Index:

BLOCKCHAIN: A PARAGON OF TECHNOLOGICAL BREAKTHROUGHS

Chistyakov A.D. (V.N. Karazin Kharkiv National University, Kharkiv)
Language supervisor: Chernyshova N.V.

Abstract

Blockchain is a groundbreaking technology, originally proposed in “Bitcoin: A Peer-to-Peer Electronic Cash System” paper, written by mysterious Satoshi Nakamoto in 2009. Bitcoin was initially intended to become a fully peer-to-peer electronic cash system that would operate without an underlying financial institution. Although Satoshi Nakamoto has pioneered indisputably ingenious and remarkable invention, they, perhaps, did not have the foggiest idea of the route the technology takes. Tens of IT companies that integrate blockchain with their workflow, thousands of blockchain startups, and billions of dollars invested into the industry make blockchain not just a “Peer-to-Peer Electronic Cash System”, but a whole new direction in modern information technologies.

Анотація

Блокчейн – новаторська технологія, спочатку запропонована в статті “Bitcoin: A Peer-to-Peer Electronic Cash System”, написаній загадковим Сатоші Накамото в 2009 році. Біткойн спочатку мав стати повністю розподіленою електронною системою готівки, яка б працювала без фінансової установи в її основі. Незважаючи на те, що Сатоші Накамото розробив, беззаперечно, геніальний і чудовий винахід, він, мабуть, не мав найменшого уявлення про шлях, яким рухатиметься ця технологія. Десятки IT-компаній, які інтегрують блокчейн зі своїм робочим процесом, тисячі блокчейн стартапів та мільярди доларів, вкладені в галузь, роблять блокчейн не просто “Розподіленою електронною системою готівки”, а цілком новим напрямком у сучасних інформаційних технологіях.

Keywords

Blockchain, block, transaction, proof of work, proof of stake, uncertainty.

General formulation of research and its topicality

The article investigates blockchain technology through a compilation of various subjects: history, blockchain methodology, the core blockchain implementation ideas together with the math under the hood, and the discussion about how the application of a blockchain may ease our existence.

Setting of the problem and the aim of the article

The main purpose of the article is to shed light on the topic of blockchain technology, to acquaint a reader with the most fundamental principles and institutes of this rapidly developing industry, and to prove that a seemingly insignificant math masterpiece is an inevitable future of ours.

The article concentrates on the following questions: What is a blockchain?; How does it function?; What are the benefits of a blockchain?; Are we on the verge of the future?

Main body

Humanity has always been passionate to discover new aspects of life and technology, regardless of their intricacy. We have always been encouraged to enhance our lives, to take control of the unknown, and to develop elaborate tools that would help sort out the ever-growing issues. However, despite being that curious, uncertainty has always been an obstacle on our way to success.

"As humans we find ways to lower uncertainty about one another so that we can exchange value." - Bettina Warburg.

We have come up with an infinite number of means to lower our uncertainty. At first, we started gathering into tribes to trust and know each other personally. When the size of a tribe reached the critical point, where the members could not memorize each other, our anxious brain introduced a God – the one that explained the origin of the inexplicable, e.g. a thunder, a volcanic eruption, or an earthquake. If one worshiped the same God as another one did, they would become trustful. The concept continued with the formation of the term “Government”. Following the interests of the “Government”, people began to believe and confide the once from the same “Country” of residence. Then the 20th century came along with countless breakthroughs in computer science and technology, bringing to life the Internet and such companies as Google, Microsoft, Amazon, Apple, etc. – the companies that we still trust and rely on. Nevertheless, our uncertainty has not decreased, and with constantly escalating fraud, we need an ultimate weapon to subdue our incertitude – the blockchain.

Blockchain

A blockchain is an elaborate, trustful, and decentralized system without underlying third-party authority verifying the workflow. A blockchain is completely autonomous due to the considered algorithms running in its core.

