to the loss of their staked tokens [3].

Table 1

Comparison of Proof-of-work and Proof-of-stake [3]

Proof-of-Work	Proof-of-Stake
Validation is done by a network of miners	Participants validate transactions by providing cryptocurrency as collateral
Cryptocurrency is paid as a reward and for transaction fees	Cryptocurrency is paid for transaction fees only
Competitive nature requires a lot of energy and computational resources	Less computational power and energy used

Evolution of Blockchain

Though Blockchain began with cryptocurrencies, it has expanded into other areas, including healthcare, government, AI, supply chain management, and more.

Cryptocurrency usage is growing faster than ever before. According to Forbes Advisor, Crypto's worldwide market capitalization was estimated at $US1.09 trillion as of August 2023.

In Figure below you can see the major phases in the evolution of Blockchain.

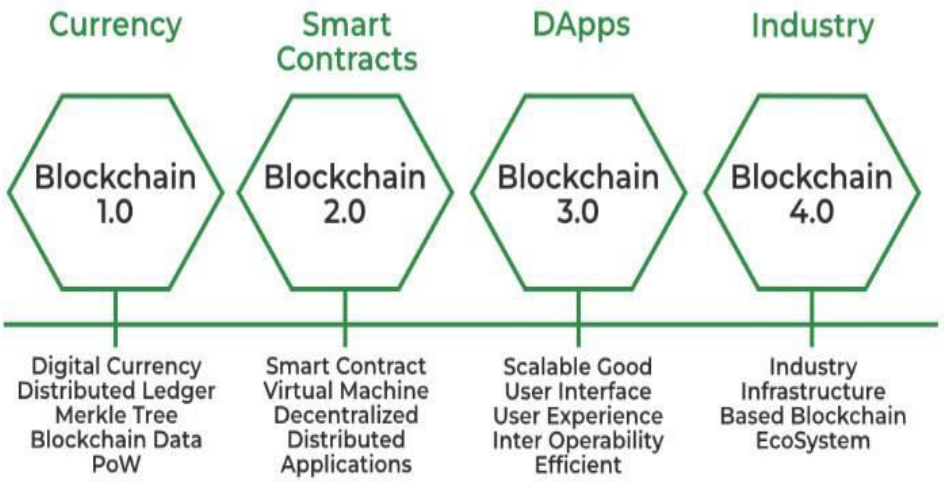

Figure 2. Evolution of Blockchain [4]

To begin with, Blockchain 1.0 was designed especially for the digital currency.

The power of Blockchain 2.0 is due to the advent of smart contracts. Ethereum was the first cryptocurrency to launch smart contract functionality. According to State of the dApps, about 80% of decentralized finance applications run on Ethereum's network [5].

Blockchain 3.0 enables scalable, user-friendly interfaces, better user experiences, and interoperable applications.

The Blockchains of the future are highly promising because numerous businesses, governments, and organizations are making substantial investments in this technology to stimulate innovation and explore new applications.

We believe that this transformative technology is being used to disrupt a wide range of industries and its impact is crucial. The healthcare industry faces a significant challenge regarding the privacy and security of patient records. One example of blockchain technology in healthcare is the Patient Master Identifier (MPI), where a single unique identifier is utilized across all healthcare providers seamlessly. Numerous researchers have focused on patient identification and permission-based systems to address these concerns. Additionally, Blockchain technology has made notable contributions to science through models like the HDG mobile app, which automates medical records while preserving privacy.

Blockchain can solve corruption issues within different financial systems by avoiding the risk of double-spending assets for the same service as well as showing clear ways of money floods.

Blockchain helps the scalability of AI by granting access to extensive data sources both within and beyond the organization. This access enables AI to generate more actionable insights, effectively manage data usage and sharing, and establish a trustworthy and transparent data economy [6].

Challenges

There are some major concerns that need to be addressed.

A huge concern for Blockchain is **privacy**. Blockchain may reveal only part of private data of its users, which is required for its functionality. At the same time, some information like account

ID or amount of money may be hidden. It is a widely spread misperception regarding the fact that blockchain networks such as Bitcoin are fully anonymous.

