ARTIFICIAL INTELLIGENCE, BLOCKCHAIN, COMPUTING AND SECURITY VOLUME 1

Edited by
Arvind Dagur, Karan Singh, Pawan Singh Mehra
and Dhirendra Kumar Shukla

CRC Press
Taylor & Francis Group

First published 2023
by CRC Press/Balkema
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN
and by CRC Press/Balkema
2385 NW Executive Center Drive, Suite 320, Boca Raton FL 33431

CRC Press/Balkema is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

SET
ISBN: 978-1-032-66966-3 (hbk)
ISBN: 978-1-032-68590-8 (pbk)

Volume 1
ISBN: 978-1-032-49393-0 (hbk)
ISBN: 978-1-032-49397-8 (pbk)
ISBN: 978-1-003-39358-0 (ebk)
DOI: 10.1201/9781003393580

Volume 2
ISBN: 978-1-032-67841-2 (hbk)
ISBN: 978-1-032-68498-7 (pbk)
ISBN: 978-1-032-68499-4 (ebk)
DOI: 10.1201/9781032684994

Typeset in Times New Roman

Block chain

Communications

Problems of developing a decentralized system based on blockchain technology

D.T. Muhamediyeva

"Tashkent Institute of Irrigation and Agricultural Mechanization Engineers" National Research University, Tashkent, Uzbekistan

A.N. Khudoyberdiev & J.R. Abdurazzokov

Research Institute for the Development of Digital Technologies and Artificial Intelligence, Tashkent, Uzbekistan

DOI: 10.1201/9781003393580-41

ABSTRACT: The article discusses the problems of developing distributed ledger systems, which is a new approach to creating databases, the key feature of which is the absence of a single control center. Each node compiles and writes registry updates independently of the other nodes. Unlike distributed databases, each participant in a distributed ledger system stores the entire history of changes and validates the addition of any changes to the system using a consensus algorithm, which mathematically guarantees that data cannot be forged.

1 INTRODUCTION

Since the 17th century, when the Dutch East India Company was the first listed company on the stock exchange, the world economy has been built around and supported by stock exchanges, where millions of transactions are made every day, helping companies increase their value. The exchange market is a set of offers to buy and sell corresponding to an asset. An asset may represent stocks or stocks of companies, bonds or other securities. The people who buy or sell assets are called investors, and the people who make the transactions are called brokers or traders [1].

Modern stock exchanges are highly computerized and can process a huge number of transactions in a short amount of time, ensuring the security, execution, and authenticity of transactions at the cost of a transaction fee, usually in direct proportion to the cost of trading. A stock exchange such as the New York Stock Exchange, London Stock Exchange facilitates the buying and selling of shares of companies through it, which is regulated by a central authority. This market architecture has many advantages due to the central authority that ensures the authenticity, security and validity of transactions. However, centralization also has many disadvantages, such as having a single point of failure, possible performance bottleneck or attack susceptibility, and time costs. In addition, the central authority charges a fee and the trading process is not transparent to the trader.

Bitcoins, Ethereum, Ripple are well-known digital (crypto) currencies that are easily bought and sold anywhere in the world [1]. This concept of cryptocurrencies has inspired the creation of digital shares, which include the use of a decentralized stock exchange architecture to overcome the shortcomings given above, using new blockchain technology [2]. The potential of the blockchain system can benefit the entire system, the execution of market orders and the correct settlement between accounts. In addition, the

guaranteed immutability of the ledger provides a valuable advantage over a centralized system. In addition, due to the decentralization of the system, no central authority or intermediary is required to place and execute orders. This allows peer-to-peer transfer, direct purchase and sale of shares between traders and investors without the need for a third intermediary party to trade. Also, the implementation of the blockchain helps to reduce the transaction cost for each transaction, provide increased security and transparency, and the time required for the transaction will be significantly reduced.

The distributed ledger technology, often known as "Blockchain" technology (from the English phrase "block chain"), is one of the most significant technologies at the moment (Dis-tributed Ledger Technology, DLT). The revolutionary alternative payment service bitcoin and the related digital currency originally surfaced in 2009 as a means of enabling decentralized, distributed operation. Due to the open code of Bitcoin, many other cryptocurrencies have already been created at this stage, and each of them is based on its own blockchain [1].

