Exploring the Evolution, Trade-offs, and Applications of Blockchain Technology

Yuguo Li

School of Computer Science & Technology, Xi'an University of Posts & Telecommunications, Xi'an, 710121, China
isotope@stu.xupt.edu.cn

Abstract. sectors including industry and academia. Central to Bitcoin's innovation is blockchain technology, which has sparked extensive research into its potential beyond simple financial transactions. This paper delves into blockchain technology, examining its historical development, the nuanced trade-offs inherent in its evolving features, and its diverse applications in both permissionless and permissioned environments. Blockchain's inception as the backbone of Bitcoin marked a revolutionary departure from traditional financial systems, emphasizing transparency, decentralization, and security. However, these characteristics bring trade-offs such as scalability, speed, and energy consumption, which have prompted ongoing debates about the technology's practicality and efficiency. Furthermore, the applications of blockchain have expanded dramatically, ranging from enhancing supply chain transparency to enabling secure electoral processes, showcasing both permissionless and permissioned blockchain frameworks. Permissionless blockchains, like Bitcoin, allow any user to join and contribute to the network, fostering an open and decentralized environment. In contrast, permissioned blockchains restrict network participation to specific entities, offering greater control and efficiency suited for corporate and governmental needs.

Keywords: Blockchain, Evolution, Trade-offs.

1 Introduction

Bitcoin, a decentralized peer-to-peer electronic currency, enables network-connected individuals to participate directly in its transactions [1]. Unlike traditional distributed ledgers, which are typically controlled by a centralized authority, the Bitcoin network operates independently of such control. It employs a proof-of-work (PoW) blockchain that uses a hash-based method to timestamp transactions, continuously extending by adding new blocks. In PoW, the integrity of the blockchain is maintained as long as the majority of the computing power is not under the control of malicious entities, thus ensuring its immutability.

Following Bitcoin's success, focus has increasingly shifted to its underlying blockchain technology, sparking the development of numerous innovations. These include colored coins, Namecoin, smart contracts, and decentralized applications.

Y. Wang (ed.), *Proceedings of the 2024 2nd International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2024)*, Advances in Computer Science Research 115,
https://doi.org/10.2991/978-94-6463-540-9_32

Ethereum, which was developed to provide a Turing-complete programming language for these applications, represents a significant evolution in blockchain technology [2]. Notably, Ethereum introduced the proof-of-stake (PoS) algorithm, which, while enhancing transaction timeliness and reducing energy consumption compared to PoW, introduces trade-offs in security. However, PoS has not fully addressed the inherent issues of resource wastage, transaction latency, and the centralization of computing power seen in PoW systems [3].

In public blockchains, which are open and modifiable by anyone, trust is established through various "proof-of-X" algorithms. These algorithms, however, lead to considerable energy consumption and high barriers to entry. To balance decentralization with efficiency, permissioned blockchains have been proposed. These systems, similar to centralized databases, are governed by select authoritative entities that regulate user access rights, raising critical questions about their relationship with traditional distributed ledgers.

2 History of Blockchain

Bitcoin's architecture integrates a range of cryptographic and distributed technologies that have been in development for decades, including the distributed ledger and timestamp concepts first proposed in 1976. Prior to Bitcoin, several cryptographic currency concepts had been articulated, such as David Chaum's distributed database in 1979 and his subsequent development of DigiCash [4]. In 1998, Wei Dai's "b-money" proposition emphasized the necessity of publicly announcing transactions [5]. Additionally, Adam Back's 2002 study on methods to combat spam via computational effort influenced Satoshi Nakamoto in the creation of the proof-of-work mechanism [6]. Satoshi Nakamoto's 2008 whitepaper and the subsequent 2009 implementation of Bitcoin introduced a comprehensive cryptocurrency system, addressing challenges such as double-spending attacks, block organization, and the use of Merkle trees for space efficiency. Bitcoin gained significant traction in 2013, sparking interest in Bitcoin-based innovations like Namecoin and off-chain transactions. The launch of the Ethereum platform in 2015 marked a shift towards more complex functionalities, such as smart contracts and decentralized applications.

As Bitcoin continued to develop, blockchain technology began to capture broader attention. This led to the exploration of various trade-offs between decentralization and efficiency within blockchain frameworks. Permissioned blockchains emerged as a solution tailored for specific use cases or to integrate blockchain technology into existing projects. These systems rely on trusted authoritative institutions to establish trust, thereby reducing the overhead typically associated with decentralized trust mechanisms, while still leveraging hash-based blockchains and selectively employing cryptographic algorithms.

