BLOCKCHAIN CAPABILITIES AND TRANSACTION MANAGEMENT

Xolmatov Numonjon Meliboyevich

Teacher of the ICT and Communication Military Institute

Melibayeva Xilolaxon Numonjon qizi

3rd year student of Tashkent State Technical University named after Islam Karimov

Abstract: *Blockchain has many advantages such as decentralization, persistence, anonymity, and auditability. There is a wide range of blockchain applications ranging from cryptocurrency, financial services, risk management, Internet of Things (IoT) to public and social services. Although a number of studies have focused on the use of blockchain technology in various aspects of application, there has not been a comprehensive review of blockchain technology from both a technological and application point of view.*

To fill this gap, we are conducting a comprehensive review of blockchain technology. Specifically, this article provides a taxonomy of blockchain, introduces typical blockchain consensus algorithms, reviews blockchain applications, and discusses technical issues as well as recent advances in solving these issues. In addition, this article also points out the future directions in blockchain technology.

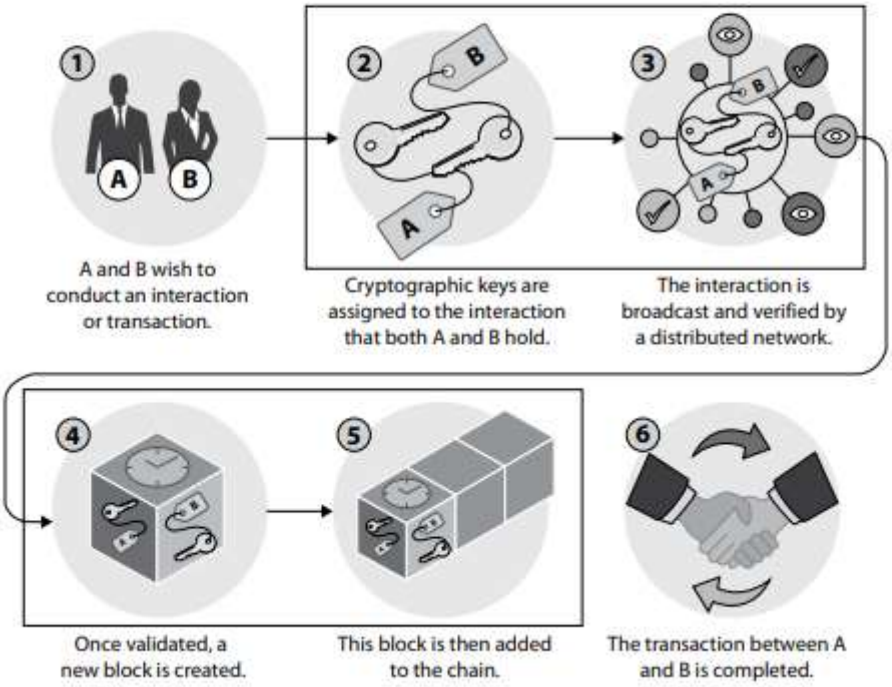
Key words: *blockchain, internet of things, smart contract*

Introduction to Blockchain

A blockchain is a distributed ledger with growing lists of records (*blocks*) that are securely linked together via cryptographic hashes. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree, where data nodes are represented by leaves). The timestamp proves that the transaction data existed when the block was created. Since each block contains information about the previous block, they effectively form a *chain*, with each additional block linking to the ones before it. Consequently, blockchain transactions are irreversible in that, once they are recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.

Public blockchain transaction flow

The blocks once recorded are designed to be resistant to modification; the data in a block cannot be altered retroactively. Through the use of a peer-to-peer network and a distributed timestamping server, a public blockchain database is managed autonomously. Blockchains are an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way as depicted in Pic 1.


1
A
B
A and B wish to conduct an interaction or transaction.
2
B
A
Cryptographic keys are assigned to the interaction that both A and B hold.
3
B
A
The interaction is broadcast and verified by a distributed network.
4
Once validated, a new block is created.
5
This block is then added to the chain.
6
The transaction between A and B is completed.

Pic 1. Public blockchain transaction flow

The ledger itself can also be programmed to trigger transactions automatically. Blockchains are secure by design and an example of a distributed computing system with high byzantine fault tolerance. Decentralized consensus can therefore be achieved with a public blockchain. As we shall discuss in detail later, these features make blockchains ideal for recording events, medical records and other records management activities, identity management, transaction processing, and a host of emerging applications. Moreover, blockchain technologies allow us to achieve large-scale and systematic cooperation in an entirely distributed and decentralized manner. This can be considered and implemented as a global governance tool, capable of managing social interactions on a large scale and dismissing traditional central authorities.

From a technical point of view, the blockchain is a distributed, transparent, immutable, validated, secured, and pseudo-anonymous database existing as multiple nodes such that if 51 percent of the nodes agree then trust of the chain is guaranteed. The blockchain is distributed because a complete copy lives on as many nodes as there are in the system. The blockchain is immutable because none of the transactions can be changed. The blockchain is validated by the miners who are compensated for building the next secure block. The blockchain is pseudo-anonymous because the identity of those involved in the transaction is represented by an address key in the form of a random string. That said, this is an evolving space and, like the cloud computing paradigm, there are public, private, and even hybrid blockchains, which we will explore in detail later in this chapter. These blockchain variations on the basic theme are the result of enterprise architects looking to implement blockchain applications to save time and fees. Enterprise requirements around scaling, performance, the need to know the identity of those involved in the transaction, and other things provide its emerging variations. Blockchain evangelists reckon distributed ledger technology has the potential to upend centralized database practices in institutional finance and most other transaction-based technology. In 2017, the technology shifted from hype to commercial reality. For blockchain to succeed, the application development life cycle, which facilitated large web applications using tools like HTML, CSS, JavaScript, REST web services, Java, SQL, and NOSQL data stores, will have to be amended to integrate the blockchain onto that stack.

