

Министерство Образования и Исследований Республики Молдова  
Технический Университет Молдовы  
Факультет Вычислительной Техники, Информатики и Микроэлектроники  
Департамент Программной Инженерии и Автоматики

Дипломная практика

**Тема:** Анализ использования технологии блокчейн

Analiza utilizării tehnologiei blockchain

Analysis of the use of blockchain technology

Студент:

\_\_\_\_\_

Подпись

Шарафудинов Николай,  
gr. TI-196

Руководитель по диплому:

\_\_\_\_\_

оценка, подпись

Cernei Irina, asist. univ.

Куратор практики из  
университета:

\_\_\_\_\_

оценка, подпись

Cernei Irina, asist. univ.

Кишинев 2022

## СОДЕРЖАНИЕ

<b>ВВЕДЕНИЕ.....</b>	<b>2</b>
<b>1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ .....</b>	<b>3</b>
1.1 Актуальность выбранной темы .....	3
1.2 Общая характеристика блокчейна.....	5
1.3 Методы взаимодействия с блокчейном .....	5
1.4 Виды блокчейн технологий .....	8
1.5 Виды Узлов.....	11
1.6 Алгоритмы консенсуса.....	13
1.7 Блокчейн в сравнение с базой данных и облаком.....	19
1.8 Сферы применения Блокчейн технологии .....	20
1.9 Пример применения блокчейн технологий в образовании.....	24
<b>2 ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН .....</b>	<b>26</b>
2.1 Как работает блокчейн. ....	26
2.2 Эмуляция блокчейна.....	29
<b>ЗАКЛЮЧЕНИЕ .....</b>	<b>34</b>
<b>СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....</b>	<b>35</b>

## **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» так как технологии на базе 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 — новейшая технология, интерес к которой вырос вместе с популярностью криптовалют. Блокчейн уже пробуют использовать 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, представленной в виде математического алгоритма, 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. Сегодня в научно-публицистической литературе технологии блокчейна уделяется огромное внимание, что обусловлено возможностями ее применения и самой сущностью данной системы, представляющей собой технологический прорыв. Эксперты сходятся во мнении, что внедрение технологии блокчейн в разнообразные сферы жизни общества способно изменить весь мир.

# 1 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.

## 1.1 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 биткойне это в среднем 10 минут) транзакций. Транзакции в сети биткойн представляют собой записи, которые фиксируют передачу какого-либо количества биткойнов 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) рис. 1. 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.

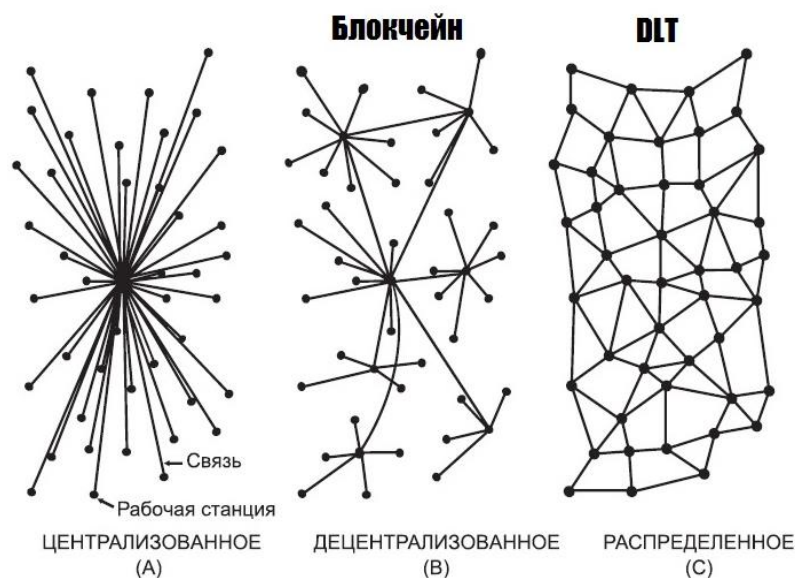


Рисунок 1.1-Три разных типа программных приложений

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 третьим лицам система становится 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.

