**Universitatea Tehnica a Moldovei**

**Анализ использования технологии блокчейн**

**Analiza utilizării tehnologiei blockchain**

**Analysis of the use of blockchain technology**

|  |  |
| --- | --- |
| Student: | gr. TI-196, |
|  | Șarafudinov Nicolae |
|  |  |
| Coordonator: | Cernei Irina |
|  | asistent universitar |

Chisinau, 2023

**MINISTERUL EDUCATIEI ȘI CERCETARII**

**Universitatea Tehnica a Moldovei**

**Facultatea Calculatoare Informatica si Microelectronica**

**Departamentul Ingineria Software și Automatica**

Admis la sustinere

Sef de departament:

Fiodorov I. dr., conf.univ.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

„\_\_\_” mai\_\_\_\_\_ 2023

**Analiza utilizării tehnologiei blockchain**

**Proiect de licenta**

|  |  |  |
| --- | --- | --- |
| **Student:** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **Șarafudinov Nicolae, TI-196** |
| **Coordonator:** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **Cernei Irina, asis. univ.** |
| **Consultant:** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **Cernei Irina, asis. univ.** |

**Chisinau, 2023**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică şi Microelectronică Departamentul Ingineria Software și Automatică Programul de studii Tehnologia Informaţiei**

**Aprob**

**şef de departament**

**Fiodorov Ion, dr.conf.univ.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**„ 30” octombrie 2022**

**CAIET DE SARCINI**

**pentru proiectul de licenţă al studentului**

***Șarafudinov Nicolae***

*(numele şi prenumele studentului)*

1. **Tema proiectului de licenţă** *Анализ использования технологии блокчейн*

**confirmată prin hotărârea Consiliului facultăţii nr***. 1* **din** *„30” octombrie 2022*

1. **Termenul limită de prezentare a proiectului de licență** *20.05.2023*
2. **Date iniţiale pentru elaborarea proiectului de licență** *Sarcina pentru elaborarea proiectului de diplomă.*
3. **Conţinutul memoriului explicativ**

*Введение*

1. *Анализ предметной области*
2. *Практическое применение технологии блокчейн*

*Заключение*

1. **Conţinutul părţii grafice a proiectului de licență**

*Imaginea generală a sistemului, Înterfața de bază a sistemului, …….*

1. **Lista consultanţilor:**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Confirmarea realizării activităţii** | |
| **Consultant** | **Capitol** |  |  |
| **Semnătura** | **Semnătura** |
|  |  |
|  |  | **consultantului (data)** | **studentului** |
| *I. Șarafudinov* | *Standarde tehnologice, Controlul* |  |  |
|  | *calităţii* |  |  |
|  |  |  |  |

1. **Data înmânării caietului de sarcini** *02.09.2022*

**Coordonator** *Cernei Irina* **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*semnătura*

**Sarcina a fost luată pentru a fi executată de către studentul** *Șarafudinov Nicolae*

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** *02.09.2023*

*semnătura, data*

**PLAN CALENDARISTIC**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nr. crt. | Denumirea etapelor de proiectare | | Termenul de realizare a etapelor | Nota |  |
| 1 | Получение задания, выбор темы проекта | | 02.09.19 – 30.09.19 | 10% |  |
| 2 | Анализ предметной области | | 01.10.19 – 30.11.19 | 20% |  |
| 3 | Изучение сферы применения | | 01.12.19 – 25.12.19 | 20% |  |
| 4 | Определение наиболее важных сегментов темы | | 16.01.20 – 14.03.20 | 25% |  |
| 5 | Описание примеров | | 15.03.20 – 10.04.20 | 10% |  |
| 6 | Моделирование примеров | | 11.04.20 – 20.04.20 | 10% |  |
| 7 | Подведение итогов затронутого материала | | 21.04.20 – 08.05.20 | 5% |  |
|  |  |  |  |  |  |
|  |  | Student | Șarafudinov Nicolae | ( | ) |
|  |  | Coordonator de proiect de licență | Cernei Irina | ( | ) |

**DECLARAŢIA STUDENTULUI**

Subsemnatа Șarafudinov Nicolae, declar pe proprie răspundere că lucrarea de faţă este rezultatul muncii mele, pe baza propriilor cercetări şi pe baza informaţiilor obţinute din surse care au fost citate şi indicate, conform normelor etice, în note şi în bibliografie. Declar că lucrarea nu a mai fost prezentată sub această formă la nici o instituţie de învăţământ superior în vederea obţinerii unui grad sau titlu ştiinţific ori didactic.

Semnătura autorului

**UNIVERSITATEA TEHNICĂ A MOLDOVEI**

**FACULTATEA CALCULATOARE, INFORMATICĂ ŞI MICROELECTRONICĂ DEPARTAMENTUL INGINERIA SOFTWARE ȘI AUTOMATICĂ PROGRAMUL DE STUDII TEHNOLOGII INFORMAŢIONALE**

**AVIZ**

la proiectul de licenţă

**Titlul:** Анализ использования технологии блокчейн

Студент Шарафудинов Николай гр. TI-196

1. **Actualitatea temei:** блокчейн-технология имеет потенциал изменить способ, которым люди взаимодействуют и проводят бизнес в целом. Технология блокчейн имеет множество преимуществ и может помочь улучшить многие аспекты нашей жизни поэтому было написано данное исследование.
2. **Caracteristica proiectului de licenţă:** было рассмотрено огромное множество вариантов где может применяться технология блокчейн и описано почему и зачем демонстрируя важность темы.
3. **Analiza prototipului:** Рассмотрев данную технологию становиться понятно где ее можно применить наилучшим образом для достижения огромных результатов в различных сферах.
4. **Estimarea rezultatelor obţinute:** Это технология прекрасно демонстрирует себя как в медицине так и в государственной деятельности такие как голосования или же образование.
5. **Corectitudinea materialului expus:** Представляемый в работе материал и указанные в ней ссылки на источники информации, написанные людьми с опытом работы в сфере информационных технологий.
6. **Calitatea materialului grafic:** Исследование подкрепляется как и сравнительными таблицами так и графическими изображениями описывающие тот или иной процесс или же объект.
7. **Valoarea practică a proiectului:** Данная технология не привязана к конкретному типу устройств и может использоваться как пожелает разработчик.
8. **Observaţii şi recomandări:** Требования к дипломному проекту были полностью соблюдены, Замечаний нет.
9. **Caracteristica studentului şi titlul conferit:** Студент, Шарафудинов Николай, проявил индивидуальность и профессионализм при создании дипломного проекта, доказал целесообразность исследования продукта, смог соблюсти все поставленный департаментом цели и требования.

Din cele relatate, urmează că lucrarea de licenţă poate fi admisă spre susţinere, cu nota \_\_\_\_\_\_\_\_\_

***Lucrarea în forma electronică corespunde originalului prezentat către susținere publică.***

**Coordonatorul proiectului de licenţă** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Cernei Irina, asis.univ**

*semnătura, data*

**АННОТАЦИЯ**

Целью данного дипломного проекта являлось создание фундамента знаний о технологии блокчейн. Данная исследовательская работа является обозревателем или же гидом в мире блокчейна. Основное достоинство блокчейна заключается в его возможности обеспечить безопасную и прозрачную передачу данных, что может помочь устранить проблемы, связанные с централизованными системами хранения данных. Благодаря своей децентрализованной природе, блокчейн-технология может предотвратить возможность манипулирования данными, что повышает доверие и уменьшает риски для бизнеса и потребителей. Суть работы заключается в изучении проблем и перспектив использования блокчейн-технологии в различных отраслях и сферах деятельности, а также в оценке ее влияния на экономику, социальные отношения и общество в целом.

Первая глава посвящена анализу предметной области. Прежде чем приступить к обсуждение где и как применяется технология блокчейн и как она влияет на различные сферы деятельности человека, необходимо понять чем же является блокчейн, из чего он состоит и как работает.

Вторая глава «Практическое применение технологии блокчейн». В данной главе рассмотрена более техническая составляющая нежели в первой. Во второй главе рассмотрен симулированный блокчейн позволяющий более точно понять работу с ним и в нем. Также помимо Эмуляции блокчейна показана также модель Смарт контракта о которой подробнее рассказано перед реализацией во второй главе.

Частью реализации стало рассмотрение распределенных приложений а так же разные виды токенов созданных на основе блокчейна.

В завершение были подведены итоги всех этапов исследований, сформулировано лаконичное и ёмкое заключение.

**REZUMAT**

Scopul acestui proiect de absolvire a fost de a crea o bază de cunoștințe despre tehnologia blockchain. Această lucrare de cercetare este un observator sau un ghid în lumea blockchain-ului. Principalul avantaj al blockchain-ului constă în capacitatea sa de a oferi transfer de date sigur și transparent, ceea ce poate ajuta la eliminarea problemelor asociate cu sistemele centralizate de stocare a datelor. Datorită naturii sale descentralizate, tehnologia blockchain poate preveni posibilitatea manipulării datelor, ceea ce crește încrederea și reduce riscurile pentru întreprinderi și consumatori. Esența lucrării este de a studia problemele și perspectivele utilizării tehnologiei blockchain în diverse industrii și domenii de activitate, precum și de a evalua impactul acesteia asupra economiei, relațiilor sociale și societății în ansamblu.

Primul capitol este dedicat analizei temei. Înainte de a discuta unde și cum este utilizată tehnologia blockchain și cum afectează diverse domenii ale activității umane, este necesar să înțelegem ce este blockchain-ul, în ce constă și cum funcționează.

Al doilea capitol este „Aplicarea practică a tehnologiei Blockchain”. În acest capitol este luată în considerare o componentă mai tehnică decât în ​​primul. În al doilea capitol, este luată în considerare un blockchain simulat, care vă permite să înțelegeți mai precis lucrul cu acesta și în el. De asemenea, pe lângă Emularea Blockchain, este prezentat și un model de Contract Smart, care este descris mai detaliat înainte de implementare în capitolul al doilea.

O parte a implementării a fost luarea în considerare a aplicațiilor distribuite, precum și a diferitelor tipuri de jetoane create pe baza blockchain-ului.

În concluzie, au fost rezumate rezultatele tuturor etapelor cercetării, s-a formulat o concluzie concisă și amplă.

**ABSTRACT**

The purpose of this graduation project was to create a foundation of knowledge about blockchain technology. This research paper is an observer or a guide in the world of blockchain. The main advantage of blockchain lies in its ability to provide secure and transparent data transfer, which can help eliminate the problems associated with centralized data storage systems. Due to its decentralized nature, blockchain technology can prevent the possibility of data manipulation, which increases trust and reduces risks for businesses and consumers. The essence of the work is to study the problems and prospects of using blockchain technology in various industries and fields of activity, as well as to assess its impact on the economy, social relations and society as a whole.

The first chapter is devoted to the analysis of the subject area. Before discussing where and how blockchain technology is used and how it affects various areas of human activity, it is necessary to understand what blockchain is, what it consists of and how it works.

The second chapter is "Practical Application of Blockchain Technology". In this chapter, a more technical component is considered than in the first. In the second chapter, a simulated blockchain is considered, which allows you to more accurately understand the work with it and in it. Also, in addition to Blockchain Emulation, a Smart Contract model is also shown, which is described in more detail before implementation in the second chapter.

Part of the implementation was the consideration of distributed applications, as well as different types of tokens created on the basis of the blockchain.

In conclusion, the results of all stages of the research were summed up, a concise and capacious conclusion was formulated.

Содержание

[ВВЕДЕНИЕ 11](#_Toc131367511)

[1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ 12](#_Toc131367512)

[1.1 Актуальность выбранной темы 12](#_Toc131367513)

[1.2 Общая характеристика блокчейна 12](#_Toc131367514)

[1.3 Методы взаимодействия с блокчейном 12](#_Toc131367515)

[1.4 Виды блокчейн технологий 12](#_Toc131367516)

[1.5 Виды Узлов 12](#_Toc131367517)

[1.6 Алгоритмы консенсуса 12](#_Toc131367518)

[1.7 Блокчейн в сравнение с базой данных и облаком 12](#_Toc131367519)

[1.8 Сферы применения Блокчейн технологии 12](#_Toc131367520)

[1.9 Пример применения блокчейн технологий в образовании 12](#_Toc131367521)

[1.10 Токены 12](#_Toc131367522)

[1.11 Виды токенов 12](#_Toc131367523)

[1.12 NFT искусство 12](#_Toc131367524)

[1.13 Плюсы и Минусы использования блокчейн технологии 12](#_Toc131367525)

[2 ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН 12](#_Toc131367526)

[2.1 Как работает блокчейн. 12](#_Toc131367527)

[2.2 Эмуляция блокчейна 12](#_Toc131367528)

[2.3 Смарт-контракты 12](#_Toc131367529)

[2.4 Смарт-контракт принцип работы 12](#_Toc131367530)

[2.5 Пример создания смарт контракта 12](#_Toc131367531)

[2.6 Dapp – распределенные приложения 12](#_Toc131367532)

[2.7 Мошенничество с децентрализованными приложениями 12](#_Toc131367533)

[ЗАКЛЮЧЕНИЕ 13](#_Toc131367534)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 14](#_Toc131367535)

# ВВЕДЕНИЕ

Ориентируясь на материал, предоставленный по предмету «Анализ и спецификация требований к программному обеспечению» а также материалы по предмету «Проектирование информационных систем» первым делом для создания курсовой работы было решено, что необходимо выявить и описать высокоуровневые требования к информационной системе в соответствии с выбранной темой.

Выбранной темой, является «Анализ использования технологии блокчейн». Рассматривая данную тему было затронуто множество таких аспектов которые описывают саму технология блокчейн так и сферы ее применения. В ходе исследования было определено две основные главы такие как «Анализ предметной области» и «Практическое применение технологии блокчейн». В первой главе рассматривается общее описание того что такое блокчейн из чего он состоит, какие алгоритмы есть и где применяется в том или ином случае. Во второй же главе рассмотрена симуляция блокчейна. Наглядно демонстрируется и описывается технология блокчейн и так же внутренние механизмы такие как смарт контракты.

Блокчейн (blockchain) в настоящее время рассматриваются как одно из наиболее важных достижений начала XXI в., способные коренным образом изменить экономические взаимоотношения между их участниками. Последние несколько лет технология распределенного реестра (distributed ledger technology, DLT), в частности блокчейн (blockchain), не только активно обсуждается, но и плотно внедряется в большинстве развитых стран во многих областях экономики. Блокчейн уже используют для хранения и обработки персональных данных и идентификации, в маркетинге и компьютерных играх. Многие организации ставят своей целью разобраться в возможном применении технологии как для поиска путей развития бизнеса, так и для оптимизации текущих процессов для сокращения издержек.

В 2008 г. в большинстве стран с развитой экономикой начался финансово-экономический кризис, спровоцировавший стремительное снижение основных экономических показателей. В результате, финансовые инструменты и учреждения, банковские институты и государство утратили доверие населения, что в свою очередь стимулировало развитие инновационной технологии – блокчейна. Отличительная особенность новейшей технологии, заключается в том, что она не требует привлечения контрагентов при заключении договоров, позволяя совершать сделки без посредников в лице государства, банков, юристов и бухгалтеров, а также без взимания комиссий, и, более того, являясь абсолютно анонимной.

# АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

В данной главе будет рассмотрено множество важных тем, без которых понимание темы без которых понимание темы будет невозможным. Рассмотрим такие темы как, актуальность темы, общая характеристика, методы и взаимодействие с блокчейном, а также перечислены типы, после чего рассмотрим сферы применения.

## Актуальность выбранной темы

Перед тем как перейти к вышеперечисленным темам необходимо рассмотреть определения основных терминов, а именно блокчейн и реестр.

Блокчейн — это система записи информации таким образом, чтобы ее было невозможно изменить, взломать или обмануть. По сути, Блокчейн, как следует из самого названия, представляет собой цепочку блоков. Каждый блок содержит в себе набор из совершенных в течение определенного периода времени (в биткоине это в среднем 10 минут) транзакций. Транзакции в сети биткоин представляют собой записи, которые фиксируют передачу какого-либо количества биткоинов от одного пользователя другому.

Каждый последующий блок имеет временную метку и ссылку на предыдущий блок. Так же в блок заносится не сама транзакция, а 32-битное значение, обозначенное, в случае биткойна, как корень меркла (merkle\_root). Помимо хеша от набора транзакций, блок содержит так называемый заголовок (block header), уникальный для каждого блока. Его уникальность достигается за счет того факта, что каждый заголовок является значением хеш-функции, носящей название SHA256, от информации, хранящейся в нем: списка транзакций (корня меркла), временной метки создания блока, версии текущего алгоритма, текущей сложности вычисления блока, nonce, а также, от заголовка предыдущего блока. Таким образом, через последовательный учет заголовков предыдущих блоков в вычислении заголовка нового осуществляется их связь, создается цепочка блоков.

Реестр – можно представить по-разному, и при этом все сведётся к тому, что реестр своего рода запись систематизирующая, учитывающая. Также реестр известен как книга для регистрации дел, документов и т. п. В бухгалтерском учёте составляется реестр карточек для аналитического учёта. На основе реестра была создана технология распределенного реестра — тот же реестр, хранящий информацию, но, при этом он не имеет центрального управляющего, также такой метод использования реестра способствует совместному использованию и предоставляет возможность синхронизировать информацию согласно алгоритму консенсуса. Самое важное в технологии распределенного реестра — это возможность распределение в разных географических точках как показано на рисунке 1.1.

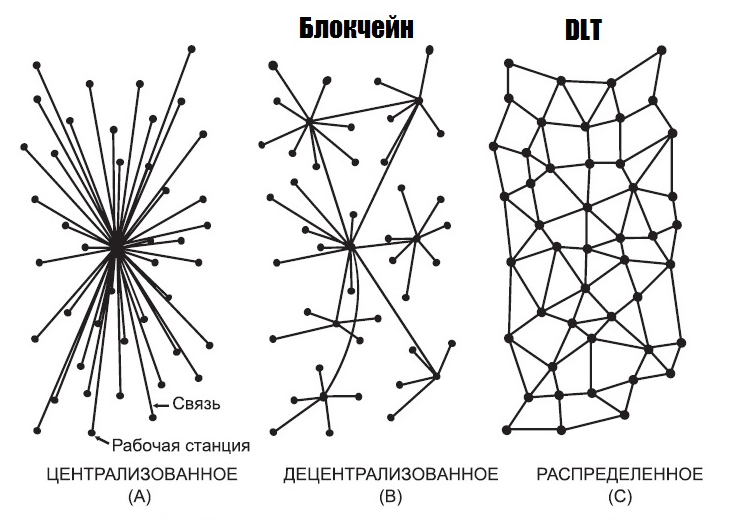


Рисунок 1.1-Три разных типа программных приложений [26]

Определившись с основными понятиями, вернемся к теме «Актуальность блокчейна».

