A Comprehensive Survey on Blockchain Technology and Its Applications

Jiajun Liu[1, *], Junhao Wu[2]

[1]School of Economics and Management, Xidian University, Xian, 710126, China

[2]School of Information Science and Technology, Guangdong University of Foreign Studies, Guangzhou, 510006, China

* Corresponding Author Email: 20069100170@stu.xidian.edu.cn, [a]20201003089@gdufs.edu.cn

Abstract. This survey paper provides a comprehensive and in-depth overview of blockchain technology and its wide-ranging applications. It begins by introducing the fundamental characteristics and structure of blockchain, with a particular focus on the five major consensus mechanisms and their unique features. The article emphasizes the crucial role of smart contracts and cryptography in the construction and operation of blockchain networks. Furthermore, the paper explores the specific applications of blockchain in three key areas: cryptocurrencies, supply chains, and healthcare security. It highlights the numerous advantages that blockchain brings to these domains, including enhanced security, transparency, and efficiency. The paper also offers valuable insights into the future potential of blockchain technology in these areas, providing a glimpse into the possibilities that lie ahead. Additionally, the article addresses the challenges posed by the "impossible triangle" of decentralization, security, and high performance in blockchain. It discusses the emerging research trends aimed at tackling these challenges, such as cross-chain protocols, privacy protection mechanisms, blockchain expansion strategies, and advanced data storage solutions. The paper presents recent advancements and breakthroughs in each of these research directions, showcasing the ongoing efforts to overcome the limitations of blockchain technology.

Keywords: Blockchain technology, Consensus mechanisms, Smart contracts, Cryptography, Cryptocurrencies.

1. Introduction

Blockchain technology is a distributed ledger that has the power to completely transform a wide range of businesses. It is a tamper-proof, transparent, and secure method of storing data. Blockchain is built on a computer network that shares a transaction ledger. The network authenticates each transaction before adding it to the ledger. This makes it very difficult to hack or corrupt the data on a blockchain.

By using the alias Satoshi Nakamoto, an unidentified individual or group of persons first used the word "blockchain" in 2008 [1]. Nakamoto used blockchain technology to create the cryptocurrency Bitcoin, which was first introduced in 2009 as the distributed ledger behind Bitcoin transactions [2]. Blockchain technology is not limited to cryptocurrencies. It has the potential to be used in a wide variety of applications, such as healthcare, supply chain management, Internet of things financial services [3-5]. The blockchain technology has huge potential advantages. It could lead to more efficient and secure transactions, improved transparency, and reduced costs. Nevertheless, in order to fully utilize the capabilities of blockchain technology, there are several issues that must be resolved. These challenges include scalability, security, and privacy [6]. This survey's goal is to give readers a broad understanding of blockchain technology's salient characteristics, various blockchain consensus algorithms, and prospective uses. This poll makes a contribution by giving a thorough review of blockchain technology that will be helpful for researchers, developers, and companies that want to understand more about this new technology.

The following are this survey's precise goals:

to give a summary of the main components of blockchain technology.

to talk about the several essential blockchain technologies.

to investigate possible uses for blockchain technology.

to determine the issues that must be resolved if blockchain technology is to reach its full potential.

This survey is organized as follows: An overview of blockchain technology, including its history, main characteristics, and organizational structure, is given in Section 2. The various blockchain technologies are covered in Section 3. The possible uses of blockchain technology are examined in Section 4. The difficulties that must be overcome in order to realize the full potential of blockchain technology are listed in Section 5. The poll is concluded in Section 6, which goes over the prospects for blockchain technology.

2. Blockchain

2.1. History of blockchain

Blockchain technology started taking shape in the early 1980s when David Chaum proposed a blockchain protocol [7]. Stuart Haber and W. Scott Stornetta described a distributed timestamping method utilizing cryptography to secure the ledger in a 1991 paper [8]. Further development came from Nick Szabo in the late 1990s, who introduced the concept of a digital currency using blockchain technology for transaction security [9].