## **1.2 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.

## **1.3 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.

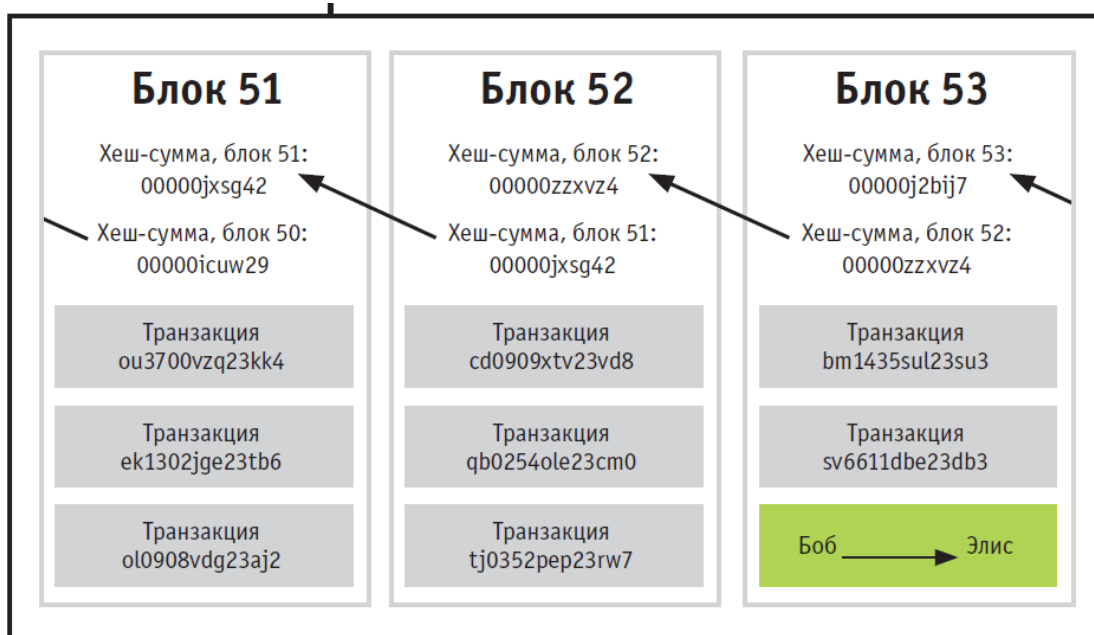


Рисунок 1.2 – Структура блоков в цепи

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

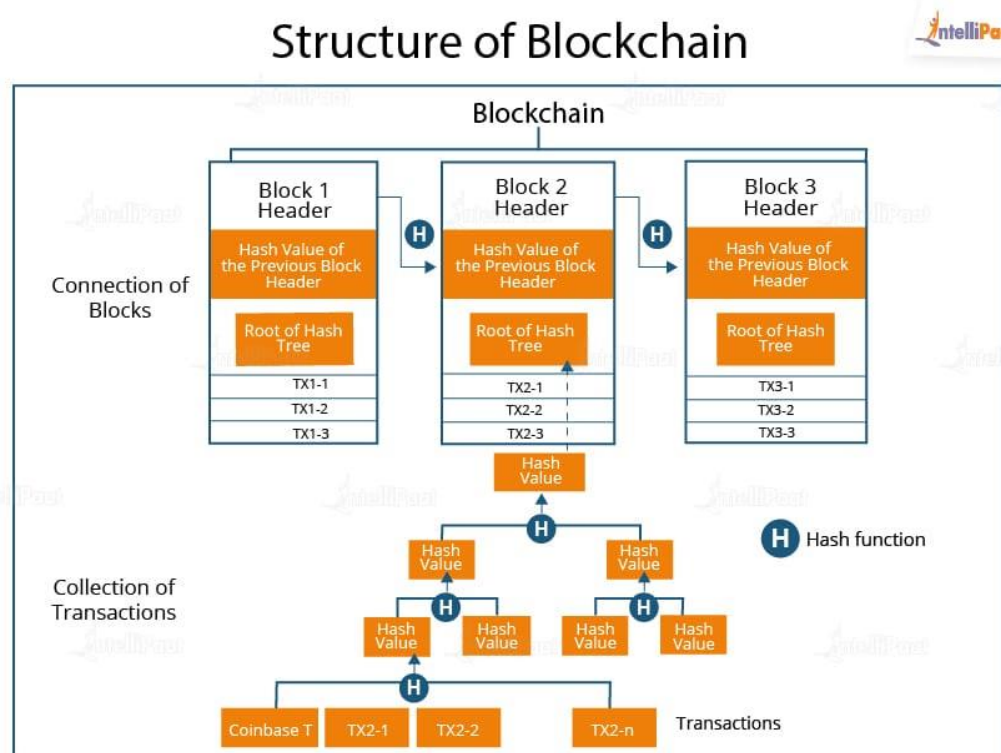


Рисунок 1.3 – Структура блокчейна

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.

