

Reading Reports on Different Types of Blockchain Technology

Sun Tianhao MC251242

1 Introduction to Blockchain-Related Concepts

In this section, some concepts and characteristics related to Blockchain are preliminarily introduced. The basic concepts are the foundation for understanding Blockchain, so this section provides a detailed introduction.

1.1 Some Important Concepts

- Peer-to-Peer (P2P) Network

The Peer-to-Peer (P2P) Network is a distributed network architecture that allows participants to share resources among themselves. Each participant node in the network acts as both a client and server, making their resources available to be shared with other participants [1]. This means that at any given time, a participant can directly request services and contents from another participant without any intermediate entities. The P2P network is designed to facilitate resource sharing among participants, including processing power, link capacity, printers, and storage capacity.

- Cryptography

Cryptography is the mathematical art of making communication secure. It is commonly used in most modern security protocols [2]. In cryptography, a mathematical value called '*key*' plays a central role. There are two types of modern cryptography: symmetric key cryptography, in which the same key is used by sender and receiver for cryptograph operations, and asymmetric key cryptography, in which each communicating party has two different keys called public and private keys used for different cryptograph operations in different ways.

- Encryption/Decryption

Encryption is a process used to encode the plaintext (intelligible data) into ciphertext (unintelligible data or un-understandable data) for the provision of confidentiality of security service. Decryption is the reverse process to convert ciphertext into plaintext. Encryption and decryption processes can be implemented by using symmetric or asymmetric cryptography [3].

- Hash

Hash is a one-way mathematical function used to protect the integrity of data. It works by calculating a fixed-sized unique value called 'hash value' for every variable input. The hash function is one-way, which means original data cannot be calculated back from the unique output [3]. Its security strength lies on one-way characteristic, which is used to protect the integrity of data [3].

- Hash Chain

A hash chain is generated by successively applying the hash function on a piece of

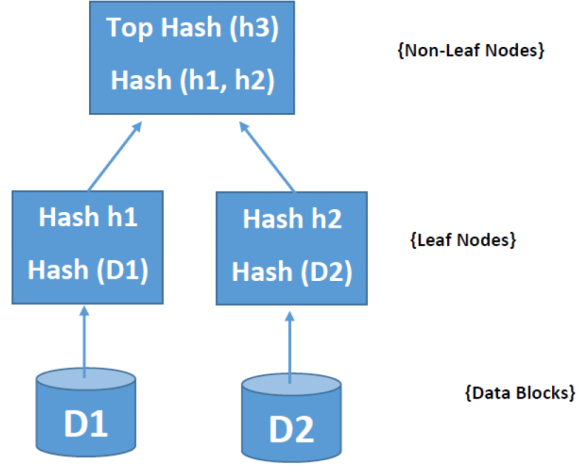


Figure 1: An example of a Merkle tree [4]

data. For example, a hash value h_1 is generated by applying a hash function $f(x)$ on data x . The h_1 is input to the other hash function $f(h_1)$ to calculate second hash value h_2 in the chain and so on. These calculated hash values h_1, h_2, \dots, h_n make a chain of hashes of length n . Hash chains have many applications for protection of data integrity and play a key role in Blockchain.

- Merkle Tree

Merkle trees, also known as hash trees, provide efficient and secure verification of data by arranging the data and corresponding hash values in the form of a tree. In the tree structure, every leaf node is labeled with the hash value of some data, and every non-leaf node contains the hash value of its child nodes. Figure 1 shows an example of a Merkle tree.

- Digital Signatures & Timestamp

Digital signatures are used as a proof of authorship along with the contents. The signatures are usually applied using public key cryptography in which, a signer uses its private key to sign a document and a recipient can verify the signatures using

signer's public key. Digital signatures are considered authentic, unforgeable, non-reusable and non-repudiated. Timestamp is the time at which event occurrence is recorded by a computer, rather than the time of event itself [5].

1.2 Some Important Characteristics

This section briefly introduces key Blockchain characteristics.