The major breakthrough in blockchain technology came in 2008 when Satoshi Nakamoto published the Bitcoin white paper [10]. This paper outlined a peer-to-peer electronic cash system that utilized blockchain for transaction security. Bitcoin was launched in 2009 and gained rapid popularity as a new form of digital currency [2]. Ethereum, introduced in 2015 by Vitalik Buterin, expanded the capabilities of blockchain as a more versatile platform [11]. Ethereum enables the development of decentralized applications (dApps) that operate on the blockchain. Various dApps, including gaming, non-fungible tokens (NFTs), and decentralized finance (DeFi), have been built on Ethereum. The Ethereum Foundation announced the Ethereum 2.0 project in 2020, aiming to enhance scalability, security, and efficiency. The project is still under development and expected to be completed by 2023. As shown in Fig. 1.

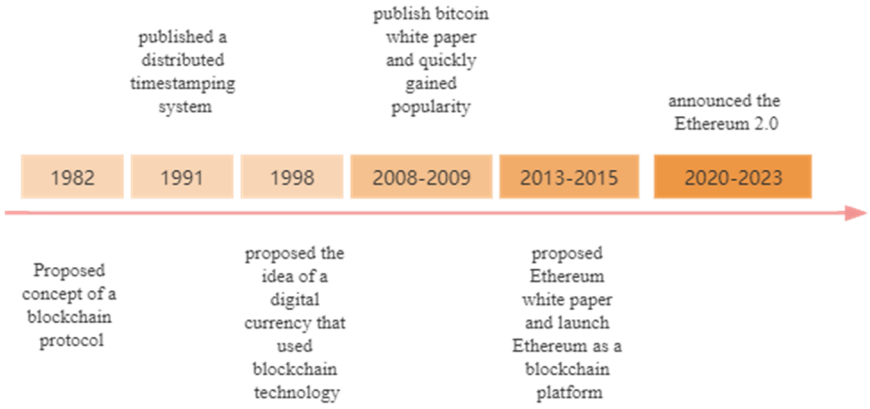

Fig. 1. History of blockchain (Photo/Picture credit: Original)

2.2. Features of blockchain

Blockchain, a distributed ledger system, enables safe, open, and unchangeable transactions. It is a network of computers' shared database that is kept up to date. Each block in the blockchain contains a set of transactions, and each block is linked to the previous block in the chain. As a result, altering the data on the blockchain requires changing every block in the chain, which makes it incredibly difficult to do. The main characteristics of blockchain are listed below. **Immutability:** The immutability of the blockchain means that once data is added to the blockchain, it cannot be easily changed or deleted. This makes the blockchain ideal for applications that require a high degree of security and transparency, such as financial transactions and supply chain management [12]. **Transparency:** Because of the transparency of blockchain, all nodes in the network have access to

the same transactions and a copy of the blockchain. This makes it extremely challenging for fraud or corruption to occur [13]. **Security:** The security of the blockchain is achieved through the use of a variety of cryptographic techniques, such as hash functions, digital signatures, and encryption. This is due to the fact that the blockchain is based on cryptography, which is a very secure technology. The cryptography used in the blockchain makes it very difficult for unauthorized users to access the data on the blockchain [10]. **Decentralization:** The decentralizaiton of the blockchain is achieved through the use of a peer-to-peer network. This means that there is no central authority that controls the blockchain. Instead, the blockchain is controlled by the nodes in the network. This makes it very difficult for any single entity to censor or manipulate the blockchain. This makes it very resistant to censorship and manipulation [14].

2.3. blockchain architecture

The blockchain, a distributed ledger, maintains an increasing list of items known as blocks that are linked and secured via encryption. A timestamp and a reference to the block preceding it are included with each block [5]. Each block in the blockchain has a hash in its header that was generated using the SHA256 cryptographic hashing method. The "previous block hash" part in the block header, commonly known as the parent block, serves as a pointer to the block that came before it for each block. In other words, each block's header contains a hash of the block that it is derived from. A blockchain's genesis block is its initial block and does not have a parent block.

2.4. the structure of block

The header of a block contains the Merkle root [15], the Nonce, the timestamp, and the hash of the block before it. A block is made up of a body and a header. The blockchain's basic architecture is depicted in Fig. 2, which can aid in our understanding of how the de-blockchain functions.

