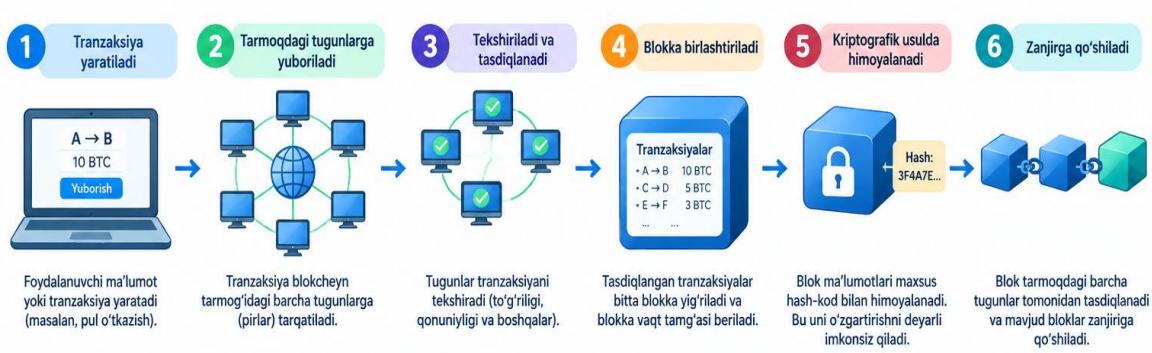
**MINISTRY OF HIGHER EDUCATION, SCIENCE AND INNOVATIONS OF THE REPUBLIC OF UZBEKISTAN**
**GULISTON STATE UNIVERSITY**
**DEPARTMENT OF INFORMATION TECHNOLOGY**

# *PRINCIPLE OF OPERATION OF BLOCKCHAIN TECHNOLOGY*

# *BLOKCHEYN TEXNOLOGIYASINING ISHLASH PRINSIPI*










***Gulistan-2026***

**Negmatulloyev Z.T. Principle of operation of blockchain technology.** (*Blokcheyn texnologiyasining ishlash prinsipi*) – Gulistan, 2026.- 36.p.

Ushbu mavzuda blokcheyn texnologiyasining ishlash prinsipi, uning asosiy tushunchalari va amaliy qo‘llanilish xususiyatlari yoritilgan. Blokcheyn - ma’lumotlarni bloklar ko‘rinishida saqlash, ularni kriptografik usullar yordamida o‘zaro bog‘lash hamda taqsimlangan tarmoq orqali himoyalash imkonini beruvchi zamonaviy texnologiyadir. Mavzuda bloklarning shakllanishi, tranzaksiyalarni tekshirish, konsensus mexanizmlari, ma’lumotlarning yaxlitligini ta’minlash va tarmoq ishtirokchilari o‘rtasida axborot almashinuvi jarayonlari tushuntiriladi. Shuningdek, blokcheyn texnologiyasining moliya, bank ishi, ta’lim, tibbiyot, logistika va elektron tijorat sohalarida qo‘llanilishi ko‘rib chiqiladi. Mazkur mavzu blokcheynning afzalliklari, xavfsizlik xususiyatlari va mavjud cheklovlarini o‘rganishga xizmat qiladi. Ushbu bilimlar talabalarda taqsimlangan ma’lumotlar bazalari, raqamli xavfsizlik va zamonaviy axborot texnologiyalari bo‘yicha nazariy hamda amaliy tushunchalarni shakllantiradi.

**Taqrizchilar:**

**Pazilov A. A.**- Xalqaro hamkorlik bo‘yicha prorektor, p.f.f.d.(PhD), dotsent.

**Turdibayev D.X.** - Axborot texnologiyalari va fizika-matematika fakultet dekani, p.f.d. (DSc), v.b. professor.

Ma’ruza matni Axborot texnologiyalari va fizika-matematika fakulteti Ilmiy Kengashi qaroriga asosan (____ ____ 2026 yil ___ -bayonnoma) nashrga tavsiya qilindi.

# PRINCIPLE OF OPERATION OF BLOCKCHAIN TECHNOLOGY

# BLOKCHEYN TEXNOLOGIYASINING ISHLASH PRINSIPI

**Objective:** To explain the operating principles of blockchain technology, the interconnection of blocks, cryptographic data protection, and transaction verification processes, and to provide students with knowledge of its practical applications.

**Plan:**

1. General concept of blockchain technology
2. History of the origin and development of blockchain
3. Structure and main components of blockchain
4. Cryptographic hash and digital signature
5. The process of executing transactions in a blockchain network
6. Consensus mechanisms: Proof of Work and Proof of Stake
7. Types of blockchains and their differences

**Maqsad:** Talabalarga blokcheyn texnologiyasining ishlash prinsipi, bloklarning o‘zaro bog‘lanishi, ma’lumotlarni kriptografik himoyalash va tranzaksiyalarni tasdiqlash jarayonlarini tushuntirish hamda uning amaliy qo‘llanilishi haqida bilim berish.

**Reja:**

1. Blokcheyn texnologiyasi haqida umumiy tushuncha
2. Blokcheynning paydo bo‘lishi va rivojlanish tarixi
3. Blokcheynning tuzilishi va asosiy tarkibiy qismlari
4. Kriptografik xesh va elektron raqamli imzo
5. Blokcheyn tarmog‘ida tranzaksiyalarni amalga oshirish jarayoni
6. Konsensus mexanizmlari: Proof of Work va Proof of Stake
7. Blokcheyn turlari va ularning farqlari

## 1. General concept of blockchain technology

Due to the rapid development of information technology today, the demand for methods of storing, transmitting, processing, and protecting data is increasing. Information reliability is especially important in electronic payments, digital documents, financial transactions, public services, and e-commerce systems. Therefore, developing decentralized data storage and management technologies is one of the urgent tasks. One such technology is blockchain. Blockchain is a technology that stores data in the form of cryptographically linked blocks and enables maintaining a distributed ledger among network participants.

The term "blockchain" consists of two English words: Block (a collection of data) and Chain (sequential connection). Thus, simply put, a blockchain can be understood as a chain of interconnected data blocks.

In a traditional database, all data can be stored on a single server or a centralized system of servers. In a blockchain, copies of the ledger are often stored on many nodes of the network. A node is a computer or other device connected to the blockchain network that operates according to its rules. The main idea of blockchain is that data does not need to be controlled by just a single central organization. Network participants can verify data based on common rules, accept new records, and maintain mutually consistent copies of the ledger. For example, in a traditional banking system, money transfer information is recorded in the bank's information system. In some blockchain systems, transactions are verified by network nodes and added to the general ledger based on established consensus rules.

Although blockchain technology became famous through cryptocurrencies, its use is not limited to digital money. It can also be applied in logistics, healthcare, education, electronic document management, digital identification, and other fields. It should be noted that blockchain is not a tool that automatically solves all problems. Its effectiveness depends on how data is entered, network rules, security measures, and governance mechanisms.

## 1. Blokcheyn texnologiyasi haqida umumiy tushuncha

Hozirgi davrda axborot texnologiyalarining jadal rivojlanishi natijasida ma’lumotlarni saqlash, uzatish, qayta ishlash va himoya qilish usullariga bo‘lgan talab ortib bormoqda. Ayniqsa, elektron to‘lovlar, raqamli hujjatlar, moliyaviy operatsiyalar, davlat xizmatlari va elektron savdo tizimlarida ma’lumotlarning ishonchliligi muhim ahamiyatga ega. Shu sababli markazlashmagan ma’lumotlarni saqlash va boshqarish texnologiyalarini ishlab chiqish dolzarb vazifalardan biri hisoblanadi. Ana shunday texnologiyalardan biri blokcheyn (Blockchain) texnologiyasidir. Blokcheyn - ma’lumotlarni o‘zaro kriptografik bog‘langan bloklar ko‘rinishida saqlaydigan va tarmoqdagi ishtirokchilar o‘rtasida taqsimlangan reyestrni yuritish imkonini beradigan texnologiya.

«Blockchain» atamasi ingliz tilidagi ikki so‘zdan tashkil topgan: Block - blok, ma’lumotlar to‘plami; Chain - zanjir, ketma-ket bog‘lanish. Demak, blokcheynni sodda qilib aytganda, bir-biri bilan bog‘langan ma’lumotlar bloklari zanjiri deb tushunish mumkin.

Oddiy ma’lumotlar bazasida barcha ma’lumotlar bitta serverda yoki markazlashgan serverlar tizimida saqlanishi mumkin. Blokcheynda esa reyestr nusxalari ko‘pincha tarmoqning ko‘plab tugunlarida saqlanadi. Tugun (node) — blokcheyn tarmog‘iga ulangan va uning qoidalariga muvofiq ishlaydigan kompyuter yoki boshqa qurilma.

Blokcheynning asosiy g‘oyasi shundan iboratki, ma’lumotlarni faqat bitta markaziy tashkilot nazorat qilishi shart emas. Tarmoq ishtirokchilari umumiy qoidalar asosida ma’lumotlarni tekshirishi, yangi yozuvlarni qabul qilishi va reyestrning o‘zaro mos nusxalarini yuritishi mumkin. Masalan, an’anaviy bank tizimida pul o‘tkazmasi haqidagi ma’lumotlar bankning axborot tizimida qayd etiladi. Ayrim blokcheyn tizimlarida esa tranzaksiya tarmoq tugunlari tomonidan tekshiriladi va belgilangan konsensus qoidalari asosida umumiy reyestrga kiritiladi.