Понятие блокчейн обозначает технологию распределенного хранения блоков данных, которые связываются в упорядоченные цепочки. Сегодня Блокчейн внедряется во многие интернет-системы, потому что эта технология обеспечивает достоверность и защищенность сохраненных сведений. И для того, чтобы достичь быть достоверной и защищенной системой блокчейн использует следующие методы:

* сложные и трудно решаемые математические алгоритмы;
* алгоритмы шифрования;
* количество участников сети, ведь чем их больше тем безопаснее сеть.

Взломать блокчейн возможно, теоретически, но на данный момент времени человечество еще не развило технологии чтобы взломать на практике, так как никакой доход не покроет огромных расходов на глобальную атаку. Из-за своей высокой безопасности и достоверности блокчейн, как «цепи блоков», является очень привлекательной технологией для разных компаний в разных областях.

Чем же Блокчейн актуален? А тем, что в современном мире обычные или же традиционные технологии баз данных создают ряд проблем, связанных с учетом финансовых операций. Для примера рассмотрим пример с продажей недвижимости. Право собственности переходит к покупателю после передачи денег. Как продавец, так и покупатель, могут регистрировать денежные операции, но ни одной из сторон нельзя доверять. Продавец может легко утверждать, что он денег не получил, а покупатель может утверждать, что деньги отправлены, даже если это не так.

Для того чтобы не избежать возможных юридических проблем необходимо доверяться третьим сторонам, которые должны контролировать и подтверждать транзакции. Тем самым доверяя поддержание транзакции третьем лицам система становиться централизованной что создает уязвимость в лице данного третьего лица.

Блокчейн способствует предотвращению вышеописанного примера путем создания защищенной от несанкционированного доступа, децентрализованной системы. В случае сделки с недвижимостью в блокчейн системе создаётся единый реестр для продавца и покупателя. Транзакции должны быть одобрены обеими сторонами в ином случае транзакция не будет добавлена в блок и не будет нести в себе никакого смысла. Записи автоматически обновляются в их реестрах в режиме реального времени. Любое несоответствие в истории транзакций отразится во всем реестре так как записи не будут соответствовать, а точнее хэш суммы блоков. Эти свойства технологии блокчейн сделали ее популярной в различных секторах.

## Общая характеристика блокчейна

Важной особенностью блокчейна является программный механизм, который обеспечивает передачу уникальных экземпляров ценности (денег, имущества, контрактов, идентификационных данных и т.д.) через интернет без необходимости привлечения сторонних посредников, таких как банки или государственные учреждения. Поэтому следует выделить некоторые важные характеристики блокчейна

**Децентрализованная сеть:** все участники сети могут проверять транзакции. Майнеры являются основными участниками этой децентрализованной сети и работают над решением вычислительных задач, которые позволяют создавать, проверять и надежно хранить транзакции.

**Криптография:** позволяет сторонам сохранять конфиденциальность информации, которую они передают друг другу.

**Временная метка:** каждой транзакции в блокчейне присваивается временная метка, которая не может быть изменена после ее записи.

## Методы взаимодействия с блокчейном

Блокчейн, переведя дословно получим что это цепь блоков, соответственно необходимо разобраться в том, что такое блок. Блок – это структура данных в базе данных блокчейна, в которую непрерывно записываются данные о транзакциях крипто-валютного блокчейна. В блоках записываются некоторые или все последние транзакции, которые не были проверены сетью. После проверки данных блок закрывается. Затем создается новый блок для включения и подтверждения новых транзакций.

Таким образом, блок – это постоянное хранилище файла, которое нельзя изменить или удалить после его записи.

Блок – это место в цепочке блоков, где хранится и шифруется информация. Блоки идентифицируются длинным номером и содержат зашифрованную информацию о транзакциях из предыдущих блоков и информацию о новых транзакциях. Блоки и информация в них должны быть подтверждены сетью перед созданием новых блоков. Блоки и блочные цепи используются не только для криптовалют. Они также используются для различных других целей.

Как работает блокчейн

Блокчейн работает следующим образом: каждый раз, когда новая транзакция добавляется в блок, она проверяется на достоверность с помощью сложных алгоритмов шифрования и децентрализованной системы проверки. Когда блок заполнен транзакциями, он добавляется в цепочку блоков и получает хэш предыдущего блока в цепочке. Это обеспечивает безопасность и надежность данных, так как любые изменения в предыдущих блоках автоматически вызывают изменения в следующих блоках, что делает подделку цепочки блоков практически невозможной.

В сетях блокчейн наблюдается большое количество транзакций. При использовании для криптовалют он ведет учет этих транзакций, чтобы знать, сколько было потрачено, сколько не было потрачено, и какие стороны были вовлечены. Транзакции, происходящие в течение определенного периода времени, записываются в записи, называемые блокчейн, которые являются основой сетей блокчейн, показано на рисунке 1.2.

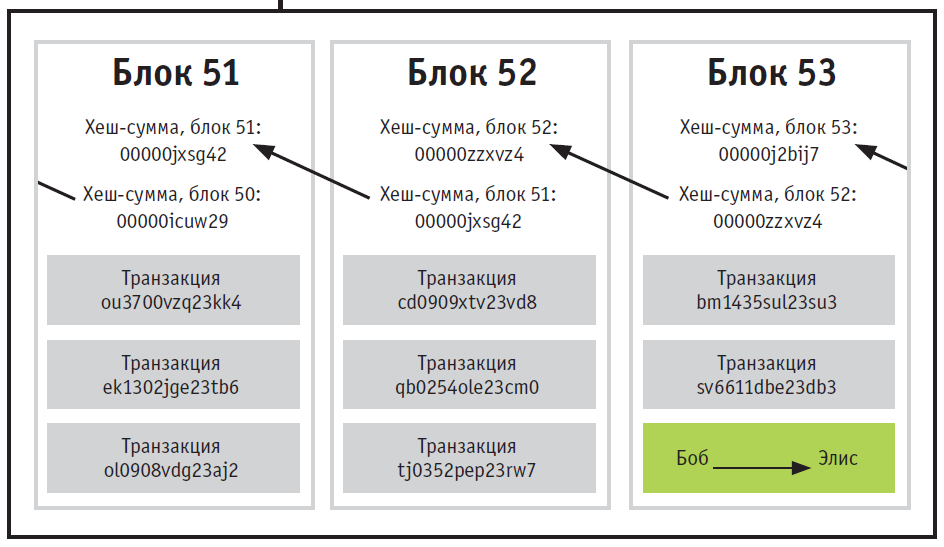


Рисунок 1.2 – Структура блоков в цепи [27]

Блокчейн хранит информацию. Блоки содержат много информации, это видно в рисунке 1.3, но их емкость не очень велика.

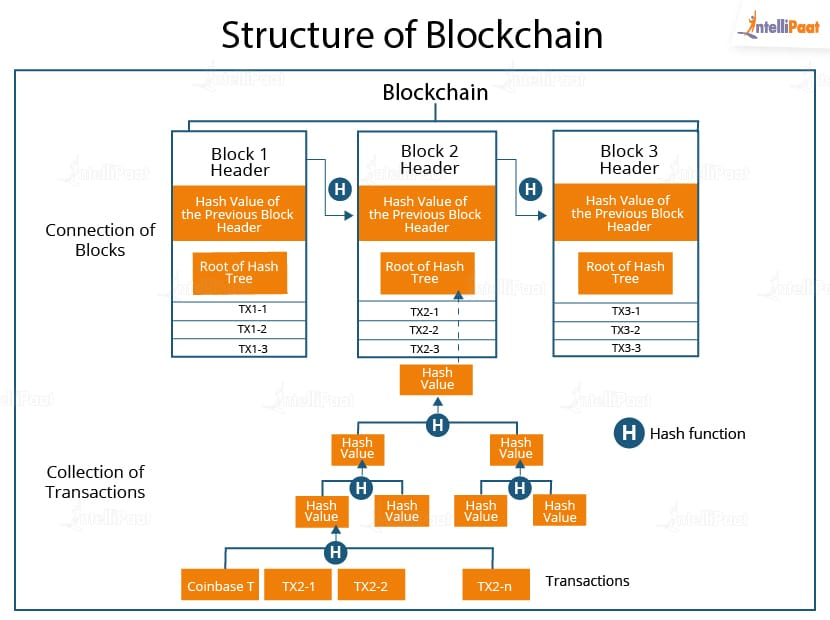


Рисунок 1.3 – Структура блокчейна [12]

Блок включает в себя:

* магическое число;
* размер блока;
* заголовок блока;
* счетчик транзакций;
* транзакции.

Поясним каждый элемент. Магическое число – это число, содержащее конкретное значение, которое идентифицирует блок как часть определенной крипто валютной сети. Размер блока – это ограничение на размер блока, чтобы можно было записать только определенный объем информации. Заголовок блока содержит информацию о блоке. Счётчик транзакций – это число, указывающее на количество транзакций, хранящихся в блоке. Список транзакций – это список всех единиц общения между двумя людьми в блоке.

Элемент транзакции является самым большим, поскольку содержит наибольшее количество информации. За ним следует заголовок блока, в зависимости от размера хранилища, и содержит следующие под-элементы:

* версия;
* хэш предыдущего блока;
* markle root hash;
* время;
* бит;
* nonce.

Дадим краткое пояснение каждого элемента. Версия в заголовке блока демонстрирует версию используемую криптовалютой. Так же в заголовке хранится хэш предыдущего блока - хэш (зашифрованное число) заголовка предыдущего сохраненного блока. Следующим не менее важным элементом заголовка блока является Markle Root hash хэш-значение транзакции в дереве Меркле текущего блока. Помимо вышеуказанных элементов в заголовке блока хранятся такие значения как время - метка времени для размещения блока в цепочке блоков, бит - уровень сложности целевого хэша, который указывает на сложность взлома числа один раз, а также изменяемое число nonce - зашифрованное число, которое майнеры должны взломать, чтобы подтвердить и закрыть блок, строение блоков, схематически все это продемонстрировано на рисунке 1.4.

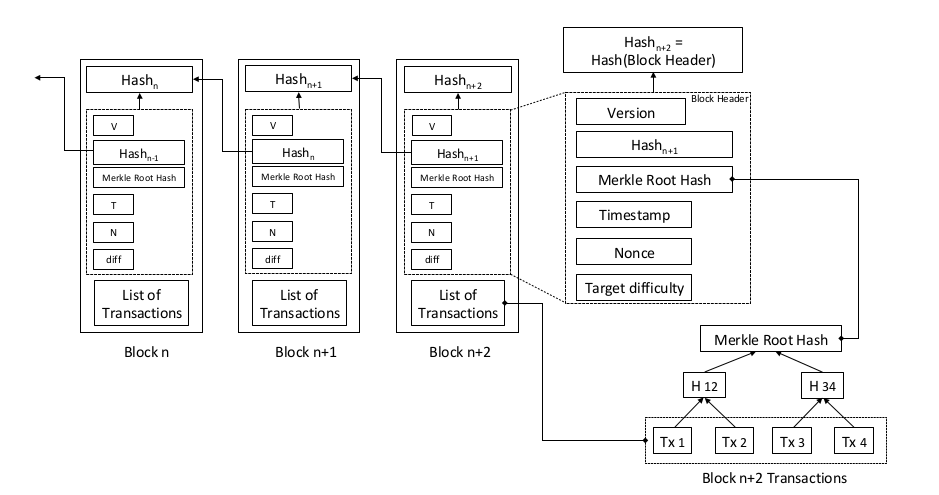


Рисунок 1.4 – Структура блоков в блокчейне [28]

## Виды блокчейн технологий

В блокчейне существует четыре основных типа децентрализованных и распределенных сетей.

**Публичные блочные цепи.**

Публичные блокчейны не требуют лицензий, и любой желающий может присоединиться к сети. Все участники блокчейна имеют равные права на чтение, обработку и проверку информации. Публичные блокчейны в основном используются для обмена и добычи криптовалют, таких как Bitcoin, Ethereum и Litecoin.

**Частные блокчейны.**

Частные блокчейны, также известные как управляемые блокчейны, управляются одним субъектом. Уполномоченная организация решает, кто может быть участником и какие права он имеет в сети. Частные блокчейны могут быть децентрализованы лишь частично, поскольку они включают ограничения доступа. Примером частного блокчейна является платформа обмена цифровых валют Ripple.

**Гибридные блокчейны.**

Гибридные блокчейны сочетают в себе функции частных и публичных сетей. Компании могут создавать частные и государственные системы лицензирования. Таким образом, они могут контролировать доступ к некоторым данным в блокчейне, сохраняя открытый доступ к другим. Они используют смарт-контракты, которые позволяют публичным участникам проверять подлинность частных транзакций. Например, гибридные блокчейны могут обеспечить публичный доступ к цифровым валютам, сохраняя при этом частный доступ к банковским валютам.

**Консорциум блокчейн.**

Блокчейн-консорциумы управляются группой организаций. Организации по умолчанию разделяют ответственность за эксплуатацию блокчейна и определение прав доступа к данным. Блокчейн-консорциумы часто предпочитают компании-единомышленники, которым выгодна совместная ответственность. Например, Global Shipping Business Network – это некоммерческий консорциум по блокчейну, призванный оцифровать судоходную отрасль и способствовать сотрудничеству между участниками судоходства.

Бывают также и другие разделения сетей блокчейн, которые сочетают в себе свойства как открытых, так и закрытых сетей.

блокчейн можно разделить по различным признакам:

**по объектам транзакций:**

* информация;
* виртуальная ценность (ценность, аналог которой отсутствует в «реальном мире» — например, bitcoin);

**по типу доступа к сети:**

* неограниченный (сети, в которых участникам позволено осуществлять любую деятельность);
* ограниченный (сети, которые ограничивают виды деятельности участников);

**по требованиям к прохождению идентификации:**

* анонимная;
* псевдоанонимная;
* полная идентификация;

**по применяемому протоколу достижения консенсуса сети:**

* PoW (Proof-of-work);
* PoS (Proof-of-stake);
* PoS + PoW;
* PBFT (Practical Byzantine Fault Tolerance), Paxos, RAFT;
* Non-BFT (Non-Byzantine Fault Tolerance).

**по наличию центрального администратора:**

* существует центральный администратор;
* отсутствует центральный администратор.

Виды блокчейн продемонстрированы на рисунке 1.5.

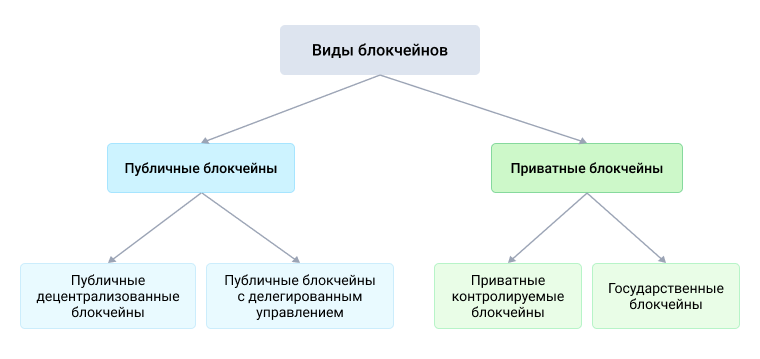


Рисунок 1.5 – Классификация блокчейн [11]

Важно отметить, что это считается новой технологической парадигмой. Технология блокчейн объединяет несколько концептуально различных идей, включая децентрализованные реестры хранения данных, алгоритмы консенсуса и криптографические механизмы защиты данных. Технология блокчейн основана на логике хранения данных, которая не зависит от центрального сервера или группы серверов. Эта технология формирует и хранит отсортированный список записей, называемых блоками. Поскольку каждый блок содержит временную метку и, что более важно, уникальный образ (хэш) предыдущего блока, технология "связывает" блоки данных вместе и предотвращает фальсификацию сформированных блоков без изменения всей последовательности блоков.

## Виды Узлов

Узел — это любой компьютер, который подключен к блокчейну, проверяющий и подтверждающий транзакции, а также хранит копию блокчейна. Узлы обеспечивают безопасность блокчейна, даже при условии, когда узел отключен от сети «offline node», или же подключена к сети непостоянно то при подключении, данные узлы должны загрузить обновлённые копии реестра для синхронизации с сетью. Синхронизируя свои хранилища с данными о последних транзакциях, большее количество узлов делает внесение изменений невозможным, а также не оставляет хакеру шансов остаться незамеченным. Хакер не сможет удалить данные с множества различных узлов, что значит — вся информация в безопасности. Более того, узлы сортируются по их доступности и в соответствии с их состоянием, в сети или же нет, принимается решение непрерывно отправляет данные в сеть или же игнорировать узлы, не подключенные к сети.

В зависимости от роли конкретного узла, он может либо:

* Принимать или отклонять транзакции.
* Проверка и управление транзакциями.
* Шифрование и хранение информации в блоках.
* Общайтесь с другими блоками как с точками связи.

Отдельные узлы могут играть различные роли. Например, некоторые узлы запрограммированы на подтверждение транзакций, в то время как другие отвечают только за регистрацию транзакций. Узлы также могут обмениваться данными друг с другом.

Кроме того, узлы классифицируются в зависимости от их доступности. Онлайн-узлы" постоянно отправляют данные в сеть. Они всегда являются активными узлами. С другой стороны, "автономные узлы" — это узлы, которые периодически подключаются к сети. Эти узлы должны загрузить обновленную копию реестра и синхронизировать ее с сетью при подключении.

Стоит также отметить, что каждый узел имеет уникальный идентификатор, присвоенный устройству, к которому он подключен. Этот уникальный идентификатор позволяет пользователям идентифицировать конкретные узлы в сети. Узлы организованы таким образом, что каждый имеет полный доступ к записям транзакций. Пользователи могут легко отслеживать транзакции, используя свои идентификаторы в блокчейне.

Поэтому узлы играют важную роль в сетях блокчейн, поскольку без них сети блокчейн не существовали бы, виды узлов или же узлов показаны на рисунке 1.6.

