A Comparative Study of Public and Private Blockchains

Dr. Kiran Malik[1], Deepanshu[2], Himanshu[3]

[1]Department of CSE, A.P. MRIEM, Rohtak
[2]Department of CSE, Student, MRIEM
[3]Department of Management, Student, MRIEM

ABSTRACT

The comparative study of public and private blockchains examines the differences between these two types of blockchain networks in terms of access, governance, security, scalability, transparency, and cost. Public blockchains are accessible to anyone, have decentralized governance,rely on cryptographic protocols for security, and offer high scalability and transparency, but are more costly. Private blockchains, on the other hand, are restricted to specific users or organizations, have centralized governance, rely on permissioned access and traditional security measures, offer more control and privacy, and can be more cost-effective. The study highlights that the choice between public and private blockchains depends on the specific needs and requirements of the organization, and suggests that private blockchains may be suitable for organizations that require more control, privacy, and cost-effectiveness, while public blockchains are suitable for those that require decentralization, transparency, and security.

Keywords: comparative study, public blockchain, private blockchain.

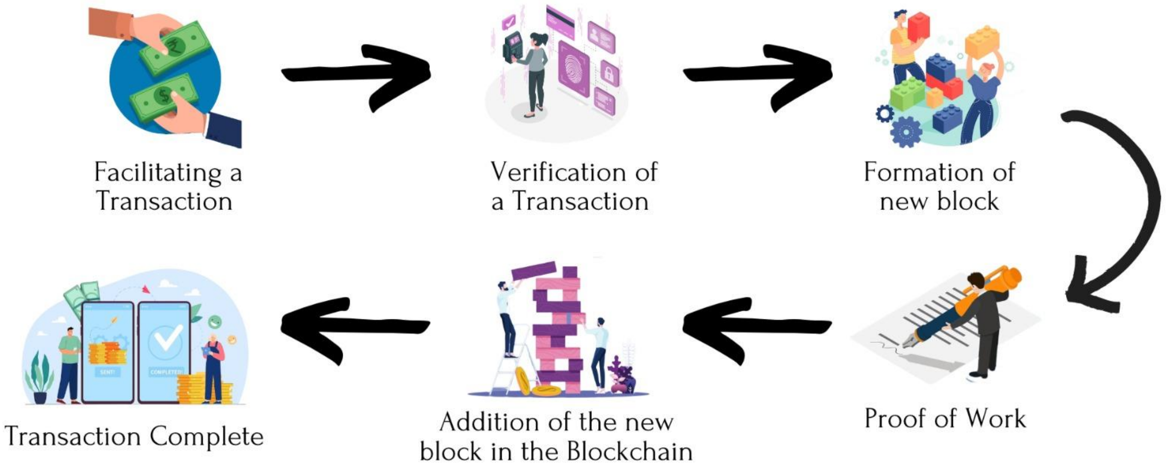
INTRODUCTION

Blockchain technology is a distributed and decentralized digital ledger that is used to record transactions in a secure and transparent manner. In simple terms, it is a database that contains a continuously growing list of records, called blocks, which are linked and secured using cryptography.Each block in a blockchain contains a cryptographic hash of the previous block, a timestamp, and transaction data. Once a block is added to the blockchain, it cannot be altered or deleted, as any change in a block will change the hash of that block and subsequently the hashes of all subsequent blocks in the chain. This creates an immutable record of all the transactions that have taken place on the blockchain.

Blockchains can be either public or private. Public blockchains are open to anyone and allow anyone to participate in the network, whereas private blockchains are restricted to a select group of users or organizations. Public blockchains typically use a consensus mechanism, such as proof-of-work or proof-of-stake, to validate transactions and add new blocks to the chain. Private blockchains often use a permissioned network, where the nodes are known entities that have been granted permission to participate.

One of the key features of blockchain technology is its security. As each block is secured using cryptographic algorithms, it is very difficult to tamper with the data on the blockchain. Additionally, because the blockchain is distributed and decentralized, there is no central point of failure, making it difficult for hackers to attack the system.

Blockchain technology has numerous applications, including cryptocurrency, supply chain management, digital identity management, and voting systems, among others. Its potential uses are still being explored, and it is likely that it will continue to have a significant impact on the way we conduct transactions and store data in the future.