Economics, analysts, and IT professionals are already investigating the potential of using the technology beyond its initial purpose in light of the significant benefits of blockchain over the antiquated financial system, and the digital market is flooded with blockchain firms. Blockchain is a database that ensures data immutability and high security. Although blockchain is equated with cryptocurrency, it is important to understand that it is a tool that can be used in a variety of ways, some of which are: storing and tracking confidential information, such as patient records and patent rights, developing decentralized applications, notarial documents and others [2].

By order of the President of the Republic of Uzbekistan, Sh.M. Mirziyoyev, dated 3.07.2018, "ON MEASURES FOR THE DEVELOPMENT OF THE DIGITAL ECONOMY IN THE REPUBLIC OF UZBEKISTAN," No. PQ-3832, this technology became a part of the country. This decision clearly explains the purpose of adopting the technology and shows that the digital economy is behind the technology. In the state plan, large-scale measures were implemented to develop the digital sector of the economy, introduce an electronic document circulation system, develop electronic payments, and improve the legal framework in the field of electronic commerce [3].

2 OPPORTUNITIES OF BLOCKCHAIN TECHNOLOGY

E-commerce often relies on financial institutions to serve as reliable middlemen for electronic payments. For the majority of transactions, this technique works well, but because it depends on trust, there are certain issues that arise. Financial institutions' necessary mediation precludes irrevocable transactions. It is not suggested to conduct frequent and minor transactions since the cost of these services raises their cost and establishes a minimum price for them. Additionally, the price of renewable services is increased by the lack of irreversible processes. The vendor is compelled to ask the customer for more information than is inherently necessary since the payment can be canceled. Additionally, some fraud is just seen as unavoidable. There is no method for direct electronic transactions, however these restrictions and payment risks can be bypassed in paper currency transactions [4].

A payment system that relies on cryptography instead of trust and enables both parties to move money directly without the use of a middleman is what is required. Sellers and purchasers are shielded from fraud by the high expense of accounting for transaction cancellations [5].

Distributed data processing makes it possible to place a database (or several databases) on different nodes of a computer network. Data distribution is performed on different computers in conditions of vertical and horizontal connections for organizations with a complex structure.

The objective need for a distributed form of data organization depends on the requirements set by end users [4]:

- centralized management of scattered information resources;

- improving the efficiency of managing databases and data banks and reducing the time of accessing information;
- support data integrity, consistency and protection;
- to provide an acceptable level in the “price - performance - reliability” ratio.

The distributed system of databases makes it possible to create and maintain various possibilities, to avoid obstacles that hinder the user's efficiency and to increase the efficiency of using information resources.

Blockchain is a continuous chain of blocks (linked list) containing information, built according to certain rules. Often, copies of blockchains are stored independently on different computers. Blocks are information about transactions, deals and contracts within the system, presented in cryptographic form. Blockchain allows people to record information, and a community of users of a particular chain can control the changes and updates of information about the record [5].

Transactions are transmitted to participants and each node creates an updated version of the events. It is this difference that makes blockchain technology so interesting - it represents an innovation in registration and information distribution that eliminates the need for a third party to simplify digital communications. However, blockchain technology is not a new technology with all its advantages. Rather, it is a combination of proven technologies applied in new ways. It is a special combination of three technologies (P2P Network, secret key cryptography and a protocol that guides the creation of new base elements). As a result, there is a system of digital interactions that does not need a trusted third party. Blockchain technology's unique elegant, simple, yet robust network architecture enables the implementation of digital communications to be hidden. In blockchain technology, cryptography provides a powerful means of ownership that meets the requirements of private key authentication. Ownership of a private key is property [6].

See the example below. During the service life of the vehicle, it goes through various stages - collection, sale, insurance, etc., until disposal. At each stage, many different documents and reports are created. If it is necessary to get an explanation, requests will be sent to the relevant authorities. This process takes a long time. Physical location, different working languages and bureaucracy are some of the challenges.

Blockchain technology avoids all these problems. All information about each vehicle can be stored in the network. This information cannot be deleted or changed without the participant's consent. It is possible to have the necessary information at any time. Based on the idea of smart-contracts, they are working on the goal of ensuring that the entire life path of any vehicle is recorded on the block chain.

A transaction is verified by every computer (i.e. host) that keeps a copy of it. At this point, the nodes check the transaction history.

Now, when the transaction is found to be valid, it goes into the pool - this is a kind of “waiting room”, and considering it in the next block, from here the transaction is accepted by the miner. At this point, the transaction is considered “unconfirmed”. As soon as a miner executes a transaction and includes it in a successfully generated block, the transaction is considered confirmed. The block contains a limited number of transactions (about 2.5 thousand), therefore, in periods of high activity, if the queue for confirmation (processing transactions through the network and adding it to the blockchain) is long, the miner must be added to the block selects the transactions based on the priority fee attached to them [5].