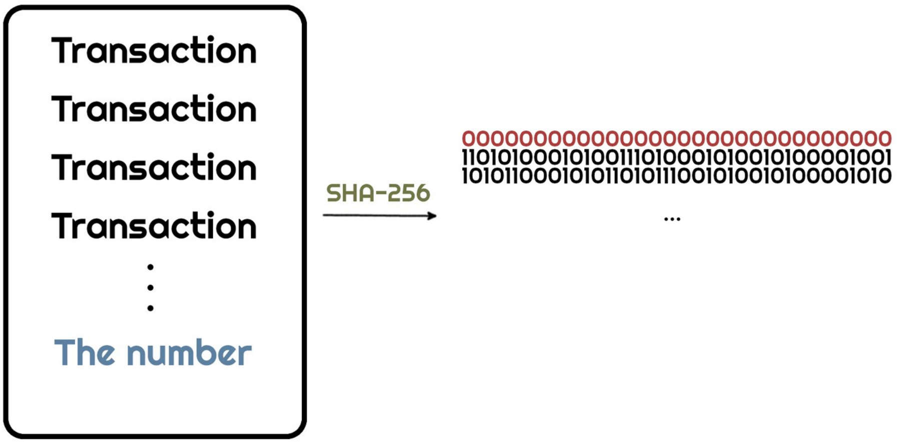
The primary component of the blockchain is a transaction. Where a transaction is nothing but a record that consists of a sender’s public key, a receiver’s public key, and a transmitting message. Every user of a blockchain disposes of their own public and private key. Those are especially generated to hold particular mathematical properties. The public key is known to every other party on the blockchain, whilst the private key is kept secret. After the sender has constructed the message, the special 256-bit signature (that is acquired from the private key and the message) is appended to the body of the transaction. The idea behind is to be able to check who exactly has signed the transaction via the sender’s public key (it is possible due to the keys’ properties). This 256-bit signature-verification algorithm ensures that nobody else is capable of creating transactions except the intended owner of the transaction. Nevertheless, there is a tiny flaw in the concept – one is still able to copy transactions, without the need to forge the signature (which is almost impossible due to the 256-bit length). In order to prevent the misuse of blockchain, each transaction is given an ordinal number, which eliminates the chances of it being copied.

Transactions are assembled into blocks. Each block may consist of an arbitrary number of transactions. For instance, Bitcoin blockchain allows maximum of 2400 transactions per block, whilst Ethereum blockchain, up to 200. The constructed blocks then have to be proved and added to the "Distributed Database".

There are two main approaches to the approval process:

- Proof of work
- Proof of stake

In the "proof of work" approach, the special-purpose processing unit (a miner) is challenged with a task to generate a particular number so that computing a cryptographic SHA-256 hash function of the block and that number, gives N heading zeros in the output, where N is automatically set by a blockchain system to balance the rate of blocks generation.

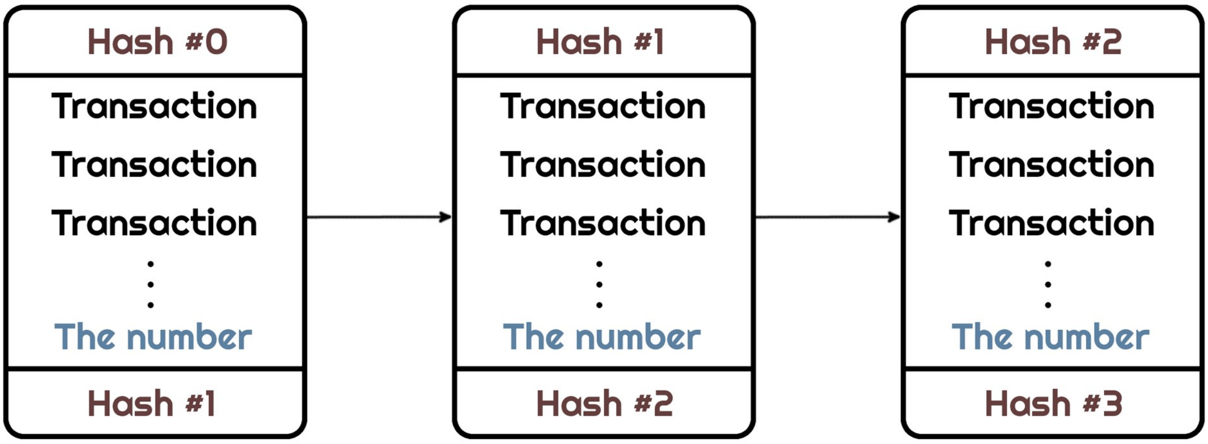


For instance, $N=30$. The probability of generating a number is $\frac{1}{2^{30}} \approx \frac{1}{1{,}000{,}000{,}000}$.

So a miner has to loop through a billion numbers to achieve the desired result. The key point of "proof of work" is that computing such hash is a highly demanding problem that needs tremendous computing power – the hacker has miserable, if any, chances of winning the computation race.

Undertaking the "proof of stake" approach, there are no miners that consume megawatts of energy involved. The validation (approval) of a block becomes a blockchain's node responsibility. Instead of computational power, the user is forced to deposit a substantial monetary amount on the blockchain to become a validator. The blockchain then randomly picks a validator based on several factors: the total value of the account, their activity, the age of the deposit, etc. The chosen validator is then signs (computes a hash of) a block and broadcasts it to the other validators. The key point of "proof of stake" is that a user has to be extremely wealthy to influence a blockchain flow. And once again, the hacker, usually not as affluent, has minuscule chances of penetrating the block's approval.

