УДК 004.056.5

Д.А. Саяков, daniyar.sayakov@yandex.ru
Национальный исследовательский ядерный университет «МИФИ», г. Москва

РОЛЬ КРИПТОГРАФИИ В РАЗВИТИИ НАЦИОНАЛЬНОЙ ЦИФРОВОЙ ВАЛЮТЫ: ЗАЩИТА ДАННЫХ И ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН

Рассматривается роль криптографии в развитии национальной цифровой валюты и ее значимость в защите данных и преимущества использования технологии блокчейн. Будут рассмотрены основные принципы криптографии, такие как симметричное и асимметричное шифрование, цифровая подпись и хэширование. Уделяется внимание их значению в защите данных от несанкционированного доступа и подделки. Будут рассмотрены основные принципы блокчейн, такие как децентрализация, надежность, прозрачность и неизменность данных. Будет рассмотрено, как технология блокчейн может обеспечить безопасность и эффективность процессов использования национальной цифровой валюты. В результате исследования будет подчеркнуто значение криптографии в развитии национальной цифровой валюты и преимущества использования технологии блокчейн для обеспечения безопасности данных и эффективного функционирования финансовой системы.

Ключевые слова: блокчейн, защита данных, cbdc, криптографическая защита данных, смарт-контракт, хэширование в блокчейн-сети, дерево Меркла, приватный блокчейн, публичный блокчейн, PoW, PoA, PoS

Введение

На сегодняшний день весь мир проводит разработки по созданию цифровой валюты центрального банка. Одни изучают плюсы и минусы цифровых валют, другие занимаются практической подготовкой проектов цифровых валют. Лидерами в этой области являются КНР, Швеция, Индия, Казахстан, РФ, Венесуэла, Нигерия. С проблематикой CBDC оказывает глубокое содействие Банк международных расчетов в Базеле, проявляя консультативное содействие центробанкам в подготовке проектов цифровых валют, а также практикуя с расширением функций для оказания трансграничных расчетов, которые должны прийти на замену доллару США в качестве мировой валюты.

В связи с этим остро стоит вопрос о важности защиты данных и конфиденциальности при работе с цифровыми валютами. Современные технологии предоставляют нам удивительные возможности для работы с деньгами. Достаточно лишь иметь доступ к интернету, чтобы отправлять и получать цифровые валюты, проводить транзакции и инвестировать в криптовалюты. Однако вместе с этим возникает и серьезная угроза утечки личной информации и финансовых данных. Защита данных и конфиденциальности при работе с цифровыми валютами является важнейшим аспектом безопасности. Пользователи должны быть осведомлены о том, как защищать свои средства и личную информацию от хакерских атак и мошенничества. Использование надежных паролей, двухфакторной аутентификации и защиты аккаунта от несанкционированного доступа — это лишь несколько шагов, которые могут быть предприняты для обеспечения безопасности при работе с цифровыми валютами.

Кроме того, необходимо быть осторожными при обмене информацией о своих финансах в сети. Никогда не разглашайте свои пароли, секретные ключи или личные данные третьим лицам или на ненадежных ресурсах. Это может привести к серьезным последствиям, включая потерю средств и даже кражу личной информации.Таким образом, важность защиты данных и конфиденциальности при работе с цифровыми валютами не может быть недооценена. Соблюдение мер безопасности и осведомленность о возможных угрозах помогут пользователям избежать проблем и сохранить свои финансы в безопасности.

Роль криптографии в развитии национальной цифровой валюты

Криптография — это важный инструмент компьютерной безопасности, который включает в себя методы **хранения и передачи информации таким образом, чтобы**

предотвратить несанкционированный доступ к ним или вмешательство в их целостность.[1, 4]

Ключевыми принципами информационной безопасности являются конфиденциальность, целостность и доступность. Криптография является важным инструментом, который помогает сохранить два из этих принципов:

- **Конфиденциальность данных** гарантирует, что данные не будут раскрыты неавторизованным лицам. Криптографические методы, такие как шифрование, могут использоваться для защиты конфиденциальности данных, делая их абсолютно нечитаемыми для тех, у кого нет соответствующего ключа для их расшифровки.[4]
- **Целостность данных** гарантирует, что данные не были изменены или повреждены. Одним из примеров международных стандартов по целостности данных является ISO/IEC 9797, который определяет алгоритмы вычисления кодов аутентификации сообщений.[4]

В дополнение к вышеописанным ключевым целям информационной безопасности криптография используется для достижения таких целей, как:

1. **Аутентификация субъекта** – проверка знания определенного секрета, аутентификация субъекта проверяет личность отправителя.
2. **Цифровые подписи** – подтверждают, что данные исходят именно от подписанта и не были изменены.
3. **Неотказуемость** – используется для обеспечения гарантии, что отправитель и получатель сообщения не смогут отрицать, что они, соответственно, отправили или получили это сообщение.
4. **Управление цифровыми правами** – защита авторских прав на цифровой контент.
5. **Электронная коммерция** – защита информации о кредитных картах и связанных с ними личными данными, а также история покупок и транзакций клиентов.
6. **Криптовалюты и блокчейн** – защита транзакций в блокчейне.

Как правило, правильный хэш блока должен иметь следующие исходные данные:

- Корень Меркла – хэш всех включенных в блок транзакций, содержащийся в структуре данных дерева Меркла [5].
- Nonce – произвольное число/буквенное сочетание, которое создает действительный хэш, удовлетворяющий текущей цели сложности[5].
- Дополнительные метаданные блока – в разных блокчейнах они разные, но могут включать в себя следующее: текущую версию программного обеспечения блокчейна, метку времени, целевую сложность майнинга, корень состояния всей цепи или номер текущего блока [5].
- Хэш предыдущего блока – действительный хэш блока, который был проверен ранее.[5]

Блоки включают в себя хэш-значение предыдущего блока, чтобы обеспечить криптографическую связь и сохранить хронологический порядок реестра. Из-за сложности отмены ранее подтвержденных блоков через реорганизацию блокчейн считается неизменяемым. Любое изменение в одной транзакции блока приведет к изменению его хэша, что будет легко обнаружено другими узлами. Не все реорганизации блоков могут быть злонамеренными; они могут произойти из-за асинхронных сетевых условий. [5]Глубокие перерегистрации в блокчейне могут быть более спорными и сложными, чем поверхностные изменения.

Блокчейн (цель блоков) – это журнал с отметкой времени добавления записей. Записи можно добавлять и нельзя удалить. Накопление блоков приводит к формированию базы данных. На сегодняшний день Биткойн содержит в себе примерно 832,246 блока (2024-02-27 16:21:43). [2]Базы данных и блокчейн используют два криптографических инструмента – хэш-функции и цифровые подписи – для обеспечения безопасности. Вопрос права изменения данных в базе данных является основным объектом дискуссий, поскольку в

централизованных системах это право принадлежит единому центру, тогда как блокчейн децентрализован и вызывает вопрос о том, кто имеет право добавлять новую информацию. Механизм консенсуса разработан для решения этой проблемы.