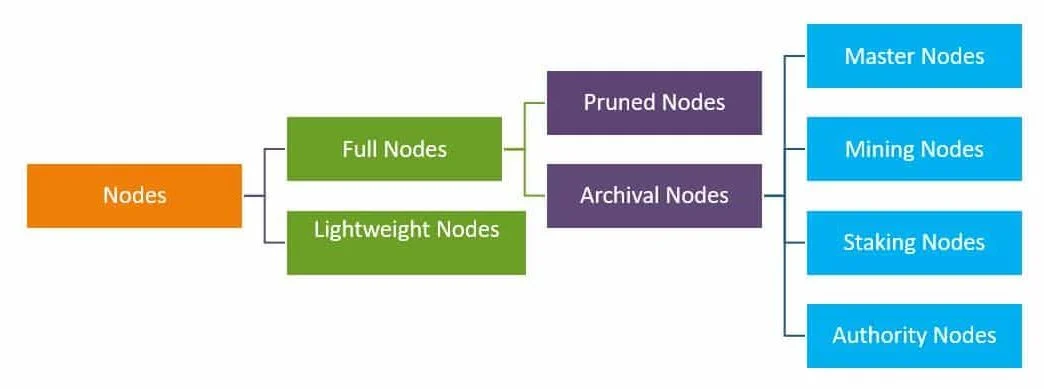


Рисунок 1.6 – Виды узлов блокчейна [13]

Полные узлы действуют как сервер в децентрализованной сети. В их основные задачи входит поддержание консенсуса между другими узлами и проверка транзакций. Они также хранят копию блокчейна, что позволяет безопасно активировать пользовательские функции, такие как мгновенная отправка и частные транзакции. При принятии решений о будущем сети полные узлы голосуют за предложения.

Сокращение полных узлов: Характерной чертой здесь является то, что эти узлы начинают загружать блоки с самого начала, и как только они достигают установленного предела, самые старые удаляются, сохраняя только их заголовки и размещение в цепочке.

Архивные полные узлы: это то, что большинство людей имеют в виду, когда говорят о полных узлах. Эти узлы представляют собой сервер, на котором размещается полная цепочка блоков в базе данных.

По сравнению с полными узлами, сами главные узлы не могут добавлять блоки в блокчейн. Их единственная цель — вести учет транзакций и подтверждать их. Будь то узлы майнинга или стейкинга, именно они создают блоки в блокчейне.

С другой стороны, узлы облегченной или простой проверки платежей (SPV) используются в повседневных операциях с криптовалютой. Эти узлы взаимодействуют с блокчейном, полагаясь на полные узлы для предоставления им необходимых наборов информации. Они не хранят копию блокчейна, а только запрашивают текущий статус последнего блока. Кроме того, они транслируют транзакции другим узлам в сети для обработки.

## Алгоритмы консенсуса

Алгоритмы консенсуса работают на основе распределенных систем, в которых участвуют множество узлов (нод), каждый из которых выполняет определенную функцию в сети. Различные алгоритмы консенсуса имеют свои специфические аспекты реализации, но общий процесс работы алгоритмов консенсуса можно описать следующим образом:

1. Начало нового раунда: каждый узел в сети начинает новый раунд консенсуса.
2. Предложение блока: один из узлов предлагает новый блок для добавления в цепочку блоков.
3. Рассылка блока: предложенный блок рассылается всем другим узлам в сети.
4. Подтверждение блока: каждый узел проверяет предложенный блок и решает, подтверждать его или нет. Если узел подтверждает блок, он начинает работу над следующим блоком, используя свой уникальный идентификатор.
5. Выбор блока: узлы собирают голоса и выбирают блок, который будет добавлен в цепочку. В зависимости от конкретного алгоритма, выбор может быть основан на вычислительной мощности, количестве монет, которыми владеет узел, или на других факторах.
6. Добавление блока: узлы достигают консенсуса и добавляют выбранный блок в цепочку.
7. Завершение раунда: раунд консенсуса завершается, и сеть готова к началу следующего раунда.

Технические детали реализации алгоритмов консенсуса могут быть сложными и разнообразными, но общая цель - обеспечить достоверность данных и защиту от атак в распределенной среде, где нет центрального узла управления.

Механизм консенсуса представляет собой некий компьютерный алгоритм, который лежит в основе распределенного реестра. Благодаря данному алгоритму децентрализованные узлы сети достигают согласия о текущем состоянии данных во всех блоках [3]. Алгоритм консенсуса необходим для проверки корректна ли транзакция, в противном транзакция не проходит. Помимо проверки транзакций алгоритм консенсуса применяется в добавление новых блоков. Другой важной задачей механизма консенсуса является разрешение конфликтов между некоторыми противоречащими транзакциями, проводимыми одновременно. Ситуация, когда два майнера одновременно сгенерировали подходящие блоки, вызывает раздвоение цепи блоков. Тогда главной цепочкой будет считаться та, ответвление которой будет быстрее продолжено. Для криптовалюты разработали механизмы консенсуса, которые позволяют решать проблемы мошенничества децентрализовано. Множество алгоритмов консенсуса находятся еще в процессе создания, а наибольшую популярность приобрел механизм консенсуса Proof-of-Work (доказательство выполнения работы).

На сегодня существует определенное количество алгоритмов консенсуса и периодически появляются новые. Разные алгоритмы используются в зависимости от конкретных целей и задач, которые ставят перед собой разработчики при построении блокчейна. Основная причина, подталкивающая разработчиков к совершенствованию алгоритмов и разработке новых — это желание решить трилемму блокчейна. Давайте рассмотрим некоторые наиболее распространённые из алгоритмов консенсуса, использующиеся сегодня в блокчейнах как показано на рисунке 1.7.

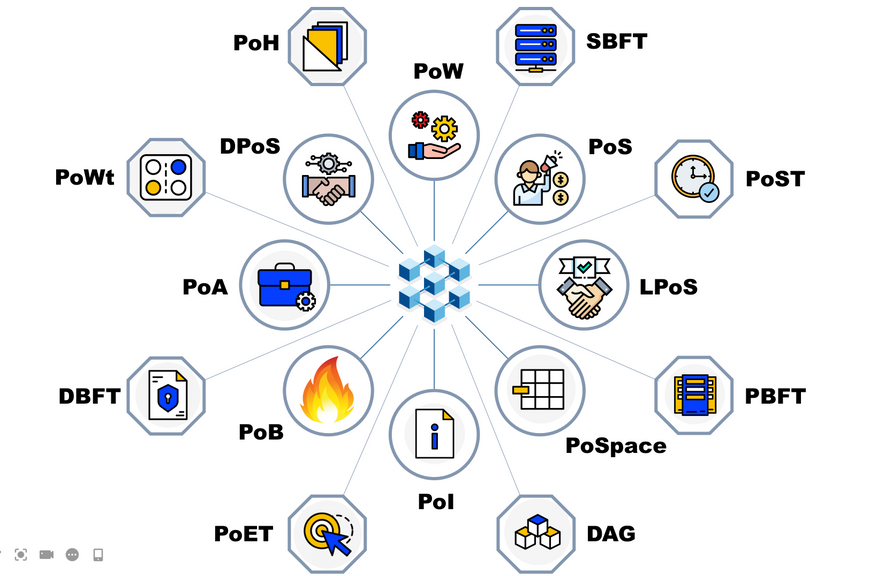


Рисунок 1.7 – Виды алгоритмов консенсусов [12]

Широко известный термин “дилемма” предполагает ситуацию с необходимостью выбора между двумя разными исходами/возможностями, которые нередко противоречат друг другу или характеризуются противоположными по влиянию последствиями. Трилемма подразумевает три таких исхода/возможности, и, применительно к блокчейну, относится к трём его основным свойствам, описанным выше: масштабируемости, децентрализации и безопасности.

Дело в том, что для обеспечения безопасности необходимо шифрование, эта процедура (процесс майнинга, алгоритм консенсуса Proof-of-Work) занимает определенное время, каждый узел владеет копией всего блокчейна и шифрует все транзакции. Пропускная способность такой сети очень низкая, а значит страдает масштабируемость.

Можно уйти от шифрования в сторону валидации транзакций несколькими надежными нодами (Deligated Proof-of-Stake), но так как нодой не может стать любой желающий, участников в сети гораздо меньше, чем при алгоритме PoW, таким образом страдает децентрализация.

В ходе развития технологии блокчейн и применения новых алгоритмов стали появляться различные мультичейны, в них осуществляется связь с различными блокчейнами через протоколы кроссчейн-коммуникации. Такие сети быстрые, (то есть масштабируемые), вполне себе децентрализованные, но их безопасность существенно ниже, чем у классических блокчейнов с алгоритмом консенсуса PoW.

Таким образом трилемма блокчейна показанная на рисунке 1.8 состоит в том, что невозможно одновременно добиться высоких показателей основных характеристик сети: масштабируемости, децентрализации и безопасности. Усиление одной характеристики автоматически ослабляет другую. При создании блокчейна приходится выбирать, чем жертвовать.

Одна из первых работ на эту тему была опубликована еще в 90-х годах прошлого века Эриком Брюэром, профессором в Беркли, он сформулировал "теорему CAP", которая гласила, что у распределенного реестра (частным случаем которого и является блокчейн) может быть только две характеристики их трёх основных, это - Последовательность (Consistency), Доступность (Availability) и Делимость (Partition).

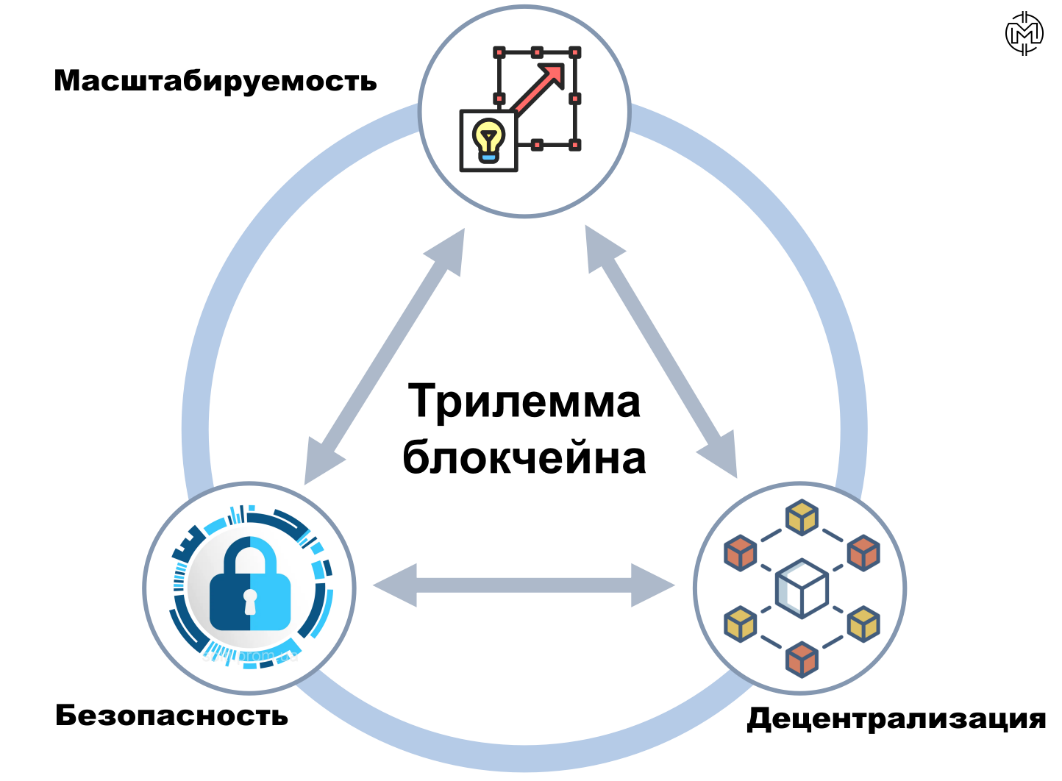


Рисунок 1.8 – Трилемма блокчейна [12]

Рассмотрим несколько алгоритмов консенсуса:

**Proof-of-Work (PoW)**

Это самый известный и один из самых распространённых алгоритмов консенсуса. По сути, с этого алгоритма и началось развитие отрасли. Proof-of-Work расшифровывается как "доказательство работы".

При формировании очередного блока узел (майнер) выполняет большое количество математических расчетов по поиску хеша криптографической функции, который в свою очередь предоставляет сети в качестве доказательства проделанной работы (вычислений).

PoW стал прорывом для своего времени и позволил запустить первые криптовалюты. Алгоритм PoW используется, например, в блокчейне Bitcoin. Он обеспечивает отличный уровень децентрализации (любой желающий может присоединиться к сети и стать майнером) и безопасности (Bitcoin практически невозможно взломать, объём вычислительных мощностей, понадобившихся бы для взлома, на практике сегодня просто невозможно собрать). Это основные преимущества алгоритма PoW, но есть и недостатки:

высокие затраты электроэнергии. С ростом сети и особенно, если алгоритмом предусмотрена какая-нибудь инфляционная модель, сложность майнинга увеличивается, компьютеры потребляют больше энергии, соответственно растут и совокупные энергозатраты сети

низкая пропускная способность. Необходимость выполнения большого количества вычислений требует существенных временных затрат, поэтому пропускная способность сети при реализации алгоритма PoW невысока

высокие комиссии. С развитием сетей на PoW появился эффект централизации. Отдельные майнеры стали объединяться в пулы для повышения результативности майнинга, сложность майнинга стала повышаться, комиссии за транзакции стали избыточно высокими для массового использования

Недостатки базового аглоритма PoW стимулировали сообщество к поиску поиску новых решений, так стали появляться новые алгоритмы консенсуса.

**Proof-of-Stake (PoS)**

Второй по популярности алгоритм консенсуса, расшифровывается как "доказательство доли владения". В PoS нет майнинга, вместо вычислительных мощностей в качестве доказательств выступают определенные “замороженные” объемы криптовалют, принадлежащие соответствующим узлам. Эти узлы называются нодами или валидаторами, их объём замороженной криптовалюты - стейком, и чем больше у конкретного узла криптовалюты, тем выше вероятность подтвердить транзакцию, а значит, получить вознаграждение.

На алгоритме PoS работают многие известные блокчейны, например Etherium (версия 2.0, после недавнего перехода с Pow на Pos), Binance Smart Chain, Cardano, Tron и другие.

PoS лишен таких недостатков PoW, как высокое энергопотребление, необходимость специализированного/мощного оборудования. Комиссии в сетях PoS ниже, а пропускная способность гораздо выше. Однако у PoS есть и недостатки. Главный из них - угроза централизации. Есть риск консолидации большого объёма криптовалюты ограниченным количеством валидаторов, в этом случае они будут иметь возможность влиять на сеть.

**Delegated Proof-of-Stake (DPoS)**

Это разновидность вышеописанного алгоритма PoS, расшифровывается как "делегированное доказательство доли владения". Основное отличие алгоритма от классического Pos - это попытка избавить алгоритм от его основного недостатка, то есть от риска централизации. В DPoS право валидаторов одобрять транзакции делегируется им держателями монет, при этом держатели голосуют за того или иного валидатора. Любой участник сети, обладающий определенным объёмом криптовалюты, может стать валидатором, но также в любой момент голоса за этого валидатора могут быть отозваны в пользу другого. DPoS в свою очередь также не лишён недостатков. В частности, риск представляет низкая активность участников сети, тогда DPoS превращается в PoS, ну и сговор делегатов тоже не исключён.

Среди известных блокчейнов с алгоритмом DPoS такие как EOS, Tezos и другие.

**Leased Proof-of-Stake (LPoS)**

Этот алгоритм также является модификацией классического PoS, расшифровывается как "арендованное доказательство доли владения". Алгоритм отличается от PoS и DPoS тем, что доля криптовалюты может быть арендована. При LPoS валидаторами могут стать даже мелкие участники. Все участники сети могут передавать (делегировать) свою криптовалюту соответствующим валидаторам. При этом непосредственно переводов не происходит, криптовалюта остаётся в кошельках у владельцев, но замораживается. Естественно, токеномикой блокчейнов предусматриваются механизмы мотивации для всех участников сети. LPoS не убирает риск централизации. При этом алгоритме крупные валидаторы могут арендовать достаточное количество криптовалюты для монополизации сети. Пример использования LPoS - блокчейн Waves.

**Proof-of-Authority (PoA)**

Это алгоритм консенсуса сети, который основывается на “авторитете” валидаторов. Расшифровывается как "доказательство полномочий". В качестве доказательств валидаторы используют собственную репутацию. Валидаторы выбираются участниками сети путём голосования, обычно их количество фиксировано. В отличии от PoS и DPoS валидаторы не получают награды за стейкинг, это основной недостаток PoA, у валидаторов отсутствуют стимулы и мотивации для участия, поэтому чаще всего алгоритм PoA используется в частных блокчейнах, где вопрос децентрализации не сильно актуален.

**Proof-of-Importance (PoI)**

Этот алгоритм основывается на “значимости” валидатора ("доказательство значимости"). При подтверждении транзакций алгоритм принимает во внимание не только объём “замороженных” средств в криптовалюте, но и активность валидатора. Оцениваются такие параметры, как количество проведённых транзакций, время в сети (доступность онлайн). Чем больше доля валидатора и его активность, тем значимее он для сети. Один из примеров блокчейнов, которые используют PoI - NEM.

**Proof-of-Space (PoSpace)**

Это алгоритм, основанный на дисковом пространстве, он так и расшифровывается: “доказательство пространства”. В качестве основного ресурса для доказательства участники используют свободное пространство своих жёстких дисков, которое резервируется под специальные функции блокчейна, например заполнение хеш-кодами для последующей валидации блоков. На этом алгоритме работает Burstcoin.

**Proof-of-Space-Time (PoST)**

Это разновидность алгоритма Proof-of-Space, которая учитывает ещё и время. Основная мысль создателей в том, что вклад участников в сеть важно оценивать не только по делегированному дисковому пространству, но также и по затратам времени, на протяжении которого это дисковое пространство было делегировано. На этом алгоритме работает Chia.

**Proof-of-Elapsed-Time (PoET)**

Это алгоритм консенсуса от компании Intel, расшифровывается как "доказательство затраченного времени". Алгоритм основан на использовании набора инструкций Software Guard Extension центрального процессора Intel. Принцип работы похож на лотерею, при “майнинге” генерируется случайное время ожидания для блока, нода “засыпает” ровно на это время, первая проснувшаяся нода получает право валидации блока. SGX следит за тем, чтобы время выбиралось действительно случайным образом.

Данный алгоритм не распространён, он используется в частных блокчейнах и требует обязательного наличия процессоров Intel с набором инструкций SGX.

**Proof-of-Burn (PoB)**

Этот алгоритм подразумевает “сжигание” криптовалюты, он так и расшифровывается: “доказательство сжигания”. При PoB майнер отправляет криптовалюту на специальный “тупиковый” кошелёк (к этому кошельку, например, отсутствуют приватные ключи, то есть нет доступа). Таким образом определённый объём криптовалюты выводится из обращения, то есть “сжигается”. После доказательства сжигания для майнера увеличивается вероятность получить право создания следующего блока и, соответственно, получить за это награду.