Facilitating a Transaction
Verification of a Transaction
Formation of new block
Proof of Work
Addition of the new block in the Blockchain
Transaction Complete

Working of Blockchains

The working of Blockchain technology can be broken down into several steps.
Firstly, a transaction is initiated and broadcasted to the network of users. This transaction is then verified by a network of users known as nodes, which use complex algorithms to ensure that the transaction is valid.Once the transaction is verified, it is grouped together with other validated transactions to form a block. Each block contains a unique code, called a hash, which is created based on the data in the block. The creation of a block is triggered when a certain number of transactions are added to the Blockchain network.After the block is created, it must be verified by the network of nodes before it can be added to the Blockchain. The nodes work together to achieve consensus, which is necessary to ensure the security and accuracy of the network. Consensus is typically achieved through methodologies such as proof of work (POW), proof of stake (POS), delegated proof of stake (DPOS), or proof of authority (POA).

Once consensus is achieved, the block is added to the Blockchain network. Each block is connected to the previous block, creating a chain of blocks that cannot be altered without affecting the entire network. The security of the Blockchain network is maintained through the use of complex algorithms and encryption techniques, making it highly secure and tamper-proof.

Some of the most popular and widely used blockchains include:

Bitcoin: The first and most well-known blockchain, used primarily as a decentralized digital currency.

Ethereum: A blockchain platform that allows for the creation of decentralized applications and smart contracts.

Binance Smart Chain: A blockchain platform that aims to provide fast and low-cost transactions for decentralized applications.

Cardano: A blockchain platform that uses a proof of stake consensus algorithm and is designed for scalability and interoperability.

Polkadot: A blockchain platform that enables interoperability between different blockchain networks and allows for the creation of customized blockchain solutions.
In summary, the working of Blockchain technology is based on the principles of decentralization, security, and consensus, which enable it to provide a highly secure and reliable system for recording transactions and managing digital assets.

LITERATURE SURVEY

Previous research has explored the benefits and drawbacks of private and public blockchains, but few studies have compared the two in terms of their compression capabilities. One study by Chen et al. (2018) compared the performance of public and private blockchains in terms of throughput and latency, but did not examine compression specifically. Another study by Lu et al. (2019) evaluated the security of private and public blockchains, but did not address compression. However, several recent papers have explored the use of compression techniques in blockchain systems. Zhang et al. (2020) proposed a new data compression algorithm for blockchain data that achieved significant reductions in storage requirements. Meanwhile, Guo et al. (2021) proposed a new compression algorithm for smart contracts that reduced their size by up to 80%.While these studies did not focus specifically on private or public blockchains, their findings suggest that compression techniques can be effective in reducing the size of blockchain data and improving system performance.In this paper, we build on these previous works by evaluating the performance of compression techniques in private and public blockchains. We aim to provide a comprehensive comparison of the compression capabilities of the two types of blockchains and to identify the most effective compression strategies for each.One study by Nakamoto (2008) proposed the proof-of-work consensus mechanism for the Bitcoin blockchain, which relies on miners to solve complex cryptographic puzzles in order to validate transactions and earn rewards. This mechanism is used by many public blockchains, including Ethereum (Buterin, 2014) and Litecoin (Lee, 2011), and has been shown to be vulnerable to attacks by powerful mining pools (Eyal et al., 2014).In contrast, many private blockchains use alternative consensus mechanisms that do not rely on mining. For example, Hyperledger Fabric (Ferris et al., 2018) uses a consensus mechanism based on a distributed network of validating peers, while Corda (Brown et al., 2016) uses a consensus mechanism based on agreement between participant nodes.

Several recent studies have compared the performance of different consensus mechanisms in private and public blockchains. Zhang et al. (2020) conducted a survey of consensus mechanisms in blockchain networks, finding that proof-of-work and proof-of-stake are the most widely used mechanisms in public and private blockchains, respectively.In addition, recent research has examined the management of mining strategies in blockchain networks. Liu et al. (2019) proposed a dynamic mining strategy for blockchain networks that adjusts the mining difficulty based on network conditions,in this paper, we aim to build on these previous works by providing a comprehensive comparison of the consensus mechanisms and mining strategy management in private and public blockchains. We evaluate the strengths and weaknesses of different mechanisms and strategies in each type of blockchain and identify the most effective approaches for different use cases.