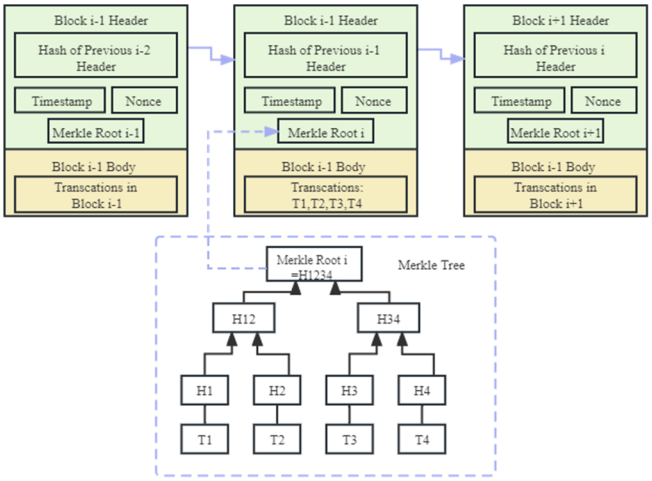

Fig. 2. Blockchain structure with a Merkle tree [15]

Timestamp: The block was made at this precise moment.

List of transactions: This is a list of all the transactions that were included in the block.

cryptographic hash of the previous block: This is a unique identifier for the previous block. It is used to link the blocks together. This means that if any of the data in a block is changed, the hash will change, and the block will no longer be linked to the previous block.

nonce: This is a random number that is used to solve a mathematical puzzle. This puzzle is designed to be difficult to solve, but easy to verify. The purpose of the nonce is to make it difficult for someone to create a new block that is linked to the previous block.

Merkle root: The block body contains the Merkle root, which is the root hash of a Merkle tree. All of the transactions in the block are hashed together. It is calculated by repeatedly hashing transaction pair pairs until only one hash is left. The block's integrity is then checked using this hash.

The Merkle root of the block will change if any of the transactions in it are modified, and the network will reject the block as a result.

3. Technology of blockchain

3.1. Consensus algorithm

The Byzantine Generals (BG) Problem is turned into a blockchain-based problem of how to obtain consensus among untrustworthy nodes. Lamport, Shostak, and Pease first presented the BG problem in 1982[16,17]. In the BG problem, a group of generals in control of a Byzantine army division circle the city. The attack would be unsuccessful if only a few of the generals attacked the city. Generals must confer with one another before deciding whether to attack or not. There might be traitors among the generals, though. Each general can receive a different decision from the traitor. This is an unreliable setting. It can be difficult to come to a consensus in such a setting.

It presents a problem for blockchain as well. Blockchain lacks a central node to ensure that the ledgers of distributed nodes are similar to one another. It is not necessary for nodes to trust one another. As a result, certain methods are needed to ensure the consistency of ledgers across various nodes.

Byzantine Fault Tolerance (BFT) is one method used in blockchain to achieve consensus [18]. A distributed system can continue to function even if some of its nodes are Byzantine, which means they might be corrupted or malevolent. BFT is a fault tolerance method. The foundation of BFT is the idea that honest nodes may still reach consensus on the system's state even if they have greater computing power than Byzantine nodes. The following is a description of further blockchain consensus techniques.

Proof of Work (PoW). Blockchain networks are protected by the consensus algorithm PoW[10]. In order to add a new block to the blockchain, PoW nodes compete to solve a challenging computational challenge. The first node to figure out the problem receives a block reward, which is a brand-new coin.A hash function that takes as inputs a nonce and the hash of the previous block and generates a 256-bit hash is the puzzle that nodes must solve. The puzzle's difficulty is raised by using the nonce, a random number. It is highly challenging to discover a nonce that generates a hash that satisfies the difficulty criteria because of how the hash function is constructed.A node broadcasts the solution to the network when it has finished the problem. The new block is then added to the blockchain when the other nodes have verified the solution. The node that found the solution receives the block reward if the solution is legitimate.