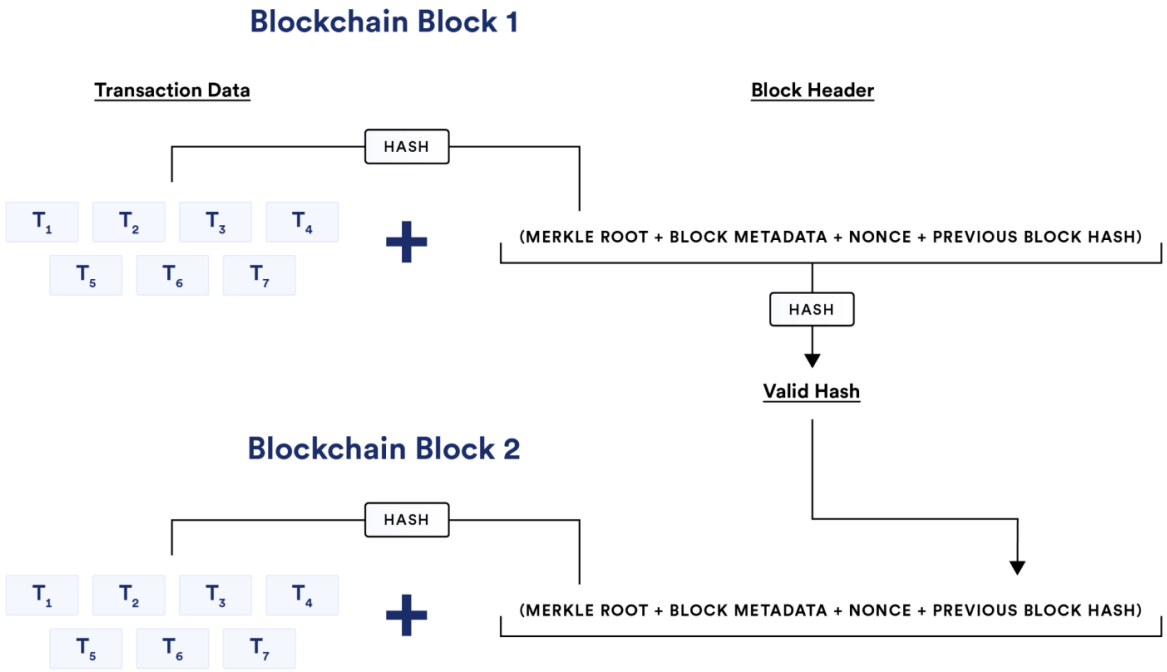

Рисунок 1 – Блоки состоят из данных транзакции, корня Меркла, других метаданных блока, действительного ключа (nonce) и хэша предыдущего блока. (Источник: https://habr.com/ru/articles/680650/, дата обращения: 27.02.2024)

Конструктивные особенности блокчейна [6]:

- Криптографические хэш-функции.
- Неудаляемые записи, помеченные временем.
- Заголовки блока и древо Меркла. Что попадает в заголовок блока, а что в тело блока.
- Ассиметричная криптография (приватный, публичный ключ) и цифровая подпись.
- Сами по себе адреса биткойна, которые отличаются от публичного ключа.
- Консенсусы.
- Нонсы. Очень важный протокол в биткойне отвечает за то, как информация распространяется по интернету. Здесь возникает вопрос сетевого общения. Это очень важная часть биткойна, как данные с одного устройства попадают на другое. На данный момент в сети биткойна есть где-то 10 000 нод или узлов. И мы не знаем, где они все находятся.
- Нативная валюта — это технологическая особенность блокчейна. Дело не только в том, что кто-то создал эту валюту, а в том, что она является частью экономической системы стимула.
- Вводные и выходные транзакции. Это как чек, где нужно записать, кто это отправляет и кто получает.
- Реестр неизрасходованных транзакций.
- Языки скриптования.