Для майнинга при PoB не требуется больших вычислительных мощностей, а сжигание криптовалюты стимулирует рост цены этой криптовалюты, потому что как правило эмиссия ограничена. Этот алгоритм очень специфичен, подходит далеко не каждому блокчейну. Он используется, например, в XCP.

## Блокчейн в сравнение с базой данных и облаком

Блокчейн — это особая система управления базами данных с более широкими возможностями.

Блокчейн подразумевает децентрализованный контроль без потери доверия к существующим данным. Этого невозможно достичь в других системах баз данных. Компании, участвующие в сделке, не могут использовать базу данных совместно. Но в блокчейн-сетях у каждой компании есть своя копия реестра, а их соответствие поддерживается системой автоматически. Хотя в большинстве баз данные можно редактировать или удалять, в блокчейн их можно только вносить.

Термин «облако» относится к вычислительным сервисам, доступ к которым можно получить онлайн. Из облака можно получить доступ к программному обеспечению как услуге (SaaS), продукту как услуге (PaaS), а также к инфраструктуре как услуге (IaaS). Облачные провайдеры предоставляют онлайн-доступ к своему оборудованию и инфраструктуре. Они предоставляют гораздо больше простого управления базами данных. Для получения доступа к публичному блокчейну необходимо предоставить данные об аппаратном обеспечении для создания копии вашего реестра. При этом для этого можно использовать облачный сервер. Также некоторые провайдеры предлагают готовое решение —блокчейн как услуга (BaaS). Что такое Блокчейн как услуга?

Это стороннее создание и управление облачными сетями для организаций для разработки приложений на основе блокчейна. Эти услуги представляют собой новую эволюцию в области технологии блокчейн. За прошедшие годы блокчейн начал свое облачное путешествие. Технология блокчейна вышла за пределы своего самого популярного использования в криптовалюте и стала широко распространенной для свидетелей всех видов транзакций. Более того, появление бизнес-модели BaaS является крупным событием и важной вехой для организаций. Блокчейн как услуга позволяет всем типам предприятий получать доступ к технологиям блокчейна без вложений в собственные разработки. Модель BaaS позволяет организациям получить доступ к услугам поставщика блокчейна, в котором они могут разрабатывать приложения блокчейна с минимальными затратами. Это преимущество сделало его неотъемлемой частью тренда технологии блокчейн, как показано на рисунке 1.9.

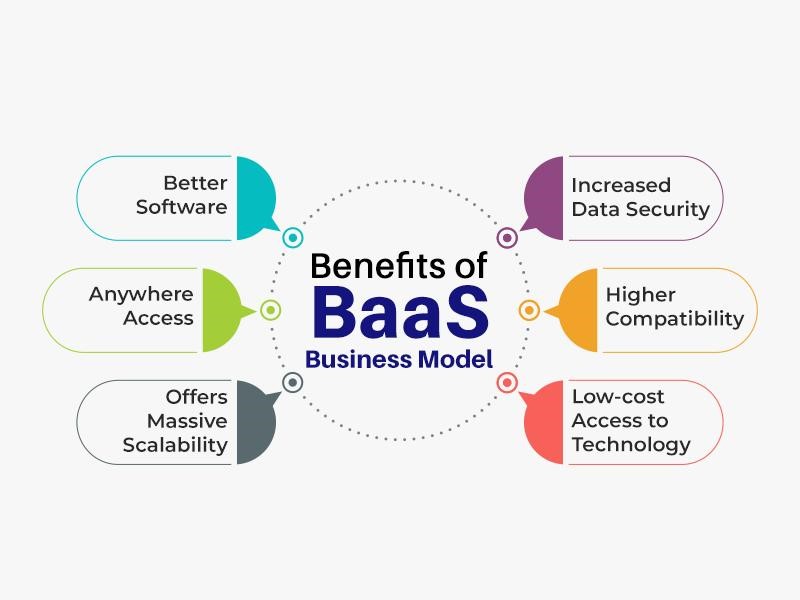


Рисунок 1.9 – Блокчейн как услуга. [14]

## Сферы применения Блокчейн технологии

Блокчейн — это развивающаяся инновационная технология, которая находит применение в различных отраслях. Вот несколько примеров его стандартизированного использования в различных отраслях промышленности

**Энергия**.

Энергетические компании используют технологию блокчейн для создания одноранговых платформ для энергетических транзакций, облегчая доступ к возобновляемым источникам энергии. В качестве примера рассмотрим следующий вариант использования.

Энергетическая компания с поддержкой блокчейна создала торговую платформу для продажи электроэнергии между физическими лицами. Домовладельцы с солнечными батареями используют платформу для продажи излишков солнечной энергии жителям соседних домов. Этот процесс в значительной степени автоматизирован: "умные" счетчики совершают транзакции, а блокчейн их отслеживает.

Краудфандинговые инициативы через блокчейн позволяют пользователям финансировать и обслуживать солнечные панели в районах, не имеющих доступа к электричеству. Спонсоры также получают лизинговые платежи за солнечные панели после их установки.

**Мультимедиа и развлечения**

Мультимедийные и развлекательные компании используют блокчейн для управления данными об авторских правах. Проверка авторских прав играет важную роль в определении соответствующих выплат авторам. Для отслеживания продажи и передачи контента, защищенного авторским правом, требуется проведение множества операций. Sony Music Entertainment Japan использует блокчейн-сервисы для повышения эффективности технических средств защиты авторских прав. Успех стратегии блокчейн позволил повысить эффективность защиты авторских прав при одновременном снижении затрат.

**Розничная торговля.**

Розничные компании используют блокчейн для отслеживания перемещения товаров между поставщиками и клиентами. Например, компания Amazon подала патент на систему распределенной бухгалтерской книги, которая использует технологию блокчейн для проверки подлинности всех товаров, продаваемых на платформе. Amazon позволяет продавцам составить карту своей глобальной цепи поставок и позволяет участникам (производителям, курьерам, дистрибьюторам, конечным и вторичным пользователям) добавлять события в бухгалтерскую книгу после регистрации в удостоверяющем центре.

**Денежные переводы.**

Первоначальная концепция изобретения технологии блокчейн по-прежнему находит широкое применение. Денежные переводы с использованием блокчейна могут быть дешевле и быстрее, чем с использованием существующих сервисов денежных переводов. Это особенно верно в отношении трансграничных транзакций, которые часто бывают медленными и дорогостоящими. Даже в современной финансовой системе США денежные переводы между счетами могут занимать дни, а транзакция в блокчейне — минуты.

**Финансовые обмены.**

За последние несколько лет появилось много компаний, предлагающих децентрализованные биржи криптовалют. Использование блокчейна для обмена позволяет проводить более быстрые и менее дорогие транзакции. Более того, децентрализованная биржа не требует, чтобы инвесторы вносили свои активы в централизованный орган, что означает, что они сохраняют больший контроль и безопасность. В то время как биржи на основе блокчейна в основном имеют дело с криптовалютой, эта концепция может быть применена и к более традиционным инвестициям.

**Кредитование.**

Кредиторы могут использовать блокчейн для выполнения обеспеченных кредитов через смарт-контракты. Смарт-контракты, построенные на блокчейне, позволяют определенным событиям автоматически запускать такие вещи, как оплата услуг, маржин-колл, полное погашение кредита и освобождение от залога. В результате обработка кредита происходит быстрее и дешевле, а кредиторы могут предлагать более выгодные ставки.

**Страхование.**

Использование смарт-контрактов на блокчейне может обеспечить большую прозрачность для клиентов и страховых компаний. Запись всех заявок в блокчейн не позволит клиентам делать дубликаты заявок по одному и тому же событию. Кроме того, использование смарт-контрактов может ускорить процесс получения платежей заявителями.

**Недвижимость.**

Сделки с недвижимостью требуют тонны документов для проверки финансовой информации и права собственности, а затем передачи документов и титулов новым владельцам. Использование технологии блокчейн для записи транзакций с недвижимостью может обеспечить более безопасные и доступные средства проверки и передачи права собственности. Это может ускорить транзакции, сократить бумажную работу и сэкономить деньги.

**Защитите личную информацию.**

Хранение данных, таких как ваш номер социального страхования, дата рождения и другая идентифицирующая информация, в общедоступном реестре (например, в блокчейне) может быть на самом деле более безопасным, чем существующие системы, более уязвимые для взлома. Технология блокчейн может быть использована для защиты доступа к идентифицирующей информации, а также для улучшения доступа для тех, кто в ней нуждается в таких отраслях, как путешествия, здравоохранение, финансы и образование.

**Голосование.**

Если личная идентификационная информация хранится в блокчейне, это делает нас всего в одном шаге от возможности голосовать с использованием технологии блокчейна. Использование технологии блокчейна может гарантировать, что никто не проголосует дважды, что только правомочные избиратели смогут голосовать, а голоса нельзя будет подделать. Более того, он может расширить доступ к голосованию, сделав его простым нажатием нескольких кнопок на вашем смартфоне. В то же время стоимость проведения выборов существенно снизится.

**Государственные льготы.**

Другой способ использования цифровых удостоверений, хранящихся в блокчейне, — это управление государственными льготами, такими как программы социального обеспечения, социального обеспечения и Medicare. Использование технологии блокчейн может снизить мошенничество и стоимость операций. Между тем, бенефициары могут быстрее получать средства за счет цифровых выплат в блокчейне.

Безопасно делитесь медицинской информацией

Хранение медицинских записей в блокчейне может позволить врачам и медицинским работникам получать точную и актуальную информацию о своих пациентах. Это может гарантировать, что пациенты, обращающиеся к нескольким врачам, получат наилучшую возможную помощь. Это также может ускорить систему извлечения медицинских карт, что в некоторых случаях позволяет проводить более своевременное лечение. А если информация о страховании хранится в базе данных, врачи могут легко проверить, застрахован ли пациент и покрывается ли его лечение.

**Гонорары художникам.**

Использование технологии блокчейн для отслеживания музыкальных и кинофайлов, распространяемых через Интернет, может гарантировать, что артистам будут платить за их работу. Поскольку технология блокчейна была изобретена для обеспечения того, чтобы один и тот же файл не существовал более чем в одном месте, ее можно использовать для борьбы с пиратством. Более того, использование блокчейна для отслеживания воспроизведений в потоковых сервисах и смарт-контракта для распределения платежей может обеспечить большую прозрачность и уверенность в том, что артисты получат причитающиеся им деньги.

**Не взаимозаменяемые токены.**

Не взаимозаменяемые токены или NFT обычно рассматриваются как способ владения правами на цифровое искусство. Поскольку блокчейн предотвращает существование данных в двух местах, размещение NFT в блокчейне гарантирует, что существует только одна копия произведения цифрового искусства. Это может сделать его похожим на инвестиции в физическое искусство, но без недостатков хранения и обслуживания.

У NFT могут быть разные приложения, и, в конечном счете, это способ передать право собственности на все, что может быть представлено данными. Это может быть документ на дом, права на трансляцию видео или метка события.

**Хранение данных.**

Добавление технологии блокчейна в решение для хранения данных может обеспечить большую безопасность и целостность. Поскольку данные могут храниться децентрализовано, будет сложнее взломать и стереть все данные в сети, тогда как поставщик централизованного хранилища данных может иметь только несколько точек резервирования. Это также означает более широкий доступ к данным, поскольку доступ не обязательно зависит от операций одной компании. В некоторых случаях использование блокчейна для хранения данных также может быть дешевле.

**Азартные игры.**

Индустрия азартных игр может использовать блокчейн, чтобы предоставить игрокам ряд преимуществ. Одним из самых больших преимуществ работы казино на блокчейне является прозрачность, которую оно обеспечивает потенциальным игрокам. Поскольку каждая транзакция записывается в блокчейн, игроки могут видеть, что игры честные, а казино выплачивает. Кроме того, при использовании блокчейна нет необходимости предоставлять личную информацию, включая банковский счет, что может стать препятствием для некоторых потенциальных игроков. Это также обеспечивает обход нормативных ограничений, поскольку игроки могут играть анонимно, а децентрализованная сеть не подвержена закрытию правительства.

Технология блокчейн имеет широкий спектр практических применений, вот некоторые из них:

Криптовалюты: блокчейн был создан для поддержки биткоина и других криптовалют. Блокчейн позволяет создавать цифровые валюты, которые могут быть переданы между пользователями без необходимости промежуточных посредников, таких как банки.

Смарт-контракты: блокчейн также позволяет создавать смарт-контракты, которые автоматически выполняются при определенных условиях. Это может быть полезно для обеспечения безопасности и эффективности в различных отраслях, например, в сфере недвижимости или медицинской индустрии.

Идентификация: блокчейн может быть использован для создания цифровых идентификаторов, которые могут быть использованы в различных ситуациях, например, для подтверждения личности при открытии банковского счета или для входа в систему электронного голосования.

Передача данных: блокчейн может использоваться для безопасной передачи данных между пользователями. Это может быть особенно полезно для компаний, которые должны передавать конфиденциальную информацию, такую как медицинские записи или финансовые данные.

Логистика: блокчейн может быть использован для отслеживания товаров на всех этапах поставки, начиная от производства до доставки. Это может помочь компаниям улучшить эффективность своей логистической цепочки и сократить затраты.

Социальная сфера: блокчейн может быть использован для улучшения эффективности социальных программ, таких как пособия по безработице или пенсионные выплаты. Благодаря технологии блокчейн можно точнее определять, кому нужна помощь, и предоставлять ее более быстро и эффективно.

Это лишь некоторые из примеров практического применения технологии блокчейн. Блокчейн может быть использован в различных отраслях и для различных целей, и его потенциал только начинает раскрываться.

## Пример применения блокчейн технологий в образовании

В начале мая 2019 года 18 учебных заведений Сингапура решили выдавать студентам цифровые дипломы при помощи блокчейн-технологии.

Эта инициатива входит в общенациональный проект под названием OpenCerts, который развивается совместно Министерством образования Сингапура, Государственным технологическим агентством, а также национальным образовательным движением SkillsFuture Singapore при участии высшего учебного учреждения Ngee Ann Polytechnic.

Использование блокчейна устранит две важные проблемы: наличие физического документа, который может быть утерян или подделан, и необходимость запросов на его проверку. Вся информация, необходимая для проверки дипломов и других сертификатов, будет храниться в защищенной от несанкционированного доступа блокчейн-платформе OpenCerts.

Студенты могут использовать цифровые дипломы, чтобы устроиться на работу или поступить в другой университет. В идеале использование блокчейна также должно снизить затраты, связанные с созданием традиционных бумажных дипломов, и повысить общую эффективность системы.

Ежегодно университет выдает более 4 тысяч дипломов и других сертификатов. Процесс проверки их подлинности может быть достаточно трудоемким. По планам введение такого типа дипломов ускорит процессы приема на работу и приема новых студентов. Работодатели будут тратить меньше времени на то, чтобы узнать о полученном образовании и знаниях кандидата.

Кроме того, полученные дипломы и сертификаты выпускники смогут сразу загрузить в свои профили в LinkedIn. Чтобы реализовать свой план, университет договорился о сотрудничестве со стартапом Attores, выпускником акселератора FinLab. Будет использовано программное обеспечение, разработанное компанией Parity Technologies.

Помимо образования, Сингапур планирует перевести на блокчейн и энергетику. Кроме того, на финтех-конференции Money20/20 Asia представители Денежно-кредитного управления Сингапура рассказали об успешном завершении эксперимента по внедрению технологии блокчейн в сфере внутренних межбанковских переводов. [17]

## Токены

Часто токенами и монетами называют одно и то же, но это не так.

Токен — это единица цифрового актива, которая представляет определенную стоимость или право на доступ к определенным ресурсам или услугам. Токены могут быть использованы в различных контекстах, включая криптовалюты, блокчейн-платформы, краудфандинговые кампании и другие.

Токены могут иметь различные функции в зависимости от их назначения. Например, токены криптовалют могут использоваться для совершения платежей и переводов, в то время как токены блокчейн могут использоваться для голосования и управления ресурсами в децентрализованных сетях.

Токены создаются поверх существующего блокчейна, как, например, Ethereum, Waves и другие, и используются для различных целей, таких как сбор средств, доступ к платформам или представление определенного актива. Токенами можно торговать, их можно покупать и продавать, как и монеты. Они также используются для доступа к определенному приложению или платформе, и зачастую стоимость токенов зависит от их эффективности.

В целом, токен представляет собой цифровую единицу актива, которая имеет определенную стоимость и функциональность в контексте своего использования. [18]

## Виды токенов

Наиболее популярные категории токенов включают:

* токены управления;
* стейблкоины;
* невзаимозаменяемые токены (nft).

**Токены управления.**

Токены управления (Management Tokens) — это цифровые активы, которые предоставляют их владельцам возможность участвовать в управлении проектом или организацией, которая выпустила токены. Эти токены часто используются в рамках децентрализованных проектов, которые работают на блокчейн-технологии.

Владельцы токенов управления могут получать различные привилегии, в зависимости от правил, установленных проектом. Например, они могут иметь право голосовать по вопросам, касающимся развития проекта, или получать дополнительные бонусы и льготы.

Токены управления могут использоваться в различных сферах, включая финансовые услуги, медиа, игровую индустрию и другие. Они могут быть выпущены в качестве части ICO (Initial Coin Offering) или IEO (Initial Exchange Offering) проекта.

В целом, токены управления предоставляют возможность владельцам активно участвовать в управлении проектом и принимать важные решения вместе с другими участниками. Это может помочь усилить децентрализацию и сделать проект более открытым и прозрачным для всех участников.

**Стейблкоины.**

Стейблкоины (Stablecoins) — это тип криптовалюты, цена которой привязана к цене другого актива, например, к фиатной валюте (например, доллар США, евро, юань и т.д.), золоту или другим ресурсам. Они созданы для того, чтобы устранить волатильность и нестабильность цен на криптовалютные рынки, что делает их более предсказуемыми и удобными для использования в повседневной жизни.

Стейблкоины могут быть выпущены на различных блокчейн-платформах, включая Ethereum, EOS, TRON и другие. Они могут быть подкреплены различными активами, такими как фиатные валюты, золото, нефть или другие ресурсы.

Стейблкоины могут иметь различные модели функционирования, например, могут быть выпущены с помощью полной гарантии, когда каждый выпущенный токен поддерживается соответствующим количеством актива, или с помощью фракционной гарантии, когда токены поддерживаются долей в активе.

Стейблкоины могут быть использованы для совершения платежей, переводов, для торговли на криптовалютных биржах, а также для хранения криптовалюты без необходимости менять ее обратно в фиатную валюту. Они также могут использоваться в качестве защиты от волатильности на рынке криптовалют.