Sarah Austin [7] mentions that many have turned to coins like Monero, a digital coin that offers a higher level of privacy and untraceability included into its design.

There are big environmental questions about the amount of energy it takes to maintain the chain, and it's not yet clear how well it will scale.

Decentralized networks like Bitcoin and Ethereum consist of numerous nodes, facilitating cryptocurrency transactions. To establish trust among entirely anonymous entities, these networks employ a computationally intensive mining-based consensus mechanism. Consequently, achieving transaction finality requires a significant amount of time, leading to low transaction throughput in the single digits. This inefficiency in public blockchains highlights the challenge of poor performance and scalability. Finally, additional strategies like side chains are employed to alleviate the burden on the main chain and enhance transaction processing capabilities. It's no surprise that more cybercriminals are using cryptocurrency. Despite the numbers not being too high, it is still a big number of illicit transactions in comparison with the usual banks' percentage.

Figure 3 illustrates tendances in illicit cryptocurrency transactions over the last years.

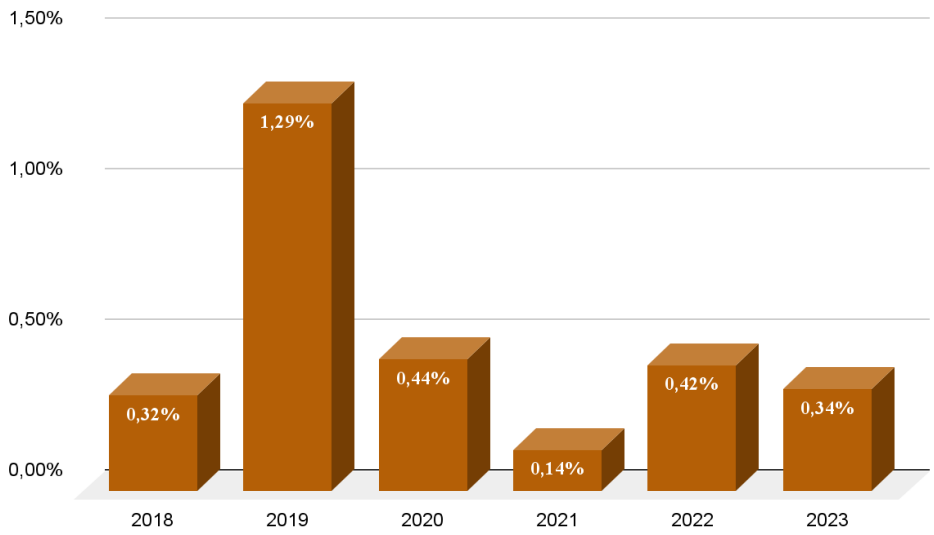

Figure 3. Illicit share of all cryptocurrency transaction volume [8]

Table 2

Cryptocurrency value received by illicit addresses [8]

Year	Amount (US Dollars, Billions)
2018	4.6
2019	12.5
2020	9.4
2021	23.2
2022	39.6
2023	24.2

Cryptocurrencies face a significant risk of lack of liquidity and the potential for complete loss or temporary inaccessibility of invested capital. These assets are characterized by high speculation, leading to volatile and fluctuating prices. Additionally, crypto assets lack regulation and may not be suitable for retail investors. Unlike regulated stock markets, there are no mechanisms in place to ensure the accurate determination of their prices. Furthermore, their heavy reliance on technology increases the likelihood of operational failures, cyber threats, and risks

associated with holding crypto assets within the relevant legal framework. The vulnerability of credentials or passwords also poses a risk of theft or loss.

Another concern is **space limitations**. Since every user of Blockchain has a full copy of the whole system, it requires a lot of memory. The emerging Blockchain platforms, based on distributed ledger technology (DLT) principles, address performance and scalability concerns by utilizing data structures like Directed Acyclic Graph (DAG). They achieve this by reducing transaction processing latency through innovative validation and voting mechanisms.