- Decentralization

Decentralization refers to the distribution of power and control across a network of nodes rather than being centralized in a single entity. In a decentralized system, there is no central authority [6][7][8] or intermediary controlling the network, and all participants have equal access to information and decision-making processes. This allows for greater transparency, security, and resilience against attacks or failures.

- Transparency

Transparency refers to the ability of anyone to see the details and history of any transaction on the Blockchain ledger. The transparency is achieved because a Blockchain network has several validating peer nodes without a centralized authority [8], as well as the fact that the holdings and transactions of each public address are accessible and open to viewing by anyone [7].

- Autonomy

Autonomy refers to the ability of the Blockchain system to function in a peer-to-peer (P2P) manner without a reliable third party required to ensure trust [7]. Blockchain technology provides a system where trust is no longer an issue, and all transactions

are based on a set of rules and algorithms called consensus protocols among the Blockchain nodes to ensure that information is consistent and incorruptible [9]. This eliminates the need for powerful central authorities and instead transfers control to the individual user, making the system fair and considerably more secure.

- Security

Security refers to the measures taken to ensure that the information stored on the Blockchain is secure and tamper-proof [6][9]. Blockchain technology uses cryptographic algorithms and a distributed network of nodes to secure transactions, making it virtually impossible for anyone to alter or delete data once it has been recorded on the Blockchain.

- Immutability

Immutability means that once data is added to the Blockchain, it cannot be altered or tampered with. This is achieved through cryptographic algorithms and time stamp, making the data permanent and secure [10]. The distributed nature of the Blockchain network also ensures that there is no single point of failure or control, making it highly resistant to hacking attempts and other malicious activities.

- Traceability

Traceability means tracking the source, destination, and sequence of updates that data goes through. This is achieved through time stamp and hash values stored in each block. Traceability also has several other benefits such as better data governance, conformity with regulations, understanding impact of change, and improvement of data quality among others .

- Anonymity

Anonymity refers to the ability to keep the identity of users private and secure. The use of Blockchain technology provides support for anonymity, ensuring privacy and protection from unauthorized intrusion or observation [11][12]. Anonymity is a key feature of Blockchain technology that supports privacy and confidentiality.

- Democratized

Democratized in blockchain means that decisions are made democratically by all nodes using a peer-to-peer approach. Consensus algorithms are used to ensure that all nodes have equal rights and obligations, share data, and jointly maintain information in the Blockchain [9].

- Integrity

Integrity means data remains accurate and consistent over its life cycle [8]. Achieved through decentralized, immutable shared ledgers, it guarantees data reliability and security [9].

- Programmability

Programmability in Blockchain means users can develop applications through a common programming interface [11][6]. The flexible script coding system can be used to create advanced smart contracts or other decentralized applications. It supports innovation and customization.

- Fault Tolerance

Fault tolerance refers to the ability of the system to continue functioning even in the presence of faults or failures. Blockchains are designed to be Byzantine Fault

Tolerant, which means the network will come to a consensus even if some nodes are down or not acting correctly [13]. Fault tolerance is a key feature of Blockchain technology that supports reliability and resilience.

- Automatic

Automatic in Blockchain refers to the ability of smart contracts to perform transaction generation, decision making, and data storage without human intervention. All nodes in the system can automatically transact and verify data using specific consensus protocols [6].

2 Introduction to the Evolution of Blockchain

In this section, we introduce the evolution of different types of Blockchains.

2.1 P2P Network

The precise definition of the P2P network was first proposed by R. Schollmeier [1] in 2001. With the rapid development and expansion of the Internet, the traditional Client/Server architecture could no longer meet the needs of users exchanging information, and P2P networks emerged. P2P networks are also the foundation of Blockchain. R. Schollmeier's accurate explanation of the definition of P2P networks in [1] laid the foundation for the development of Blockchain.

2.2 Blockchain 1.0 [\[14\]](#)

2.2.1 Background

Bitcoin was proposed as a solution to the problem of needing a trusted third party to prevent double-spending in electronic payment systems. The proposed solution uses a peer-to-peer network and cryptographic proof instead of trust to allow any two willing parties to transact directly with each other without the need for a trusted third party. This system is designed to be secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2.2.2 Key Contributions

- Proposing a purely peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution.
- Using digital signatures and a peer-to-peer network to prevent double-spending without the need for a trusted third party.
- Introducing the concept of Blockchain technology, which is used to record and verify transactions decentralized and transparently.

