Blockchain-based distributed database management technology

Maryam Ghazi Ali

Department of Mathematics and computer science, College of Science, Al Muthanna University

*Corresponding Author: mariamghazi@mu.edu.iq

Received 31 March 2022, Accepted 7 September 2022, published 31 December 2022.
DOI: 10.52113/2/09.02.2022/23-30

Abstract: currently, the development of a new class of software called “decentralized applications” is gaining popularity. Its foundations were laid by the technologies of Bitcoin and BitTorrent, aroused the interest of developers in the methods of their implementation.

Over the past few years, the whole world has been excited by the explosion in popularity of cryptocurrencies, which has brought blockchain technology into the spotlight. its application is not limited to the creation of electronic money and platforms for their exchange. One of the promising areas for the introduction of blockchain technology is its use in the banking sector to improve the security of operations and reduce costs.

This paper focuses on Blockchain technology and investigates its applications, implementations, and constituents. and how blockchain applications enhancing database management.

Keyworks: Bitcoin, BitTorrent, Blockchain, database management.

1. Introduction

Blockchain is a distributed, decentralized, encrypted database in which every completed transaction is recorded and becomes known to all network members. Data about completed transactions is stored in a certain order and form an invariable sequence of related blocks. After that, the information contained in the block is replicated and copied to every node in the network. This algorithm ensures the stability of usually managed using a peer-to-peer network. Once recorded, the data in any block cannot be changed without completely changing all subsequent blocks, which requires the consent of the majority of network participants.

Currently, there are three types of blockchain:

a) Blockchain 1.0 is a cryptocurrency. Examples are Bitcoin, Ethereum, Litecoin, etc.

b) Blockchain 2.0 is smart contracts. This is a wide class of financial applications that work with stocks, bonds, futures, mortgages and many other financial assets.

c) Blockchain 3.0 - all other applications based on this technology and beyond the financial sector.

2. Principle of Blockchain work

Despite the fact that the Blockchain is a distributed system, and each participant can conduct a transaction, not all of them are equal. Participants in the system are divided into operators conducting the transaction, network regulators responsible for registration, and ordinary users.

There are several major stages of block formation are shown in the figure1.

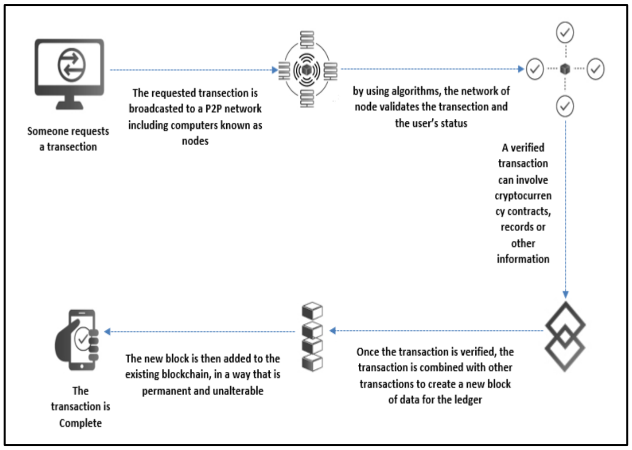
Someone requests a transection
The requested transection is broadcasted to a P2P network including computers known as nodes
by using algorithms, the network of node validates the transection and the user's status
A verified transaction can involve cryptocurrency contracts, records or other information
Once the transaction is verified, the transaction is combined with other transactions to create a new block of data for the ledger
The new block is then added to the existing blockchain, in a way that is permanent and unalterable
The transaction is Complete

Figure1: principle of Blockchain work.

a) The first step is to define the transaction. The sender creates a transaction that contains information about the recipient's address, the subject of the transaction (amount of funds, goods, etc.) and a cryptographic digital signature that confirms the authenticity of the transaction and its legitimacy. Network nodes are notified about the transaction and verify its validity by decrypting the electronic signature. If the transaction passes the verification, then it stands in the pending mode for inclusion in the block[1].