**Невзаимозаменяемые токены (NFT)**.

Невзаимозаменяемые токены (NFT) — это уникальные цифровые активы, которые создаются на блокчейн-платформах и не могут быть заменены другими активами в рамках данного блокчейна. Каждый NFT имеет свой уникальный идентификатор, который гарантирует его неповторимость и уникальность.

Основное отличие NFT от других цифровых активов (например, криптовалют) заключается в том, что каждый NFT имеет уникальные свойства, которые определяют его ценность. Например, это может быть цифровое произведение искусства, уникальный предмет в игре или эксклюзивный доступ к какому-то контенту.

NFT используют технологию блокчейн для создания идентификаторов, которые гарантируют уникальность каждого NFT и их историю владения. Таким образом, они обеспечивают уникальность и подлинность цифровых активов, которые были созданы с использованием этой технологии.

NFT могут использоваться в различных сферах, таких как искусство, музыка, игры и другие. Они могут быть проданы на аукционах или торговых площадках, и их ценность может расти в зависимости от популярности и уникальности актива.

## NFT искусство

С помощью NFT можно продать почти любой виртуальный объект — изображения, музыку, тексты, 3D-модели. Но чаще всего речь идет об объектах цифрового (или оцифрованного) искусства.

Одним из наиболее заметных примеров NFT является продажа цифровой картины, показанной на рисунке 1.10, Beeple на аукционе Christie's за 69 миллионов долларов в марте 2021 года.

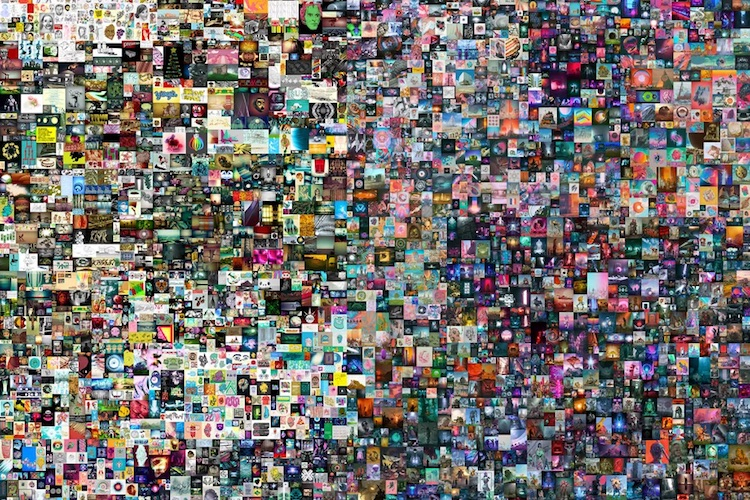


Рисунок 1.10 – Картина "Каждый день — первые 5000 дней". [19]

Как цифровые объекты превращаются в NFT?

Это происходит на специальных платформах, работающих с NFT. Есть несколько популярных площадок — например, Rarible, Mintable, OpenSea. Последняя — самая крупная. Все они являются одновременно NFT-маркетплейсами и NFT-мастерскими.

Для создания токена понадобится кошелек в системе Ethereum, а также файл с цифровым контентом. Обычно алгоритм действий похож на работу с виртуальным фотоальбомом. Просто создаете коллекцию и добавляете в нее медиафайл (или файлы) в любом из доступных форматов — от PNG до MP4. Каждому файлу нужно придумать название и, желательно, описание.

Теперь остается только нажать кнопку Create. Площадка сама создает токен и отправляет его на верификацию. Некоторые платформы делают это с отсрочкой: токен создается уже после того, как на медиаконтент нашелся покупатель.

Схема монетизации у платформ разная: одни берут комиссию с покупателей NFT, другие — с автора (продавца). Размер комиссии тоже отличается — от десятых долей процента до 10% и более процентов от суммы сделки.

NFT, как и блокчейн с криптовалютами, — это всего лишь инструмент. Использовать его можно по-разному. Теоретически, в NFT можно упаковать что угодно, любой цифровой объект.

Сейчас NFT как инструмент активнее всего используют для распространения цифровых коллекционных предметов. «Криптокотики» (CryptoKitties) — популярная игра на блокчейне Ethereum, запущенная в конце 2017 года. Здесь пользователи создают, покупают, продают и разводят виртуальных котят, стартовая страница приложения показана на рисунке 1.11.

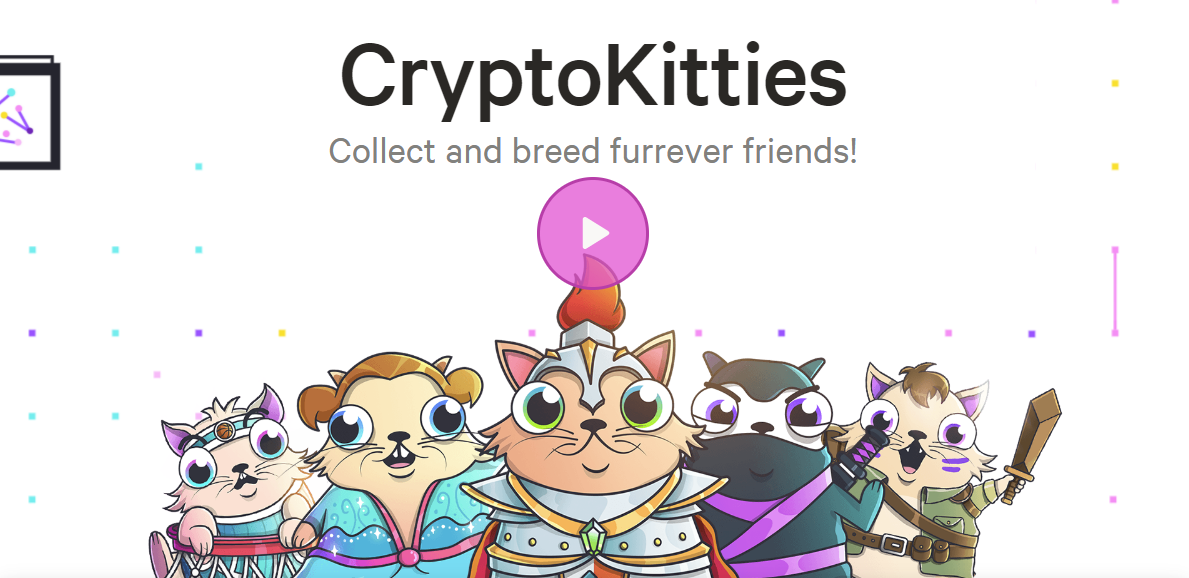


Рисунок 1.11 - Онлайн игра CryptoKitties [21]

Криптокотики, карточки с покемонами, работы Покраса Лампаса, Бэнкси и Beeple прекрасно оцифровываются и, с одной стороны, удовлетворяют тягу людей к коллекционированию, с другой — поддерживают создателей искусства.

В этом же ряду стоят видеокарточки от NBA с хайлайтами баскетбольных матчей: избранные моменты с топовым игроком Джеймсом Леброном продаются в диапазоне от $210 до $179 тыс.

Сюда же можно отнести продажу гифки с мемным котом-печенькой Nyan Cat. Ее создатель Крис Торрес получил благодаря механизму NFT более $560 тыс. в эфирах по текущему курсу. А глава Twitter Джек Дорси продал свой самый первый твит в формате NFT за $2,5 млн.

Потенциально NFT можно использовать как объект инвестиций. По данным NonFungible, в 2020 году объем рынка NFT составил $250 млн. По сравнению с 2019-м показатель вырос почти на 300%.

В 2021 году рынок NFT еще раз рванул вверх. Но как долго продлится этот рост и что будет с ценами на уже реализованные цифровые объекты, предсказать невозможно. Так, за первую половину 2022 года мировой рынок NFT уже дважды заметно «потряхивало».[20]

## Плюсы и Минусы использования блокчейн технологии

Блокчейн-технологии имеют как положительные, так и отрицательные экологические и социальные аспекты.

Одним из наиболее обсуждаемых негативных аспектов блокчейн-технологий является их влияние на потребление энергии. Большинство блокчейн-систем используют концепцию "доказательства работы" (Proof of Work), которая требует большого количества вычислительной мощности и энергии для подтверждения транзакций и создания новых блоков. Это приводит к значительному потреблению энергии и высокому уровню выбросов углекислого газа, что может негативно влиять на окружающую среду и усиливать глобальное потепление.

Однако, некоторые блокчейн-системы используют другие алгоритмы консенсуса, такие как "доказательства ограниченного участия" (Proof of Stake), которые требуют значительно меньше энергии и снижают негативное воздействие на окружающую среду.

С другой стороны, блокчейн-технологии также могут оказывать положительное влияние на экономику и справедливость в обществе. Они позволяют улучшить прозрачность, уменьшить издержки и повысить эффективность в различных сферах, таких как финансы, здравоохранение и право. Кроме того, блокчейн-технологии могут способствовать более справедливому распределению благ и улучшению условий для микропредприятий и малых бизнесов.

**Плюсы блокчейна**

Каждый блокчейн — это реестр с информацией, существующей в виде неизменных блоков, которые можно просматривать и дополнять, но нельзя изменить. С технической точки зрения цепочки блоков отличаются от обычных баз данных, и эти отличия — преимущества технологии блокчейна.

Безопасность

В блокчейне используются криптографические протоколы шифрования, поэтому данные во многих распределенных реестрах надежно защищены. Например, мессенджеры на блокчейне часто используют end-to-end шифрование: прочесть сообщение могут только адресат и отправитель. Также у «цепочек блоков» нет единого сервера, который можно взломать и получить все данные.

Большинство блокчейнов допускают анонимную регистрацию. Например, онлайн-кошельки биткоина не привязаны к паспорту, телефону, имени владельца. Это исключает возможность того, что личность пользователя будет установлена, а его данные и финансовые операции — преданы огласке.

Децентрализация

Информация блокчейна распределена по всей сети. В экосистеме нет «главных» и «второстепенных» компьютеров, и в этом ключевые преимущества системы блокчейн. Нельзя причинить ей вред, выведя из строя несколько устройств. Блокчейн перестанет существовать, только если отключить от Сети все поддерживающие его компьютеры. Поскольку нет «главного» компьютера, сложно получить контроль над системой. Поэтому крупные блокчейны независимы: они не сонтролируются государством, банками и даже компаниями-разработчиками.

Объем и хранение данных

Для создания и поддержания блокчейна не нужны мощные сервера, достаточно создать сеть из обычных компьютеров. При этом данные не пострадают от действий злоумышленников: здесь нет главного хранилища информации, которое можно вывести из строя. Данные в блокчейне невозможно исправить или изменить, поэтому любая информация, добавленная в него, будет храниться в изначальном виде. Но объем хранилища, занимаемого блокчейном, больше, чем у стандартной базы данных. содержащей аналогичную информацию, поэтому по мере роста экосистемы блокчейн должен привлекать новых участников.

Скорость обработки транзакций

Передача данных внутри блокчейна происходит мгновенно. Поэтому он получил популярность в сфере финансов: криптовалюты внутри одной экосистемы можно за секунду перевести любому из её пользователей. Поэтому блокчейн и находит серьезное применение там, где важны скорость и надежность передачи информации. Например, при заключении контрактов на перевозку товаров или в сфере банкинга и финансов.

Широкая область применения

Блокчейн — замена цифровой подписи: он делает ненужными посредников, которые подтверждают подлинность данных. Поскольку информацию в его цифровой системе невозможно изменить и переписать, её подлинность не вызывает сомнений. Это делает блокчейн востребованной и универсальной технологией, обеспечивая широкую сферу его применения.

Блокчейн называют «системой, не требующей доверия»: в нём, отсутствуют риски, связанные с доверием к организации-посреднику, поскольку посредник не нужен. Сделки совершаются напрямую, а информация прозрачна и достоверна. Поэтому блокчейн позволяет не оплачивать услуги «третьей стороны» (банка, нотариуса и т.д.), что существенно снижает затраты.

**Недостатки блокчейна**

Блокчейн также не идеален, и его недостатки не позволяют внедрить его повсюду.

Неизменность данных

В этом не только плюсы блокчейна, но и его минусы: после добавления данных их очень сложно изменить. Поэтому на его базе сложно вести реестры данных, которые могут меняться.

Эффективность

Блокчейны, созданные по принципу биткоина, требуют колоссальных ресурсов для поддержания сети. Сегодня майнинг главной криптовалюты пожирает огромное количество электроэнергии и создает дефицит на рынке компьютерных комплектующих, и любой крупный распределенный реестр ждёт та же судьба. Также со временем реестр нуждается всё в большем дисковом пространстве, и, если его не добавлять, есть риск потерять узлы сети.

Атака 51%

Традиционные методы хакеров в блокчейне не работают, но у него есть свои уязвимости. Одна из них — «Атака 51%»: происходит, когда атакующему удается взять под контроль более 50% всей мощности сети. Это позволяет менять порядок транзакций и отменять их. Пока ни в одном из крупных блокчейнов это не было реализовано на практике, но технически возможность есть.

Технология совершенствуется, и сейчас разработчики преодолевают минусы блокчейна: например, уже разработаны новые алгоритмы консенсуса (базовые принципы работы блокчейнов), которые требуют меньше энергии и дискового пространства. [22]

В целом, экологические и социальные аспекты блокчейн-технологий являются сложными и многогранными. Разработчики и пользователи должны учитывать как их позитивные, так и негативные воздействия на окружающую среду и общество, и работать над созданием более устойчивых и социально ответственных систем на основе блокчейн-технологий.

# ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

В данной главе будет рассмотрено как работает блокчейн как строится блоки и добавляются в сеть, так же будет рассмотрено как работают алгоритмы консенсуса для валидации блоков.

## Как работает блокчейн.

В последние годы вы, возможно, заметили, что многие компании по всему миру интегрируют технологию блокчейн. Но как именно работает технология Blockchain? Это существенное изменение или простое дополнение? Достижения Blockchain все еще молоды и могут стать революционными в будущем. Цель блокчейна — позволить записывать и распространять цифровую информацию, но не редактировать ее. Таким образом, блокчейн является основой для неизменяемых регистров или записей транзакций, которые нельзя изменить, удалить или уничтожить. Вот почему блокчейны также известны как технология распределенного реестра (DLT).

Впервые предложенная в качестве исследовательского проекта в 1991 году, концепция блокчейна предшествовала своему первому широко распространенному применению: биткойн в 2009 году. С тех пор использование блокчейнов резко возросло благодаря созданию различных криптовалют, приложений децентрализованного финансирования (DeFi), невзаимозаменяемые токены (NFT) и смарт-контракты. Блокчейн представляет собой комбинацию трех ведущих технологий:

* криптографические ключи;
* одноранговая сеть, содержащая общий реестр;
* средство вычислений для хранения транзакций и записей сети.

Ключи шифрования состоят из двух ключей — закрытого ключа и открытого ключа. Эти ключи помогают в выполнении успешных транзакций между двумя сторонами. У каждого человека есть эти два ключа, которые он использует для создания безопасной цифровой идентификационной ссылки. Эта защищенная идентификация является наиболее важным аспектом технологии Blockchain. В мире криптовалют эта идентификация называется «цифровой подписью» и используется для авторизации и контроля транзакций.

Цифровая подпись объединяется с одноранговой сетью; большое количество лиц, выступающих в качестве органов власти, используют цифровую подпись, среди прочего, для достижения консенсуса по транзакциям. Когда они разрешают сделку, она подтверждается математической проверкой, что приводит к успешной защищенной транзакции между двумя сторонами, подключенными к сети. Подводя итог, можно сказать, что пользователи блокчейна используют криптографические ключи для выполнения различных типов цифровых взаимодействий в одноранговой сети.

При работе блокчейна первым делом пользователь создает транзакцию, которая может содержать для контрактов записи или другую информацию, после чего транзакция рассылается по узлам peer to peer компьютерной сети. Узлы в этой сети проверяют транзакцию и статус пользователя, используя известные алгоритмы, которые были перечислены ранее. После проверки узлами следует верификация транзакции, и добавление новой транзакции к другим транзакциям для создания блока данных в реестре. Новый блок навсегда добавляется к существующей последовательности блоков, что делает внесение изменений после невозможным. После чего транзакция, совершенная пользователем в первом шаге, будет подтверждена и выполнена, что и показано на рисунке 2.1.

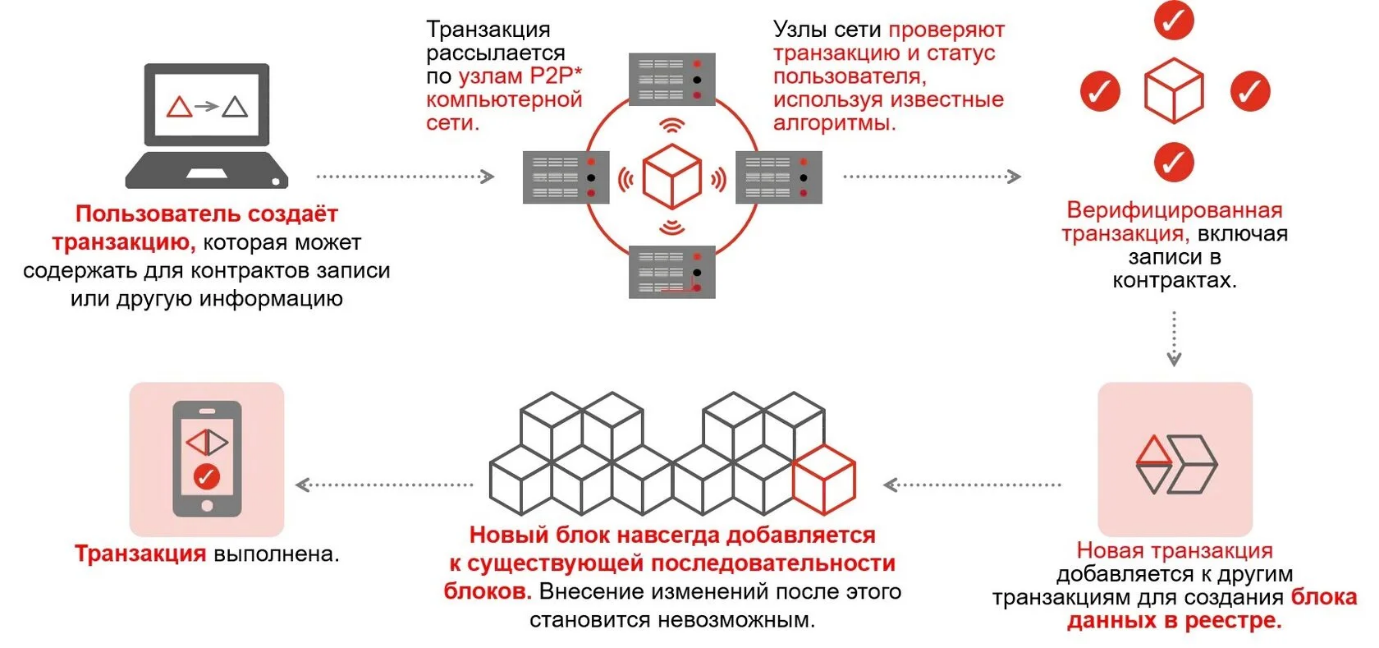


Рисунок 2.1 - Как работает блокчейн [9]

В основном концепцию блокчейна объясняют на примере работы биткойн, поскольку он неразрывно связан с биткойном как показано на рисунке 2.2. Тем не менее, технология блокчейн применима к любым транзакциям с цифровыми активами, которыми обмениваются онлайн. Блокчейн — это децентрализованный распределенный реестр. Говоря человеческим языком — это сеть компьютеров, имеющих идентичную копию базы данных и меняющих свои записи состояния) по общему соглашению, основанному на чистой математике. цифровая валюта, в основе работы которой лежит блокчейн, может создаваться, перемещаться и храниться вне компетенции любого правительства, финансового учреждения или личного юриста, но тем не менее каждая транзакция записывается в блокчейн и публична.