Thus, the commission is designed to show the miner how urgent the transaction is - if the user wants it faster, he should offer a higher payment, and if the user is not in a hurry, he will be able to pay less [6].

Previously, fees were charged according to different rules: if the transaction was small enough or “priority”, it could be free. Today, a commission is always required. The size of each transaction is similar to the size of a file on a computer. As miners try to maximize their earnings, they first select transactions with the best ratio of commission and volume - the smaller the transaction, the better. Here is an example from the real estate market. When a customer comes to buy or rent an apartment, he pays per square

meter. The client pays the price of the apartment in full, but can compare it with the price per square meter of other apartments. The fee rate is the ratio of commission and volume (fee rate) managed by miners - this is the price per square meter. This ratio is measured in “Satoshi” per byte. – how many Satoshi's (the smallest unit of account in the Bitcoin network) users are willing to pay for each byte of a transaction. There are services that allow you to check how much money will be spent to enter the transaction into the nearest block. This indicator always changes depending on network traffic [7].

A public network holds that users can join the network by supplying their own hardware, hence boosting network sharing, computational power, and data storage. Equipment owners should be rewarded for their honest labor in order to promote these attitudes [1].

This means that database operations are paid for by the end user. This situation may seem strange to someone new to blockchain, but it makes sense. The reality is that blockchain projects are often ownerless. The community owns them. As a result, the community will have to pay the project costs. The money is very little, but not zero. Existing decentralized file storage tools charge the user to store files. And we can’t ignore that, at a basic level, the operation of the equipment needs to be paid for by its users. Later, these costs can be covered from other sources.

3 METHOD

A transaction block is a structure for recording groups of transactions in a distributed ledger. The block contains a header and a list of transactions. The block header contains the hash of the previous block, the information hash, and the hash constructed by the Merkle tree containing each operation [4].

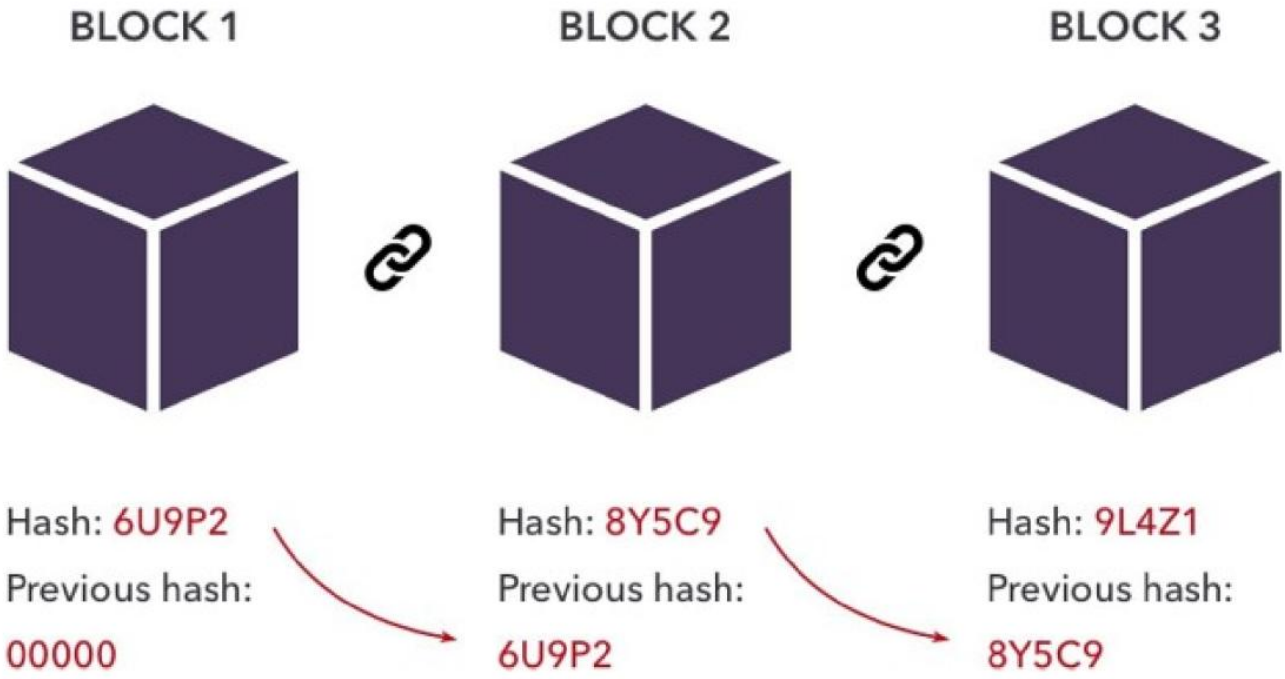

Figure 1. Chain of blocks.