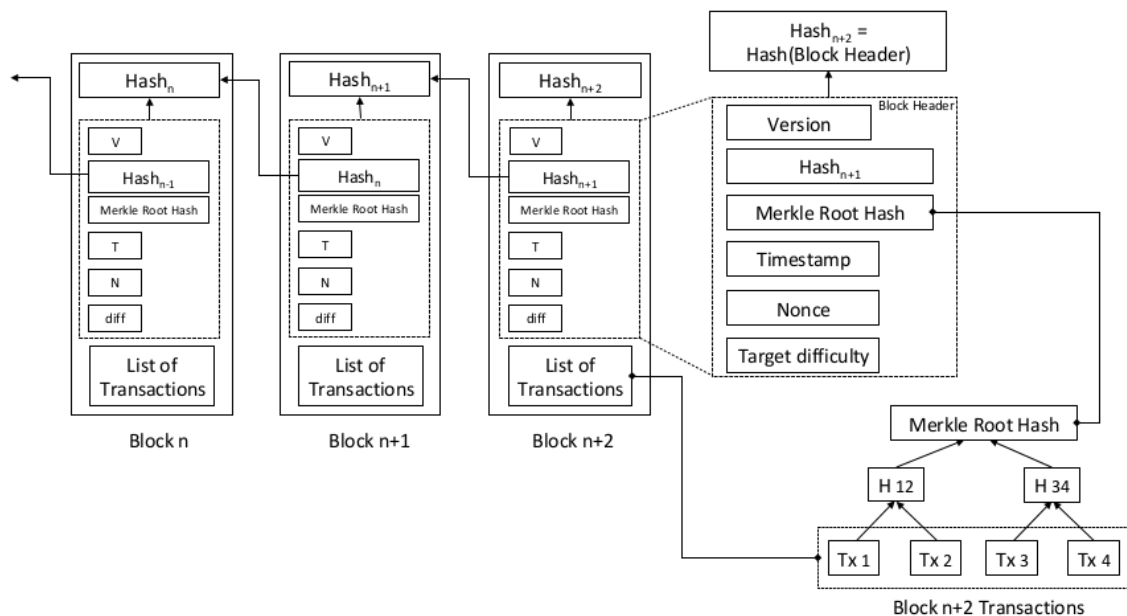


Рисунок 1.4 – Структура блоков в блокчейне

## 1.4 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.

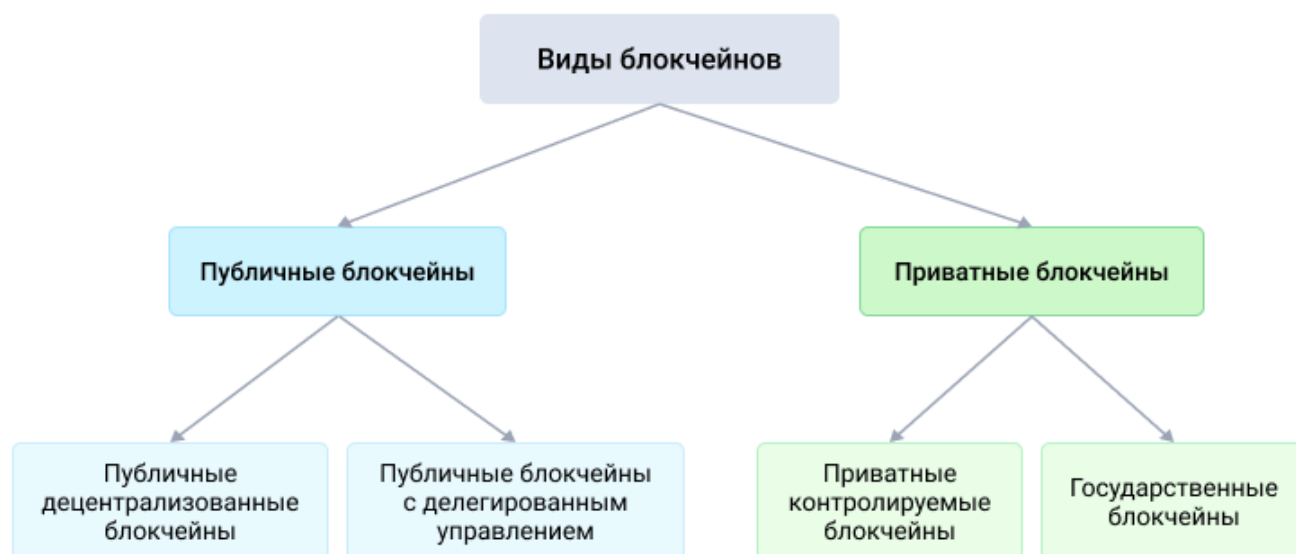


Рисунок 1.5 – Классификация блокчейн [11]

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.