However, a blockchain protocol described so far is more like a block-set, not a block-chain. What makes a set a chain, is that every proceeding block is linked with the preceding one, resulting in drastic changes in the hash function output. The consequence of the linkage makes it impossible to interchange, interconnect, or delete blocks from the existing blockchain, making it immutable.



Nevertheless, a blockchain has to be stored somewhere – it does not float in the midair, of course. It can not be installed on a centralized server of any authority, because that would yield uncertainty and mistrust among the users. Moreover, a hacker or an authority itself could potentially break into the blockchain's workflow and change its behavior, or even worse – switch it off. The solution is to entirely decentralize a blockchain's database, so every desirous person could become a host, therefore supporting a blockchain. The technology used to implement the idea is called "Distributed ledger technology".

When a block is approved on a blockchain, it is broadcasted to the connected distributed ledgers and added to their database. These ledgers should only "trust" the longest blockchain, because a hacker still has chances, yet miserable, of winning a block-approval lottery and broadcasting malicious transactions. Due to the probability distribution principle, if a hacker has negligible computational power (or deposit), the malicious blocks will not emerge that often.

The last, but not the least topic that needs to be mentioned, is a block reward. When a block gets approved, a special transaction is appended to a block's body, stating that an approver has obtained a reward. The reward itself is usually coins that a blockchain embodies: Bitcoin, Ethereum, EOS, etc.

Summarizing, blockchain technology is a fully decentralized, trustful, self-supported, autonomous, and versatile tool that, if applied properly, will annihilate our uncertainty.

Application

Blockchain, being secure, public, and reliable, has numerous applications in various industries, that may carry a great improvement in their transparency and usage.

Supply chain

Supply chains usually consist of a number of intermediaries, that form a complex route for a product to reach its customer. The complexity and lack of traceability makes supply chain a perfect use case for blockchain. A blockchain infrastructure may lower the cost-savings and raise the transparency of such a network. The immutability of blockchain will make it impossible to counterfeit important delivery data, e.g. delivery cost, product quantity, or delivery time, and having a fully transparent supply chain will lead to the unforgeable delivery status of high-value goods, that is updated on the fly.

Cryptocurrency

The very first association with blockchain that comes to many minds is indeed Bitcoin and the volatility of the cryptocurrencies market. Despite being volatile and highly news-influential, the market still has to mature and grow a lot. The main ideas behind cryptocurrency are the ability to send and trade money across the world instantly, not paying enormous fees (talking of big funds), and the confidence that nothing fails in the middle of a process.

Health care

One of the most vital industry that is expected to be altered by blockchain is health care. Patients' health records, their medical history, and a list of dispensed remedies should be immutable throughout a life. The blockchain technology fits right in to become a backbone of this fateful and fragile business.

Art

Struggling from permanent forgeries and thefts, the art industry may thrive when it merges with blockchain technology. Nobody could duplicate or fabricate the original masterpiece due to blockchain constraints, leading to a new era of digital art and trustworthiness.

Conclusion

The blockchain industry, although still being in its infant state, is a paragon of technological breakthroughs we have already encountered in the 21st century. Being refined in the core and polyhedral outwardly, blockchain has myriad applications that all may change the way we live and perceive technology. Behold, the future is incoming.

References

[1] 3Blue1Brown (2017). No kak na samom dele rabotaet bitkojn? [But how does bitcoin actually work?]. Available at: https://youtu.be/bBC-nXj3Ng4

[2] Bettina Warburg (2016). Kak blokchejn radikal'no izmenit ekonomiku [How the blockchain will radically transform the economy]. Available at: https://youtu.be/RplnSVTzvnU

[3] Everett Muzzy (2020). CHto takoe dokazatel'stvo stavki? [What Is Proof of Stake?]. Available at: https://consensys.net/blog/blockchain-explained/what-is-proof-of-stake/

[4] Kacee Johnson (2020). 3 glavnyh scenariya ispol'zovaniya blokchejna v 2020 godu [Top 3 Blockchain Use Cases of 2020]. Available at: https://www.cpa.com/blog/top-3-blockchain-use-cases-2020

[5] Satoshi Nakamoto (2009). Bitkojn: odnorangovaya sistema elektronnyh deneg [Bitcoin: A Peer-to-Peer Electronic Cash System]. Bitcoin.org (in English)

[6] Wikipedia (2020). Dokazatel'stvo raboty [Proof of work]. Available at: https://en.wikipedia.org/wiki/Proof_of_work

[7] Wikipedia (2020). Dokazatel'stvo stavki [Proof of stake]. Available at: https://en.wikipedia.org/wiki/Proof_of_stake

[8] Wikipedia (2020). Raspredelennyj reestr [Distributed ledger]. Available at: https://en.wikipedia.org/wiki/Distributed_ledger

[9] Wikipedia (2020). Kriptovalyuta [Cryptocurrency]. Available at: https://en.wikipedia.org/wiki/Cryptocurrency