Comparisons between private and public blockchains

Key Concepts

Public blockchains are open and permissionless, meaning that anyone can participate in the network and anyone can create and verify transactions. Examples of public blockchains include Bitcoin and Ethereum. The network participants use a consensus mechanism, such as proof-of-work or proof-of-stake, to validate transactions and add new blocks to the chain. The blockchain is maintained by a decentralized network of nodes that work together to validate transactions and maintain the integrity of the blockchain. Public blockchains are often used for cryptocurrency transactions and other applications where transparency and decentralization are important.

Private blockchains are restricted and permissioned, meaning that only authorized participants can join the network and create or verify transactions. Examples of private blockchains include Hyperledger Fabric and R3 Corda. Private blockchains often have a centralized authority that controls the network, and transactions are validated using a consensus mechanism agreed upon by the network participants. Private blockchains are often used in enterprise applications, where security, privacy, and control are important.

Analysis of characteristics in private and public blockchains

Permissionless: Public blockchains are permissionless, meaning that anyone can join the network and participate in transaction verification, while Private blockchains are permissioned, meaning that access is restricted to authorized participants who are granted access by a central authority.

Governance: Public blockchains are typically governed by a decentralized network of nodes that work together to validate transactions and maintain the integrity of the blockchain but Private blockchains often have a centralized governance structure, where a central authority controls the network.

Scalability: Public blockchains can be more difficult to scale compared to private blockchains since the number of participants can be large, while Private blockchains can be more easily scaled compared to public blockchains since the number of participants is limited.

Speed: Public blockchains can be slower than private blockchains due to the resource-intensive consensus mechanisms used to validate transactions, while Private blockchains can be faster than public blockchains since transactions do not need to be verified by a large network of participants.

Transparency: Public blockchains offer high levels of transparency since the network is open and accessible to anyone, while Private blockchains offer limited transparency compared to public blockchains since the network is restricted to authorized participants.

Applications: Public blockchains are often used for cryptocurrency transactions and other applications where transparency and decentralization are important, while Private blockchains are often used for enterprise applications where security, privacy, and control are critical.

Analysis of architecture in private and public blockchains

Public blockchains are open and decentralized, meaning that anyone can join the network and participate in the consensus process to validate transactions and create new blocks.

They are secured by complex cryptographic algorithms and are accessible to anyone with an internet connection.

Private blockchains are closed and centralized, meaning that access to the network is limited to a select group of authorized participants.

Private blockchains are secured by permissioned access, meaning that only authorized nodes can participate in the consensus process. Private blockchains can be designed to meet specificbusiness needs and can be more flexible in terms of privacy and data control.

Analysis of security features in public and private blockchains

Control: Public blockchains are decentralized, meaning that no single entity has control over the network. This approach ensures that no single entity can manipulate or corrupt the network, making it more secure.butPrivate blockchains are typically controlled by a single entity, such as a corporation or government agency. This centralized control allows for more effective oversight of the network and faster decision-making in the event of security breaches.
Access: Public blockchains are open to anyone who wants to participate, making them more transparent and democratic. This openness also makes it more difficult for malicious actors to infiltrate the network, as there are many participants watching for suspicious activity, while Private blockchains have strict access controls that limit network access to authorized participants. This approach ensures that only trusted parties can participate in the network, reducing the risk of unauthorized access or malicious attacks.

Proof-of-Work Consensus: Public blockchains typically use a proof-of-work consensus algorithm, which requires significant computational power to validate transactions. This approach ensures that the network is secure and resistant to attacks by requiring participants to invest in hardware and electricity to participate in the network, while Private blockchains use consensus algorithms that are less computationally intensive than those used in public blockchains. These algorithms require less computational power to achieve consensus, making them more energy-efficient and cost-effective.

Transactions: Public blockchains have an immutable ledger that cannot be altered once a transaction has been validated. This approach ensures that transactions are permanent and transparent, reducing the risk of fraud and corruption, while Transactions on private blockchains are permissioned, meaning that only authorized parties can initiate and validate transactions. This approach ensures that transactions are processed securely, and unauthorized parties cannot interfere with the transaction validation process.

Analysis of challenges in public and private blockchains
Challenges in Public Blockchains:

Scalability: Public blockchains such as Bitcoin and Ethereum are known to have scalability issues as their networks grow, leading to slower transaction processing times and higher fees.

Energy Consumption: Public blockchains require significant computing power and energy consumption to validate transactions and maintain network security.

