

**BLOCKCHAIN TECHNOLOGY****Sunatova Dilduza Abatovna<sup>1</sup>**<sup>1</sup>TUAS senior teacher of the department of mathematics  
and computer engineering mirmoh@mail.ru**Tursunova Zukhra Botyrovna<sup>2</sup>**<sup>2</sup> is a senior teacher of TUAS Department of Mathematics  
and Computer Engineering**Sadullaeva Mavluda Ziyadullaevna<sup>3</sup>**<sup>3</sup>is a senior teacher at Tashkent State Transport University  
<https://doi.org/10.5281/zenodo.7223379>

Annotation: A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. Bitcoin, the decentralized peertopeer digital currency, is the most popular example that uses blockchain technology. The digital currency bitcoin itself is highly controversial but the underlying blockchain technology has worked flawlessly and found wide range of applications in both financial and nonfinancial world. The main hypothesis is that the blockchain establishes a system of creating a distributed consensus in the digital online world.

Key words: DLT, digital, NFT

Introduction of Blockchain Technology. Blockchain, sometimes referred to as distributed ledger technology (DLT), makes the history of any digital asset unalterable and transparent through the use of a decentralized network and cryptographic hashing.

A simple analogy for how blockchain technology operates can be compared to how a Google Docs document works. When you create a Google Doc and share it with a group of people, the document is simply distributed instead of copied or transferred. This creates a decentralized distribution chain that gives everyone access to the base document at the same time. No one is locked out awaiting changes from another party, while all modifications to the document are being recorded in real-time, making changes completely transparent. A significant gap to note however is that unlike Google Docs, original content and data on the blockchain cannot be modified once written, adding to its level of security. Of course, blockchain is more complicated than a Google Doc, but the analogy is apt because it illustrates critical ideas of the technology:

**BLOCKCHAIN MEANING: BLOCKCHAIN EXPLAINED.** A blockchain is a digital ledger or database where encrypted blocks of digital asset data are stored and chained together, forming a chronological single-source-of-truth for the data.

Digital assets are distributed, not copied or transferred.

Digital assets are decentralized, allowing for real-time accessibility, transparency and governance amongst more than one party.

Blockchain ledgers are transparent — any changes made are documented, preserving integrity and trust.

Blockchain ledgers are public and constructed with inherent security measures, making it a prime technology for almost every sector.

**Importance of Blockchain.** Blockchain is an especially promising and revolutionary technology because it helps reduce security risks, stamp out fraud and bring transparency in a scalable way. Popularized by its association with cryptocurrency and NFTs, blockchain technology has since evolved to become a management solution for all types of global industries. Today, you can find blockchain technology providing transparency for the food supply chain, securing healthcare data, innovating gaming and overall changing how we handle data and ownership on a large scale.

**How Does Blockchain Work?** For proof-of-work blockchains, this technology consists of three important concepts: blocks, nodes and miners. Every chain consists of multiple blocks and each block has three basic elements: The data in the block.

The nonce — “number used only once.” A nonce in blockchain is a whole number that’s randomly generated when a block is created, which then generates a block header hash.

The hash — a hash in blockchain is a number permanently attached to the nonce. For Bitcoin hashes, these values must start with a huge number of zeroes (i.e., be extremely small).

When the first block of a chain is created, a nonce generates the cryptographic hash. The data in the block is considered signed and forever tied to the nonce and hash unless it is mined.



Miner in Blockchain. Miners create new blocks on the chain through a process called mining. In a blockchain every block has its own unique nonce and hash, but also references the hash of the previous block in the chain, so mining a block isn't easy, especially on large chains.

Miners use special software to solve the incredibly complex math problem of finding a nonce that generates an accepted hash. Because the nonce is only 32 bits and the hash is 256, there are roughly four billion possible nonce-hash combinations that must be mined before the right one is found. When that happens miners are said to have found the "golden nonce" and their block is added to the chain.

Making a change to any block earlier in the chain requires re-mining not just the block with the change, but all of the blocks that come after. This is why it's extremely difficult to manipulate blockchain technology. Think of it as "safety in math" since finding golden nonces requires an enormous amount of time and computing power.

When a block is successfully mined, the change is accepted by all of the nodes on the network and the miner is rewarded financially.

What Is Decentralization in Blockchain? One of the most important concepts in blockchain technology is decentralization. No one computer or organization can own the chain. Instead, it is a distributed ledger via the nodes connected to the chain. Blockchain nodes can be any kind of electronic device that maintains copies of the chain and keeps the network functioning. Every node has its own copy of the blockchain and the network must algorithmically approve any newly mined block for the chain to be updated, trusted and verified. Since blockchains are transparent, every action in the ledger can be easily checked and viewed, creating inherent blockchain security. Each participant is given a unique alphanumeric identification number that shows their transactions.