The architecture of Blockchain 1.0, also known as cryptocurrencies, is a distributed ledger system designed to store digital cash transactions between two parties efficiently. The transactions are recorded in blocks that are linked together in a chain using cryptographic techniques, ensuring the immutability and security of the ledger. [Figure 2](#) shows a block in the Blockchain architecture. [Figure 3](#) shows the categorization of Blockchain nodes.

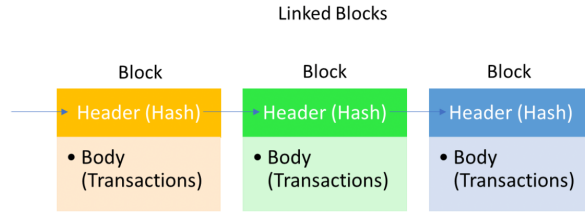


Figure 2: A block in the Blockchain architecture. [4]

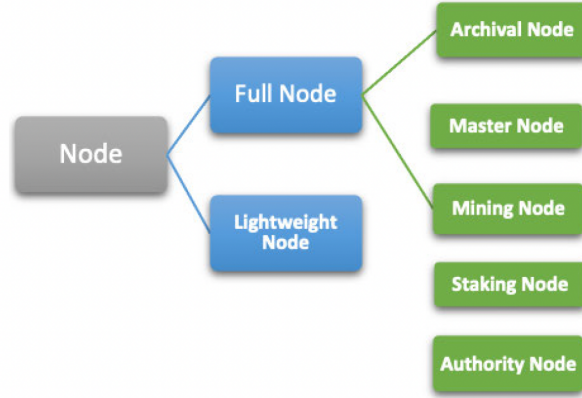


Figure 3: The categorization of Blockchain nodes. [4]

2.3 Blockchain 2.0

The biggest change introduced by Blockchain 2.0 compared to Blockchain 1.0 is the concept of Smart Contracts. The concept of Smart Contracts is defined as "a computerized transaction protocol that executes the terms of a contract".

2.3.1 Background

[15] Studied the application of Blockchain and Smart Contracts to the Internet of Things. [15] want to create a distributed peer-to-peer network where non-trusting members can interact with each other without a trusted intermediary, in a verifiable manner. Blockchain allows for a secure and transparent way of recording transactions, while Smart Contracts enable the automated execution of agreements between parties. By leveraging these technologies, IoT devices can communicate and transact with each other securely and efficiently,

without the need for centralized control or intermediaries.

2.3.2 Key Contributions

The key contributions of applying blockchain and smart contracts to the Internet of Things (IoT) [15] are:

- Facilitating the sharing of services and resources between devices, leading to the creation of a marketplace of services.
- Allowing for the automation of existing, time-consuming workflows in a cryptographically verifiable manner.
- Enabling secure and transparent recording of transactions without the need for centralized control or intermediaries.
- Providing a distributed peer-to-peer network where non-trusting members can interact with each other in a verifiable manner.

Blockchain 2.0 is the next tier in the development of Blockchain technology. It extends the functionality of digital money beyond just being a payment system and supports the transfer of many different kinds of assets like stocks, loans, smart properties, etc. Smart contracts are designed to be transparent, secure, and tamper-proof, ensuring that all parties involved in a transaction can trust the outcome without relying on intermediaries or third parties. Compared to Blockchain 1.0 (cryptocurrency), Blockchain 2.0 offers more robust functionality and has the potential to revolutionize various industries by enabling new business models.