### **1.5 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.

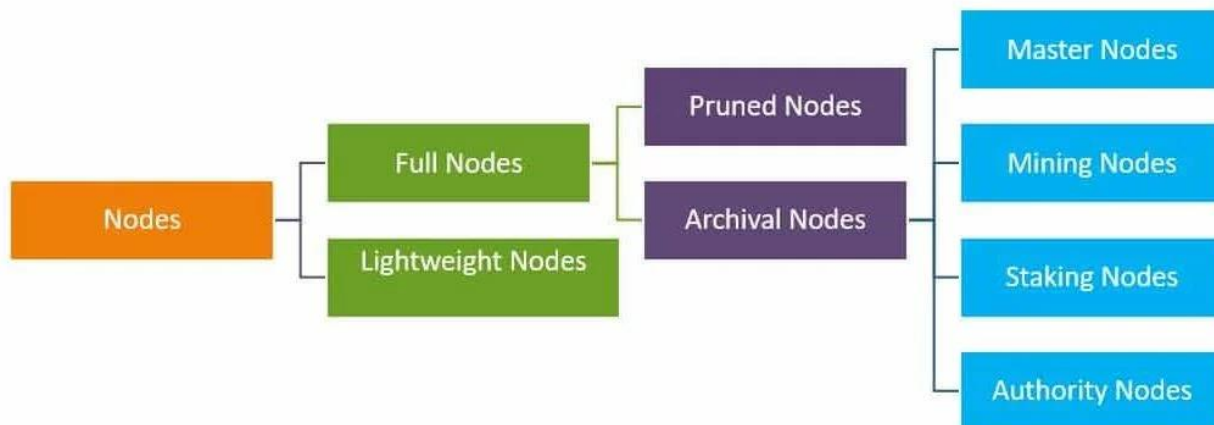


Рисунок 1.6 – Виды узлов блокчейна [13]

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.

### **1.6 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 децентрализованно.

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.

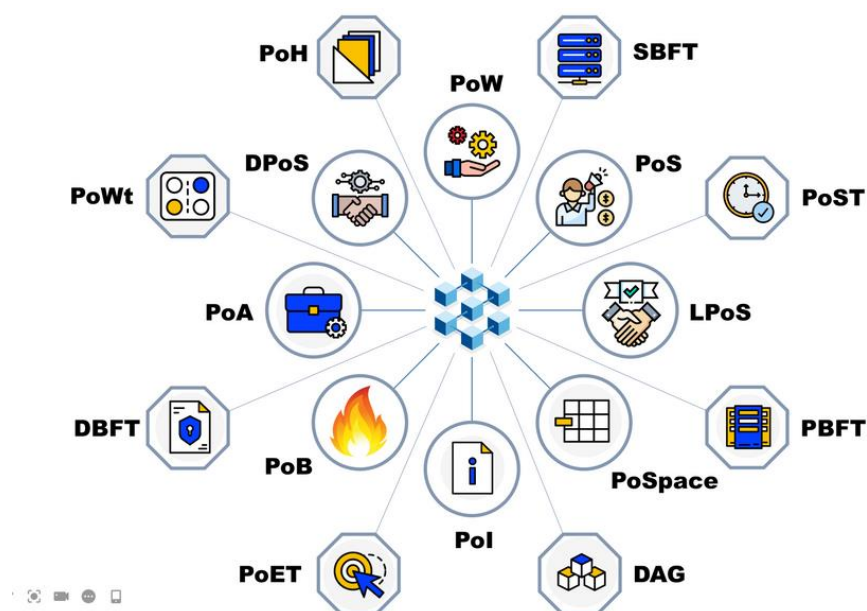


Рисунок 1.7 – Виды алгоритмов консенсусов [12]

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 (Delegated 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 мультчейны, 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).

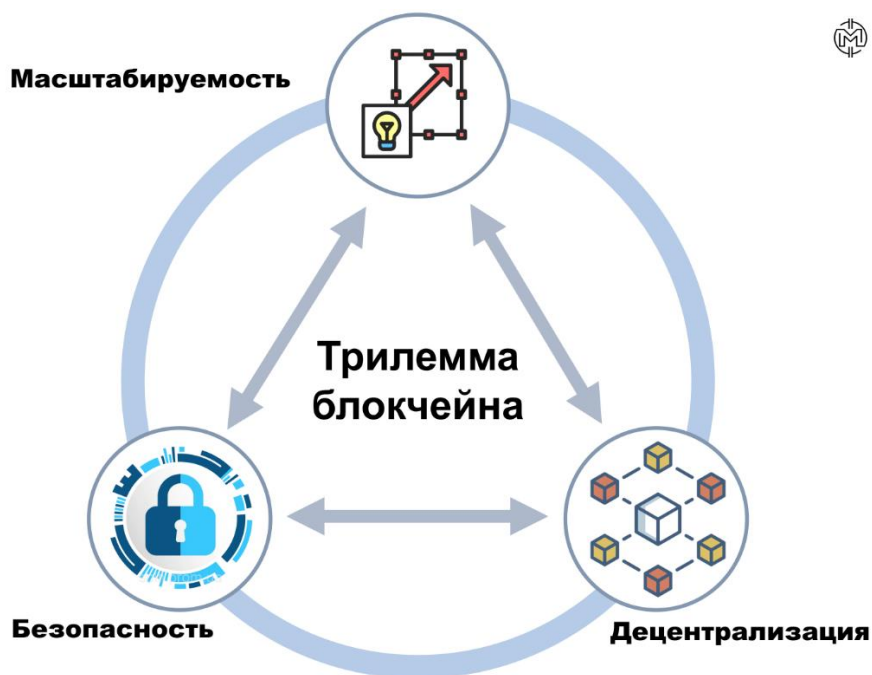


Рисунок 1.8 – Трилемма блокчейна [12]

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, объем 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 алгоритма PoW стимулировали сообщество к 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 объем 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 Ethereum (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 отличие 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 PoW 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 ХСР.