Combining public information with a system of checks-and-balances helps the blockchain maintain integrity and creates trust among users. Essentially, blockchains can be thought of as the scalability of trust via technology.

HOW BLOCKCHAIN WORKS. The blockchain is a digital database, composed of encrypted blocks of data which are "chained" together and secured by complex math problems

The math problems involving matching nonces and hashes is almost impossible to change later — the record of previous actions on the blockchain is highly accurate and secure from manipulation.

The blockchain is distributed identically across different decentralized nodes, ensuring no one organization can own or manipulate it.

## Blockchain Applications

Blockchain isn't only used for financial transactions. Due to its secure and transparent nature, the technology is versatile to needs beyond one area of expertise. Industries covering energy, logistics, education and more are utilizing the benefits

**Cryptocurrency: Blockchain vs Cryptocurrency.** Blockchain's most well-known use (and maybe most controversial) is in cryptocurrencies. Cryptocurrencies are digital currencies (or tokens), like Bitcoin, Ethereum or Litecoin, that can be used to buy goods and services. Just like a digital form of cash, crypto can be used to buy everything from your lunch to your next home. Unlike cash, crypto uses blockchain to act as both a public ledger and an enhanced cryptographic security system, so online transactions are always recorded and secured.

The term Bitcoin, for example, is used interchangeably to refer to both the blockchain and the cryptocurrency, but they remain as two separate entities. [The very first blockchain application appeared in 2009 as Bitcoin](#), a crypto system using the distributed ledger technology. This also marked Bitcoin as the first "blockchain." The aspect of blockchain being used to house this new digital currency is what brought both entities into association, and what led them quickly into the spotlight. The Bitcoin blockchain describes only the technology in which the currency is housed, while the Bitcoin cryptocurrency describes only the currency itself.

Cryptocurrencies are digital currencies that use blockchain technology to record and secure every transaction. A cryptocurrency (Bitcoin, for example) can be used as a digital form of cash to pay for everyday items as well as larger purchases, like cars and homes. It can be bought using one of several digital wallets or trading platforms, then digitally transferred upon purchase of an item, with the blockchain recording the transaction and the new owner. The appeal of cryptocurrencies is that everything is recorded in a public ledger and secured using cryptography, making an irrefutable, timestamped and secure record of every payment.

To date, there are [more than 20,000 cryptocurrencies](#) in the world that have a total market cap around \$1 trillion, with Bitcoin holding a majority of the value. These tokens have become incredibly popular over the last few years, with the value of one Bitcoin fluctuating between several thousands of dollars.

Here are some of the main reasons behind cryptocurrency's recent popularity: Blockchain's security makes theft much harder since each cryptocurrency has its own irrefutable identifiable number that is attached to one owner.

Crypto reduces the need for individualized currencies and central banks.

With blockchain, crypto can be sent to anywhere and anyone in the world without the need for currency exchanging or without interference from central banks.

Cryptocurrencies can make some people rich. Speculators have been driving up the price of crypto, especially Bitcoin, helping some [early adopters to become billionaires](#). Whether this is actually a positive has yet to be seen, as some detractors believe that speculators do not have the long-term benefits of crypto in mind.

More and more large corporations came around to the idea of a blockchain-based digital currency for payments. In February 2021, [Tesla announced](#) that it would invest \$1.5 billion into Bitcoin and accept it as payment for their cars.

Of course, there are many legitimate arguments against blockchain-based digital currencies. First, crypto isn't a very regulated market. Many governments were quick to jump into crypto, but few have a staunch set of codified laws regarding it. Additionally, crypto is incredibly volatile due to speculators. Lack of stability has caused some people to get very rich, while a majority have still lost thousands of dollars.

Whether or not digital currencies are the future remains to be seen. For now, it seems as if blockchain's meteoric rise is more starting to take root in reality than pure hype. Though it's still making headway in this entirely-new, highly-exploratory field, blockchain is also showing promise beyond Bitcoin.

While a blockchain network describes the distributed ledger infrastructure, a blockchain platform describes a medium where users can interact with a blockchain and its network. Blockchain platforms are created to be scalable and act as extensions from an existing blockchain infrastructure, allowing information exchange and services to be powered directly from this framework. An example of a blockchain platform includes Ethereum, a software platform which houses the Ethereum, or ether, cryptocurrency. With the Ethereum platform, users can also create programmable tokens and smart contracts which are built directly upon the Ethereum blockchain infrastructure.

Beyond Bitcoin: Ethereum Blockchain. Originally created for Bitcoin to operate on, blockchain has long been associated with cryptocurrency, but the technology's transparency and security has seen growing adoption in a number of areas, much of which can be traced back to the development of the Ethereum blockchain.

In late 2013, Russian-Canadian developer Vitalik Buterin published a white paper that proposed a platform combining traditional blockchain functionality

with one key difference: the execution of computer code. Thus, the [Ethereum Project](#) was born.