3 Efficiency-Decentralization Trade-off

Proof-of-work, one of the most crucial technologies in Bitcoin, enables multiple nodes to achieve consensus in a trustless network environment. However, it also leads to significant energy consumption and a fixed 10-minute block generation delay. Subsequent alternatives like PoS and Proof-of-Spacetime(PoST) have made varying degrees of compromises but can only achieve 99% accuracy after a certain period of time. To address the issues of existing public blockchains or to introduce new features to existing distributed ledgers, permissioned blockchains have been proposed.

The next two subsections will discuss permissionless and permissioned blockchains, respectively, and analyze them using practical applications as examples.

3.1 Permissionless Blockchain

Blockchain represented by Bitcoin and Ethereum is a permissionless (public) blockchain. Anyone can read the data on the chain, send write requests, and verify changes to the blockchain.

Taking Bitcoin as an example, the process of validating transactions is called mining, and the validators are called miners. Miners create new blocks by solving a specific mathematical puzzle, and the computational effort required to solve this puzzle serves as proof of honesty, known as "proof-ofwork." During the mining process, miners need to provide the hash of the previous block, the transactions they want to verify, and a nonce value to the SHA256 encryption function. They adjust the nonce value to modify the resulting hash. If the resulting hash meets the requirements of the Bitcoin application, mining is successful. After successfully mining a block, miners need to broadcast their findings to the network nodes to seek consensus.

If two miners simultaneously mine a block, nodes will choose which chain to follow. Eventually, one chain will become the longest chain, and nodes will discard their own maintained chain once they receive the longer chain. This resolves the problem of chain split (fork), but it also means that Bitcoin transactions can never achieve 100% accuracy.

Like all other cryptocurrencies, Bitcoin also needs to consider the possibility of attacks. The PoW algorithm has a tolerance threshold of 51% for dishonest nodes. As mentioned earlier, if 51% of the CPU power is honest, the blocks produced by the consensus algorithm will always become the longer chain. As of April 2024, there hasn’t been a successful attack implemented on the Bitcoin blockchain, despite the theoretical possibility of such attacks.

Apart from applications, there is still research dedicated to addressing the inefficiencies of permissionless blockchains. For instance, efforts are made to increase throughput in the blockchain without modifying the consensus mechanism [7].

3.2 Permissioned Blockchain

If a blockchain does not allow open participation in submitting or validating transactions, it is considered permissioned. Such blockchains are typically operated by authoritative entities, restricting access to nodes outside the permitted scope, while still retaining the organizational characteristics of a blockchain.

The use of permissioned blockchains is common in financial systems, where transactional processes and the concept of "Unspent Transaction Outputs (UTXO)" are well-suited for this scenario.

Next, this paper will analyze the XRP Ledger (XRPL) proposed by Ripple. Ripple is a US-based technology company founded in 2012, aiming to provide global real-time payment solutions. XRPL is an open-source, distributed ledger technology developed by Ripple initially to support its cryptocurrency, XRP. It is a blockchain-based distributed ledger known for its speed, security, and low costs. Despite XRPL.org claiming it to be a decentralized, public blockchain, according to the definition provided earlier, it falls under the category of permissioned blockchains [8].

The key characteristics of XRPL include:

Trust Model. Initially, the validation nodes in XRPL were directly designated by the XRPL organization. Subsequent validation nodes require permission from existing validation nodes to join. As more diverse nodes join, XRPL evolves from its initial centralization towards decentralization. In XRPL, users' trust stems from their trust in the validation node cluster.

Consensus Algorithm. As the trust foundation is provided by trust in the validation node cluster, XRPL does not use "Proof-of-X" series algorithms but employs the XRP Ledger Consensus Protocol (XRP LCP). Therefore, XRPL's transaction confirmation speed is faster, and it can handle higher throughput.

No Mining. Since XRPL does not use "Proof-of-X" series algorithms, it does not need to incentivize transaction validation through mining rewards. Its native currency, XRP, is pre-allocated. Validator rewards are provided by transaction fees.