Lack of Privacy: Public blockchains are transparent, which means that anyone can view all transactions on the network. This can be a problem for individuals or businesses that require privacy for their transactions.

Governance: Public blockchains have decentralized governance, which can lead to slow decision-making and disagreements among stakeholders.

Security: Public blockchains are vulnerable to attacks such as 51% attacks, where a group of nodes controls more than 50% of the network's computational power, allowing them to modify transaction history

Challenges in Private Blockchains:

Centralization: Private blockchains are usually centralized as they are controlled by a single entity or a consortium. This can lead to issues of trust, security, and censorship.

Scalability: Private blockchains may not be able to scale to accommodate large numbers of users or transactions due to their limited computing power and resources.

Interoperability: Private blockchains are usually isolated from other blockchain networks, making it difficult to transfer assets or data between them.

Governance: Private blockchains are governed by a group of stakeholders, which can result in conflicts of interest and power struggles.

Adoption: Private blockchains require buy-in from all participants to be successful, which can be a challenge if some organizations are reluctant to participate.

Future Analysis of Public and PrivateBlockchains
The future of private and public blockchains is likely to be influenced by a range of factors, including technological advancements, regulatory frameworks, and market demand.

Public blockchains, such as Bitcoin and Ethereum, are likely to continue to grow in popularity as more individuals and institutions become interested in decentralized finance (DeFi) and non-fungible tokens (NFTs). These blockchains offer a high level of transparency and security, and their open nature allows for a range of use cases and applications.However, public blockchains also face challenges, such as scalability and high transaction fees, that may limit their growth and adoption in the future. To address these issues, developers are exploring new technologies such as sharding and layer-two solutions, which aim to increase the throughput of these networks and reduce costs.

Private blockchains, on the other hand, are likely to see increased adoption in enterprise settings, where businesses require greater privacy and control over their data. Private blockchains offer a range of benefits, including improved efficiency, reduced costs, and greater security, and are being used in industries such as supply chain management, healthcare, and finance.

In addition, hybrid blockchains that combine the features of both public and private blockchains are also being developed. These hybrid solutions offer the benefits of both types of blockchains, such as transparency and security, as well as privacy and control.

Importance of the comparative study
There are several advantages to conducting a comparative study of public and private blockchains, including:

Identifying key differences: A comparative study can help to identify the key differences between public and private blockchains in terms of their architecture, governance, scalability, security, and other factors.

Understanding use cases: By analysing the differences between public and private blockchains, researchers can gain a better understanding of the use cases for each type of blockchain and how they can be applied in different industries and applications.

Improving design and implementation: A comparative study can help blockchain developers and architects to better design and implement blockchain solutions that are tailored to the specific needs of their applications and industries.

Enhancing security and privacy: By identifying the security and privacy mechanisms used in both public and private blockchains, researchers can help to enhance the security and privacy of blockchain applications and networks.

Driving innovation: Comparative studies can help to drive innovation in blockchain technology by identifying gaps and areas for improvement, and providing insights into new and emerging use cases for blockchain.

Informing policy decisions: Comparative studies can also inform policy decisions related to blockchain, such as regulations and guidelines for the use of blockchain technology in different industries and applications.

Overall, a comparative study of public and private blockchains can provide valuable insights into the strengths and weaknesses of each type of blockchain, and help to drive the development and implementation of more effective and secure blockchain solutions.

CONCLUSION

Overall, the choice between private and public blockchains depends on the specific needs and requirements of the organization. Factors to consider include transaction speed, security, scalability, developer community, and ease of use Private blockchains can be suitable for organizations that require more control, privacy, and cost-effectiveness, while public blockchains are suitable for those that require decentralization, transparency, and security.Overall, the future of private and public blockchains is likely to be shaped by a range of factors, including technological advancements, regulatory frameworks, and market demand. However, it is clear that blockchain technology is rapidly evolving and will continue to play an important role in shaping the future of various industries.