### **1.7 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]

### 1.8 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, получают 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 получают 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 децентрализованно, 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.

### **1.9 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 устранил 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]

## 2 ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

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

### 2.1 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.

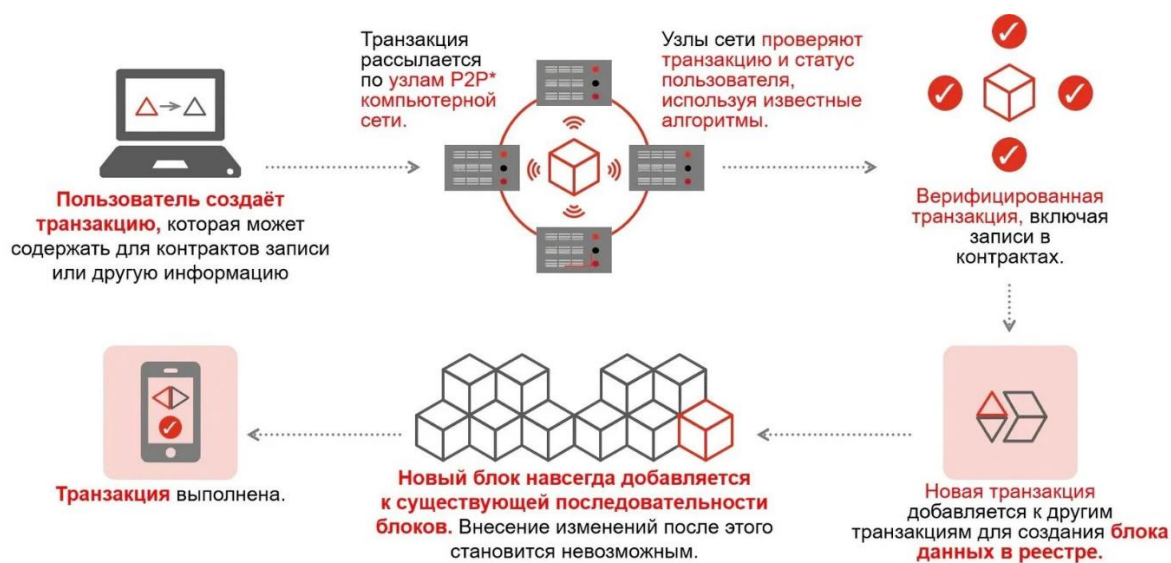


Рисунок 2.1 - Как работает блокчейн [9]

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.