Блоки в сети добавляются с помощью процедуры майнинга. За каждый новый блок майнер получает вознаграждение, которое составляет финансовую основу его деятельности. После того как совершена первая транзакция, она должна быть подтверждена несколькими участниками сети — в этом и состоит суть децентрализации блокчейна без конкретных посредников. Это означает еще одно преимущество блокчейна перед классической финансовой системой — в отличие от банков блокчейн работает круглосуточно и не зависит от центрального банка конкретной страны, совершение перевода криптовалюты от одного человека другому демонстрируется на рисунке 2.2.

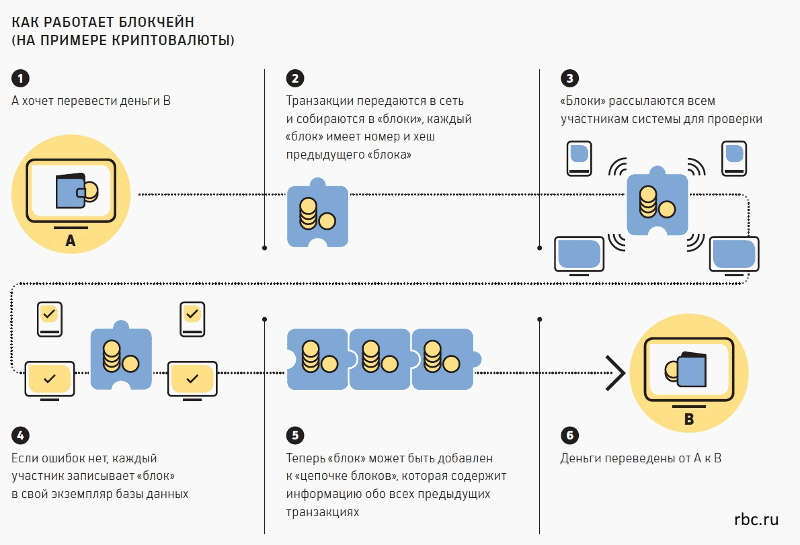


Рисунок 2.2 - как работает блокчейн пример с криптовалютой [10]

Блок блокчейна

Блок — перманентно записываемые файлы в сети Bitcoin, содержащие информацию о произошедших транзакциях. Блок — это запись части или всех недавних транзакций, которые еще не были записаны в предыдущие блоки. Практически во всех случаях блоки добавляются в конец цепи, которая содержит все транзакции и носит название block chain ("блокчейн"). Когда блок добавлен в конец цепи, он не может быть изменен. Каждый блок содержит информацию обо всём, что произошло в предыдущих блоках, перед тем как он был создан.

Каждый блок, помимо остальных компонентов, содержит в своем заголовке запись о нескольких или всех последних транзакциях и запись о блоке, который шел непосредственно перед текущим. Для создания нового блока майнеру необходимо решить на своём оборудовании задачу, которую выдает сеть. У каждого блока — свое уникальное решение, которое так же записывается в заголовок блока. Эта задача сложна для решения и занимает большое количество времени, но как только один из пользователей (майнеров) решает задачу, остальная сеть очень быстро подтверждает, что решение верно. Существует несколько решений для каждого блока – достаточно найти хотя бы одно из них.

## Эмуляция блокчейна

Создадим эмуляцию блокчейна, если свести к минимуму, то блокчейн представляет собой связанный список причем однонаправленный. И так в каждом блоке находятся транзакции, являющиеся содержимым данных, как и показано на рисунке 2.3 в зависимости от содержимого мы получаем то или иное значение хэш функции.

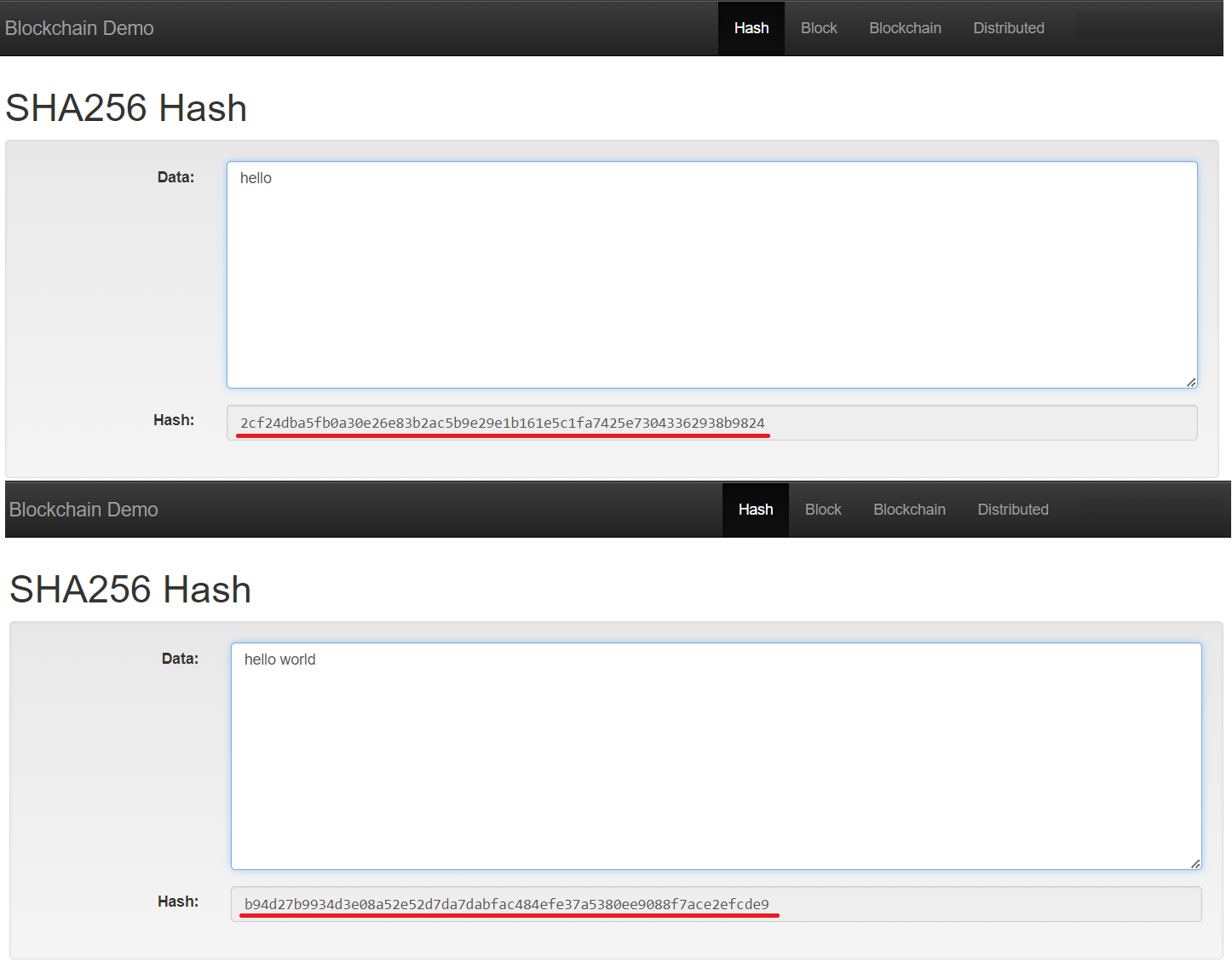


Рисунок 2.3 - Пример транзакции [16]

Далее рассмотрим место, в котором, собственно, хранятся данные транзакции, а хранятся они в блоках как показано на рисунке 2.4. было создано подобие блока содержащие в себе номер блока, число nonce, данные, которые в нем хранятся, адрес предыдущего блока и хэш данного блока. Почему в поле адреса находятся только нули. Это объясняется тем, что этот блок является первым в сети так же этот блок называется Генезис блок. Правило в симулированной сети такое: хэш блока должен содержать на первом месте четыре нуля. Хоть на изображение и показано что все поля изменяемые, но на самом деле все они не меняются в момент образования хэша меняться только то самое число nonce которое необходимо для того, чтобы создать такой хэш, который будет удовлетворять условия сети.

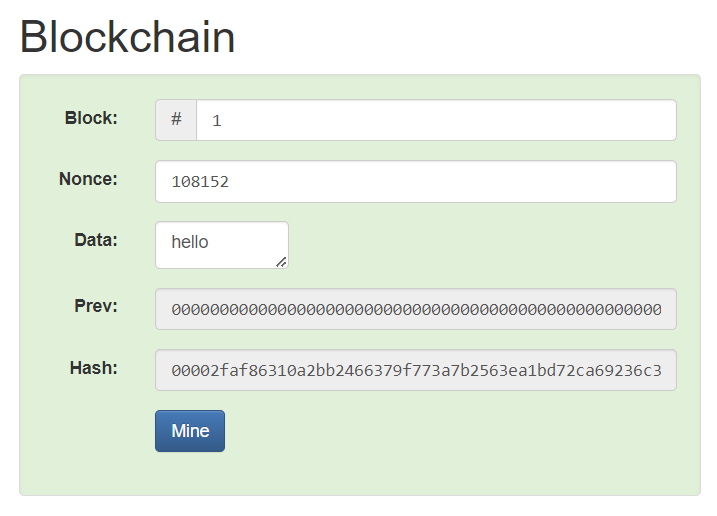


Рисунок 2.4 – Блок [16]

В случае если хэш блока не будет соответствовать правилам, то он не будет ни добавлен в блокчейн ни нести никакой смысловой нагрузки поэтому на рисунке 2.5. казано как выглядит неправильный блок и блок, соответствующий сети.

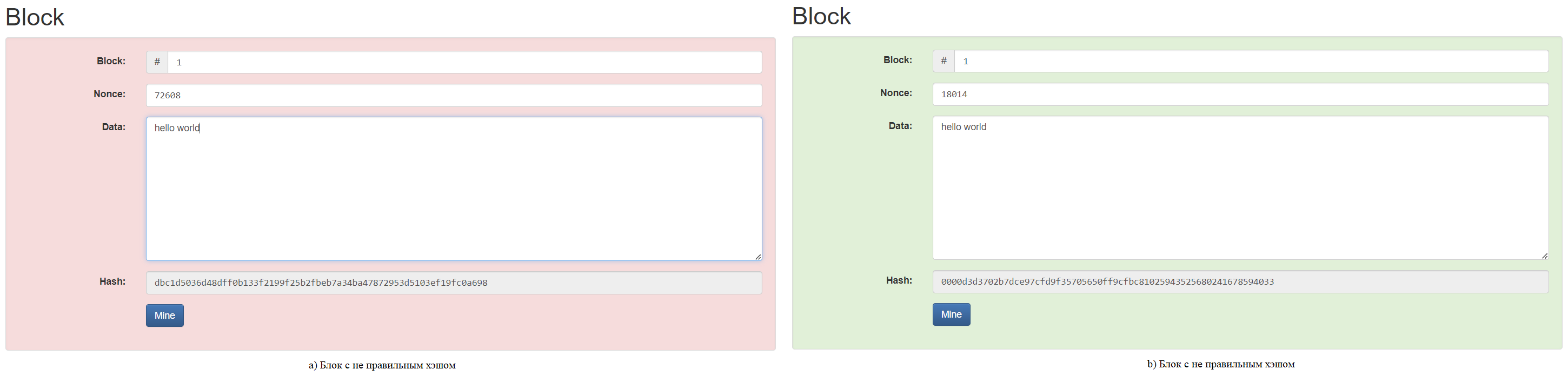


Рисунок 2.5 - Представление блоков в блокчейне [16]

После рассмотрения транзакции и блока можно перейти к рассмотрению симуляции блокчейна. На рисунке 2.6. показан блокчейн содержащий в себе 3 блока. Каждый пронумерован и содержит в себе адрес предыдущего блока.

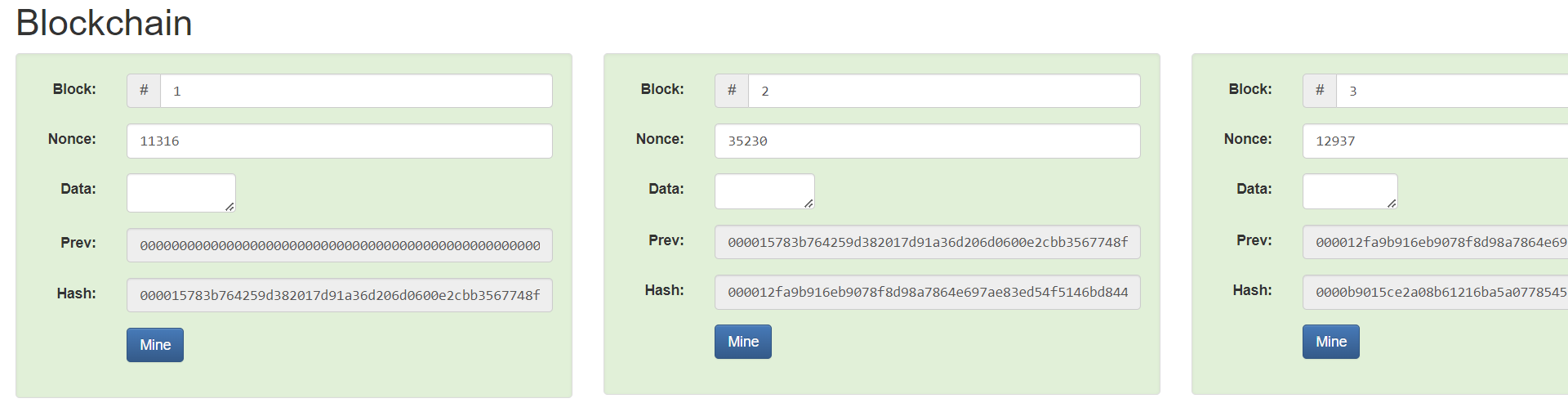


Рисунок 2.6 - Пример блокчейна [16]

Но в случае, если, что-то поменяется в поле данные то и хэш блока поменяется что повлечет за собой изменение и неправильность всех последующих блоков, как и показано на рисунке 2.7.

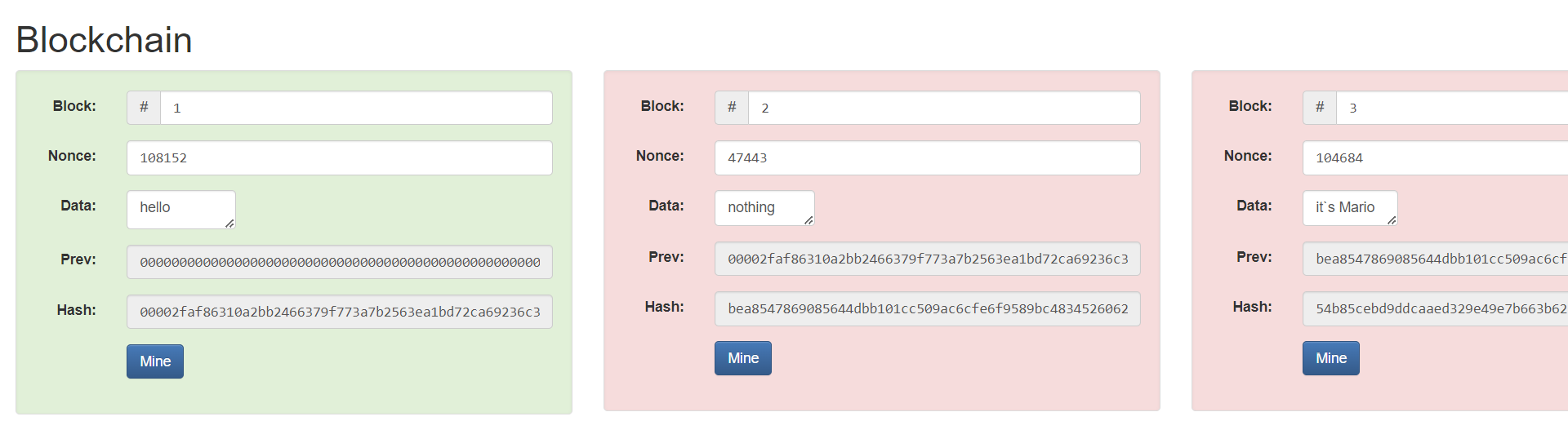


Рисунок 2.7 - Изменили значение в блоке [16]

Это и есть одна из причин безопасности блокчейна, так как для того, чтобы все встало на свои места вновь необходимо с момента блока, который был изменен изменить все последующие блоки соответственно проведя все вычисления хэш значений по-новому. После пересчета хэш значений для каждого блока мы получим результат как показан на рисунке 2.8.