Blockchain is dealing with **mining issues** and **energy consumption**. As reported by digiconomist.net, the energy required to mine 1 bitcoin is equivalent to powering 2641 U.S. households. The energy consumption for mining coins is exceptionally high, resulting in a carbon footprint of 382.9kg of CO2 per transaction. Additionally, the presence of millions of anonymous and unverified miners poses a potential security risk to the integrity of the entire system.

According to The New York Times [9], if the blockchain could be scaled to reach the transaction number of Visa (40,000 ~ 50,000 TPS), the energy requirement will be equivalent to 5,000 nuclear reactors. If Blockchain stopped using proof-of-work methods, it would highly reduce energy consumption. Another option is to use solar energy to power up the Blockchain network [10].

Conclusions

To sum up, Blockchain technology is extremely promising. Its decentralized and secure nature makes it appealing for applications where transparency, security and trust are crucial. Moreover, it can also increase the resilience of the system in the face of cyber-attacks and other forms of tampering. Blockchain still has issues to overcome, such as energy consumption, illegal activity or data inefficiency.

Smart contracts are the engines behind the emerging decentralized finance industry. The revolutionary Blockchain technology has garnered considerable interest for its applications across diverse fields beyond cryptocurrency, including supply chain management, healthcare, AI, e-commerce, and more. We believe that the convergence of AI and blockchain has the potential to influence various industries and offer dynamic solutions for privacy, energy efficiency, data regulation, security, and scalability. Finally, blockchains of the future will have a huge impact on our lives.

References:

[1] Cryptocurrency Statistics 2024. Written by Andrew Michael, September 2023. Available online: https://www.forbes.com/advisor/au/investing/cryptocurrency/cryptocurrency-statistics (accessed on 05.02.2024)

[2] Blockchain Integration in the Era of Industrial Metaverse, January 2023. Available online: https://www.researchgate.net/publication/367324333_Blockchain_Integration_in_the_Era_of_Industrial_Metaverse (accessed 19.02.2024) https://www.researchgate.net/figure/Consensus-Mechanisms-in-Blockchain-Technology-13_fig4_367324333

[3] What Is Proof of Work (PoW) in Blockchain? Investopedia. May 2023. Available online: https://www.investopedia.com/terms/p/proof-work.asp (accessed on 03.02.2024)

[4] Phases of Evolution of Blockchain. Available online : https://www.geeksforgeeks.org/phases-of-evolution-of-blockchain/ (accessed 19.02.2024)

[5] Six Top Cryptocurrencies With Smart Contracts, September 21, 2021. Written by Emma Newbery. Available online: https://www.nasdaq.com/articles/6-top-cryptocurrencies-with-smart-contracts-2021-09-21 (accessed on 19.02.2024)

[6] Unlocking The Future: How AI And Blockchain Are Working Together. Available online: https://www.ucanwest.ca/blog/education-careers-tips/unlocking-the-future-how-ai-and-blockchain-are-working-together/#:~:text=By%20providing%20access%20to%20large,trustworthy%20and%20transparent%20data%20economy (accessed on 19.02.2024)

[7] Making Blockchain Easier and More Convenient, November 2018. Available online: https://medium.com/@FOTONBANK/making-blockchain-easier-and-more-convenient-fa5d6ab9f1c (accessed on 18.02.2024)

[8] 2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Ransomware and Darknet Markets See Growth. January 2024. Available online: https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/ (accessed on 03.02.2024)

[9] Bitcoin Uses More Electricity Than Many Countries. How Is That Possible? The New York Times, 201. Available online: https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html (accessed on 04.02.2024)

[10] Future Of Energy: How Solar Power Is Fueling The Cryptocurrency Boom. Available online: https://www.forbes.com/sites/digital-assets/2024/02/01/future-of-energy-how-solar-power-is-fueling-the-cryptocurrency-boom/?sh=57466a2b62de (accessed on 05.02.2024)