Blokcheyn texnologiyasi kriptovalyutalar bilan mashhur bo‘lgan bo‘lsa-da, undan foydalanish faqat raqamli pullar bilan cheklanmaydi. U logistika, tibbiyot, ta’lim,

elektron hujjat aylanishi, raqamli identifikatsiya va boshqa sohalarda ham qo‘llanilishi mumkin.

Shuni ta’kidlash kerakki, blokcheyn barcha muammolarni avtomatik hal qiladigan vosita emas. Uning samaradorligi ma’lumotlarning qanday kiritilishi, tarmoq qoidalari, xavfsizlik choralari va boshqaruv mexanizmlariga bog‘liq.

## 2. History of the origin and development of blockchain

The formation of blockchain technology is closely connected with scientific research in cryptography, distributed computing systems, and reliable electronic data storage. In the 1970s–1990s, cryptographic algorithms, hash functions, and digital signature methods were developed. These technologies created an important basis for verifying the integrity and confirming the authorship of electronic data. In 1991: Stuart Haber and W. Scott Stornetta described a cryptographically chained system that allowed securing time-stamps on digital documents and verifying that the documents were not subsequently altered.In 2008: An author or group of authors using the name Satoshi Nakamoto published an article outlining the concept of the Bitcoin system. It proposed a distributed system allowing electronic payments without a central financial intermediary. In 2009: The Bitcoin network was launched. This system demonstrated the maintenance of a transaction history through the combined use of a chain of blocks, cryptographic hashes, digital signatures, and consensus mechanisms.

In subsequent years, blockchain technology developed in new directions. In particular, the concept of smart contracts became widespread through the Ethereum platform. Smart contracts are sets of rules executed automatically based on software code when predefined conditions are met. Today, blockchain systems are designed for various tasks. Some networks are open and accessible to everyone, while others are intended only for authorized organizations or users.

| Year / Period | Main milestone |
|---|---|
| 1991 | Methods for protecting the integrity of digital documents and recording time-stamps. |
| 2008 | An article about the Bitcoin concept was published. |
| 2009 | The Bitcoin network was launched. |
| 2015 | The Ethereum platform was launched, expanding the |

| | |
|---|---|
| | possibilities of smart contracts. |
| Present time | Blockchain is used in finance, logistics, digital assets, and document management. |

## 2. Blokcheynning paydo bo‘lishi va rivojlanish tarixi

Blokcheyn texnologiyasining shakllanishi kriptografiya, taqsimlangan hisoblash tizimlari va elektron ma’lumotlarni ishonchli saqlashga oid ilmiy izlanishlar bilan chambarchas bog‘liq. 1970–1990-yillarda kriptografik algoritmlar, xesh funksiyalari va elektron raqamli imzo usullari rivojlandi. Ushbu texnologiyalar elektron ma’lumotlarning yaxlitligini tekshirish va muallifligini tasdiqlash uchun muhim asos yaratdi. 1991-yilda Stuart Haber va W. Scott Stornetta raqamli hujjatlarga qo‘yilgan vaqt belgilarini himoyalash hamda hujjatlarning keyinchalik o‘zgartirilmaganligini tekshirishga imkon beradigan kriptografik zanjirlangan tizimni tavsifladilar. 2008-yilda Satoshi Nakamoto nomidan foydalanilgan muallif yoki mualliflar guruhi Bitcoin tizimining konsepsiyasini bayon qiluvchi maqolani e’lon qildi. Unda markaziy moliyaviy vositachisiz elektron to‘lovlarni amalga oshirishga imkon beradigan taqsimlangan tizim taklif etildi. 2009-yilda Bitcoin tarmog‘i ishga tushirildi. Ushbu tizim bloklar zanjiri, kriptografik xeshlar, raqamli imzolar va konsensus mexanizmlaridan birgalikda foydalanish orqali tranzaksiyalar tarixini yuritishni namoyish etdi.

Keyingi yillarda blokcheyn texnologiyasi yangi yo‘nalishlarda rivojlandi. Xususan, Ethereum platformasi orqali aqlli shartnomalar (smart contracts) tushunchasi keng tarqaldi. Aqlli shartnomalar - oldindan belgilangan shartlar bajarilganda dasturiy kod asosida avtomatik bajariladigan qoidalar to‘plamidir. Bugungi kunda blokcheyn tizimlari turli vazifalar uchun ishlab chiqilmoqda. Ba’zi tarmoqlar ochiq va hammaga foydalanish imkonini bersa, boshqalari faqat ruxsat berilgan tashkilotlar yoki foydalanuvchilar uchun mo‘ljallangan.

| Yil / davr | Asosiy bosqich |
|---|---|
| 1991 | Raqamli hujjatlar yaxlitligini himoyalash va vaqt belgilarini qayd etish usullari. |
| 2008 | Bitcoin konsepsiyasi haqida maqola e’lon qilindi. |

| | |
|---|---|
| 2009 | Bitcoin tarmog‘i ishga tushirildi. |
| 2015 | Ethereum platformasi ishga tushib, aqlli shartnomalar imkoniyatlari kengaydi. |
| Hozirgi davr | Blokcheyn moliya, logistika, raqamli aktivlar va hujjat aylanishida qo‘llanmoqda. |

## 3. Structure and main components of blockchain

A blockchain system consists of several interconnected components. Each of them performs a specific task in recording, verifying, storing, and distributing data across the network.

### 3.1. The concept of a block

A block is a collection of data entered into the blockchain ledger. Its composition depends on the blockchain protocol being used. A block typically includes the following parts:

- **Block header -** technical information describing the block.
- **Previous block hash -** a value providing cryptographic connection with the previous block.
- **Timestamp -** information about the time the block was created or recorded.
- **Transactions -** records of operations performed in the network.
- **Merkle root -** a summarizing hash value formed from transaction hashes.
- **Consensus-related data -** fields like nonce in a Proof of Work system, depending on the protocol.

Not every block needs to have all the above elements in the exact same format. In some blockchains, block structure and verification rules are organized differently.

### 3.2. Chain of blocks

The main feature of blockchain is that blocks are cryptographically linked. A new block typically references the hash value of the previous block. As a result, blocks form a sequential chain.

| Block 1 | Block 2 | Block 3 |
|---|---|---|
| Hash: H1 | Previous hash: H1; Hash: H2 | Previous hash: H2; Hash: H3 |

If data in a previous block is altered, its hash value also changes. As a result, the match with the previous hash field in the subsequent block is broken. Therefore, secretly altering past data in a chain of blocks becomes complicated. However, this mechanism does not make data modification completely impossible. If an attacker has sufficient computing power or a large influence in the consensus on a particular blockchain, they may attempt to reorganize some historical records. The level of security depends on the network architecture and consensus mechanism.

### 3.3. Nodes and distributed ledger

Nodes in a blockchain network perform tasks such as storing data, verifying transactions, and distributing new blocks. Not all nodes perform the same task: some store a full copy of the ledger, while others use limited data. The advantage of a distributed ledger is that data is not tied to a single server. However, a large number of nodes does not automatically make the system secure. The independence of nodes, their verification of rules, and the proper organization of the consensus mechanism are also crucial.

## 3. Blokcheynning tuzilishi va asosiy tarkibiy qismlari

Blokcheyn tizimi bir nechta o‘zaro bog‘langan tarkibiy qismlardan tashkil topadi. Ularning har biri ma’lumotlarni qayd etish, tekshirish, saqlash va tarmoq bo‘ylab tarqatishda muayyan vazifani bajaradi.

### 3.1. Blok tushunchasi

Blok - blokcheyn reyestriga kiritiladigan ma’lumotlar to‘plami. Uning tarkibi foydalanilayotgan blokcheyn protokoliga bog‘liq. Odatda blok quyidagi qismlarni o‘z ichiga oladi:

**Blok sarlavhasi** - blokni tavsiflovchi texnik ma’lumotlar.

**Oldingi blok xeshi** - avvalgi blok bilan kriptografik bog‘lanishni ta’minlovchi qiymat.

**Vaqt belgisi** - blok yaratilgan yoki qayd etilgan vaqtga oid ma’lumot.

**Tranzaksiyalar** - tarmoqda amalga oshirilayotgan operatsiyalar haqidagi yozuvlar.

**Merkle ildizi** - tranzaksiyalar xeshlaridan hosil qilinadigan umumlashtiruvchi xesh qiymati.

**Konsensusga oid ma’lumotlar** - protokolga qarab, masalan, Proof of work tizimidagi nonce kabi maydonlar.

Har bir blokda yuqoridagi barcha elementlar aynan bir xil shaklda bo‘lishi shart emas. Ayrim blokcheynlarda blok tuzilishi va tekshirish qoidalari boshqacha tashkil etiladi.