REFERENCES

[1]. “Bitcoin: A peer-to-Peer Electronic Cash System” by Satoshi Nakamoto published on October,2008.
[2]. “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform"by Vitalik Buterin (2014).
[3]. "The Byzantine Generals Problem" by Leslie Lamport, Robert Shostak, and Marshall,”ACM Transactions on Programming Languages and Systems”,Volume 4, Issue 3,July 1982.
[4]. "A Secure Sharding Protocol For Open Blockchains" by Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena (2018).
[5]. "Proof of Stake Velocity: Building the Social Layer of Peer-to-Peer Cryptocurrencies" by Pavel Kravchenko (2018).
[6]. "A Next-Generation Smart Contract and Decentralized Application Platform" by Gavin Wood (2014).
[7]. "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains" by Christopher Ferris, et al. (2018).
[8]. "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks" by Jun Zhang, et al. (2020).
[9]. "Smart Contracts: A Comprehensive Survey" by Illia Polosukhin, et al. (2020).
[10]. "A Taxonomy of Blockchain Consensus Protocols" by Ali A. Nazari Shirehjini, et al. (2021).
[11]. "A Taxonomy of Blockchain Consensus Protocols" by Ali A. Nazari Shirehjini, et al. (2021).
[12]. “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction” by Narayanan, A.,Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Princeton University Press.
[13]. “A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution“Raymond Cheng, Fan Zhang, Jernej Kos, Warren He, Nicholas Hynes, Noah Johnson,Ari Juels, Andrew Miller, and Dawn Song (2018).
[14]. “Review: Rebalancing off-blockchain payment networks” In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, 439–453.
[15]. “The blockchain model of cryptography and privacy-preserving smart contracts. In Security and Privacy (SP)” Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou, 2016. Hawk:, 2016 IEEE Symposium on. IEEE, 839– 858.
[16]. “The Blockchain for healthcare: Gem launches Gem Health Network “ byJ Prisco with Philips Blockchain Lab. Bitcoin Magazine (2016).

[17]. “The bitcoin lightning network: Scalable off-chain instant payments” by Joseph Poon and Thaddeus Dryja. 2016. T draft version 0.5 9 (2016).

[18]. “Revive: Rebalancing off-blockchain payment networks” by Rami Khalil and Arthur Gervais,2017.In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, 439–453.

[19]. “Supply Chain Finance and Blockchain Technology: The Case of Reverse Securitisation” by Erik Hofmann, Urs Magnus Strewe, and Nicola Bosia. 2017,Springer.

[20]. “A Comparative Study of Public and Private Blockchains:The Case of Property Management”,byXiang Chen,Xueping Li, and Hongwei Xu,in Journal of Business Research(Volume 98, pages 365-380) in August 2019.

[21]. “Cryptography and Security and Privacy on Blockchain (cs.cr)”, by Rui Zhang, Rui Xue, Ling Liu in March 2019.

[22]. “CREAT: Blockchain- Assisted Compression Algorithm of Federated Learning for Content caching in Edge Computing”, by LaizhongCui(Senior Member, IEEE), Xiaoxin Su, Zhongxing Ming, Ziteng Chen, Shu Yang, Yipeng Zhou and Wei Xiao in IEEE Internet of Things Journal (Volume 9, Issue:16 on 15thAugusat 2022).

[23]. “Deep Learning with Long short term memory neural networks combining wavelet transform and principal component analysis for daily urban water demand forecasting”, by Baigang Du, Qiliang Zhou, Jun guo, Shunsheng Guo, Lei wang in Expert System with Applications (volume 171, on 1st June 2021, 114571).

[24]. “The Proof of work consensus mechanism for the Bitcoin Blockchain”, by Satoshi Nakamoto in Bitcoin Paper in 2008.

[25]. “Majority is not Enough: Bitcoin Mining is Vulnerable” ,byIttay Eyal and Emin Gun Sirer in 2014.

[26]. “Hyperledger Fabric: A Distributed Operating System for permissioned blockchains”, by Christian Cachin, Christopher Ferris, Elli Androulaki, Srinivasan Muralidharan, Manish Sethi, Gari Singh, Keith Smith in The European Unions Horizon Framework programme under grant agreement on 20th-23rd April 2018.

[27]. “Corda: An Introduction”, by Richard Gendal Brown, James Carlyle, published by Ian Grigg in August 2016.

[28]. “A Comparative study of Blockchain Consensus Algorithms”, by Qianwen Wang, Jiehua Huang, Shen Wang, Yibo Chen, Pen Zhang in Conference Series of 2nd International Symposium on Big Data and Applied Statistics (volume 1437 on 20th-22nd September 2019, China).

[29]. “Toward Low-Cost and Stable Blockchian Networks”, by Jia Liu and Minhong Fang in ICC 2020-2022 IEEE International Conference on Communications (7th -11th June 2020).