Proof of Stake (PoS) [19]. PoS is a consensus algorithm that is used to secure blockchain networks. In PoS, nodes are selected to add blocks to the blockchain based on their stake in the network. This means that nodes with more coins have a greater chance of being selected, but they are not guaranteed to be selected. The stake of a node is the amount of cryptocurrency that they have locked up in the network. The likelihood that a node will be chosen to add a block to the blockchain increases with the number of bitcoin they have staked. A block reward, which is a brand-new coin, is given to a node when it is chosen to add a block to the block-chain. The block reward often varies in accordance with the node's stake.

Proof of Capacity (PoC) [20]. PoC is a consensus algorithm that is used to secure blockchain networks. In PoC, nodes are selected to add blocks to the blockchain based on their storage capacity. This means that nodes with more storage space have a greater chance of being selected, but they are not guaranteed to be selected.The storage capacity of a node is the amount of data that they can store on their hard drive. The more data that a node can store, the greater their chance of being selected to add a block to the blockchain. When a node is selected to add a block to the blockchain, they are rewarded with a block reward, which is a new cryptocurrency. The block reward is typically proportional to the amount of storage capacity that the node has.

Delegated Proof of Stake (DPoS) [21]. A consensus technique called DPoS combines Proof of Stake (PoS) and Proof of Work (PoW) elements. Nodes choose representatives in DPoS who contribute new blocks to the network. These representatives are responsible for staking their coins

and validating transactions. The delegation process in DPoS is similar to the voting process in a democracy. Nodes can delegate their stake to any representative that they trust. The more coins that a node delegates, the more votes that they have. The representatives are selected based on the number of votes that they receive. The representatives with the most votes are the ones that are responsible for adding blocks to the blockchain. A representative receives a block reward, which is a brand-new coin, for adding a block to the blockchain. Usually, the block payment is inversely correlated to the amount of votes the representative earned.

Practical Byzantine Fault Tolerance (PBFT) [22]**.** A consensus algorithm that can withstand Byzantine failures is called PBFT. A maliciously motivated failure is referred to as a Byzantine failure. Compared to the other consensus algorithms discussed here, PBFT is a more complicated algorithm but offers a high level of security. A group of nodes known as replicas that concur on the blockchain's state make up the PBFT consensus mechanism. To agree on the state of the blockchain, the clones communicate with one another. The other replicas have the option to vote to exclude a replica from the consensus process if it is thought to be Byzantine. Even if up to one-third of the copies are Byzantine, the PBFT consensus method is made to be safe. This is due to the algorithm's employment of a voting mechanism to guarantee that the majority of clones concur on the blockchain's current state. This is due to the algorithm's employment of a voting mechanism to guarantee that the majority of clones concur on the blockchain's current state. The comparisons of the five consensus algorithms are listed in Table 1.

Table 1. Comparison of consensus algorithms [23][24][25]

	PoW	PoS	PoC	DPoS	PBFT
Setup	Public/private blockchain	Public/private blockchain	Public/private blockchain	Public/private blockchain	Private permissioned blockchain
Finality	Probabilistic	Probabilistic	Probabilistic	Probabilistic	Immediate
Speed	Low	High	High	High	High
Energy Effciency	Very low	High	High	High	Medium
Scalability	Good	Good	Good	Good	Bad
Resource Requirements	High	Medium	High	Medium	High
Example of use	Bitcoin Ethereum, Litecoin	Tezos, Ethereum2.0	NXT	EOS BitShares	Hyperledger, Chain

3.2. Smart contract

A smart contract is a piece of computer code that is recorded on a blockchain and is intended to run automatically when specific criteria are satisfied. Smart contracts are often used to facilitate the exchange of money or assets, but they can also be used to automate other tasks, such as the execution of contracts or the provision of services.

In 1994, Nick Szabo made the first mention of smart contracts [26]. Szabo was a legal scholar and computer scientist who was passionate in the intersection between law and technology. He recognized that smart contracts had the power to fundamentally alter the way that contracts are carried out. A smart contract is described as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises" by Szabo in his initial description. He believed that smart contracts may be used to establish "self-enforcing contracts" that do not need the involvement of a judge or an attorney. The concept of smart contracts was revived in the early 2000s with the advent of blockchain technology. Blockchain is a distributed ledger system that enables safe and

impenetrable transaction recording. This makes it perfect for smart contract storage, which is likewise done via distributed ledger technology.