b) Block creation. Blocks containing information about transactions are linked cryptographically and chronologically into a “chain” using complex mathematical algorithms. New blocks are always added strictly to the end of the chain. One of the network nodes once in a certain time interval collects pending transactions, forms a block from them and sends them for confirmation to other network participants for verification and joining the chain.

c) Block validation. The nodes responsible for block validation are asked to validate the generated block. They run an iterative process that requires approval from other node operators in order for the block to be valid. The encryption process, known as hashing, is performed by a large number of different computers operating on the same network. the block is assigned a unique digital signature (signature)[1].

d) Attaching a block to the chain. When all transactions in a block are approved, the new block becomes attached to the general chain. Once the registry is updated and a new block is created, it can no longer be changed. Thus, it is impossible to fake it. The users can only add new entries to it. It is important to take into account that the registry is updated on all computers in the network simultaneously [2].

3. Features of the problem solved by blockchain technology

The main task for which the blockchain technology is applicable is the coordination of the actions of the participants in the system, united by one goal, but deprived of trust in each other.

This technology has a huge potential for those systems where there is no mutual trust between the participants, because it provides reliable storage of personal data, making it inaccessible to change them for fraud purposes. Moreover, the blockchain allows the users to make various kinds of transactions without intermediaries, which significantly saves money and time. All this is relevant for banking systems [3].

4. Consensus mechanisms

The most valuable link in blockchain technology is consensus algorithms, because they provide it with reliability. There are three main mechanisms for reaching agreement.

a) Proof of work - system security protocol.

Anyone who wants to write a block to the database must perform a certain hard-to-compute task built on the principle of a one-way function. The calculation process takes a long time, while the receiving party quickly checks the result.

Before sending the message, a certain mark will be added to the header, the validity of which can only be confirmed by exhaustive enumeration. Verification of calculations on the receiving side is fast - due to a single calculation of SHA-1 with a pre-prepared label [3,4].

At the moment, the proof-of-work algorithm has earned the greatest authority among other mechanisms for creating reliable systems.

Carrying out such an attack makes the proof-of-work algorithm more difficult, since the fraudster will have to spend enormous computing power to perform it. Also, most Blockchains charge a fee for participating in the consensus, therefore, the “sybil attack” will become a very costly operation. Often, the proof-of-work algorithm is criticized due to excessive energy consumption, but so far this is the only way to resist interference in the system of this kind.

b) Proof-of-stake (proof of share) - security protocol,

alternative proof-of-work, in which it is necessary to confirm the storage of a certain amount in the account as evidence. With a higher probability, when forming the next block, the system will choose a miner with a large amount of funds in the account, while the probability of this choice does not depend on the power of its processors. In order to undermine the reliability of the system, one of the participants must collect in their hands more than 50% of all the funds of the system, which is very costly [4].

Proof-of-stake has more advantages than proof-of-work. The main thing is lower time costs (no need for long calculations), but this does not eliminate possible problems. There is also no evidence of effectiveness in protecting against risks arising in cryptocurrencies [4].

Two significant advantages of this protocol are that an attack on the system is very expensive, and if any participant carry it out, he will suffer significantly from this, since it will violate the stability of the system.

Arguments against: the method gives motivation to accumulate funds in separate accounts, which calls into question decentralization; in the event of the formation of a small number of participants who have concentrated in their hands the majority of the funds, this group can impose its own conditions for the functioning of the system.

c) Delegated-proof-of-stake: an improved version of the proof-of-stake protection protocol, the specifics of which is that blocks are generated by a predetermined set of system users who are rewarded for their duty and punished for malicious behavior (such as participation in double spending). The list of users eligible for block signing changes periodically in accordance with certain rules; Delegated-proof-of-stake has the same advantages and disadvantages as proof-of-stake.

5. The general range of tasks solved by the blockchain

Reducing costs, increasing security and greater transparency of transactions are the three strengths of blockchain. The need of banks and businesses in these aspects makes the blockchain attractive for professionals working on software development [5].