### 3.2. Bloklar zanjiri

Blokcheynning asosiy xususiyati - bloklarning kriptografik jihatdan bog‘langanligidir. Yangi blok odatda oldingi blokning xesh qiymatiga ishora qiladi. Natijada bloklar o‘zaro ketma-ket zanjir hosil qiladi.

| 1-blok | 2-blok | 3-blok |
|---|---|---|
| Xesh: H1 | Oldingi xesh: H1; Xesh: H2 | Oldingi xesh: H2; Xesh: H3 |

Agar oldingi blokdagi ma’lumot o‘zgartirilsa, uning xesh qiymati ham o‘zgaradi. Natijada undan keyingi blokdagi oldingi xesh maydoni bilan moslik buziladi. Shu sababli bloklar zanjiridagi avvalgi ma’lumotlarni yashirincha o‘zgartirish murakkablashadi. Biroq bu mexanizm ma’lumotni o‘zgartirishni mutlaqo imkonsiz qilmaydi. Muayyan blokcheynda hujumchi yetarli hisoblash quvvatiga yoki konsensusdagi katta ta’sirga ega bo‘lsa, ayrim tarixiy yozuvlarni qayta tashkil etishga urinishi mumkin. Xavfsizlik darajasi tarmoq arxitekturasi va konsensus mexanizmiga bog‘liq.

### 3.3. Tugunlar va taqsimlangan reyestr

Blokcheyn tarmog‘idagi tugunlar ma’lumotlarni saqlash, tranzaksiyalarni tekshirish va yangi bloklarni tarqatish kabi vazifalarni bajaradi. Barcha tugunlar bir xil vazifani bajarishi shart emas: ayrimlari to‘liq reyestr nusxasini saqlaydi, boshqalari esa cheklangan ma’lumotlardan foydalanadi. Taqsimlangan reyestrning afzalligi shundaki, ma’lumotlar bitta serverga bog‘lanib qolmaydi. Biroq tugunlarning soni ko‘pligi o‘z-o‘zidan tizimni xavfsiz qilmaydi. Tugunlar mustaqilligi, ularning qoidalarni tekshirishi va konsensus mexanizmining to‘g‘ri tashkil etilishi ham muhimdir.

## 4. Cryptographic hash and digital signature

The security of blockchain is based on the extensive use of cryptographic methods. Hash functions and digital signatures are of particular importance in this process.

### 4.1. Cryptographic hash function

A hash function is a mathematical algorithm that converts data of variable length into a fixed-length value. In blockchains, hashes are used to check data integrity, link blocks together, and compactly represent transactions. For example, the Bitcoin system uses the SHA-256 hashing algorithm. The SHA-256 algorithm generates a 256-bit hash value.

- **Determinism -** identical input data and the same algorithm always produce the same hash result.
- **Fast computation -** calculating the hash value should be practically fast.
- **Sensitivity to changes -** even a small change in the input data can drastically change the hash value.
- **Pre-image resistance (One-wayness) -** when using a strong hash function, it is practically very difficult to recover the original data from the hash value itself.
- **Collision resistance -** it should be practically very difficult to find the same hash value for different data.

A hash function is not the same as data encryption. In encryption, data can be decrypted using a special key, whereas a hash is typically used to verify data. Example: Even if there is a difference of only a single capitalized letter between the words "Salom" and "salom", in a hash algorithm like SHA-256, the result is usually completely different. This feature helps detect if data has been modified.

### 4.2. Digital signature

A digital signature allows verifying that digital data was signed by a specific person or key owner. It is based on asymmetric cryptography, which uses public and private keys.

- **Private key –** kept secret by the owner and used to create signatures.
- **Public key –** used to verify signatures.
- **Digital signature –** a cryptographic result bound to the relevant data.

For example, when a user creates a transaction on a blockchain, they can generate a signature with their corresponding private key. Nodes in the network verify the authenticity of the signature using the public key. If the signature fails verification, the

transaction is not accepted. Through this, a protection mechanism is provided against an unauthorized person creating a transaction without the corresponding private key. However, a digital signature does not automatically determine the user's real name. Primarily, it confirms the connection with the respective key. Additional identification mechanisms may be required to determine the identity of the key owner.

### 4.3. Interrelation of cryptographic methods

The hash function and digital signature complement each other. The hash helps detect changes in data, while the digital signature allows checking the authenticity of the signature and its association with the key. The reliability of blockchain depends not only on cryptography, but also on network participants following rules and the robustness of the consensus mechanism.

## 4. Kriptografik xesh va elektron raqamli imzo

Blokcheynning xavfsizligi kriptografik usullardan keng foydalanishga asoslanadi. Xesh funksiyasi va elektron raqamli imzo bu jarayonda alohida ahamiyatga ega.

### 4.1. Kriptografik xesh funksiyasi

Xesh funksiyasi - turli uzunlikdagi ma’lumotni belgilangan uzunlikdagi qiymatga aylantiruvchi matematik algoritm. Blokcheynlarda xeshlar ma’lumotlarning yaxlitligini tekshirish, bloklarni o‘zaro bog‘lash va tranzaksiyalarni ixcham ifodalash uchun ishlatiladi. Masalan, Bitcoin tizimida SHA-256 xesh algoritmi qo‘llaniladi. SHA-256 algoritmi natijada 256 bitli xesh qiymatini hosil qiladi.

**Deterministiklik** - bir xil kirish ma’lumoti va bir xil algoritm har doim bir xil xesh natijasini beradi.

**Tez hisoblash** - xesh qiymatini hisoblash amaliy jihatdan tez bajarilishi kerak.

**O‘zgarishga sezgirlik** - kirish ma’lumotidagi kichik o‘zgarish ham xesh qiymatini keskin o‘zgartirishi mumkin.

**Bir tomonlamalik** - kuchli xesh funksiyasidan foydalanilganda xesh qiymatining o‘zidan dastlabki ma’lumotni tiklash amaliy jihatdan nihoyatda qiyin.

To‘qnashuvga chidamlilik - turli ma’lumotlar uchun bir xil xesh qiymatini topish amaliy jihatdan juda qiyin bo‘lishi kerak.

Xesh funksiyasi ma’lumotni shifrlash bilan bir xil emas. Shifrlashda maxsus kalit yordamida ma’lumotni qayta ochish mumkin, xesh esa, odatda, ma’lumotni tekshirish uchun ishlatiladi. Misol: “Salom” va “salom” so‘zlari orasida faqat bitta harfning katta-kichikligi farq qilsa ham, SHA-256 kabi xesh algoritmida natija odatda butunlay boshqacha bo‘ladi. Bu xususiyat ma’lumot o‘zgarganini aniqlashga yordam beradi.

### 4.2. Elektron raqamli imzo

Elektron raqamli imzo raqamli ma’lumotning muayyan shaxs yoki kalit egasi tomonidan imzolanganini tekshirishga imkon beradi. U ochiq va yopiq kalitlardan foydalanadigan asimmetrik kriptografiyaga asoslanadi.

- Yopiq kalit - egasi tomonidan maxfiy saqlanadi va imzo yaratishda ishlatiladi.
- Ochiq kalit - imzoni tekshirish uchun ishlatiladi.
- Elektron raqamli imzo - tegishli ma’lumotga bog‘langan kriptografik natija.

Masalan, foydalanuvchi blokcheynda tranzaksiya yaratganda, tegishli yopiq kalit bilan imzo hosil qilishi mumkin. Tarmoqdagi tugunlar ochiq kalit yordamida imzoning haqiqiyligini tekshiradi. Agar imzo tekshiruvdan o‘tmasa, tranzaksiya qabul qilinmaydi. Shu orqali begona shaxsning tegishli yopiq kalitsiz tranzaksiya yaratishiga qarshi himoya mexanizmi ta’minlanadi. Biroq elektron imzo foydalanuvchining haqiqiy ismini o‘z-o‘zidan aniqlamaydi. U, eng avvalo, tegishli kalit bilan bog‘liqlikni tasdiqlaydi. Kalit egasining shaxsini aniqlash uchun qo‘shimcha identifikatsiya mexanizmlari talab etilishi mumkin.

### 4.3. Kriptografik usullarning o‘zaro bog‘liqligi

Xesh funksiyasi va elektron raqamli imzo bir-birini to‘ldiradi. Xesh ma’lumotlarning o‘zgarganini aniqlashga yordam beradi, elektron imzo esa imzoning haqiqiyligini va kalitga bog‘liqligini tekshirish imkonini beradi. Blokcheynning ishonchliligi faqat kriptografiyaga emas, balki tarmoq ishtirokchilarining qoidalarni bajarishi va konsensus mexanizmining mustahkamligiga ham bog‘liq.

## 5. The Process of executing transactions in a blockchain network

To fully understand how blockchain works, it is necessary to examine the process from the moment a user creates a transaction until it is recorded in the ledger. As an example, let us look at a user named Ali sending a digital asset to Vali.

### 5.1. First Stage- Creating a transaction

Ali enters Vali's address and the amount to be sent in his electronic wallet. The wallet generates transaction data in accordance with the relevant blockchain rules. The electronic wallet itself does not physically store money or digital assets. It typically allows the user to manage keys and perform operations related to assets in the blockchain ledger.

### 5.2. Second Stage - Signing the transaction

The transaction is signed with the user's corresponding private key. The signature depends on the transaction data. Therefore, unauthorized alteration of the signed data can cause signature verification to fail. Keeping the private key secure is critically important.