The block consists of the following features:

Table 1. Description of the block.

hash	SHA-256 block header hash
ver	Block diagram version

prev_block	hash of previous block in the chain
mrkl_root	A merkle root is a hash list of transactions
time	uint32_t block creation time
bits	the short form of the target hash value
nonce	A number that is incremented after each iteration of the hash calculation, starting from zero
n_tx	The number of transactions in the list
size	Block size in bytes

3.1 *Merkle tree construction algorithm*

The construction of a Merkle tree is shown in Figure 2. Merkle tree construction algorithm:

- The hashes of each operation in the block are calculated: hash (L1), hash (L2), etc.
- Hashes are calculated from the sum of transaction hashes: hash (hash (L1) + hash (L2)). Since the tree is binary, the number of elements in each iteration must be even. If there is an odd number of transactions in the block, then the last one is repeated and added to itself;
- The second point occurs until the calculation of a single hash, which is the root of the Merkle tree.

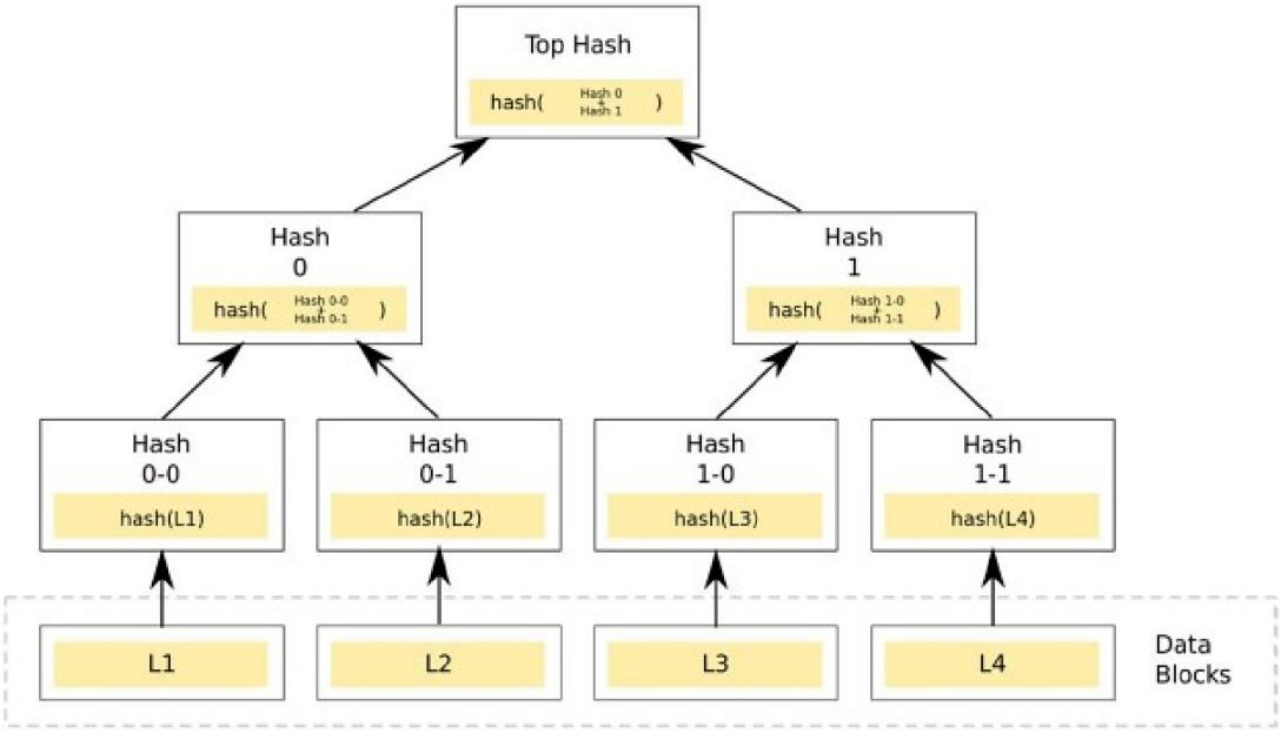

Figure 2. Merkle tree.