Today, we have become accustomed to making payments through the Web. But this process often involves inefficient, outdated systems like Automated Clearing House (ACH), in which all operations are performed centrally, which negatively affects the speed of work.A huge advantage of this technology is the fact that the blockchain does not depend on a centralized computer architecture, which leads to the fact that the loss of individual nodes will not disrupt the entire system[5,6].

technology is capable of completely transforming the structure of banks [7]. The ability to avoid the mediation of third parties in various transactions can make a huge layer of banking services useless. However, the implementation of this idea is far from unhindered and has a huge number of subtleties, which we will examine in detail later.

6. Limits of applicability of blockchain technology

Blockchain is certainly an attractive and very promising technology, but it is not suitable for every system. There are a number of prerequisites that indicate the possibility of blockchain implementation:

a) Use of a publicly accessible database;

b)There is no trust between the participants;

c)The need for the absence of intermediaries;

d) Interdependence of operations, the need to create chains[3].

However, it should be borne in mind that even for those systems where blockchain technology is applicable, its implementation has a number of obstacles caused by the structure and principles of the technology. below some of them.

a) Security and privacy issues. Despite the existence of security solutions using complex encryption algorithms, cybersecurity issues remain one of the most discussed. The more complex it becomes, the faster the number of vulnerabilities grows. In addition, software and network integrity are fundamental to building blockchain infrastructure technology. If the blockchain is intertwined with all the major financial systems of the world, then powerful attacks on it can lead to disastrous consequences.

b) Issues of implementation and integration. When an organization adopts technology to modernize its business processes, it faces the challenge of migrating its old data to the new format. In this situation, the implementation of the blockchain is no easier than other similar tasks, which means that the issue of planning the transition from current systems to the blockchain remains open. The cost savings that blockchain adoption promises are encouraging, but implementation will require high upfront costs that cannot be ignored.

c) Understanding technology. One of the biggest operational risks is that relatively few people understand how it works. If you plan to introduce blockchain into a system whose users are the general population, then this can lead to unpleasant consequences .the blockchain does not protect against the most popular type of fraud - phishing, the essence of which is to steal confidential user data. Key compromise can result in permanent loss of cryptographically protected funds. Unfortunatel, not every ordinary user today can boast of knowledge of the elementary rules for protecting personal data. There is a possible solution to the problem of identity theft: to associate public keys with a physical person or legal entity, but this mechanism will incur additional costs.

d) The question of the speed of operations. In order to protect against a 51% attack (when one network member takes over more than half of the computing power of the system), the block size (for example, Bitcoin) remains no more than 1 megabyte, which allows maintaining decentralization, but significantly limits the transaction speed - 3.3 per second, while the same Visa spends 22 thousand per second. Expanding the throughput to at least 10 transactions per second would require increasing the block size to 1.6 gigabytes, which, firstly, would cause problems for low-powered miners, and, secondly, would make it difficult to distribute blocks across nodes. Already today, the Bitcoin block chain weighs about 38 GB of memory. If its later appear that Blockchain systems store not only information about transactions, but also other, more voluminous data, then they are highly likely to fail, because by forcing miners to store other people's data for free, the developer deprives them of the incentive to maintain the network, since the costs miners will exceed their income [7].

7. Types of blockchain systems

Blockchain systems are divided into two types: private and public. In private blockchains, blocks are created centrally, and all the rights to conduct operations belong to one organization. External participants can only monitor transactions, while only trusted nodes manage the ledger [6].

Private Blockchains have a number of advantages:

a) Lower transaction cost - achieved due to the fact that validity is checked by several high-performance nodes, and not by many user devices, as in public blockchains;

b) The rate of transactions per second is significantly higher than that of public blockchains;

c) Greater control over the system by the company;

d) Creation of blocks in a private blockchain often does not require proof-ofwork. There are a set number of transaction processors, each with a public and private key. Block creators are known and identified by the digital signature in the header.

At the same time, proof-of-work can still be connected to increase the confidence in the system from external participants (if necessary). Without this verification mechanism, the level of trust in a private blockchain is equivalent to the level of trust in the organization that created it. With its implementation, end users can already rely on objective mathematical laws that indicate the high economic cost of attacking the system [1].