XRPL has provided many technological innovations, such as the transition from centralization to decentralization. However, there are also some criticisms, such as company control, scalability, security, and attack risks. Among these, security and attack risks are the most important for all cryptocurrency systems. The fault tolerance of PoW is 50%, while classical Byzantine Fault Tolerance (BFT) protocols can tolerate $f < (n - 1)/3$, where n is the number of nodes and f is the number of Byzantine (faulty) nodes. In contrast, XRPL can tolerate $f < n/5$ [9]. The controversial aspect of trading off fault tolerance for performance improvement in XRPL stems from the fact that the selection of validation nodes in XRPL is based on its standards, making fault tolerance not merely a technical issue.

4 Why Blockchain over Traditional Distributed Ledgers

After Bitcoin and other blockchain applications attracted significant attention, more enterprises or organizations decided to embrace blockchain technology. However,

how to apply blockchain, which form of blockchain to use, and where to apply blockchain are still challenging issues in the technology industry.

Permissionless blockchains trade performance for a trust foundation that doesn't rely on trusted third parties. They are often used in scenarios where nodes in a network distrust each other and are unwilling to seek trusted third parties. While achieving decentralization, this introduces considerable performance overhead and energy consumption. Developers should balance the trade-offs between seeking trust relationships and the overhead brought by various proof-of-X consensus algorithms when analyzing requirements." Do you Need a Blockchain" provides a detailed analysis of when blockchain is needed and what type of blockchain is required, along with a process flowchart for determining whether blockchain is the appropriate technical solution to a problem [10].

Areas such as supply chain management and government transparency are considered suitable for permissoned blockchain use. However, some argue that in closed networks, there may not be a need for blockchain-based transactions, and centralized blockchains cannot truly guarantee irreversibility [11].

Blockchain, as an emerging technology, is often misunderstood. For instance, Estonia's X-Road project was once thought to be utilizing blockchain technology, which was not the case [12]. The ongoing analysis of whether actual scenarios require blockchain technology or if traditional distributed databases can suffice continues.

5 Applications of Blockchain

In this section, the paper will analyze several real-world applications of blockchain. These applications choose between permissionless and permissioned blockchains based on their respective core requirements. Additionally, optimizations are made to the protocols, providing new perspectives for the study of the evolution direction of blockchain.

5.1 Teechain

Teechain is an off-chain payment protocol that utilizes Trusted Execution Environments (TEEs) to securely, efficiently, and scalably execute fund transfers on the blockchain. It features asynchronous blockchain access.

As the applications of blockchain-based cryptocurrencies continue to grow, the performance bottleneck of permissionless blockchains has become a hindrance to deploying transactions. Payment channels offer a new approach by reducing direct operations on the blockchain and offloading the workload "off-chain." However, due to technical complexity and lack of trust foundation, payment channels are rarely implemented. Teechain's most notable technological feature is the use of TEEs to protect collateral and provide the trust foundation required for transactions.

As shown in Figure 1, in Teechain's trust model, each node trusts the TEEs of other nodes in addition to the common trust foundation in other permissionless blockchains. This allows TEEs to serve as trusted third parties providing a trust

foundation, while the blockchain application remains decentralized because it is not controlled by any specific entity.

The Teechain protocol enables transaction parties to perform handshake verification using key pairs securely generated within the TEE. This allows transactions to be securely conducted even when the rest of the system outside the TEE is untrusted. However, it also implies that Teechain does not provide additional security enhancements to the blockchain. Teechain does not consider scenarios such as side-channel attacks.

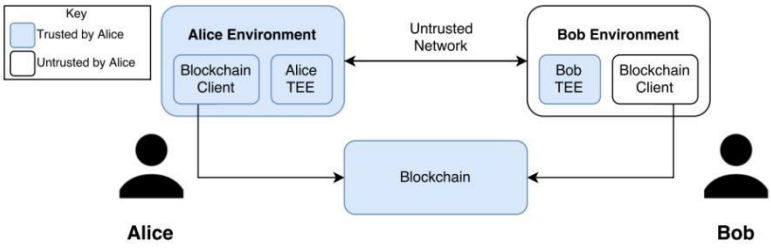

Fig. 1. Trust Model in Teechain.

5.2 FalconDB

FalconDB is a blockchain database designed with low hardware requirements for individual clients (e.g., storage, computation, bandwidth). It achieves high query efficiency similar to centralized database designs while ensuring strong security guarantees at the blockchain level [14]. FalconDB is designed as a collaborative database that operates when participant identities are known, aligning with the definition of permissioned blockchain. Therefore, FalconDB is based on permissioned blockchain technology.