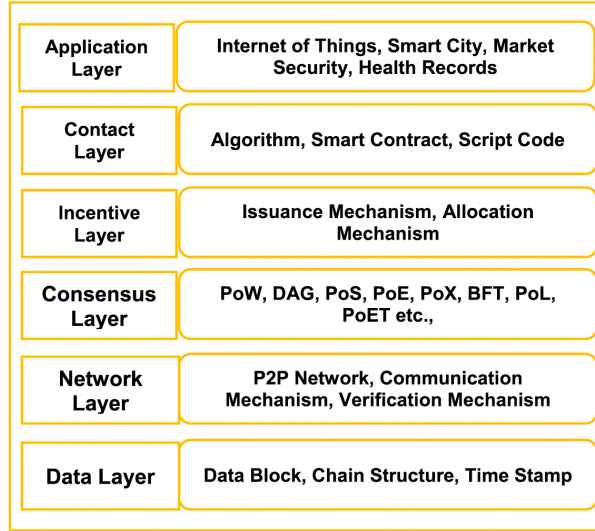


Figure 4: The general Blockchain layered architecture. [4]

2.4 Blockchain 3.0

With the development of technology, Blockchain is no longer limited to the applications of cryptocurrency (Blockchain 1.0) and Smart Contract (Blockchain 2.0). More and more Blockchain Applications beyond financial markets in areas including government, health, literature, culture, and so on emerge.

Blockchain 3.0 is designed to create secure and distributed applications for various industries beyond monetary markets. Blockchain 3.0 supports a universal and global scope by interconnecting with web technology and aims to contribute to the development of the Smart World. It has the potential to enable new use cases for Blockchain technology in different industries like games, the Internet of Things (IoT), supply chain, source tracing, etc. Figure 4 shows the general Blockchain layered architecture.

Decentralized applications are an important part of blockchain applications. [16] describes decentralized applications in detail.

2.4.1 Background

The emergence of decentralized applications can be attributed to the limitations of traditional centralized systems, which are vulnerable to single points of failure and can be controlled by a single entity. Decentralized applications, on the other hand, are built on top of Blockchain technology and are designed to be distributed across a network of nodes, making them more secure and resistant to censorship or control by any single entity. This allows for greater transparency and trust in the system.

2.4.2 Key Contributions

The key contributions of decentralized applications are [16]:

- Decentralized applications have no central point of failure, making them more secure and resistant to censorship or control by any single entity.
- Decentralized applications also allow for greater transparency and trust in the system.
- Different flavors of Blockchains can be used for different application scenarios, such as finance or infrastructure projects, allowing for more efficient and streamlined processes.
- Decentralized applications have the potential to revolutionize various industries by providing a more secure and transparent way of conducting transactions and managing data.

2.5 Challenges and Future Trends

Blockchain technology has the potential to revolutionize various industries, but it also faces several challenges and security issues [8].

The decentralized nature of Blockchain makes it difficult to regulate and control, which can lead to privacy concerns. Additionally, scalability and interoperability are still major challenges for Blockchain adoption. Blockchain technology also faces issues related to energy consumption and environmental impact. The process of mining cryptocurrencies like Bitcoin requires a significant amount of computational power, which consumes a lot of energy and contributes to carbon emissions.

Despite these challenges, the future trends for blockchain technology are promising. Blockchain is being explored for various use cases beyond financial transactions, such as supply chain management and healthcare. In terms of algorithms, the future direction is the transition from PoW (Proof of Work) to new algorithms such as PoS (Proof of Stake). The combination of Blockchain and the Internet of Things (IoT) is also one of the highly concerned directions that people are focusing on.

3 Differences Between Different Types of Blockchains

From Blockchain 1.0 to Blockchain 2.0 and further to Blockchain 3.0, each upgrade represents a significant technological advancement. We first discuss the similarities. The foundation of Blockchain is a P2P network. Built upon this, Blockchain can protect transactional information between parties while allowing everyone to view the details and history of any transaction. Thanks to the security and decentralization of Blockchain technology, decentralization has been achieved. Blockchain has been widely applied in various industries,

including finance, supply chain management, and the Internet of Things (IoT).