4 RESULT

Using the Merkle tree, it is possible to easily verify that a particular transaction is included in a given block, thereby reducing the cost of this process both technically and financially for the users of the network itself. Since each subsequent block of transactions references the previous one, knowing the current block, all transactions on the network can be easily read, continuing to trace the block chain up to the first line, which is called the “genesis” block.

On our server, timestamps are searched for a value with the desired hash by iterating over the value (nonce) of the repeating join field in the data block. Once a block is found that satisfies the condition, its contents cannot be changed without redoing all the work. If this block is not the last part of the chain, this operation involves recalculating all the blocks that follow it.

5 CONCLUSION

It also solves the problem of determining the version supported by the majority by hashing. If a single IP address is considered a voice, then such a scheme can be broken if a large number of addresses are managed. Our scheme is based on the principle of "one processor - one voice". The longest of the hash chains represents the opinion of the majority who contributed the most resources to it. If more than half of the computing power belongs to uncorrupted nodes, then the uncorrupted transaction chain will grow faster and outperform any competing chain. In order to make changes to one of the previous blocks, the attacker may have to redo the work in that block and all subsequent blocks, and then overtake the honest participants of the new blocks. In such a situation, the probability of such success for an attacker with fewer resources decreases dramatically with the number of blocks.

To compensate for the ever-increasing processing power of processors and the change in the number of working nodes in the network, the hashing complexity must be changed to ensure the speed of block production. If they appear more often, the complexity increases and vice versa.

REFERENCES

1. Nakamoto, Satoshi (October 2008). "*Bitcoin: A Peer-to-Peer Electronic Cash System*" (PDF). bitcoin.org. Archived (PDF)from the original on 20 March 2014. Retrieved 28 April 2014.
2. O'Keeffe, M.; Terzi, A. (7 July 2015). "*The Political Economy of Financial Crisis Policy*". Bruegel. Archived from the original on 19 May 2018. Retrieved 8 May 2018.
3. PQ-3832-son 03.07. 2018, "*O'zbekiston Respublikasida Raqamli Iqtisodiyotni Rivojlantirish Chora-Tadbirlari To'g'risida*"
4. Iansiti, Marco; Lakhani, Karim R. (January 2017). "*The Truth about Blockchain*". Harvard Business Review. Harvard University. Archived from the original on 18 January 2017. Retrieved 17 January 2017. The Technology at the Heart of Bitcoin and Other Virtual Currencies, Blockchain is an Open, Distributed Ledger that can Record Transactions between Two Parties Efficiently and in a Verifiable and Permanent Way.
5. Voorhees, Erik (30 October 2015). "*It's All About the Blockchain*". Money and State. Archived from the Original on 1 November 2015. Retrieved 2 November 2015.
6. Kopfstein, Janus (12 December 2013). "*The Mission to Decentralize the Internet*". The New Yorker. Archived from the original on 31 December 2014. Retrieved 30 December 2014. The Network's 'Nodes' — Users Running the Bitcoin Software on their Computers — Collectively Check the Integrity of Other Nodes to Ensure that no one Spends the Same Coins Twice. All Transactions are Published on a Shared Public Ledger, called the "Block Chain".
7. Gervais, Arthur; Karame, Ghassan O.; Capkun, Vedran; Capkun, Srdjan. "Is Bitcoin a Decentralized Currency?". *InfoQ. InfoQ & IEEE Computer Society*. Archived from The Original on 10 October 2016. Retrieved 11 October 2016.
8. Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017) "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends". *2017 IEEE International Congress on Big Data (BigData Congress)*, Honolulu, 25–30 June 2017, 557–564.

9. Stuart Haber and W. Scott Stornetta, "*How to Time-Stamp a Digital Document*". 1991 International Association for Cryptologic Research, Morristown, NJ 07960-1910, U.S.A, J. Cryptology (1991) 3:99–111.
10. Tanweer Alam. "*Blockchain and its Role in the Internet of Things (IoT).*" *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. Vol 5(1), 2019. DOI: 10.32628/CSEIT195137
11. Applications for blockchain. https://www.unpri.org/sustainable-financial-system/stock-exchange-innovation-applications-for-blockchain/3597.article
12. Finoa. (2018) *The Era of Tokenization — Market Outlook on a $24trn business opportunity*. Retrieved from: https://medium.com/finoa-banking/market-outlook-on-tokenized-assets-ausd24trn-opportunity-9bac0c4dfefb.