FalconDB divides nodes into servers and clients and implements an incentive model based on smart contracts on the server side: clients need to pay query fees to the server for queries. Additionally, clients can request verification of received data, and if the server is found to be dishonest, it will be punished accordingly.

FalconDB leverages blockchain technology to provide several security features:

Immutability Database updates are committed to a blockchain maintained by multiple servers or clients with validation capabilities. This ensures that the database remains immutable over time.

Transparency Any user can request data from the blockchain to inspect historical updates. This transparency enhances trust and accountability within the system.

While the blockchain incurs overhead primarily in consensus and identity verification, the cost of these aspects is significantly lower than the hardware costs saved by clients. Additionally, the impact of consensus and identity verification on the system's throughput and latency is minimal, allowing FalconDB to maintain high throughput and low latency. FalconDB utilizes a consensus algorithm similar to BFT, with a tolerance limit of 1/3 of the nodes being dishonest. Similar to XRPL, although both are based on permissioned blockchains, they still require consensus algorithms

and incentive models to prevent potential dishonest behavior and encourage the development of the blockchain network. They choose to abandon "Proof-of-X" series algorithms to gain efficiency but continue to move towards decentralization.

6 Industrial Applications

In the following section, this paper will analyze several industrial sectors where blockchain technology is applied and highlight the characteristics that blockchain adds to these domains.

6.1 Medicine and Healthcare

Healthcare typically involves a significant amount of data input, output, and cross-device/platform dissemination, much of which is highly sensitive. The transmission and storage of large amounts of sensitive data pose significant challenges [15]. Another major challenge in the transmission of medical data lies in securely and reliably exchanging data between multiple healthcare or research institutions using different database systems.

The transparency and immutability characteristics of blockchain technology have attracted the attention of researchers for data preservation [16, 17]. In the proposed applications, there are different ways of applying blockchain. Some studies tend to use private blockchains (as defined earlier as permissioned blockchains) as a centralized database system and distinguish different access and control permissions [18,19]. There are also studies that prefer to use existing permissionless blockchains as a secure and long-term data storage service, storing encrypted medical data on blockchain networks [20].

There are still many blockchain healthcare applications that hold practical value and innovative significance. These applications primarily leverage the immutability, transparency, and other characteristics of blockchain compared to traditional applications that do not use blockchain technology. However, there is currently a lack of explicit research discussing the necessity of blockchain in the healthcare sector. This paper remains skeptical about some blockchain healthcare projects in certain scenarios.

6.2 Internet of Things

The Internet of Things (IoT) aims to facilitate communication and interaction between devices via the internet. With advancements in IoT technology, the number of devices participating in IoT networks is increasing, presenting challenges for traditional IoT applications. The primary challenges lie in data integrity and security. The distributed design principles of blockchain, along with its peer-to-peer connectivity model, enhance the efficiency of IoT networks and ensure the security of information transmission [21].

The architecture of modern IoT needs to support a large number of devices, often with limited hardware resources. Blockchain enables nodes to perform data verification without relying on third parties. This also means that nodes do not need to store large amounts of data (similar to mining nodes in Bitcoin and lightweight nodes that only retrieve transaction history or send transactions), which alleviates performance pressure on IoT device nodes.

Despite the data integrity verification provided by blockchain technology, namely cross-domain authentication, there are still potential risks associated with cross-domain validation in the current environment, especially on platforms with low hardware capabilities such as IoT devices. The overhead and complexity of cross-domain validation pose serious threats to data security. Some research suggests using Trusted Execution Environment (TEE) technology to assist in secure authentication between devices, such as Blockchain and tee assisted authentication(BTAA) [22]. Similar to Teechain mentioned earlier, BTAA utilizes Identity-Based Signatures (IBS) and TEE technology to ensure secure authentication between devices.

7 Conclusion

In conclusion, blockchain technology has significantly evolved since its inception with Bitcoin. The development of permissionless and permissioned blockchains marks critical milestones in this technological landscape. These paradigms have been successfully implemented in various contexts, demonstrating blockchain's adaptability and robustness. However, the proliferation of blockchain has not been without its challenges. In some cases, the technology has been seamlessly integrated into existing infrastructures, enhancing efficiency and transparency. In others, it has been adopted superficially, driven more by its novelty than by its applicability [23]. Despite these varied trajectories, blockchain's core attributes—such as enhanced traceability and immutability—have profoundly influenced numerous sectors. Beyond merely transforming financial transactions, blockchain is reshaping the foundations of digital interaction and decentralized systems. As such, it continues to offer promising avenues for future innovations that could redefine global digital architecture.