The first blockchain-based smart contract was deployed in 2014 on the Ethereum blockchain [11]. Since then, there has been a growing interest in smart contracts, and they are now being used in a variety of applications. Smart contracts, according to Sarah Meiklejohn and Nick Szabo, have the ability to completely change how contracts are enforced [27]. They contend that with smart contracts, agreements may be made that are more effective, transparent, and secure than conventional agreements.

3.3. Cryptography in Blockchain

Cryptography is a critical component of blockchain technology. It is used to secure the network, verify transactions, and create digital signatures.

Public Key Cryptography. An encryption key and a decryption key are used in public key cryptography, a kind of asymmetric cryptography. While the decryption key is kept secret, the encryption key is made public. With the public key, anybody may encrypt data; however, only the owner of the private key can decode it. Public key cryptography is used in blockchain to secure the network and verify transactions. For example, when a transaction is made, the sender's public key is used to encrypt the transaction data. The receiver can then use their private key to decrypt the data and verify that the transaction is valid. The creation of digital signatures is another function of public key cryptography, in addition to network security and transaction verification [28]. A digital signature is a safe method of authenticating a communication or document using cryptography. The sender encrypts a message or document's hash using their private key to produce a digital signature. The recipient may then decode the hash and confirm that the message or document hasn't been tampered with by using the sender's public key.

Zero-Knowledge Proofs. A sort of cryptographic procedure called zero-knowledge proofs enables one party to demonstrate to another party that they are aware of a secret without actually disclosing the secret. This is accomplished by creating a mathematical proof that is verifiable by the other party but conceals the details of the secret. Zero-knowledge proofs are used in blockchain to provide privacy and security [29]. For example, a user can use a zero-knowledge proof to prove to a blockchain node that they own a certain amount of cryptocurrency without revealing their identity or the amount of cryptocurrency they own. Blockchain technology also makes use of zero-knowledge proofs to build secure smart contracts. A self-executing contract that is kept on the blockchain is known as a smart contract. Without making the specifics of the contract public, zero-knowledge proofs can be used to confirm the validity of the contract's conditions.

Hash Functions. One class of cryptographic function is the hash function, which accepts inputs of arbitrary size and outputs results with a set size. A hash value or digest is the result of a hash function. Blockchain technology uses hash functions to protect the network and validate transactions. For instance, a block's hash value is calculated and saved when it is added to the blockchain. The block's hash value is then used to check to see if it has been tampered with. It is obvious that the block has been altered if the block's hash value changes. Blockchain technology also use hashing operations to build safe data structures. A safe and effective hash tree type is the Merkle tree, which is used to store data. Blockchain uses Merkle trees to preserve the history of its transactions [30].

4. Blockchain Applications

4.1. Cryptocurrencies

Cryptocurrencies, digital or virtual currencies secured by cryptography, offer distinctive qualities and a compelling allure. Unlike traditional fiat currencies, cryptocurrencies are theoretically protected from government intervention or manipulation since they are not issued by a single entity.

Since the invention of Bitcoin in 2009, over 4,000 alternative cryptocurrencies, known as altcoins, have emerged. These altcoins provide various features such as faster transaction speeds, lower fees,

or increased anonymity. When designed and implemented correctly, cryptocurrencies have the potential to significantly improve payment systems. Cryptocurrencies are commonly traded on decentralized exchanges and can be used for purchasing goods and services, although their adoption is still in the early stages [31]. Pros of cryptocurrencies include enhanced security through cryptographic protection of transactions and user privacy, transparency due to visible and auditable transactions on a public ledger, immutability preventing manipulation, and decentralization without a central issuing authority. Cons of cryptocurrencies include high price volatility, complexity in usage and technology, and uncertain regulatory status, which can limit certain applications. Cryptocurrencies represent a cutting-edge technology that can reshape the concept of money. However, several challenges need to be addressed before broader adoption can occur. As the technology advances and regulatory frameworks become clearer, cryptocurrencies are expected to play a larger role in the global economy.

4.2. Supply Chain

Blockchain technology has the potential to revolutionize supply chain management by providing a secure, transparent, and immutable record of transactions. This transformation can bring several advantages, including increased visibility, enhanced traceability, and improved security.