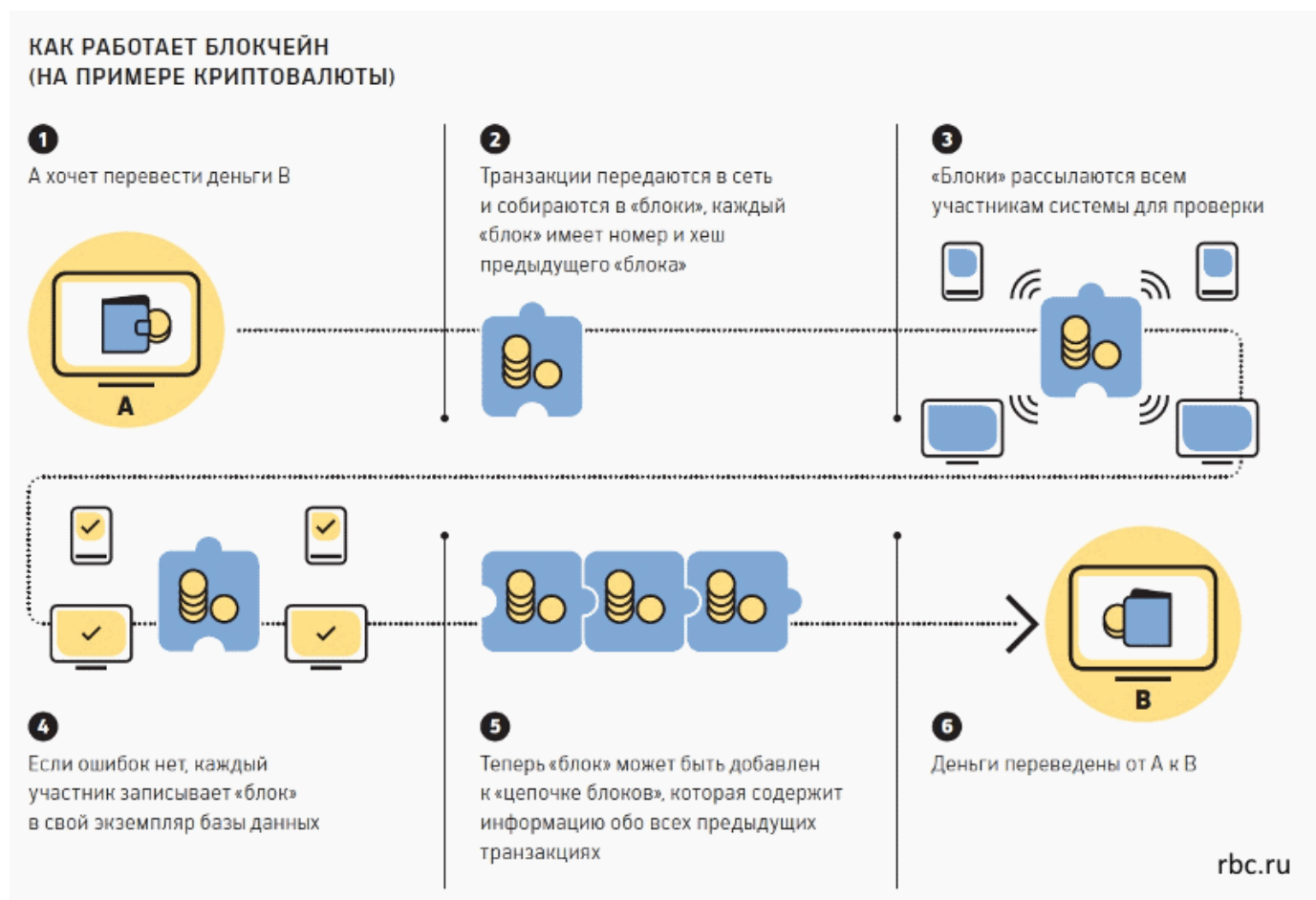


Рисунок 2.2 - как работает блокчейн пример с криптовалютой [10]

### Блок блокчейна

Блок — permanently 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.

## 2.2 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.

Blockchain Demo

HashBlockBlockchainDistributed

SHA256 Hash

Data:hello

Hash:2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

Blockchain Demo

HashBlockBlockchainDistributed

SHA256 Hash

Data:hello world

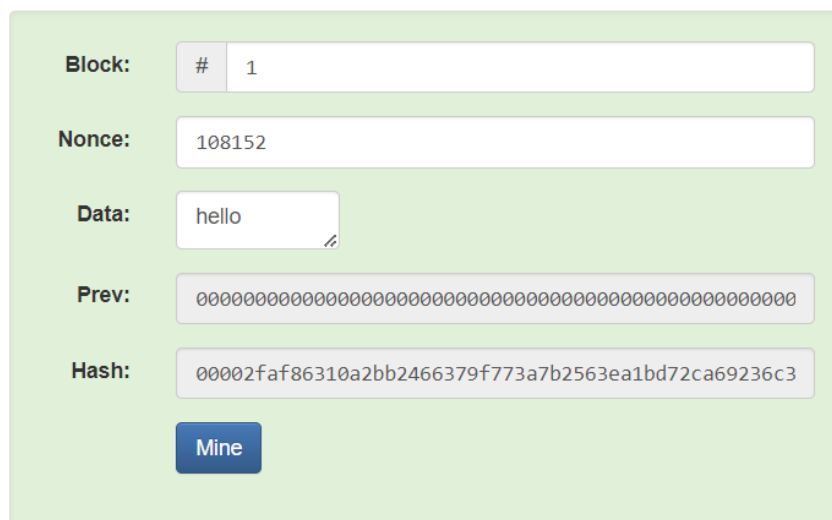
Hash:b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

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 поппе, 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. Хотя 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.

## Blockchain



A web interface for creating a blockchain block. It features a light green background with several input fields and a button. The fields are labeled 'Block:', 'Nonce:', 'Data:', 'Prev:', and 'Hash:'. The 'Block:' field has a dropdown menu showing '# 1'. The 'Nonce:' field contains the value '108152'. The 'Data:' field contains 'hello'. The 'Prev:' field contains a long string of zeros. The 'Hash:' field contains a hexadecimal string. A blue 'Mine' button is located at the bottom.