The concept of private blockchains makes them far from the general concept of decentralized applications. In public blockchains, any user can create a block of transactions - it is enough to go through the appropriate verification mechanism (proof-of-work or proof-of-stake)[1,2].

Benefits of public blockchains are listed below:

a) Have the important property of network effects. The relationship between two systems operating on the blockchain leads to the fact that the user of one with a high probability will become the user of the second;

b) The problem of the transfer of "goods" is resolved. In the classical system, the seller-buyer requires an intermediary to guarantee the transfer of money in one direction and "goods" in the other (a commission is naturally due for this). However, the presence of a currency and a domain name system makes it possible to eliminate this link through the use of smart contracts.

8. Legal aspects of the operation of blockchain systems

At the moment, there are no clear legal guidelines regarding blockchain applications. Opinions about whether or not additional laws are needed to regulate their work are divided into two camps. Some experts believe that the regulatory fixation of technology can slow down its development, so it is not necessary [7]. However, this does not exclude that instead of legislative regulation, an industry standard of technology will be developed and adopted. Given that the use of standardization documents is voluntary, developers are not required to join and implement the provisions of the standard in their developments.

However, there is an exception: the law will require the mandatory application of standards: in relation to defense products, work on the state defense order, state secrets and other restricted access information protected by law, as well as developments in the field of the use of atomic energy. There are already restrictions on blockchain products that use legally protected information in their work. Products created on the basis of blockchain technology fall under the definition of information systems, which means that they are subject to the provisions of the Federal Law "On Information, Information Technologies and Information Protection"[4]

Smart contracts deserve special attention in the field of legal regulation. One of the main reasons for this is the fact that only persons with legal capacity can be parties, full automated mechanisms cannot be independent economic entities and make transactions. That is, the introduction of smart contracts should take into account that transactions are concluded on behalf of the owner of the equipment through the transfer of data from the equipment.

Another aspect is that legal costs, which can be avoided at the execution stage with the help of a smart contract, can be transferred to the drafting stage. Parties will likely want to specify a more detailed set of contingencies and outcomes before they are required to comply with the decisions of software-driven contracts, and hence the need for transactional attorneys[3].

9. Conclusion

Blockchain technology opens up a huge range of opportunities for us, from money transfers and payments to smart contracts and document verification. Its strengths, such as cost reduction, improved security and transparency of transactions, have attracted the attention of the banking sector. But not all operations that, before the advent of distributed database technology, were carried out with the help of intermediaries and third parties, can be simplified using the blockchain. The technology has a number of subtleties associated with insufficient knowledge, understanding of technical implementation, and flexibility. Therefore, it is too early to talk about a complete change in the current appearance of banks under its influence. But the undeniable fact is that the blockchain is able to transform their internal structure. However, for distributed database technology to become widespread in the banking industry, issues relating to legal legitimacy, regulation, technical viability, and standardization and widespread adoption of the technology need to be addressed.

References

[1] Mougayar, W., 2015, Understanding the blockchain, O'Reilly Media, Available at https://www.oreilly.com/radar/understanding-the-blockchain/

[2] Nofer, M., Gomber, P., Hinz, O., Schiereck, D., 2017, Blockchain, Bus Inf Syst Eng 59 (3), 183–187.

[3] Nakamoto, S., 2008, Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org. https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf

[4] Nofer M., Gomber, P., Hinz, O., 2017, Blockchain- A Disruptive Technology. Bus. Inf. Syst. Eng. 59 (3), 183–187.

[5] Swan, M., 2015, Blockchain Thinking : the Brain as a Decentralized Autonomous Corporation, IEEE Technol. Soc. Mag. 34 (4) 41-52

[6] Wright, A., De Filippi, P., 2015, Decentralized blockchain technology and the rise of lex cryptographia, SSRN Electronic Journal. https://dx.doi.org/10.2139/ssrn.2580664

[7] Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K., 2016, Where is current research on blockchain technology? – a systematic review, PLOS One, 11, (10), e0163477.