### 5.3. Third Stage - Sending the transaction to the network

The signed transaction is sent to one or more nodes in the network. The node verifies it and, if it complies with protocol rules, may distribute it to other nodes. Verification reviews the signature, availability of funds, transaction format, and other requirements.

### 5.4. Fourth Stage - Inclusion in a block

Based on the relevant network rules, the transaction is selected for inclusion in a new block. In a Proof of Work system, miners perform computational work to create a new block. In a Proof of Stake system, validators propose or validate blocks in accordance with protocol rules.

### 5.5. Fifth Stage - Verifying the block

Verifying nodes in the network check whether the block complies with the rules. This may include verifying the block's connection to the previous block, the validity of transactions, and compliance with consensus requirements. Non-compliant blocks can be rejected by nodes.

### 5.6. Sixth Stage – Transaction confirmation

Once the block is accepted according to blockchain network rules, the transaction is recorded in the ledger. In some networks, the probability of transaction reorganization decreases as new blocks are added. In other networks, a transaction is considered finalized when established finality rules are met.

### 5.7. The Issue of data modification in blockchain

Blockchain is often described as an immutable data system. To be precise, in many blockchains, it is very difficult to secretly alter confirmed historical records. This is because such changes affect cryptographic links and consensus rules. Nevertheless, if incorrect data is entered into a blockchain, the technology itself does not guarantee that its content is correct. For example, if a logistics employee enters incorrect cargo data into the system, this record can be registered in the blockchain. To fix the problem, a new correcting record must be introduced or other organizational measures taken. Thus, blockchain helps protect data history, but does not always guarantee the accuracy of initial data.

## 5. Blokcheyn tarmog‘ida tranzaksiyalarni amalga oshirish jarayoni

Blokcheynning ishlash prinsipini to‘liq tushunish uchun foydalanuvchi tranzaksiya yaratganidan boshlab, uning reyestrda qayd etilishigacha bo‘lgan jarayonni ko‘rib chiqish lozim. Misol tariqasida, Ali ismli foydalanuvchi Valiga raqamli aktiv yuborishini ko‘rib chiqamiz.

### 5.1. Birinchi bosqich - tranzaksiyani yaratish

Ali o‘zining elektron hamyonida Vali manzilini va yuboriladigan miqdorni kiritadi. Hamyon tegishli blokcheyn qoidalariga muvofiq tranzaksiya ma’lumotlarini shakllantiradi. Elektron hamyonning o‘zi pul yoki raqamli aktivlarni jismonan saqlamaydi. U odatda foydalanuvchiga kalitlarni boshqarish va blokcheyn reyestridagi aktivlarga tegishli operatsiyalarni amalga oshirish imkonini beradi.

### 5.2. Ikkinchi bosqich - tranzaksiyani imzolash

Tranzaksiya foydalanuvchining tegishli yopiq kaliti bilan imzolanadi. Imzo tranzaksiya ma’lumotlariga bog‘liq bo‘ladi. Shu sababli imzolangan ma’lumotni ruxsatsiz o‘zgartirish imzo tekshiruvining muvaffaqiyatsiz bo‘lishiga olib kelishi mumkin. Yopiq kalitni xavfsiz saqlash juda muhim.

### 5.3. Uchinchi bosqich - tranzaksiyani tarmoqqa yuborish

Imzolangan tranzaksiya tarmoqdagi bir yoki bir nechta tugunga yuboriladi. Tugun uni tekshiradi va protokol qoidalariga mos bo‘lsa, boshqa tugunlarga tarqatishi mumkin.

Tekshiruvda imzo, mablag‘ mavjudligi, tranzaksiya formati va boshqa talablar ko‘rib chiqiladi.

### 5.4. To‘rtinchi bosqich - blokka kiritish

Tarmoqning tegishli qoidalari asosida tranzaksiya yangi blokka kiritish uchun tanlanadi. Proof of Work tizimida maynerlar yangi blokni yaratish uchun hisoblash ishlarini bajaradi. Proof of Stake tizimida esa protokol qoidalariga muvofiq validatorlar bloklarni taklif qiladi yoki tasdiqlaydi.

### 5.5. Beshinchi bosqich - blokni tekshirish

Tarmoqdagi tekshiruvchi tugunlar blokning qoidalarga mosligini tekshiradi. Bunda blokning oldingi blok bilan bog‘lanishi, tranzaksiyalarning haqiqiyligi va konsensus talablariga muvofiqligi tekshirilishi mumkin. Qoidalarga mos bo‘lmagan blok tugunlar tomonidan rad etilishi mumkin.

### 5.6. Oltinchi bosqich - tranzaksiyaning tasdiqlanishi

Blokcheyn tarmog‘ining qoidalariga muvofiq blok qabul qilingach, tranzaksiya reyestrda qayd etiladi. Ayrim tarmoqlarda yangi bloklar qo‘shilishi bilan tranzaksiyaning qayta tashkil etilish ehtimoli kamayadi. Boshqa tarmoqlarda esa belgilangan yakuniylik qoidalari bajarilganda tranzaksiya yakunlangan hisoblanadi.

### 5.7. Blokcheynda ma’lumotlarni o‘zgartirish masalasi

Blokcheyn ko‘pincha o‘zgartirib bo‘lmaydigan ma’lumotlar tizimi sifatida ta’riflanadi. Aniqroq aytganda, ko‘plab blokcheynlarda tasdiqlangan tarixiy yozuvlarni yashirincha o‘zgartirish juda qiyin. Chunki bunday o‘zgarish kriptografik bog‘lanishlar va konsensus qoidalariga ta’sir qiladi. Shunga qaramay, noto‘g‘ri ma’lumot blokcheynga kiritilgan bo‘lsa, texnologiyaning o‘zi uning mazmunan to‘g‘ri ekanini kafolatlamaydi. Masalan, logistika xodimi yuk haqidagi noto‘g‘ri ma’lumotni tizimga kiritsa, bu yozuv blokcheynda qayd etilishi mumkin. Muammoni bartaraf etish uchun yangi tuzatuvchi yozuv kiritish yoki boshqa tashkiliy choralarni ko‘rish talab etiladi. Demak, blokcheyn ma’lumotlar tarixini himoyalashga yordam beradi, lekin dastlabki ma’lumotning to‘g‘riligini har doim ham kafolatlamaydi.

## 6. Consensus mechanisms: proof of work and proof of stake

A blockchain network can contain many nodes. Without reporting to a single central server, they must reach a mutual agreement on which state of the ledger to accept. This task is performed by the consensus mechanism.

A consensus mechanism is a set of rules and algorithms serving to determine the validity of blocks and ledger state among network participants:

- Determining the order of accepting new blocks.
- Verifying transaction validity.
- Ensuring agreement among network nodes.
- Creating protection against the acceptance of invalid blocks.
- Supporting stable network operation.

### 6.1. Proof of Work (PoW)

Proof of Work is a consensus mechanism that requires performing a certain amount of computational work to create a new block. This mechanism is used in the Bitcoin network. In a PoW system, miners change variable values in the block header to find a hash matching the specified requirement. In the case of Bitcoin, the block hash value must meet the difficulty requirement set by the network. Achieving this may require calculating hashes many times.

- Miner prepares a block from transactions.
- Necessary data for the block is formulated.
- The miner calculates hashes by changing variable values.
- If a result meeting the requirement is found, the block is proposed to the network.
- Other nodes independently verify the block.
- A rule-compliant block can be accepted.

The fact that a miner has performed a lot of computational work does not automatically mean all data in the block is correct. Nodes independently verify transactions and blocks based on established rules.

The advantage of the PoW mechanism is that because it requires large computational resources, carrying out certain types of attacks becomes expensive. The disadvantage is the high demand for electricity and specialized computing hardware.

### 6.2. Proof of stake (PoS)

Proof of Stake is a consensus mechanism that uses validators who have staked relevant network assets during the block creation or validation process. A validator is a participant who proposes or validates blocks in accordance with network rules. In a PoS system, participants can stake a specified amount of cryptocurrency. Validators are selected according to protocol rules and work with blocks.

- Participant stakes assets according to network requirements.
- The protocol determines the validator selection procedure.
- The validator proposes or validates a block.
- Other validators check the block.
- If sufficient confirmations and consensus conditions are met, the block is accepted.

Validators who follow the rules may receive rewards, while certain violations lead to penalties. In many cases, the PoS mechanism consumes less electricity compared to the PoW system. However, its security depends on validator selection, asset distribution, slashing rules, and the quality of the consensus algorithm.

### 6.3. Comparison of PoW and PoS mechanisms

This comparison reflects general features. The exact operating procedure of each network is determined by its protocol.

| Criterion | Proof of Work (PoW) | Proof of Stake (PoS) |
|---|---|---|
| Main approach | Performing computational work | Staking assets and validation via validators |
| Participants | Miners | Validators |
| Resource requirement | Often high computing power and electricity | Often less electricity |
| Basis of security | Computing resources and economic costs | Staking, validators, and economic penalties |

| | | |
|---|---|---|
| Reward | Block reward and fees according to protocol | Staking rewards and fees according to protocol |
| Example | Bitcoin | Ethereum |

### 6.4. Other consensus mechanisms

- **Proof of Authority (PoA) -** a mechanism where the right to validate blocks belongs to specially authorized validators. It is often used in permissioned or managed networks.
- **Byzantine fault tolerance (BFT) -** family mechanisms are designed to reach agreement among participants even in conditions where some nodes fail or send incorrect messages. Some of them are used in enterprise blockchains.