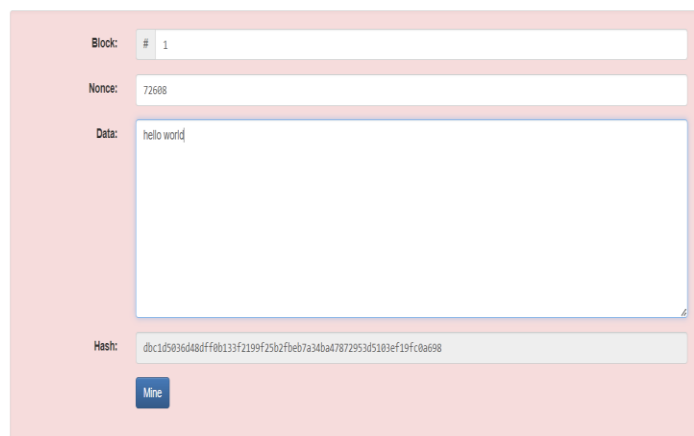
Block:	# 1
Nonce:	108152
Data:	hello
Prev:	00
Hash:	00002faf86310a2bb2466379f773a7b2563ea1bd72ca69236c3

Mine

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.

### Block



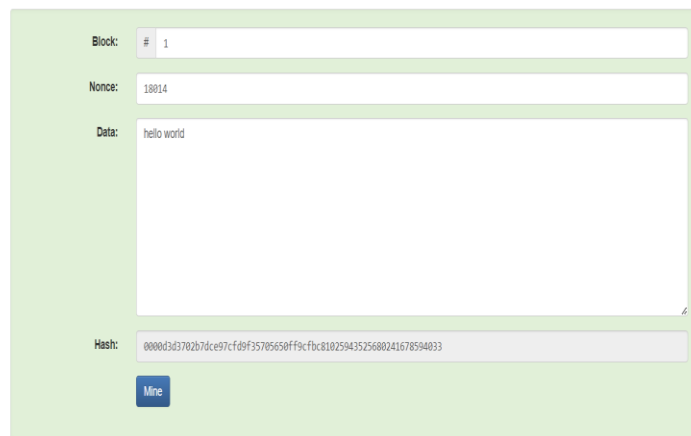
A web interface for creating a block, similar to the one in Figure 2.4, but with a pink background. The 'Block:' field shows '# 1', 'Nonce:' shows '72688', 'Data:' shows 'hello world', and 'Hash:' shows a long hexadecimal string. A blue 'Mine' button is at the bottom.

Block:	# 1
Nonce:	72688
Data:	hello world
Hash:	0bc1d5936d48dffb0133f2199f25b2f0eb7a34ba47872953d5183ef19fcd8e98

Mine

а) Блок с не правильным хешом

### Block



A web interface for creating a block, similar to the one in Figure 2.4, but with a light green background. The 'Block:' field shows '# 1', 'Nonce:' shows '18014', 'Data:' shows 'hello world', and 'Hash:' shows a long hexadecimal string. A blue 'Mine' button is at the bottom.

Block:	# 1
Nonce:	18014
Data:	hello world
Hash:	0000d3d3702b7dce97cfdbf35705650ff9cfc81025943525680241678594033

Mine

б) Блок с не правильным хешом

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.

## Blockchain

Block:	#	1	2	3
Nonce:		11316	35230	12937
Data:				
Prev:		00	000015783b764259d382017d91a36d206d0600e2cbb3567748f	000012fa9b916eb9078f8d98a7864e69
Hash:		000015783b764259d382017d91a36d206d0600e2cbb3567748f	000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd844	0000b9015ce2a08b61216ba5a0778545
Mine				

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.

## Blockchain

Block:	#	1	2	3
Nonce:		108152	47443	104684
Data:		hello	nothing	it's Mario
Prev:		00	00002faf86310a2bb2466379f773a7b2563ea1bd72ca69236c3	bea8547869085644dbb101cc509ac6cf
Hash:		00002faf86310a2bb2466379f773a7b2563ea1bd72ca69236c3	bea8547869085644dbb101cc509ac6cf6f9589bc4834526062	54b85ceb9ddcaed329e49e7b663b62
Mine				

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.

## Blockchain

Block:	#	1	2	3
Nonce:		108152	47443	104684
Data:		hello	world	it's Mario
Prev:		00	00002faf86310a2bb2466379f773a7b2563ea1bd72ca69236c3	00006c749a68a2e269f1d15a29a77fea
Hash:		00002faf86310a2bb2466379f773a7b2563ea1bd72ca69236c3	00006c749a68a2e269f1d15a29a77fea6d56c36f3cb592c4ce6	000077967d67ca35842f18c503e50904
Mine				

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 находится 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.