The blockchain will have to operate efficiently, scale well, handle the know-your client (KYC) process, create the aforementioned oracles or APIs that produce and consume off-chain services to verify events and data and handle/convert real-world money to and from cryptocurrencies, and integrate well with different chains. This is all in progress, and we will explore some of these IDEs and development processes in detail as we proceed.

Blockchain-Based Cloud Storage Access Control Systems

Using blockchain technology, a cloud environment may be made safe by controlling access to information that cannot be trusted. You must store your data in a cloud storage environment that cannot be trusted. User access is controlled using attribute-based encryption that contains dynamic features. As a result of the decentralized ledger technology used by blockchain, all security-relevant operations, such as key revocation and creation, the designation of administrators of access policies, and the submission of access requests, are preserved without modification. In reference, a blockchain-based access control system is being developed. Authentication, identification, and authorization are three discrete yet interrelated procedures in access control. It is the framework that is in charge of keeping track of which particular activities clients are allowed to engage in. Customers' EHR data is kept in a blockchain-based data pool, and customers may use the new framework provided to verify their identity and cryptographic keys before accessing the data. Validation based on identification fulfils the authentication needs of the client. Customers and companies are discouraged from maliciously repeating roles and flexibility by preventing customers and businesses from enforcing their duties. To ensure that only authorized individuals have access to sensitive data, a new access control system is being developed based on smart contracts. An authentication procedure that confirms a user's ownership of positions may be authenticated by using blockchain and smart contracts as adaptable systems in the RBAC-SC, which utilizes blockchain and smart contracts to represent the connection of trust that is vital inside the RBAC. This approach confirms that a user owns positions using blockchain and smart contracts, verifying the challenge response's authenticity.

Smart Manufacturing

The Internet of Things (IoT) may impact this emerging field of smart manufacturing. Intelligent machines are a critical part of smart manufacturing because they can perform certain jobs with a higher level of intelligence than is currently achievable. This sector uses Internet-enabled technology, and service-oriented manufacturing. Modern manufacturing faces difficulties such as centralized industrial networks and authority dependent on third parties via smart manufacturing. Production methods that rely on centralized management are inflexible, inefficient, and unreliable.

Blockchain as a Driver of Digital Business Transformation

"Blockchain" is an open-source distributed database that uses cutting-edge encryption. One of the most widely used blockchain applications is Bitcoin, which utilizes an open ledger. Everyone can observe what is going on with an open-source platform, since anyone can update the underlying code. There are no middlemen to validate or to settle transactions, making it a real peer-to-peer (P2P) system. Various structured data may be stored in the system, including who paid whom, what money belongs to whom, or what light source provided the electricity. Although recent studies have shown security vulnerabilities on various platforms, blockchain is generally uncrackable, making it a trustworthy platform. For example, the cost of confirming transaction data may be reduced thanks to the blockchain, and intermediaries can be eliminated. Blockchain transactions function by broadcasting every block in the system to all parties, each receiving an exact copy of the transaction. An irreversible and transparent transaction record is created when all parties in the network agree on the transaction, such as sending money from one party to another.

In the financial service industry, blockchain is widely used to conduct financial transactions, also known as cryptocurrencies. Currently, cryptocurrencies are among the most prominent software systems. The first transaction occurs during the creation of the first block, or genesis block.

Using taxonomies in blockchain technology can help analyze blockchains and design and test software architectures. Using their taxonomy, they cover all the main architectural features of blockchains and the impact of various decisions. This taxonomy aims to assist in evaluating the performance and quality attributes of blockchain-based systems.

Conclusion

Blockchain technology provides verification efficiencies, including operational, regulatory, enhanced visibility, and traceability. This technology is also a powerful database that could easily be combined with big data. Blockchain solutions can help cut costs and make many services more competitive. There are a lot of small transactions happening in the real time. The applicability of blockchain technology in government accounting is relevant, but it is not considered a strategic priority. According to the respondents, blockchain use cases in their institution may be related to digital records, auditing, and smart contracts.

REFERENCES:

1. Libra Association (2019). Libra white paper. Retrieved July 12, 2019.
2. Iansiti M, Lakhani K (2017) The truth about blockchain. Harvard Business Review. January–February Issue. Retrieved April 12, 2019.
3. Rijmenam (2018) Why blockchain is quickly becoming the gold standard for supply chain. November 21. Retrieved April 18, 2019.
4. Velasco-Castillo E (2016) Nine blockchain opportunities that telecoms operators should explore. Knowledge Center, June, 13. Retrieved April 12, 2019
5. Strilets, B. Current state and prospects for the legal regulation of cryptocurrencies in the European Union. Actual Probl. Law 2022, 70–76.
6. Ramadoss, R. Blockchain technology: An overview. IEEE Potentials 2022, 41, 6–12.