When choosing a consensus mechanism, network size, level of trust among participants, processing speed, energy consumption, and security requirements are taken into account.

## 6. Konsensus mexanizmlari: Proof of Work va Proof of Stake

Blokcheyn tarmog‘ida ko‘plab tugunlar mavjud bo‘lishi mumkin. Ularning barchasi bitta markaziy serverga bo‘ysunmasdan, reyestrning qaysi holatini qabul qilish bo‘yicha umumiy kelishuvga kelishi kerak. Bu vazifani konsensus mexanizmi bajaradi.

- Konsensus mexanizmi - tarmoq ishtirokchilari o‘rtasida bloklar va reyestr holatining haqiqiyligini aniqlashga xizmat qiladigan qoidalar va algoritmlar majmuasi;
- Yangi bloklarning qabul qilinish tartibini belgilash;
- Tranzaksiyalarning haqiqiyligini tekshirish;
- Tarmoq tugunlari o‘rtasida kelishuvni ta’minlash;
- Noto‘g‘ri bloklarning qabul qilinishiga qarshi himoya yaratish;
- Tarmoqning barqaror ishlashini qo‘llab-quvvatlash.

### 6.1. Proof of Work - bajarilgan ishni isbotlash

Proof of Work (PoW) - yangi blok yaratish uchun muayyan hisoblash ishini bajarishni talab qiladigan konsensus mexanizmi. Ushbu mexanizm Bitcoin tarmog‘ida qo‘llaniladi. PoW tizimida maynerlar blok sarlavhasidagi o‘zgaruvchan qiymatlarni o‘zgartirib, belgilangan talabga mos xesh topishga harakat qiladi. Bitcoin misolida blok xeshining

qiymati tarmoq belgilagan murakkablik talabiga javob berishi kerak. Bunga erishish uchun ko‘p marta xesh hisoblash talab etilishi mumkin.

1. Mayner tranzaksiyalardan blok tayyorlaydi;
2. Blok uchun zarur ma’lumotlar shakllantiriladi;
3. Mayner o‘zgaruvchan qiymatlarni o‘zgartirib, xeshlarni hisoblaydi;
4. Talabga javob beradigan natija topilsa, blok tarmoqqa taklif etiladi;
5. Boshqa tugunlar blokni mustaqil tekshiradi;
6. Qoidalarga mos blok qabul qilinishi mumkin.

Maynerning ko‘p hisoblash ishini bajargani blokdagi barcha ma’lumotlar avtomatik ravishda to‘g‘ri degani emas. Tugunlar tranzaksiyalar va blokni belgilangan qoidalar asosida mustaqil tekshiradi. PoW mexanizmining afzalligi - katta hisoblash resurslarini talab qilishi sababli ayrim turdagi hujumlarni amalga oshirish qimmatlashadi. Kamchiligi esa elektr energiyasi va maxsus hisoblash qurilmalariga katta ehtiyoj mavjudligidir.

### 6.2. Proof of Stake - ulushni isbotlash

Proof of Stake (PoS) - blok yaratish yoki tasdiqlash jarayonida tarmoqning tegishli aktivlarini steykingga joylashtirgan validatorlardan foydalanadigan konsensus mexanizmi. Validator - tarmoq qoidalariga muvofiq bloklarni taklif qiluvchi yoki tasdiqlovchi ishtirokchi. PoS tizimida ishtirokchilar belgilangan miqdordagi kriptovalyutani steykingga joylashtirishi mumkin. Protokol qoidalariga muvofiq validatorlar tanlanadi va ular bloklar bilan ishlaydi.

1. Ishtirokchi tarmoq talablariga muvofiq aktivlarini steykingga joylashtiradi;
2. Protokol validatorlarni tanlash tartibini belgilaydi;
3. Validator blokni taklif qiladi yoki tasdiqlaydi;
4. Boshqa validatorlar blokni tekshiradi;
5. Yetarli tasdiqlar va konsensus shartlari bajarilsa, blok qabul qilinadi;
6. Qoidalarga rioya qilgan validatorlar mukofot olishi mumkin, ayrim qoidabuzarliklar esa jazoga olib keladi.

PoS mexanizmi ko‘plab hollarda PoW tizimiga nisbatan kamroq elektr energiyasi sarflaydi. Biroq uning xavfsizligi validatorlarni tanlash, aktivlarni taqsimlash, jazolash qoidalari va konsensus algoritmining sifatiga bog‘liq.

### 6.3. PoW va PoS mexanizmlarini taqqoslash

| Mezon | Proof of Work | Proof of Stake |
|---|---|---|
| Asosiy yondashuv | Hisoblash ishini bajarish | Aktivlarni steykingga joylashtirish va validatorlar orqali tasdiqlash |
| Ishtirokchilar | Maynerlar | Validatorlar |
| Resurs talabi | Ko‘pincha yuqori hisoblash quvvati va elektr energiyasi | Ko‘pincha kamroq elektr energiyasi |
| Xavfsizlik asosi | Hisoblash resurslari va iqtisodiy xarajatlar | Steyking, validatorlar va iqtisodiy jazolar |
| Mukofot | Protokolga muvofiq blok mukofoti va komissiyalar | Protokolga muvofiq steyking mukofotlari va komissiyalar |
| Misol | Bitcoin | Ethereum |

Ushbu taqqoslash umumiy xususiyatlarni ifodalaydi. Har bir tarmoqning aniq ishlash tartibi o‘z protokoli bilan belgilanadi.

### 6.4. Boshqa konsensus mexanizmlari

- **Proof of Authority (PoA)** - bloklarni tasdiqlash huquqi maxsus vakolat berilgan validatorlarga tegishli bo‘lgan mexanizm. U ko‘pincha ruxsatli yoki boshqariladigan tarmoqlarda ishlatiladi.

- **Byzantine Fault Tolerance (BFT)** -oilasidagi mexanizmlar ayrim tugunlar ishlamay qolgan yoki noto‘g‘ri xabarlar yuborgan sharoitda ham ishtirokchilar o‘rtasida kelishuvga erishishga mo‘ljallangan. Ularning ayrimlari tashkilotlararo blokcheynlarda qo‘llaniladi. Konsensus mexanizmini tanlashda tarmoqning hajmi, ishtirokchilar o‘rtasidagi ishonch darajasi, ishlash tezligi, energiya sarfi va xavfsizlik talablari hisobga olinadi.

## 7. Types of blockchains and their differences

Blockchain networks are divided into several types depending on who can use them, who manages the network, and what rights are granted to participants.

### 7.1. Public blockchain

A public blockchain is a network accessible to the general public. Typically, any user can send transactions, observe the ledger, or run a node based on the network's established rules. Examples include Bitcoin and Ethereum networks. Advantages: wide accessibility, many independent participants, independent verification of ledger data, and reduced dependence on a central operator. Disadvantages may be related to limited transaction speed, variable fees, and public visibility of certain data.

### 7.2. Private blockchain

A private blockchain is a system where access and execution rights within the network are controlled by a single organization or an authorized administrator. For example, a large enterprise can create a private blockchain to record internal document management or manufacturing processes. Its advantages include user management, access restrictions, compliance with privacy requirements, and faster transaction processing. However, a private blockchain may be more dependent on central management.

### 7.3. Consortium blockchain

A consortium blockchain is a network jointly managed by several independent organizations. For example, several banks, insurance companies, or logistics enterprises can create a shared ledger to exchange data among themselves. Management rights are granted to multiple participants based on agreed-upon rules.

### 7.4. Hybrid blockchain

A hybrid blockchain combines certain features of public and private systems. For example, an enterprise can store internal data in a restricted circle while making certain validation data open to external users.

### 7.5. Comparison of blockchain types

Before choosing a blockchain type, it is necessary to determine what data will be stored in the system, who will use it, and which participants can trust each other.

| Feature | Public | Private | Consortium | Hybrid |
|---|---|---|---|---|
| Participation | Open to the general public | By permission | Selected organizations | Open and restricted parts |
| Governance | Protocol & participants | Mainly single org | Multiple orgs | Mixed |
| Privacy | Limited / extra tools | More strictly controlled | Based on agreement | Depending on task |
| Example | Open digital assets | Enterprise internal ledger | Inter-org exchange | Internal & external ledger |

### 7.6. Main advantages of blockchain

- Data integrity protection - Cryptographic linking of blocks and consensus rules make it difficult to secretly alter historical records.
- Transparency - In public blockchains, users can track transactions and independently verify data in the ledger.
- Distributed storage - The presence of data copies across multiple nodes can reduce the risk of a single server failure halting the entire system.
- Audit capability - Transaction history serves to analyze operational sequences and verify the origin of records.
- Process automation - Smart contracts allow certain operations to be executed automatically based on predefined conditions.
- Reduction of intermediaries - In some systems, transactions can be verified and recorded without a central intermediary.