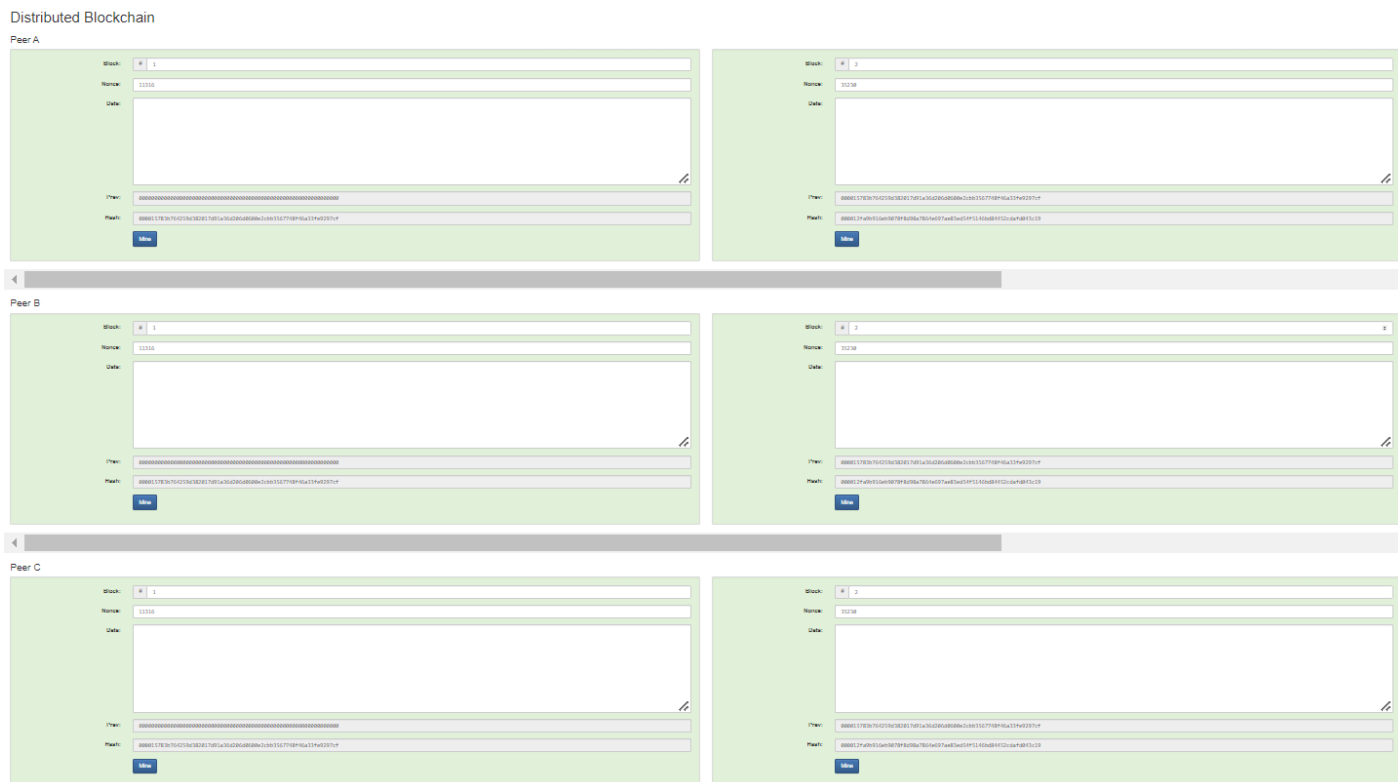


Рисунок 2.9 - Сеть из 3-х пользователей [16]

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.

## Peer A

The screenshot displays a distributed ledger simulation with four nodes: Peer A, Peer B, Peer C, and Peer D. Each node has a block number, a name, a date, and a list of transactions. The transactions are represented as long strings of alphanumeric characters. A red box highlights a transaction in Peer A's block 2, and a green box highlights a transaction in Peer B's block 2.

**Peer A**

- Block: 1
- Name: 12345
- Date:
- Transaction:
- Peer:
- Block: 2
- Name: 12345
- Date:
- Transaction:
- Peer:

**Peer B**

- Block: 1
- Name: 12345
- Date:
- Transaction:
- Peer:
- Block: 2
- Name: 12345
- Date:
- Transaction:
- Peer:

**Peer C**

- Block: 1
- Name: 12345
- Date:
- Transaction:
- Peer:
- Block: 2
- Name: 12345
- Date:
- Transaction:
- Peer:

**Peer D**

- Block: 1
- Name: 12345
- Date:
- Transaction:
- Peer:
- Block: 2
- Name: 12345
- Date:
- Transaction:
- Peer:

Рисунок 2.10 - Изменённая цепь в сети блокчейн [16]

## **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 напрямую без сторонних лиц при этом регистрируя все в базу хорошо защищённую и не изменяемую, что способствует надёжности 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 связано 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](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 биткойна? [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.techexpert.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-Singapore-nachinayut-vydavat-dipl.html>