Today, the Ethereum blockchain lets developers create sophisticated programs that can communicate with one another through the blockchain itself.

Similarly to Bitcoin, it's worth noting that the Ethereum blockchain and the Ethereum cryptocurrency are two separate entities. Ethereum programmers can create tokens to represent any kind of digital asset, track its ownership and execute its functionality according to a set of programming instructions.

Tokens can be music files, contracts, concert tickets or even a patient's medical records. In the past couple of years, [non-fungible tokens \(NFTs\)](#) grew in popularity. NFTs are unique blockchain-based tokens that store digital media (like a video, music or art). Each NFT has the ability to verify authenticity, past history and sole ownership of the piece of digital media. NFTs have become wildly popular because they offer a new wave of digital creators the ability to buy and sell their creations, while getting proper credit and a fair share of profits.

Newfound uses for blockchain have broadened the potential of the ledger technology to permeate other sectors like media, government and identity security. Thousands of companies are currently researching and developing products and ecosystems that run entirely on the burgeoning technology.

Blockchain is challenging the current status quo of innovation by letting companies experiment with groundbreaking technology like peer-to-peer energy distribution or decentralized forms for news media. Much like the definition of blockchain, the uses for the ledger system will only evolve as technology evolves.

**Blockchain Applications for Industries.** As mentioned, blockchain technology is being used far beyond just its roots in cryptocurrency — almost every modern industry is being morphed by the technology in some way.

Alongside banking and finance, blockchain is revolutionizing healthcare, record-keeping, smart contracts, supply chains and [even voting](#). While the capabilities of such technology continue to grow, all the [possible applications of blockchain](#) are very much yet to be discovered.

The Bitcoin solved this problem by a mechanism that is now popularly known as Blockchain technology. The Bitcoin system orders transactions by placing them in groups called blocks and then linking these blocks through what is called Blockchain. The transactions in one block are considered to have happened at the same time. These blocks are linked to each-other (like a chain) in a proper linear, chronological order with every block containing the hash of the previous

block. There still remains one problem. Any node in the network can collect unconfirmed transactions and create a block and then broadcasts it to rest of the network as a suggestion as to which block should be the next one in the blockchain. How does the network decide which block should be next in the blockchain? There can be multiple blocks created by different nodes at the same time. One can't rely on the order since blocks can arrive at different orders at different points in the network.

Bitcoin solves this problem by introducing a mathematical puzzle: each block will be accepted in the blockchain provided it contains an answer to a very special mathematical problem. This is also known as “proof of work”—node generating a block needs to prove that it has put enough computing resources to solve a mathematical puzzle. For instance, a node can be required to find a “nonce” which when hashed with transactions and hash of previous block produces a hash with certain number of leading zeros. The average effort required is exponential in the number of zero bits required but verification process is very simple and can be done by executing a single hash.

### References:

1. R Beck, JS Czepluch, N Lollike, S Malone, Blockchain – The Gateway to Trust-Free Cryptographic Transactions. In Research Papers from ECIS2016, (Istanbul, 2016)
2. M Chung, J Kim, The internet information and technology research directions based on the fourth industrial revolution. KSII Trans. Internet Inf. Syst. 10(3), 1311–1320 (2016)
3. R Collins, Blockchain: A new architecture for digital content. EContent 39(8), 22–23 (2016)
4. P Devine, Blockchain learning: can crypto-currency methods be appropriated to enhance online learning? Presented at the ALT Online Winter Conference 2015, Online, (United Kingdom, 2015)
5. K Fanning, DP Centers, Blockchain and its coming impact on financial services. J. Corp. Account. Finance 27(5), 53–57 (2016) <https://doi.org/10.1002/jcaf.22179> S Haber, WS Stornetta, How to time-stamp a digital document.
6. J. Cryptol. 3(2), 99–111 (1991) <https://doi.org/10.1007/BF00196791> MB Hoy, An introduction to the Blockchain and its implications for libraries and medicine. Med. Ref. Serv. Q. 36(3), 273–279 (2017) <https://doi.org/10.1080/02763869.2017.1332261>
7. A Kosba, A Miller, E Shi, Z Wen, C Papamanthou, in 2016 IEEE Symposium on Security and Privacy (SP). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts (2016), pp. 839–858 <https://doi.org/10.1109/SP.2016.55>
8. D Kraft, Difficulty control for blockchain-based consensus systems. Peer Peer Netw. Appl. 9(2), 397–413 (2016) <https://doi.org/10.1007/s12083-015-0347-x>
9. S Nakamoto, Bitcoin: A peer-to-peer electronic cash system. (2008) Retrieved from <https://bitcoin.org/bitcoin.pdf> M Peck, A blockchain currency that beat s bitcoin on privacy. IEEE Spectr. 53(12), 11–13 (2016) <https://doi.org/10.1109/MSPEC.2016.7761864>