### 7.7. Disadvantages of blockchain

- **Scalability issue -** Some blockchains face difficulties in quickly processing large transaction flows.
- **Energy consumption -** The Proof of Work mechanism can require high computing power and electricity.
- **Complexity of data correction -** Deleting or modifying an incorrect record in a simple way is often impossible.
- **Privacy issues -** Transactions in public networks can be publicly observed.

- **Risk of key loss -** If a private key is lost, recovering access to the respective assets can be very difficult or impossible.
- **Software bugs -** Errors in smart contracts can lead to financial losses or system malfunctions.
- **Implementation costs -** Funds and qualified specialists are required for development, testing, management, and maintenance.

### 7.8. Ensuring security in blockchain

The security of a blockchain system is not determined solely by the cryptographic linking of blocks. Network infrastructure, user devices, software, and governance rules are also of great importance.

- Storing private keys in secure devices.
- Using reliable electronic wallets and software.
- Conducting security audits of smart contracts before deployment.
- Properly distributing user rights.
- Developing backup copies and emergency plans.
- Regularly monitoring abnormal activity in the network.
- Protecting users from fraud and phishing links.

### 7.9. Blockchain and cyberattacks

The cryptographic structure of blockchain makes certain attacks difficult, but does not eliminate all attacks. For example, if an attacker acquires a user's private key, they can create a transaction with a valid signature. In such cases, the blockchain is likely to accept the transaction as rule-compliant. Another risk is attacking the network's consensus mechanism. In some PoW networks, controlling a large portion of computing power may allow attempts to reorganize historical history. In PoS networks, validator stake distribution and protocol rules affect security. Therefore, when implementing blockchain, cryptographic protection, software security, key management, and economic risks must be evaluated together.

## 7. Blokcheyn turlari va ularning farqlari

Blokcheyn tarmoqlari ulardan kim foydalanishi, tarmoqni kim boshqarishi va ishtirokchilarga qanday huquqlar berilishiga qarab bir necha turga bo‘linadi.

### 7.1. Ochiq blokcheyn

Ochiq blokcheyn - keng jamoatchilik foydalanishi mumkin bo‘lgan tarmoq. Odatda, istalgan foydalanuvchi tranzaksiyalarni yuborishi, reyestrni kuzatishi yoki tarmoqning belgilangan qoidalari asosida tugun ishga tushirishi mumkin. Misollar sifatida Bitcoin va Ethereum tarmoqlarini keltirish mumkin. Afzalliklari: foydalanish imkoniyatining kengligi, ko‘plab mustaqil ishtirokchilar, reyestr ma’lumotlarini mustaqil tekshirish va markaziy operatorga qaramlikning kamayishi. Kamchiliklari esa tranzaksiyalar tezligining cheklanishi, komissiyalarning o‘zgaruvchanligi va ayrim ma’lumotlarning ommaviy ko‘rinishi bilan bog‘liq bo‘lishi mumkin.

### 7.2. Xususiy blokcheyn

Xususiy blokcheyn - tarmoqqa kirish va undagi amallarni bajarish huquqlari bitta tashkilot yoki vakolatli boshqaruvchi tomonidan nazorat qilinadigan tizim. Masalan, yirik korxona ichki hujjat aylanishi yoki ishlab chiqarish jarayonlarini qayd etish uchun xususiy blokcheyn yaratishi mumkin. Uning afzalliklari foydalanuvchilarni boshqarish, kirish huquqlarini cheklash, maxfiylik talablariga moslashish va tranzaksiyalarni tezroq qayta ishlash imkoniyatlarini o‘z ichiga oladi. Biroq xususiy blokcheyn markaziy boshqaruvga ko‘proq bog‘liq bo‘lishi mumkin.

### 7.3. Konsorsium blokcheyni

Konsorsium blokcheyni - bir nechta mustaqil tashkilot hamkorlikda boshqaradigan tarmoq. Masalan, bir nechta bank, sug‘urta kompaniyasi yoki logistika korxonasi o‘zaro ma’lumot almashish uchun umumiy reyestr yaratishi mumkin. Boshqaruv huquqi kelishilgan qoidalar asosida bir nechta ishtirokchiga beriladi.

### 7.4. Gibrid blokcheyn

Gibrid blokcheyn ochiq va xususiy tizimlarning ayrim xususiyatlarini birlashtiradi. Masalan, korxona ichki ma’lumotlarni cheklangan doirada saqlashi, ayrim tasdiqlash ma’lumotlarini esa tashqi foydalanuvchilar uchun ochiq qilishi mumkin.

### 7.5. Blokcheyn turlarini taqqoslash

| Xususiyat | Ochiq | Xususiy | Konsorsium | Gibrid |
|---|---|---|---|---|
| Ishtirok etish | Keng jamoatchilik uchun ochiq | Ruxsat asosida | Tanlangan tashkilotlar | Ochiq va cheklangan qismlar |

| | | | | |
|---|---|---|---|---|
| Boshqaruv | Protokol va tarmoq ishtirokchilari | Asosan bitta tashkilot | Bir nechta tashkilot | Aralash |
| Maxfiylik | Cheklangan yoki qo‘shimcha vositalarga bog‘liq | Kengroq nazorat qilinadi | Kelishuv asosida | Vazifaga qarab |
| Misol | Ochiq raqamli aktivlar | Korxona ichki reyestri | Tashkilotlararo almashuv | Ichki va tashqi reyestr |

Blokcheyn turini tanlashdan oldin tizimda qanday ma’lumotlar saqlanishi, kimlar undan foydalanishi va qaysi ishtirokchilar bir-biriga ishonishi mumkinligi aniqlanishi lozim.

### 7.6. Blokcheynning asosiy afzalliklari

- Ma’lumotlar yaxlitligini himoyalash. Bloklarning kriptografik bog‘lanishi va konsensus qoidalari tarixiy yozuvlarni yashirincha o‘zgartirishni qiyinlashtiradi.
- Shaffoflik. Ochiq blokcheynlarda foydalanuvchilar tranzaksiyalarni kuzatishi va reyestrdagi ma’lumotlarni mustaqil tekshirishi mumkin.
- Taqsimlangan saqlash. Ma’lumotlar nusxalarining bir nechta tugunda mavjudligi bitta serverdagi nosozlikning butun tizimni to‘xtatib qo‘yish xavfini kamaytirishi mumkin.
- Audit imkoniyati. Tranzaksiyalar tarixi operatsiyalar ketma-ketligini tahlil qilish va yozuvlarning kelib chiqishini tekshirish uchun xizmat qiladi.
- Jarayonlarni avtomatlashtirish. Aqlli shartnomalar yordamida ayrim operatsiyalarni oldindan belgilangan shartlar asosida avtomatik bajarish mumkin.
- Vositachilarga bo‘lgan ehtiyojni kamaytirish. Ayrim tizimlarda operatsiyalarni tekshirish va qayd etish markaziy vositachisiz bajarilishi mumkin.

### 7.7. Blokcheynning kamchiliklari

**Masshtablash muammosi** - ayrim blokcheynlar katta tranzaksiya oqimini tez qayta ishlashda qiyinchilikka duch keladi.

**Energiya sarfi** - Proof of Work mexanizmi katta hisoblash quvvati va elektr energiyasini talab qilishi mumkin.

**Ma’lumotlarni tuzatish murakkabligi** - noto‘g‘ri yozuvni oddiy usulda o‘chirib tashlash yoki o‘zgartirish ko‘pincha mumkin emas.

**Maxfiylik muammolari** - ochiq tarmoqlardagi tranzaksiyalar ommaviy kuzatilishi mumkin.

**Kalitlarni yo‘qotish xavfi** - yopiq kalit yo‘qolsa, tegishli aktivlarga kirishni tiklash juda qiyin yoki imkonsiz bo‘lishi mumkin.

**Dasturiy xatolar** - aqlli shartnomadagi xatolar moliyaviy yo‘qotishlarga yoki tizimning noto‘g‘ri ishlashiga olib kelishi mumkin.

Joriy etish xarajatlari - ishlab chiqish, tekshirish, boshqarish va texnik xizmat ko‘rsatish uchun mablag‘ va malakali mutaxassislar talab qilinadi.

### 7.8. Blokcheynda xavfsizlikni ta’minlash

Blokcheyn tizimining xavfsizligi faqat bloklarning kriptografik bog‘lanishi bilan belgilanmaydi. Tarmoq infratuzilmasi, foydalanuvchi qurilmalari, dasturiy ta’minot va boshqaruv qoidalari ham muhim ahamiyatga ega.

1. Yopiq kalitlarni himoyalangan qurilmalarda saqlash.
2. Ishonchli elektron hamyon va dasturiy ta’minotdan foydalanish.
3. Aqlli shartnomalarni ishga tushirishdan oldin xavfsizlik auditidan o‘tkazish.
4. Foydalanuvchilar huquqlarini to‘g‘ri taqsimlash.
5. Zaxira nusxalari va favqulodda vaziyat rejalarini ishlab chiqish.
6. Tarmoqdagi g‘ayritabiiy faoliyatni muntazam kuzatish.
7. Foydalanuvchilarni firibgarlik va soxta havolalardan himoyalash.