By providing real-time visibility of goods and resources, blockchain enhances visibility throughout the supply chain, reduces errors and delays, and strengthens decision-making. Solutions like IBM's blockchain-based data sharing platform for supply chains facilitate secure data sharing and increase efficiency. Blockchain's tamper-resistant record of movements across the supply chain improves traceability, safeguards products, and prevents fraud and counterfeiting. Companies like VeChain utilize blockchain to collect and monitor logistical information, ensuring open, regulated, secure, and reliable data exchange. The distributed nature of blockchain makes it highly secure, challenging to hack or alter. This feature enables its application in securing Industry 4.0 smart manufacturing, achieving sustainability in manufacturing systems, and bridging the gap between global planning and local execution in customized manufacturing systems. Leading companies such as IBM, VeChain, and ManuChain are already utilizing blockchain to trace the movement of commodities and materials in supply chains. As the technology evolves, we can anticipate further cutting-edge applications that enhance supply chain management through secure, transparent, and effective traceability.

4.3. Health care

Blockchain, a distributed ledger technology, holds the potential to transform the healthcare sector by creating secure, transparent, and unalterable patient data records. This can lead to improved patient care, reduced costs, and enhanced security. Although still in its infancy, several initiatives explore blockchain's benefits in healthcare.

Promising blockchain applications in healthcare include: Electronic Health Records (EHRs): Blockchain can generate a shared record of patient data for EHRs, simplifying and expediting access for healthcare professionals and potentially improving patient care. Pharmaceutical supply chain management: Blockchain can track the movement of drugs across the supply chain, ensuring medication safety and authenticity while reducing counterfeiting. Clinical trials: Blockchain can facilitate clinical trials management, reducing costs and ensuring data integrity. Blockchain's potential in healthcare is being actively investigated, and its implementation has the capacity to revolutionize the sector. From EHRs to supply chain management and clinical trials, blockchain offers secure and transparent solutions that can transform healthcare processes and outcomes.

5. Challenges and further trend

Blockchain technology, as a foundational technology for the future development of the digital society, has been continuously evolving to solve various technical challenges. However, many problems and challenges arise alongside the development of blockchain, which revolves around the

"impossible triangle" of decentralization, security, and high performance. To address these challenges, researchers have proposed numerous optimization solutions tailored to different scenarios.

5.1. Cross-chain protocol

In the realm of blockchain technology, various blockchain systems have emerged, each with its own algorithms and platforms. However, this has resulted in low interoperability among major platforms, leading to a fragmented and isolated environment among different blockchains. To address this challenge and enhance the overall usability of blockchain technology, Ripple introduced the concept of cross-chain technology, which enables the exchange of information between different chains through specific algorithms [32]. Currently, the main technologies in this domain include Notary mechanisms, Sidechains, Hash Locking, and Distributed Private Key Control. Notary mechanisms are based on the Interledger protocol and act as trusted intermediaries to ensure the security and reliability of transactions between parties. They can be categorized as single-signature, multi-signature, and distributed signature Notaries. Notaries perform tasks such as data collection, transaction confirmation, and identity authentication during the transaction process. Sidechain technology refers to a blockchain system that relies on the main chain while possessing independent functionality. Sidechains complement the main chain by providing additional features such as transaction oversight, privacy protection, and smart contracts. They are connected to the main chain through a two-way peg mechanism.

Hash Locking is a mechanism that utilizes time-based locking in smart contracts to facilitate secure transactions with zero confirmation. It encompasses two types: Expiry Sequence Revocable Contracts and Hash Time-Lock Contracts. The Expiry Sequence Revocable Contract requires both parties to sign for each transaction and allows either party to request withdrawal at any time, preventing alterations to the transaction outcome. The Hash Time-Lock Contract ensures that the recipient either completes the transaction before the deadline or returns the funds to the initiator. Distributed Private Key Control is a mechanism that maps cryptocurrencies to asset chains on the blockchain protocol and controls the assets through smart contracts using protocols for generating and managing private keys. It employs key locking and unlocking mechanisms to prevent any node on the asset chain from modifying asset ownership until the smart contract confirms the completion of the transaction and unlocks the assets.