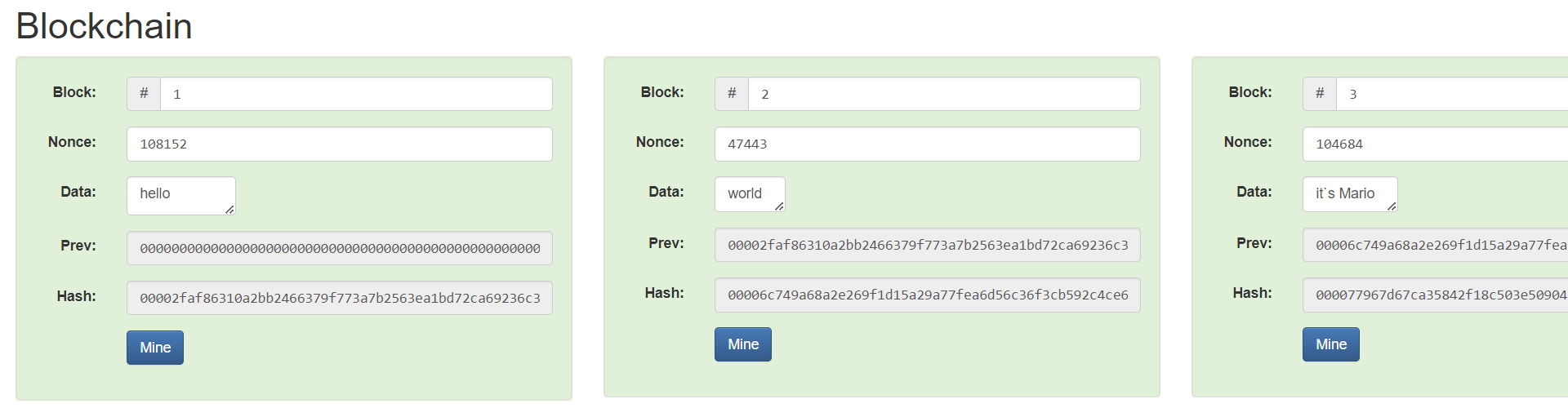


Рисунок 2.8 - Пересчитанный блокчейн [16]

Но ранее же говорилось, что блокчейн очень безопасный и невозможно изменить данные в нем. Как видно это возможно, но то, что было показано это было сделано лишь в одной блокчейн цепи блоков поэтому пересчитав все прошло успешно и было возможно заменить данные. Но блокчейн это же распределенная база данных соответственно цепь блоков находиться не у одного пользователя, а у нескольких. Самый минимальный уровень безопасности — это сеть из 3 независимых пользователей что могут с помощью алгоритма консенсуса определить кто прав, а кто нет. Чем больше пользователей в сети блокчейн, тем безопасней она, но почему, ранее говорилось об атаке 51% что же это, в качестве примера возьмем эмуляцию распределенного блокчейна, как показано на рисунке 2.9 видно, что есть 3 цепи что означает что в сети 3 пользователя.

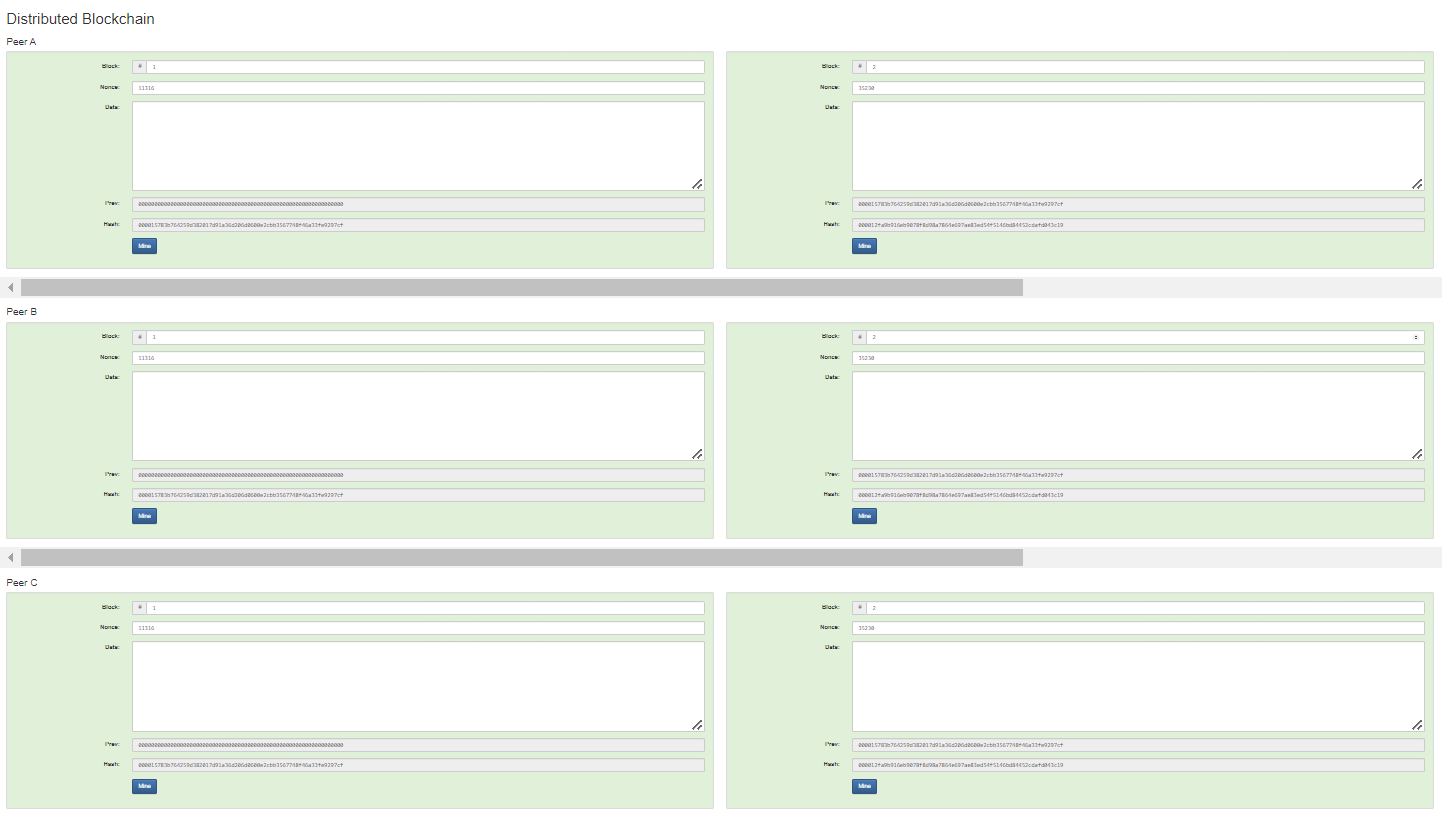


Рисунок 2.9 - Сеть из 3-х пользователей [16]

Если рассматривать тот случай, когда все блоки были пересчитаны после изменений, что же произойдет здесь. В цепи А введем другие данные что повлияет на хэш блоков соответственно пересчитав их мы не получим ошибок в цепи и все будет прекрасно, но есть проблема. Пересчет был лишь в цепи А что привело к изменению блоков в сети А но остальные цепи В и С не были изменены и тут вступает алгоритмы верификации которые сверяют цепи и из за различий находят неверный блок а именно тот что был изменен, это показано на рисунке 2.10. И из-за этого и не возможна, пока что атака 51% так как это не выгодно и очень сложно необходимо затратить ресурсы на пересчет 51% цепей в сети что приведет к подтверждению изменения но выгоды никакой не будет.

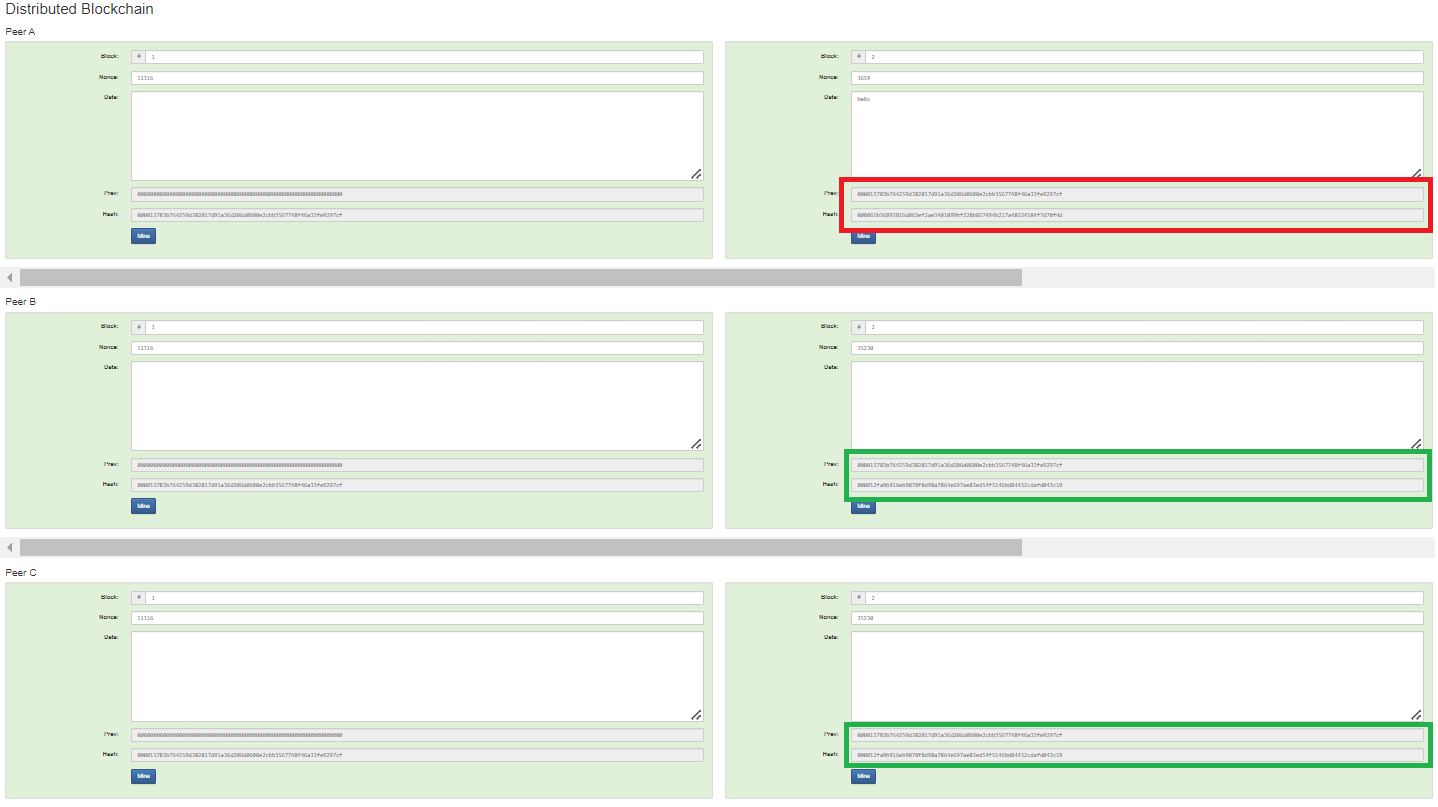


Рисунок 2.10 - Изменённая цепь в сети блокчейн [16]

## Смарт-контракты

Технология блокчейн гарантирует, что данные не будут изменены в процессе передачи. Поэтому она может найти применение не только в сфере финансов, но и в других областях, включая недвижимость и здравоохранение. Блокчейн предлагает особые функции, которые получили название смарт-контракты. Смарт-контракты автоматически создаются в системе, копируются в разные хранилища и исполняются с помощью распределенных вычислений. Поэтому после исполнения смарт-контракта его нельзя исправить, даже если позже в нем обнаружатся уязвимости.

Смарт-контракты (Smart Contracts) — это программный код, который автоматически выполняет и контролирует условия договоренности между двумя или более сторонами. Они используют технологию блокчейн для обеспечения прозрачности, безопасности и автоматизации процессов.

Смарт-контракты работают на базе блокчейн-платформы и выполняются автоматически, когда определенные условия, записанные в контракте, выполняются. Это позволяет сторонам сократить время и избежать необходимости доверять друг другу, так как смарт-контракты самостоятельно следят за выполнением условий и автоматически выполняют определенные действия.

Смарт-контракты могут использоваться в различных сферах, таких как финансы, право, здравоохранение, энергетика и другие. Они могут выполнять такие функции, как обмен активами, подписание договоров, автоматическое распределение средств, контроль качества и многое другое.

Смарт-контракты являются ключевым элементом технологии блокчейн, так как они обеспечивают прозрачность и безопасность сделок, а также уменьшают необходимость в промежуточных услугах и сторонах, таких как банки и правовые консультанты.

## Смарт-контракт принцип работы

Стороны подписывают умный контракт, используя аналогичные подписанию отправки средств в действующих криптовалютных сетях методы.

Смарт-контракты на блокчейн-платформах подписываются криптографическими ключами, также известными как цифровые подписи. Цифровая подпись — это математический алгоритм, который используется для проверки авторства документа или транзакции.

При подписании смарт-контракта, каждая сторона использует свой личный криптографический ключ, чтобы подписать контракт. Этот ключ генерируется с использованием криптографического алгоритма и является уникальным для каждой стороны.

Когда контракт подписан обеими сторонами, он становится неподдельным и невозможно изменить условия контракта без согласия всех участников сделки. Благодаря этому, смарт-контракты на блокчейн-платформах обеспечивают прозрачность, безопасность и надежность сделок.

Цифровые подписи также используются для подписания транзакций на блокчейн-платформах. При отправке транзакции на блокчейн, пользователь использует свой личный криптографический ключ для подписи транзакции. После этого, транзакция отправляется на сеть для проверки и подтверждения другими участниками блокчейн-сети. Если транзакция подписана правильно, то она будет выполнена и включена в блокчейн. После подписания сторонами контракт вступает в силу. Для обеспечения автоматизированного исполнения обязательств контракта непременно требуется среда существования, которая позволяет полностью автоматизировать выполнение пунктов контракта. Это означает, что умные контракты смогут существовать только внутри среды, имеющей беспрепятственный доступ исполняемого кода к объектам умного контракта.

Все условия контракта должны иметь математическое описание и ясную логику исполнения. В связи с этим первые умные контракты имеют задачу формализации наиболее простых взаимоотношений, состоящих из небольшого количества условий. Умные контракты, к примеру, могут следить за выполнением условий долгосрочных кредитов.

Разработчики пишут смарт-контракты на высокоуровневых языках программирования с синтаксисом Python, Pascal, JS или Haskel. Опытные разработчики часто пишут байт-код на Michelson.

Смарт-контракты на языке PascalLIGO состоят из переменных и функций. Виртуальная машина исполняет контракт начиная с точки входа — главной функции main. В нее можно вставить псевдо-точки входа — дополнительные функции.

Смарт-контракт всегда возвращает результат исполнения: список операций и значение хранилища storage, пример онлайн компилятора на рисунке2.11 .

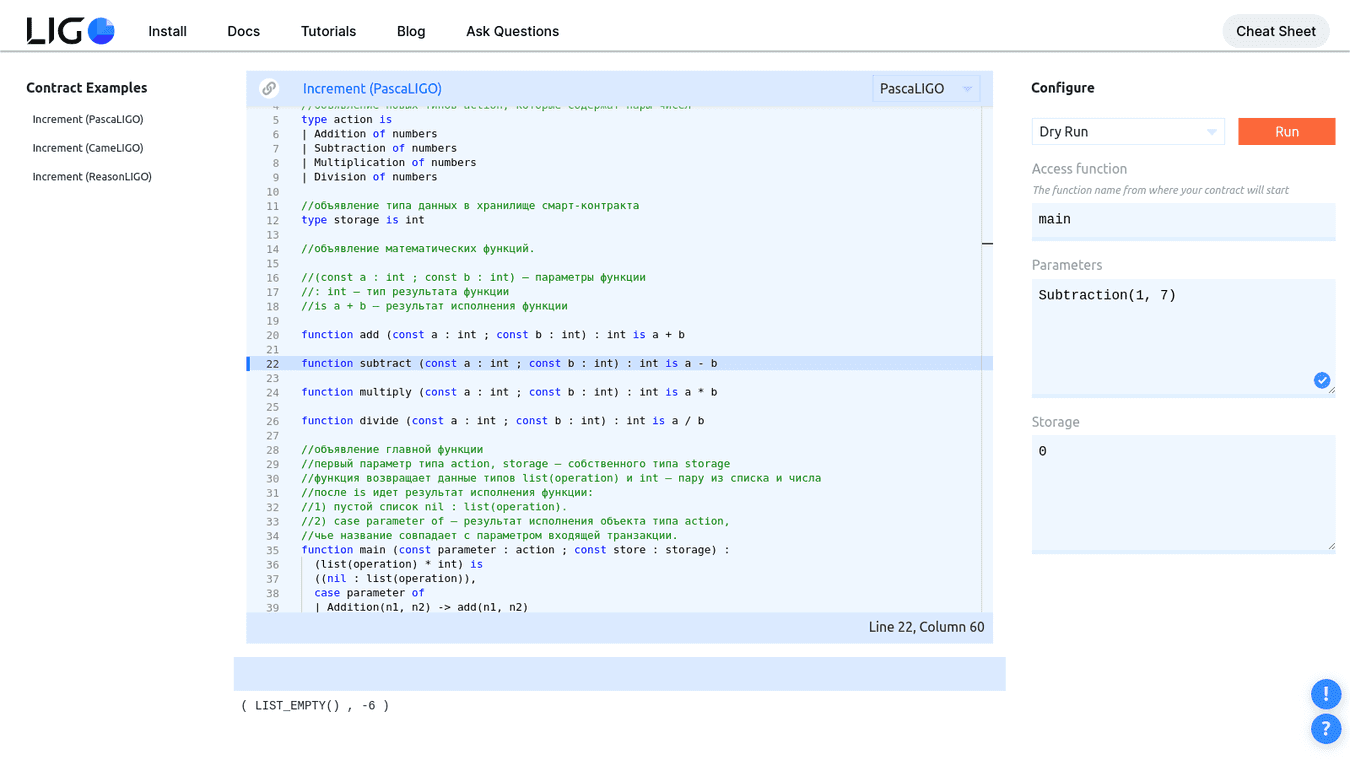


Рисунок 2.11 - Онлайн компилятор смарт-контрактов [23][24]

**Пример**

Примером смарт-контракта на блокчейн-платформе может быть контракт, который управляет автоматической оплатой и доставкой товаров в интернет-магазине.

Предположим, что интернет-магазин работает на блокчейн-платформе и использует смарт-контракт, чтобы автоматизировать процесс оплаты и доставки товаров. В контракте могут быть следующие условия:

Когда покупатель добавляет товары в корзину, он указывает свой адрес доставки и выбирает способ оплаты.

Покупатель отправляет оплату на адрес смарт-контракта.

Контракт автоматически проверяет полученный платеж и, если он правильный, отправляет уведомление продавцу о необходимости отправки товара.

Продавец отправляет товар по указанному адресу.

Контракт автоматически выплачивает продавцу сумму продажи минус комиссия платформы.

Таким образом, смарт-контракт позволяет автоматизировать процесс оплаты и доставки товаров, что упрощает процесс покупки для покупателя и продажи для продавца. Контракт также обеспечивает прозрачность и безопасность сделки, так как он выполняется автоматически и нельзя изменить его условия без согласия всех участников.