### 7.9. Blokcheyn va kiberhujumlar

Blokcheynning kriptografik tuzilishi ayrim hujumlarni qiyinlashtiradi, ammo barcha hujumlarni bartaraf etmaydi. Masalan, hujumchi foydalanuvchining yopiq kalitini qo‘lga kiritsa, haqiqiy imzoga ega tranzaksiyani yaratishi mumkin. Bunday holatda blokcheyn tranzaksiyani qoidaga mos deb qabul qilishi ehtimoli bor. Yana bir xavf - tarmoqning konsensus mexanizmiga hujum qilish. Ayrim PoW tarmoqlarida hisoblash quvvatining katta qismini nazorat qilish tarixiy yozuvlarni qayta tashkil etishga urinish imkonini berishi mumkin. PoS tarmoqlarida esa validatorlar ulushining taqsimlanishi va protokol qoidalari xavfsizlikka ta’sir qiladi. Shuning uchun blokcheynni joriy etishda kriptografik himoya, dasturiy xavfsizlik, kalitlarni boshqarish va iqtisodiy xavflar birgalikda baholanishi kerak.

## Practical application and development prospects of blockchain technology

Although blockchain technology initially developed in connection with cryptocurrencies, today its application possibilities have expanded significantly. It can be particularly useful in situations where multiple organizations or users need reliable access to a shared data history.

**In finance and banking:** Blockchain is used for transferring digital assets, maintaining transaction history, automating certain settlement processes, and working with tokenized assets. In traditional financial systems, information systems of multiple organizations exchange data to record and reconcile operations. In a specific blockchain solution, participants can use a shared ledger. This process can simplify certain calculations, but legal requirements, privacy, fees, and cross-system compatibility issues must also be addressed.

**In logistics and transport:** Blockchain can be used in transport and logistics systems to maintain records of the origin, shipment, reception, and delivery of cargo (cargo order ID, timestamp, vehicle ID, delivery status, operations approved by responsible persons). Blockchain can help track data history and reduce inter-organizational disputes. However, if a GPS device sends incorrect data or an employee enters a wrong record, blockchain does not automatically guarantee the accuracy of this data. Therefore, it is advisable to use blockchain together with GPS, Transport Management Systems (TMS), Warehouse Management Systems (WMS), and other information systems.

**In education:** In education, blockchain can expand opportunities for verifying degrees, certificates, and academic results. Higher education institutions issue electronic diplomas to graduates, and verification data is entered into the blockchain ledger. Employers or other institutions can verify authenticity. It is not recommended to store students' personal data entirely on a public blockchain; confidential documents can be stored in a secured database while only necessary verification data is recorded in the blockchain.

**In Public Services & Documents:** In public services, blockchain can be used for recording document history, cross-registry data exchange, and automating certain processes. However, the presence of blockchain in state registries does not automatically determine the legal force of a document. This requires relevant legislation, authority, and approval procedures.

**Smart Contracts & Automation:** A smart contract is a software code running on a blockchain platform that executes specific actions when defined conditions are met. It automates operations, ensures consistent execution, verifies history, and reduces intermediary actions. If a smart contract is programmed incorrectly, errors execute automatically, making testing and auditing essential.

**Blockchain and AI:** AI serves to analyze large volumes of data, forecast, and support decisions, while blockchain helps verify data exchanges and operation histories. For example, AI can optimize transport routes while blockchain maintains delivery records. However, blockchain does not automatically guarantee the correctness of AI conclusions.

**Future development of blockchain**

1. Increasing transaction speed and system scalability
2. Secure data exchange between different blockchains
3. Digital identification and electronic document verification
4. Using privacy-preserving cryptographic methods
5. Enhancing smart contract security
6. Integrating blockchain with enterprise information systems
7. Reducing energy consumption and infrastructure costs

When choosing a blockchain, the novelty of the technology should not be the main criterion, but rather the nature of the problem being solved. If a task can be performed faster, cheaper, and safer through a simple database, implementing blockchain is not always appropriate.

## Blokcheyn texnologiyasining amaliy qo‘llanilishi va rivojlanish istiqbollari

Blokcheyn texnologiyasi dastlab kriptovalyutalar bilan bog‘liq holda rivojlangan bo‘lsada, bugungi kunda uning qo‘llanish imkoniyatlari ancha kengaygan. U ayniqsa bir nechta tashkilot yoki foydalanuvchi umumiy ma’lumotlar tarixiga ishonchli tarzda ega bo‘lishi zarur bo‘lgan vaziyatlarda foydali bo‘lishi mumkin.

### 💡 Moliya va bank tizimida

Blokcheyn raqamli aktivlarni o‘tkazish, tranzaksiyalar tarixini yuritish, ayrim hisob-kitob jarayonlarini avtomatlashtirish va tokenlashtirilgan aktivlar bilan ishlashda qo‘llaniladi. An’anaviy moliyaviy tizimlarda operatsiyalarni qayd etish va solishtirish uchun bir nechta tashkilotning axborot tizimlari o‘zaro ma’lumot almashadi. Muayyan blokcheyn yechimida esa ishtirokchilar umumiy reyestrdan foydalanishi mumkin. Bu jarayon ayrim hisob-kitoblarni soddalashtirishi mumkin, lekin huquqiy talablar, maxfiylik, komissiyalar va tizimlararo moslik masalalarini ham hal qilish lozim.

### 💡 Logistika va transport sohasida

Blokcheyn transport va logistika tizimlarida yukning kelib chiqishi, jo‘natilishi, qabul qilinishi va yetkazib berilishi haqidagi yozuvlarni yuritishda qo‘llanishi mumkin.

- Yuk buyurtmasining identifikatori;
- Yukni qabul qilish va topshirish vaqti;
- Transport vositasining identifikatori;
- Jo‘natish va yetkazib berish holati.
- Mas’ul shaxslar tomonidan tasdiqlangan operatsiyalar.

Blokcheyn ma’lumotlar tarixini kuzatish va tashkilotlararo kelishmovchiliklarni kamaytirishga yordam berishi mumkin. Ammo GPS qurilmasi noto‘g‘ri ma’lumot yuborsa yoki xodim noto‘g‘ri yozuv kiritsa, blokcheyn bu ma’lumotning haqiqiyligini o‘z-o‘zidan kafolatlamaydi. Shu sababli blokcheynni GPS, transportni boshqarish tizimlari (TMS), ombor boshqaruvi (WMS) va boshqa axborot tizimlari bilan birgalikda ishlatish maqsadga muvofiq.

### 💡 Ta’lim tizimida

Ta’lim sohasida blokcheyn diplomlar, sertifikatlar va o‘quv natijalari haqidagi ma’lumotlarni tekshirish imkoniyatlarini kengaytirishi mumkin. Oliy ta’lim muassasasi bitiruvchiga elektron diplom beradi. Diplom haqidagi muhim tekshiruv ma’lumotlari blokcheyn reyestriga kiritiladi yoki hujjatning kriptografik xeshi qayd etiladi. Ish beruvchi yoki boshqa ta’lim muassasasi taqdim etilgan hujjatning haqiqiyligini tekshirishi mumkin. Bunda talabalarning shaxsiy ma’lumotlarini ommaviy blokcheynda to‘liq saqlash tavsiya etilmaydi. Maxfiy hujjatlar himoyalangan bazada saqlanib, blokcheynda faqat zarur tasdiqlovchi ma’lumotlar qayd etilishi mumkin.

### 💡 Sog‘liqni saqlash tizimida

Tibbiyotda blokcheyn tibbiy hujjatlarga kirish huquqlarini boshqarish, ma’lumotlar almashinuvi tarixini qayd etish va tibbiy mahsulotlar yetkazib berilishini kuzatish kabi vazifalarda qo‘llanishi mumkin. Tibbiy ma’lumotlarning maxfiyligi va bemor roziligini himoyalash birinchi o‘rinda turadi. Blokcheyn bemor haqidagi barcha ma’lumotlarni bevosita zanjirda saqlashi shart emas. Ko‘pincha ma’lumotlar himoyalangan bazada saqlanib, blokcheyn yordamida ularning yaxlitligi yoki operatsiyalar tarixi tekshiriladi.

### 💡 Davlat xizmatlari va elektron hujjatlar

Davlat xizmatlarida blokcheyn hujjatlar tarixini qayd etish, reyestrlararo ma’lumot almashinuvi va ayrim jarayonlarni avtomatlashtirish uchun ishlatilishi mumkin. Hujjat yaratilgan vaqti, unga tegishli o‘zgartirishlar yoki vakolatli shaxs tomonidan tasdiqlangan operatsiyalar haqida qaydlar yuritilishi mumkin. Biroq davlat reyestrlarida blokcheynning mavjudligi hujjatning huquqiy kuchini o‘z-o‘zidan belgilamaydi. Buning uchun tegishli qonunchilik, vakolat va hujjatlarni tasdiqlash tartiblari talab etiladi.

### 💡 Aqlli shartnomalar va avtomatlashtirish

Aqlli shartnoma - blokcheyn platformasida ishlaydigan va belgilangan shartlar bajarilganda muayyan amallarni bajaradigan dasturiy kod. Masalan, yetkazib berish shartnomasida tovar qabul qilingani tasdiqlangandan keyin to‘lovni amalga oshirish qoidasi belgilanishi mumkin.