References

1. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
2. Vitalik Buterin. Ethereum white paper: A next generation smart contract & decentralized application platform. 2013.
3. Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, and Chen Qijun. A review on consensus algorithm of blockchain. In 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pages 2567– 2572, 2017.
4. David Lee Chaum. Computer Systems established, maintained and trusted by mutually suspicious groups. Electronics Research Laboratory, University of California Riverside, CA, USA, 1979.
5. Wei Dai. b-money. http://www.weidai.com/ bmoney.txt, 1998.
6. Adam Back et al. Hashcash-a denial of service countermeasure. 2002.

7. Soujanya Ponnapalli, Aashaka Shah, Souvik Banerjee, Dahlia Malkhi, Amy Tai, Vijay Chidambaram, and Michael Wei. RainBlock: Faster transaction processing in public blockchains. In 2021 USENIX Annual Technical Conference (USENIX ATC 21), pages 333–347. USENIX Association, July 2021.
8. Xrp ledger. https://xrpl.org/. Mar.2024.
9. Brad Chase and Ethan MacBrough. Analysis of the xrp ledger consensus protocol. arXiv preprint arXiv:1802.07242, 2018.
10. Karl Wüst and Arthur Gervais. Do you need a blockchain? In 2018 crypto valley conference on blockchain technology (CVCBT), pages 45–54. IEEE, 2018.
11. Siamak Solat, Philippe Calvez, and Farid NaïtAbdesselam. Permissioned vs. permissionless blockchain: How and why there is only one right choice. J. Softw., 16(3):95–106, 2021.
12. Petteri Kivimäki,There is no blockchain technology in X-Road. https://www.niis.org/blog/2018/4/26/there-is-no-blockchain-technology-in-the-x-road,2018. Mar.2024.
13. Joshua Lind, Oded Naor, Ittay Eyal, Florian Kelbert, Emin Gün Sirer, and Peter Pietzuch. Teechain: a secure payment network with asynchronous blockchain access. In Proceedings of the 27th ACM Symposium on Operating Systems Principles, pages 63–79, 2019.
14. Yanqing Peng, Min Du, Feifei Li, Raymond Cheng, and Dawn Song. Falcondb: Blockchain-based collaborative database. In Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data, SIGMOD '20, page 637–652, New York, NY, USA, 2020. Association for Computing Machinery.
15. Lena Griebel, Hans-Ulrich Prokosch, Felix Köpcke, Dennis Toddenroth, Jan Christoph, Ines Leb, Igor Engel, and Martin Sedlmayr. A scoping review of cloud computing in healthcare. BMC medical informatics and decision making, 15(1):1–16, 2015.
16. Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. Medrec: Using blockchain for medical data access and permission management. In 2016 2nd international conference on open and big data (OBD), pages 25–30. IEEE, 2016.
17. Jie Zhang, Nian Xue, and Xin Huang. A secure system for pervasive social network-based healthcare. Ieee Access, 4:9239–9250, 2016.
18. Kristen N Griggs, Olya Ossipova, Christopher P Kohlios, Alessandro N Baccarini, Emily A Howson, and Thaier Hayajneh. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of medical systems, 42:1–7, 2018.
19. Xiao Yue, Huiju Wang, Dawei Jin, Mingqiang Li, and Wei Jiang. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 40:1–8, 2016.
20. Drew Ivan. Moving toward a blockchain-based method for the secure storage of patient records. In ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST, volume 1170. sn, 2016.
21. Laphou Lao, Zecheng Li, Songlin Hou, Bin Xiao, Songtao Guo, and Yuanyuan Yang. A survey of iot applications in blockchain systems: Architecture, consensus, and traffic modeling. ACM Comput. Surv., 53(1), feb 2020.
22. Wenze Mao, Peng Jiang, and Liehuang Zhu. Btaa: Blockchain and tee assisted authentication for iot systems. IEEE Internet of Things Journal, 2023.
23. Gideon Greenspan. Avoiding the pointless blockchain project. https:// www. multichain. com/blog/2015/11/ avoiding-pointless-blockchain-project/, 2015. Mar.2024.