Then we talk about the differences between different types of Blockchains. Blockchain 1.0 was essentially a part of Bitcoin. Bitcoin [14] was proposed by Satoshi Nakamoto in 2008. Blockchain 1.0 provided a secure way to transact Bitcoin. Technological advancements made it apparent that Blockchain could be utilized for more than just Bitcoin transactions. Smart contracts are the biggest advancement of Blockchain 2.0 compared to Blockchain 1.0. Smart contracts have similarities to traditional business contracts, but they are completed using Blockchain, greatly enhancing transactional security. Smart contracts have enabled Blockchain to transact different commodities, significantly attracting the attention of the financial market. Smart Contracts-based Blockchain 2.0 is widely used in the financial market.

The development of the Internet of Things promotes the birth of Blockchain 3.0. In this stage, Blockchain is no longer only used for transactions but has different applications in various scenarios. Blockchain 3.0 is composed of various Blockchain applications. Different industries, such as the Internet of Things (IoT), the financial market, Healthcare, and supply chain management use different types of Blockchain applications. The different types of Blockchain applications are an important feature of Blockchain 3.0.

4 Own Understanding and Conclusion

Blockchain is a very powerful technology. As Blockchain technology evolves, a single concept alone can no longer fully define Blockchain technology. Blockchain is now a collection of complex technologies.

Blockchain 1.0 is only a component of the cryptocurrency, Bitcoin, which is used to

ensure secure transactions of Bitcoin. The most significant feature of Blockchain 2.0 is the introduction of the Smart Contract. This allows Blockchain to trade various commodities, no longer limited to cryptocurrencies. This has also led to the Blockchain being recognized by a larger area and has greatly attracted the interest of the financial market. The development of the Internet of Things (IoT) and other related industries, has given birth to Blockchain 3.0. Blockchain 3.0 is a collection of complex technologies, which is no longer limited to transactions, but different application scenarios using different Blockchain applications.

In my opinion, Blockchain is now a collection of technologies with features such as secure encryption, decentralization, etc. This technology fits well with the Internet and the Internet of Things (IoT) based on big data. Based on the P2P network, Blockchain provides a basis to develop distributed and secure applications for all industries beyond the monetary markets. Blockchain still has challenges and issues to be researched. Blockchain cryptographic algorithms, Smart Contracts, and other Blockchain applications have the potential for further research. Blockchain will be of greater value in various fields.

References

- [1] R. Schollmeier, “A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications,” in *Proceedings first international conference on peer-to-peer computing*, pp. 101–102, IEEE, 2001.
- [2] R. Anderson, “A guide to building dependable distributed systems,” 2001.
- [3] S. Bruce, “Applied cryptography: Protocols, algorithms, and source code in c.-2nd,” 1996.

- [4] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, “A survey on blockchain technology: Evolution, architecture and security,” *Ieee Access*, vol. 9, pp. 61048–61073, 2021.
- [5] P. A. Bernstein and E. Newcomer, *Principles of transaction processing*. Morgan Kaufmann, 2009.
- [6] Y. Lu, “Blockchain: A survey on functions, applications and open issues,” *Journal of Industrial Integration and Management*, vol. 3, no. 04, p. 1850015, 2018.
- [7] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, “A survey of blockchain technology applied to smart cities: Research issues and challenges,” *IEEE communications surveys & tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019.
- [8] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, “Integrated blockchain and edge computing systems: A survey, some research issues and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.
- [9] Y. Xinyi, Z. Yi, and Y. He, “Technical characteristics and model of blockchain,” in *2018 10th international Conference on communication Software and networks (ICCSN)*, pp. 562–566, IEEE, 2018.
- [10] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, “The blockchain as a decentralized security framework [future directions],” *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18–21, 2018.
- [11] I.-C. Lin and T.-C. Liao, “A survey of blockchain security issues and challenges,” *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017.

- [12] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in *2017 IEEE international congress on big data (BigData congress)*, pp. 557–564, Ieee, 2017.
- [13] A. Baliga, “Understanding blockchain consensus models,” *Persistent*, vol. 4, no. 1, p. 14, 2017.
- [14] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Decentralized business review*, p. 21260, 2008.
- [15] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” *Ieee Access*, vol. 4, pp. 2292–2303, 2016.
- [16] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. Leung, “Decentralized applications: The blockchain-empowered software system,” *IEEE access*, vol. 6, pp. 53019–53033, 2018.