Ayrim operatsiyalarni avtomatlashtirish.

Kelishilgan qoidalarni bir xil bajarish.

Jarayonlar tarixini tekshirish.

Ayrim vositachilik amallarini kamaytirish.

Aqlli shartnoma noto‘g‘ri dasturlashtirilsa, xatolar avtomatik tarzda amalga oshishi mumkin. Shuning uchun kodni sinash, audit qilish va xavfsizlik talablariga rioya etish muhim.

### 💡 Blokcheyn va sun’iy intellekt

Blokcheyn va sun’iy intellekt birgalikda qo‘llanilganda turli imkoniyatlar yuzaga keladi. Sun’iy intellekt katta hajmdagi ma’lumotlarni tahlil qilish, prognozlash va qarorlarni qo‘llab-quvvatlash uchun xizmat qiladi. Blokcheyn esa ayrim ma’lumotlar almashinuvi va operatsiyalar tarixini tekshirishga yordam beradi. Masalan, logistika tizimida sun’iy intellekt transport yo‘nalishini optimallashtirishi, blokcheyn esa buyurtmalar va yetkazib berish bosqichlari bo‘yicha qaydlarni yuritishi mumkin. Biroq blokcheyn sun’iy intellekt xulosasining to‘g‘riligini avtomatik kafolatlamaydi.

### 💡 Blokcheynning kelajakdagi rivojlanishi

1. Tranzaksiyalar tezligini oshirish va tizimlarni masshtablash
2. Turli blokcheynlar o‘rtasida xavfsiz ma’lumot almashish
3. Raqamli identifikatsiya va elektron hujjatlarni tasdiqlash
4. Maxfiylikni ta’minlaydigan kriptografik usullardan foydalanish.
5. Aqlli shartnomalar xavfsizligini oshirish
6. Blokcheynni korxona axborot tizimlari bilan integratsiya qilish
7. Energiya sarfi va infratuzilma xarajatlarini kamaytirish

Blokcheynni tanlashda texnologiyaning yangiligi emas, balki hal qilinayotgan muammoning xususiyati asosiy mezon bo‘lishi kerak. Agar vazifani oddiy ma’lumotlar bazasi orqali tezroq, arzonroq va xavfsizroq bajarish mumkin bo‘lsa, blokcheyn joriy etish har doim ham maqsadga muvofiq bo‘lmaydi.

## Conclusion

Blockchain technology is a modern information technology that allows storing data in cryptographically linked blocks and maintaining a distributed ledger among network participants. Its working principle is based on several important mechanisms:

creating transactions, cryptographic signing, calculating hash values, forming blocks, verifying based on consensus, and adding to the ledger according to rules. One of the main features of blockchain is the cryptographic connection between blocks. This connection makes it difficult to secretly alter historical data. A distributed ledger allows storing data across multiple independent nodes.

Consensus mechanisms such as Proof of Work and Proof of Stake offer different ways to reach agreement among network participants. Each of them has unique characteristics in terms of security, resource consumption, and governance. Blockchain can be applied in finance, logistics, education, healthcare, public services, and digital document management. At the same time, its security also depends on key protection, software code quality, the consensus mechanism, and proper data entry.

In short, blockchain technology is one of the important tools for creating a reliable digital environment. To apply it effectively, it is necessary to deeply understand the working principles of the technology, evaluate its advantages and disadvantages, and choose a solution suited to the practical task.

**Xulosa**

Blokcheyn texnologiyasi ma’lumotlarni kriptografik jihatdan bog‘langan bloklarda saqlash va tarmoq ishtirokchilari o‘rtasida taqsimlangan reyestr yuritish imkonini beradigan zamonaviy axborot texnologiyasidir. Uning ishlash prinsipi bir nechta muhim mexanizmlarga asoslanadi: tranzaksiyalarni yaratish, kriptografik imzolash, xesh qiymatlarini hisoblash, bloklarni shakllantirish, konsensus asosida tekshirish va qoidalarga muvofiq reyestrga qo‘shish. Blokcheynning asosiy xususiyatlaridan biri -bloklar o‘rtasidagi kriptografik bog‘lanishdir. Ushbu bog‘lanish tarixiy ma’lumotlarni yashirincha o‘zgartirishni qiyinlashtiradi. Taqsimlangan reyestr esa ma’lumotlarni bir nechta mustaqil tugunda saqlash imkonini beradi.

Proof of Work va Proof of Stake kabi konsensus mexanizmlari tarmoqdagi ishtirokchilar o‘rtasida kelishuvga erishishning turli usullarini taklif etadi. Ularning har biri xavfsizlik, resurs sarfi va boshqaruv nuqtayi nazaridan o‘ziga xos xususiyatlarga ega. Blokcheyn moliya, logistika, ta’lim, sog‘liqni saqlash, davlat xizmatlari va raqamli hujjatlarni boshqarishda qo‘llanishi mumkin. Shu bilan birga, uning xavfsizligi

kalitlarni himoyalash, dasturiy kod sifati, konsensus mexanizmi va ma’lumotlarni to‘g‘ri kiritishga ham bog‘liq.

Xulosa qilib aytganda, blokcheyn texnologiyasi ishonchli raqamli muhit yaratish uchun muhim vositalardan biri hisoblanadi. Uni samarali qo‘llash uchun texnologiyaning ishlash prinsiplarini chuqur tushunish, afzallik va kamchiliklarini baholash hamda amaliy vazifaga mos yechim tanlash zarur.

# GLOSSARY (ГЛОССАРИЙ)

| Atamaning nomlanishi | | | | Atamaning ma’nosi |
|---|---|---|---|---|
| № | O‘zbek tilida | Rus tilida | Ingliz tilida | |
| 1 | **Blokcheyn** | **Блокчейн** | **Blockchain** | Ma’lumotlar bloklar ko‘rinishida saqlanadigan va kriptografik usullar orqali o‘zaro bog‘langan taqsimlangan raqamli reyestr. |
| 2 | **Tranzaksiya** | **Транзакция** | **Transaction** | Tizimda ma’lumot yoki raqamli aktivlarni bir manzildan boshqasiga o‘tkazish bilan bog‘liq operatsiya. |
| 3 | **Kriptografiya** | **Криптография** | **Cryptography** | Axborotni himoyalash, maxfiyligini ta’minlash va uning haqiqiyligini tekshirish usullarini o‘rganuvchi soha. |
| 4 | **Kriptografik kalit** | **Криптографический ключ** | **Cryptographic Key** | Ma’lumotlarni shifrlash, deshifrlash yoki raqamli imzoni yaratish va tekshirishda ishlatiladigan maxsus qiymat. |
| 5 | **Raqamli imzo** | **Цифровая подпись** | **Digital Signature** | Elektron ma’lumotning yaxlitligi va uning muayyan kalit egasi tomonidan imzolanganini tekshirish imkonini beruvchi kriptografik mexanizm. |
| 6 | **Blokcheyn tarmog‘i** | **Сеть блокчейна** | **Blockchain Network** | Tugunlar o‘zaro aloqa qiladigan va blokcheyn ma’lumotlarini almashadigan tizim. |
| 7 | **Konsensus** | **Консенсус** | **Consensus** | Tarmoq ishtirokchilarining ma’lumotlar yoki bloklarning haqiqiyligi bo‘yicha umumiy kelishuvga erishish mexanizmi. |
| 8 | **Mayning** | **Майнинг** | **Mining** | Ayrim blokcheynlarda tranzaksiyalarni tekshirish va yangi |

| | | | | |
|---|---|---|---|---|
| | | | | bloklarni yaratish jarayoni. |
| 9 | **Mayner** | **Майнер** | **Miner** | Mayning asosida ishlaydigan blokcheyn tarmog‘ida hisoblash ishlarini bajarib, blok yaratishda qatnashuvchi ishtirokchi. |
| 10 | **Aqlli shartnoma** | **Смарт-контракт** | **Smart Contract** | Belgilangan shartlar bajarilganda blokcheyn platformasida avtomatik ishlaydigan dasturiy kod. |
| 11 | **Kriptovalyuta** | **Криптовалюта** | **Cryptocurrency** | Kriptografik usullardan foydalanadigan raqamli aktiv. |
| 12 | **Bitcoin** | **Биткоин** | **Bitcoin** | Markazlashmagan raqamli pul tizimi bo‘lib, uning tranzaksiyalari blokcheyn orqali qayd etiladi. |
| 13 | **Tranzaksiyalar bloki** | **Блок транзакций** | **Transaction Block** | Bir yoki bir nechta tranzaksiya haqidagi ma’lumotlarni o‘z ichiga oladigan blok. |
| 14 | **Kiberxavfsizlik** | **Кибербезопасность** | **Cybersecurity** | Axborot tizimlari, tarmoqlar va ma’lumotlarni raqamli tahdidlardan himoyalash choralari. |
| 15 | **Hamyon** | **Криптовалютный кошелёк** | **Cryptocurrency Wallet** | Kriptografik kalitlarni boshqarish va blokcheyndagi raqamli aktivlar bilan operatsiyalarni amalga oshirish vositasi. |