## Пример создания смарт контракта

Для создания своего смарт контракта в рамках знакомства была использована инструкция от компании Microsoft «Создание смарт-контрактов Ethereum с помощью Solidity»:

* объяснить, что такое смарт-контракты;
* разбираться в вариантах использования смарт-контрактов;
* Установите Truffle.
* Устанавливать расширение Truffle для VS Code.
* Создавать смарт-контракты с помощью расширения Truffle для VS Code.
* протестировать смарт-контракт с помощью Truffle.

Truffle — это самая популярная платформа среды разработки и тестирования для Ethereum. Ее можно установить с помощью диспетчера пакетов Node (npm), установка показана на рисунке 2.12.

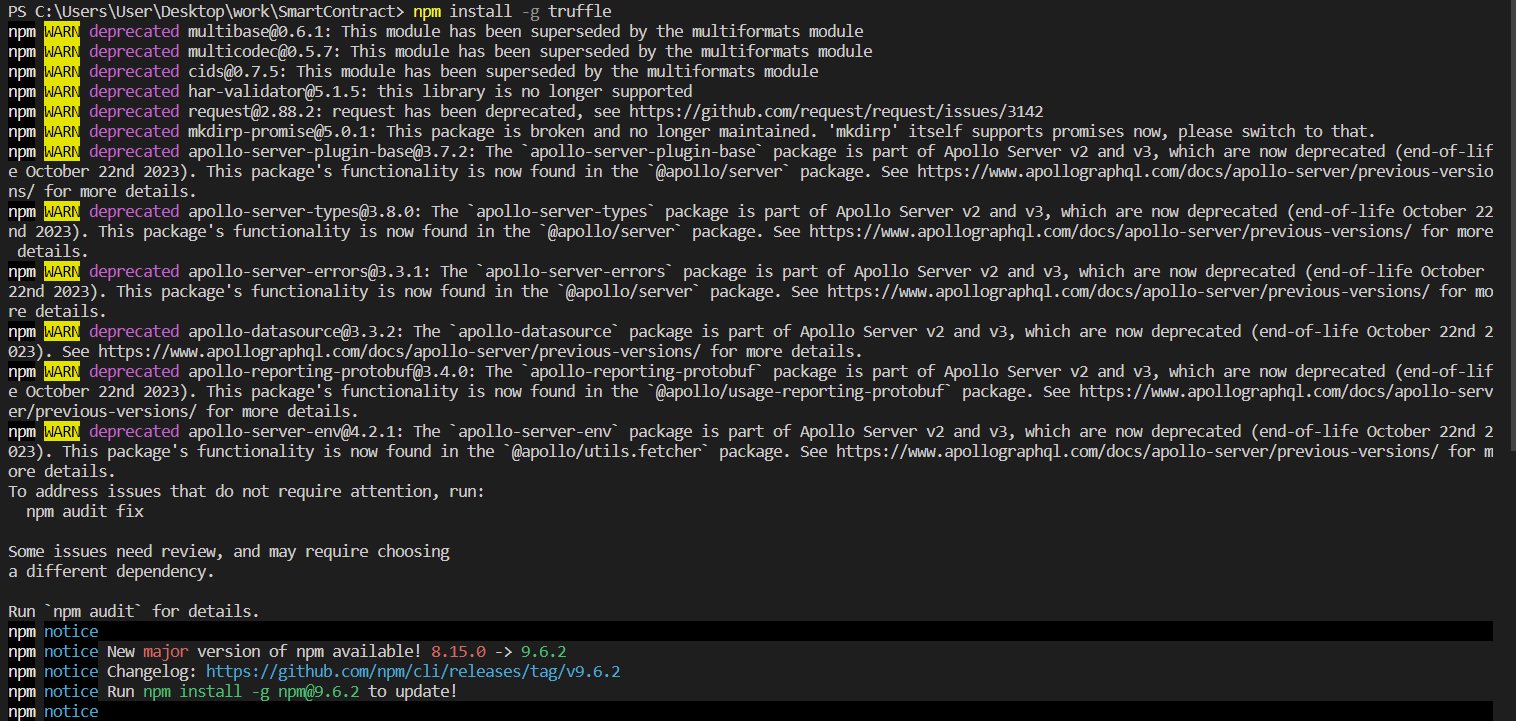


Рисунок 2.12 - Скачивание Truffle

Так же устанавливаем расширение для среды разработки как показано на рисунке 2.13.

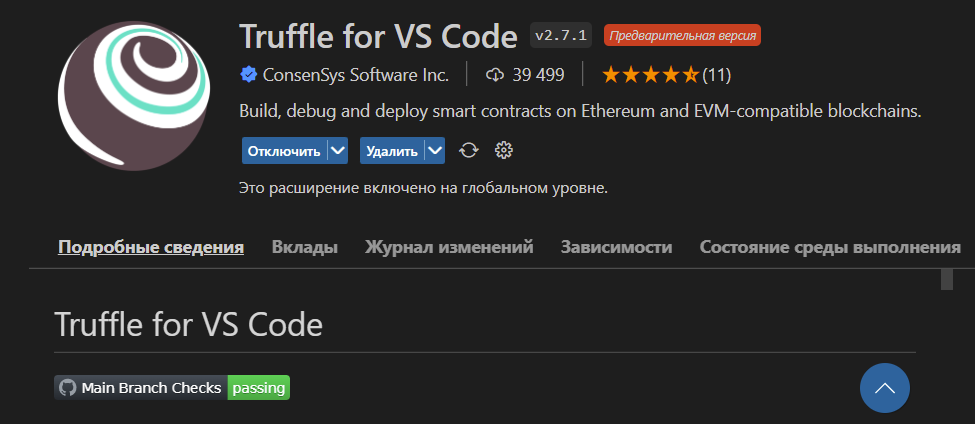


Рисунок 2.13 - установка Truffle

После того как все расширения скачены и установлены, и убедились в том, что установлено следующее:

* Node.js и npm — чтобы проверить наличие Node.js, откройте терминал и введите node. Если Node.js установлен, в окне терминала отобразятся сведения об установленной на компьютере версии Node.js. Кроме того, можно убедиться, что установлен диспетчер пакетов Node (npm). Для этого введите npm в терминале.
* Git. Чтобы проверить наличие Git, откройте терминал и введите git. Если Git установлен, в окне терминала отобразится список доступных команд git.
* Truffle Suite: расширение предоставляет ссылку на установку средств разработчика Truffle Suite (требуется, пока расширение находится в общедоступной предварительной версии).
* Ganache — расширение предоставляет ссылку на установку Ganache (требуется, пока расширение предоставляется в общедоступной предварительной версии).

Добавляем на компьютер пустой каталог для проекта. Чтобы создать каталог из среды Visual Studio Code, последовательно выберите элементы Terminal (Терминал)>New Terminal (Новый терминал), а затем вводим mkdir newSolidityProject.

В Visual Studio Code последовательно открываем разделы View (Просмотр)>Command Palette (Палитра команд). В поле поиска введите Truffle: New Solidity Project. По мере ввода появляется список предложений. В качестве типа для проекта Solidity выберите вариант Create basic project (Создать базовый проект). [25]

После создания получим следующую сборку проекта как на рисунке 2.14



Рисунок 2.14 - Браузер файлов

Получив все файлы для тестовой конфигурации можно собрать проект и локально развернуть его тем самым посмотрев важные сведения и метаданные для развернутого контракта, как показано на рисунке 2.15.

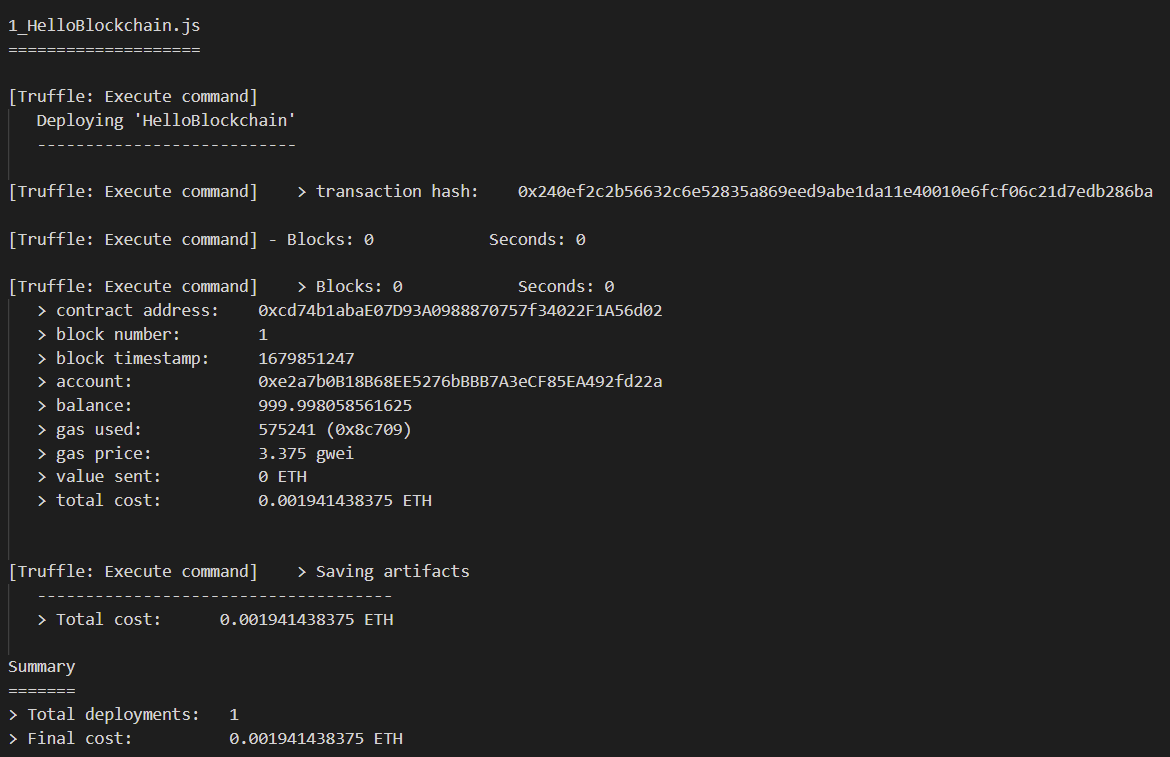


Рисунок 2.15 - развертка смарт контракта

Важными данными являются:

* адрес контракта;
* метка времени того блока, в который включена транзакция создания контракта;
* адрес учетной записи, с помощью которой развернут контракт;
* остаток на счете этой учетной записи (в единицах эфира) после транзакции. Этот остаток на счете равен 100 ETH (начальное значение по умолчанию) за вычетом общей стоимости;
* количество и стоимость использованного газа. Термин газ здесь определяет стоимость выполнения транзакции или контракта на платформе блокчейна Ethereum. Можно провести параллель между ним и топливом для автомобиля. Общая стоимость вычисляется как произведение цены газа и использованного объема газа.

Целью описания этого модуля является желание показать что создание смарт-контрактов не является чем-то за гранью понимания и каждый при желание способен создать свой смарт-контракт для той или иной сети блокчейн.

## Dapp – распределенные приложения

## Мошенничество с децентрализованными приложениями

# ЗАКЛЮЧЕНИЕ

Блокчейн – система записи информации таким образом, чтобы ее было невозможно изменить, взломать или обмануть, но легко проверить.

Блокчейн как представитель децентрализованного распределённого реестра применяется и в других сферах что способствует популяризации данной технологии, так как позволяет продавцу и покупателю взаимодействовать на прямую без сторонних лиц при этом регистрируя все в базу хорошо защищённую и не изменяемую, что способствует надежности выполнения транзакций.

Данная технология все еще развивается и в скором будущем вытеснит устоявшиеся порядки изменив вид отношений между поставщиком и получателем. Система прозрачна так как ничего не скрывается, возможность защиты и неизменности данных на сегодняшний день очень важны, именно поэтому технология в ближайшем будущем не утратит, а на оборот приобретёт еще большую популярность и востребованность. Технология сложна для понимания так как эта относительно новая технология записей, статей, блогов не так уж и много по сравнению с другими темами, что приводит к отталкивающему эффекту. Но уверен, что в скором времени человечество примет и будет активно использовать блокчейн повсеместно, а связанно это с тем, что это упрощает систему передачи исключая третье лицо.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ОСИПОВ Н. Р., КРОТОВА Е. Л.: технология блокчейн. преимущества и недостатки   
   [цитирован 29.11.2022] Режим доступа: <http://info-secur.ru/is_26/4(26)-2017_28-30.pdf>
2. ДОГУЧАЕВА СВЕТЛАНА МАГОМЕДОВНА: актуальность применения блокчейн технологий в российских компаниях [цитирован 29.11.2022] Режим доступа: <http://nauteh-journal.ru/files/4a2443ff-26b3-49d5-b2d7-c4a0ab755926>
3. AWS: Что такое технология блокчейн? [цитирован 20.12.2022] Режим доступа: <https://aws.amazon.com/ru/what-is/blockchain>.
4. ADAM HAYES: Learn how these digital public ledgers enable crypto and NFTs   
   [цитирован 20.12.2022] Режим доступа: <https://www.investopedia.com/terms/b/blockchain.asp>
5. SAM DALEY: Blockchain. What Is Blockchain Technology? How Does It Work?   
   [цитирован 20.12.2022] Режим доступа: <https://builtin.com/blockchain>
6. МИЛА ВАСИЛЬЕВА: что такое блокчейн, где применяется и что его ждет в будущем   
   [цитирован 28.12.2022] Режим доступа: <https://www.banki.ru/news/daytheme/?id=10975614>
7. BYBIT LEARN: Что такое узлы (ноды) блокчейна и биткоина? [цитирован 28.12.2022] Режим доступа: <https://learn.bybit.com/ru/blockchain/what-are-nodes/>
8. CSCALP: Что такое блокчейн и как он устроен: обзор для начинающих [цитирован 28.12.2022] Режим доступа: <https://fsr-develop.ru/chto-takoe-blokchejn-i-kak-on-ustroen-obzor-dlja-nachinajushhih>
9. SEENECO: Что такое Блокчейн (Blockchain)? Технология распределенного реестра простыми словами [цитирован 28.12.2022] Режим доступа: <https://www.seeneco.com/ru/blog/chto-takoe-blokchejn/>
10. BITBON: Классификация блокчейнов [цитирован 28.12.2022] Режим доступа: <https://www.bitbon.space/ru/knowledge-base/distributed-ledger-technologies-blockchain/technological-aspects-of-blockchain/classification-of-blockchains>
11. IXBT: Алгоритмы консенсуса: что это и какие бывают [цитирован 02.01.2023] Режим доступа: <https://www.ixbt.com/live/crypto/algoritmy-konsensusa-chto-eto-k-i-kakie-byvayut.html>
12. ROSHAN RAJ: How does Blockchain work? [цитирован 02.01.2023] Режим доступа: <https://intellipaat.com/blog/tutorial/blockchain-tutorial/how-does-blockchain-work/>
13. VARUN BHAGAT: What is Blockchain-as-a-Service & its Business Benefits? [цитирован 02.01.2023] Режим доступа: <https://www.techiexpert.com/what-is-blockchain-as-a-service-its-business-benefits/>
14. ADAM LEVY: Applications for Blockchain Technology [цитирован 10.01.2023] Режим доступа: <https://www.fool.com/investing/stock-market/market-sectors/financials/blockchain-stocks/blockchain-applications/>
15. ПАВЕЛ ФЕДОРОВ: Что такое блокчейн: все, что нужно знать о технологии [цитирован 10.01.2023] Режим доступа: <https://www.forbes.ru/mneniya/456381-cto-takoe-blokcejn-vse-cto-nuzno-znat-o-tehnologii>
16. ANDERS94: blockchain-demo [цитирован 10.01.2023] Режим доступа: <https://github.com/anders94/blockchain-demo>
17. TADVISER: В Сингапуре начинают выдавать дипломы через блокчейн [цитирован 11.01.2023] Режим доступа: <https://www.iksmedia.ru/news/5585510-V-Singapure-nachinayut-vydavat-dipl.html>
18. Денис Давыдов-Громадин: Что такое токен и чем он отличается от монеты [цитирован 20.03.2023] Режим доступа: <https://www.rbc.ru/crypto/news/63dbefd29a79477dedd4b62c>
19. Максим Шевченко: Картина цифрового художника Beeple продана на аукционе за $69 миллионов [цитирован 20.03.2023] Режим доступа: <https://3dnews.ru/1034693/kartina-tsifrovogo-hudognika-beeple-prodana-na-auktsione-za-69-millionov>
20. Марат Селезнев. Что такое NFT и почему они приносят миллионы [цитирован 20.03.2023] Режим доступа: https://trends.rbc.ru/trends/industry/641d4acc9a79473f95345650
21. Cryptokitties: Видеоигра [цитирован 20.03.2023] Режим доступа: <https://www.cryptokitties.co/>
22. Ilink: Преимущества использования технологии блокчейн [цитирован 25.03.2023] Режим доступа: <https://vc.ru/u/1194168-ilink/428413-preimushchestva-ispolzovaniya-tehnologii-blokcheyn>
23. Павел Скоропляс: Что такое смарт-контракты и как они работают блокчейн [цитирован 25.03.2023] Режим доступа: <https://forklog.com/sp/dev-on-tezos/tezos-introduction/>
24. Ligolang: Compiler [цитирован 25.03.2023] Режим доступа: <https://ide.ligolang.org/local/default-project>
25. Microsoft: Создание смарт-контрактов Ethereum с помощью Solidity [цитирован 26.03.2023] Режим доступа: <https://learn.microsoft.com/ru-ru/training/modules/blockchain-solidity-ethereum-smart-contracts/>
26. Рустам Сабиров: Зал славы интернета: 7 пионеров Глобальной сети [цитирован 26.03.2023] Режим доступа: https://skillbox.ru/media/code/zal-slavy-interneta/
27. Петр Давыдов: Будущее денег: что такое биткоин, блокчейн и как они работают [цитирован 26.03.2023] Режим доступа: <https://ichip.ru/tekhnologii/budushhee-deneg-chto-takoe-blokchejjn-i-kak-on-rabotaet-98932>
28. Ruslan Ospanov: СИСТЕМАТИЗАЦИЯ ЗНАНИЙ ПО ИСПОЛЬЗУЕМОЙ КРИПТОГРАФИИ В БЛОКЧЕЙНЕ. ОСНОВНЫЕ ПОНЯТИЯ БЛОКЧЕЙНА. КРИПТОГРАФИЧЕСКАЯ ХЭШ-ФУНКЦИЯ. [цитирован 26.03.2023] Режим доступа: <https://cryptography.kz/ru/assets/templates/T1/images/figure2.png>