5.2. Privacy protection

Blockchain technology, by its very nature of decentralization and anonymity, has strong privacy protection capabilities. However, in the practical application of blockchain, the anonymity protection system of blockchain based on asymmetric encryption algorithms has been greatly challenged. Attackers have shifted from cracking passwords to analyzing user behavior by clustering IP data packets, transaction record addresses, transaction behavior models, and other data on the network. They can decipher the data content of users by analyzing the relationship between behavior and users. Currently, the most commonly used privacy protection technology is coin mixing. This technique combines multiple different transactions together to disrupt the original transaction relationships exposed on the network. Coin mixing technology is mainly divided into centralized coin mixing and decentralized coin mixing. Both methods require intermediary nodes to hide the relationship between input and output nodes. The difference is that centralized coin mixing relies on pre-established third-party coin mixing nodes as intermediaries, while decentralized coin mixing relies on protocol-based automatic selection of intermediary nodes from all coin mixing participants. To prevent the leakage of transaction information by the intermediary nodes, current coin mixing mechanisms utilize cryptographic knowledge such as ring signatures, zero-knowledge proofs, and blind signatures to protect the security of data during the mixing process and at the intermediary nodes, ensuring the security of transaction information during the coin mixing process.

5.3. Scalability of blockchain

With the continuous development of blockchain technology, the amount of data that blockchain needs to process is increasing. Traditional methods of processing data on the blockchain are no longer able to meet the current demands. As a result, various structures and algorithms have been designed to enhance the scalability of blockchain. The technologies for improving blockchain scalability can be broadly categorized into on-chain scaling and off-chain scaling.

On-chain scaling involves modifying the underlying framework of the blockchain protocol by changing block capacity, adopting sharding to manage blocks, or designing new consensus algorithms. On-chain scaling usually involves subtle modifications to the protocol structure, and the implementation methods can be complex. The scalability achieved through on-chain scaling is relatively limited due to the constraints of the protocol structure. Off-chain scaling, on the other hand, focuses on expanding capacity at the application layer without modifying the protocol framework. The core idea of off-chain scaling is to transfer specific data computations to chains outside the main chain through sidechains, state channels, lightning networks, etc. The main chain only records the computed results. By reducing the amount of information that needs to be stored in each block, the blockchain is effectively scaled. Currently, the mainstream approach for scalability is off-chain scaling because it is not limited by the inherent structure of the blockchain, and there is no upper limit to the expansion capacity. However, it also raises concerns about the risks associated with data computations not being on the main chain.

5.4. Data storage

In traditional blockchain storage systems, every node in the network is required to store all data, including previous versions, leading to significant data redundancy. This imposes a heavy memory burden on the blockchain nodes. To address this issue, two storage schemes have been developed: on-chain storage and on-chain/off-chain collaborative storage. In the current on-chain storage scheme, a sharding approach is adopted to optimize data redundancy. The complete blockchain data is divided into smaller shards, and an appropriate and secure shard size and quantity are calculated. These shards are then distributed and stored across the nodes in a proportional manner, significantly reducing the memory requirements for data storage. However, this approach compromises querying speed since complete data retrieval is not possible from a single node. Additionally, the reduced number of full nodes in the network increases the potential risks associated with malicious behavior.

On-chain/off-chain collaborative storage separates the on-chain data into two parts: on-chain storage and off-chain storage. To ensure the safety of off-chain data and mitigate potential risks, collaborative storage solutions utilize smart contracts and distributed hash tables to establish indexes. Furthermore, all off-chain data undergoes hashing operations, and the resulting hash values are stored on-chain, ensuring data integrity and availability.

6. Conclusion

This article provides an introduction to the characteristics and structure of blockchain. It elaborates on the five major consensus mechanisms involved in blockchain and highlights their differences. Additionally, it discusses the specific applications of smart contracts in blockchain and underscores the crucial role of cryptography in blockchain construction. Furthermore, the article offers a detailed and comprehensive overview of three important application directions of blockchain: cryptocurrencies, supply chains, and healthcare security. It explains the significant advantages that blockchain brings in these areas and provides a certain degree of outlook for future development. Lastly, it addresses the various challenges posed by the "impossible triangle" of decentralization, security, and high performance in blockchain. It introduces four major research trends: cross-chain protocols, privacy protection, blockchain expansion, and data storage. The recent research achievements in each direction are also presented.

Authors Contribution

All the authors contributed equally and their names were listed in alphabetical order.

Reference

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review.

[2] Sheldon, R. (2021). A timeline and history of blockchain technology. Retrieved from https://whatis.techtarget.com/feature/A-timeline-and-history-of-blockchain-technology

[3] Tandon, A., Dhir, A., Islam, A. K. M. N., & Mäntymäki, M. (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Computers in Industry, 122, 103290.

[4] Dai, H., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. IEEE Internet of Things Journal, 6, 8076–8094.

[5] Lin, I., & Liao, T. (2017). A survey of blockchain security issues and challenges. International Journal of Network Security, 19(5), 653-659.

[6] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

[7] Chaum, D. (1982). Computer systems established, maintained, and trusted by mutually suspicious groups. PhD thesis, University of California, Berkeley, CA, USA.

[8] Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. Journal of Cryptology, 3(2), 99-111.

[9] Sharma, R. (2021). Bitgold: Meaning, Overview, Differences From Bitcoin. Investopedia. Retrieved from https://www.investopedia.com/terms/b/bit-gold.asp

[10] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review.

[11] Buterin, V. (2013). Ethereum whitepaper. Retrieved from https://ethereum.org/en/

[12] Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World.

[13] Swan, M. (2015). Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media, Inc.

[14] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. White Paper, 3(37), 2-1.

[15] Merkle, R. C. (1980). Protocols for public key cryptosystems. In 1980 IEEE Symposium on Security and Privacy (pp. 122-122).

[16] King, V., & Saia, J. (2010). Scalable Byzantine computation. ACM SIGACT News, 41(3), 89-104.

[17] Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, 4(3).

[18] Santos, R., Bennett, K., & Lee, E. (2021). Blockchain: Understanding its uses and implications. The Linux Foundation.

[19] Vasin, P. (n.d.). BlackCoin's Proof-of-Stake Protocol v2. Retrieved from https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf

[20] Hayes, A. (2020). Proof of Capacity (cryptocurrency). Investopedia. Retrieved from https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp

[21] Crushcrypto. (2018). WHAT IS DELEGATED proof-OF-STAKE? Crushcrypto. Retrieved from https://crushcrypto.com/what-is-delegated-proof-of-stake/

[22] Castro, M., & Liskov, B. (1999). Practical Byzantine fault tolerance. In OSDI (pp. 173-186).

[23] Kozak, T. (2018). Consensus Protocols that Meet Different Business Demands, Part I. Intellectsoft. Retrieved from https://blockchain.intellectsoft.net/blog/consensus-protocols-that-meet-different-business-demands/

[24] Khan, M., den Hartog, F., & Hu, J. (2022). A Survey and Ontology of Blockchain Consensus Algorithms for Resource-Constrained IoT Systems. Sensors, 22(2), 8188.

[25] Guo, H., Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: Research and Applications, 3(2), 100067.

[26] Szabo, N. (1994). Smart Contracts: The Next Revolution in Contract Law. SSRN Electronic Journal.

[27] Tapscott, D., & Tapscott, A. (2016). The Future of Money: How the Blockchain Will Revolutionize Finance.

[28] Leng, J., et al. (2021). Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51(1), 237-252. https://doi.org/10.1109/TSMC.2020.304078

[29] Leng, J., et al. (2020). Blockchain-empowered sustainable manufacturing and product lifecycle management in Industry 4.0: A survey. Renewable and Sustainable Energy Reviews, 132, 110112.

[30] Leng, J., et al. (2019). ManuChain: Combining permissioned blockchain with a holistic optimization model as bi-level intelligence for smart manufacturing. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(1), 182-192.

[31] Tandon, A., Dhir, A., Islam, A. K. M. N., & Mäntymäki, M. (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Computers in Industry, 122, 103290.

[32] Sun, H., Mao, H., Zhang, Y., et al. (2022). Development and Application of Blockchain Cross-chain Technology. Computer Science, 49(05), 287-295.