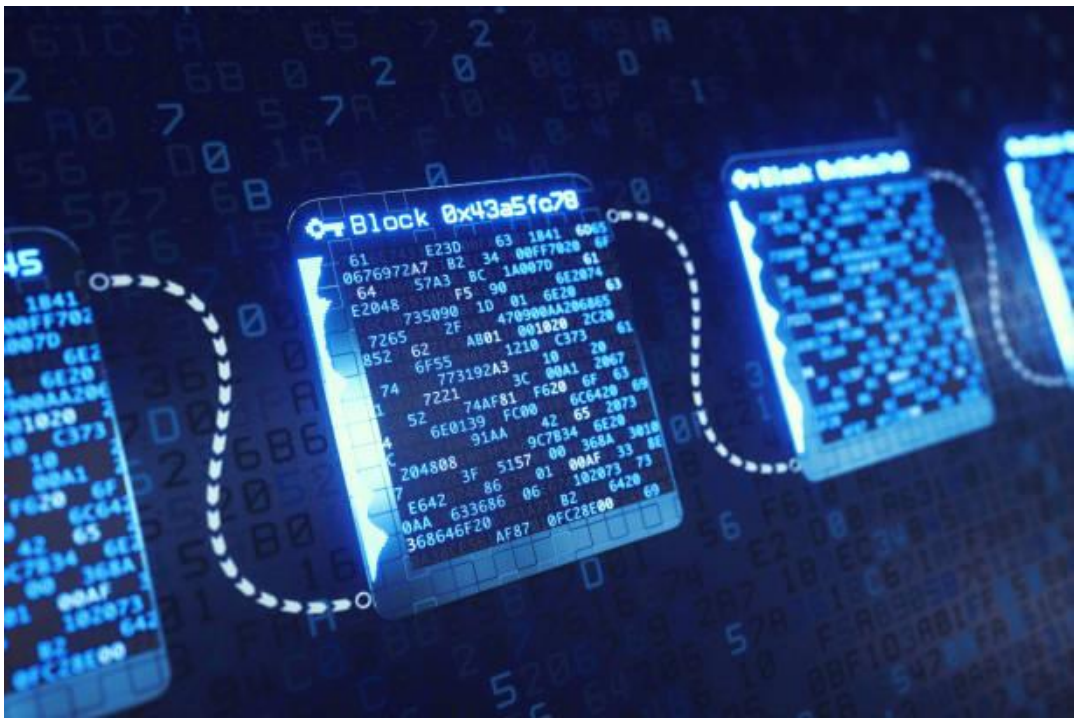

Рисунок 1– Пример представления блокчейна (Источник: https://www.istockphoto.com/ru/%D1%84%D0%BE%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8/%D0%B1%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD, дата обращения: 27.02.2024)

Добавление неудаляемой записи с временной меткой в блокчейне

Дерево Меркла (хеш-дерево) — это алгоритм, позволяющий получить один хеш для множества фрагментов данных. Метод используют для определения целостности файлов и верификации информации.[3]

Дерево Меркла представляет собой структуру, от основания которой до промежуточных узлов расходятся ветви. На концах разветвлений размещены листья, представляющие фрагменты данных. В основании дерева находится корневой хеш (корень Меркла). Последний является обязательным элементом заголовка блока биткоина. Корневой хеш позволяет верифицировать каждую транзакцию. Для проверки требуется скачать только заголовок блока и аутентификационный путь операции. Благодаря дереву Меркла снижается объем необходимых вычислений, что дает возможность реализовать упрощенную проверку платежей (SPV).[3]

Централизованная система предоставляет данные из одного источника, на который полагаются все пользователи. Последний гарантирует корректность полученной информации. Для снижения вычислительных затрат можно использовать деревья Меркла. Они позволяют уменьшить объем загружаемых данных и оптимизировать их проверку благодаря хешированию. Метод используется в сетях биткоина, Ethereum и других криптовалютах. С его помощью получают строку данных, которая верифицирует группу транзакций. Алгоритм также применяется в файловых системах и базах данных. С помощью деревьев Меркла информацию проверяют на наличие ошибок и проводят синхронизацию.

У технологии блокчейна и криптовалютных платформ появляется много преимуществ при использовании дерева Меркла для проверки транзакций – от эффективной проверки до простого обнаружения ошибки:

- Эффективный процесс проверки данных – использование деревьев Меркла в блокчейне существенно сокращает объем данных, необходимых для проверки целостности транзакций, и значительно уменьшает требуемую вычислительную мощность.

- Более высокая скорость обработки – каждый валидатор одновременно работает над другой транзакцией в результате распределения транзакций в блоке, что делает этот метод намного эффективнее, чем последовательная проверка каждой транзакции.
- Использование криптокошелька – простая проверка платежа (SPV), которая позволяет вам подтвердить транзакцию без загрузки всего блока или блокчейна.
- Обнаружение любого вмешательства – структура хеша позволяет майнерам легко идентифицировать вмешательство в транзакции. Создание хеш-значения для каждого блока с использованием корня Меркла связывает блоки между собой и предотвращает изменение транзакций. Это помогает создать неизменяемую запись транзакций и предотвратить двойное расходование.

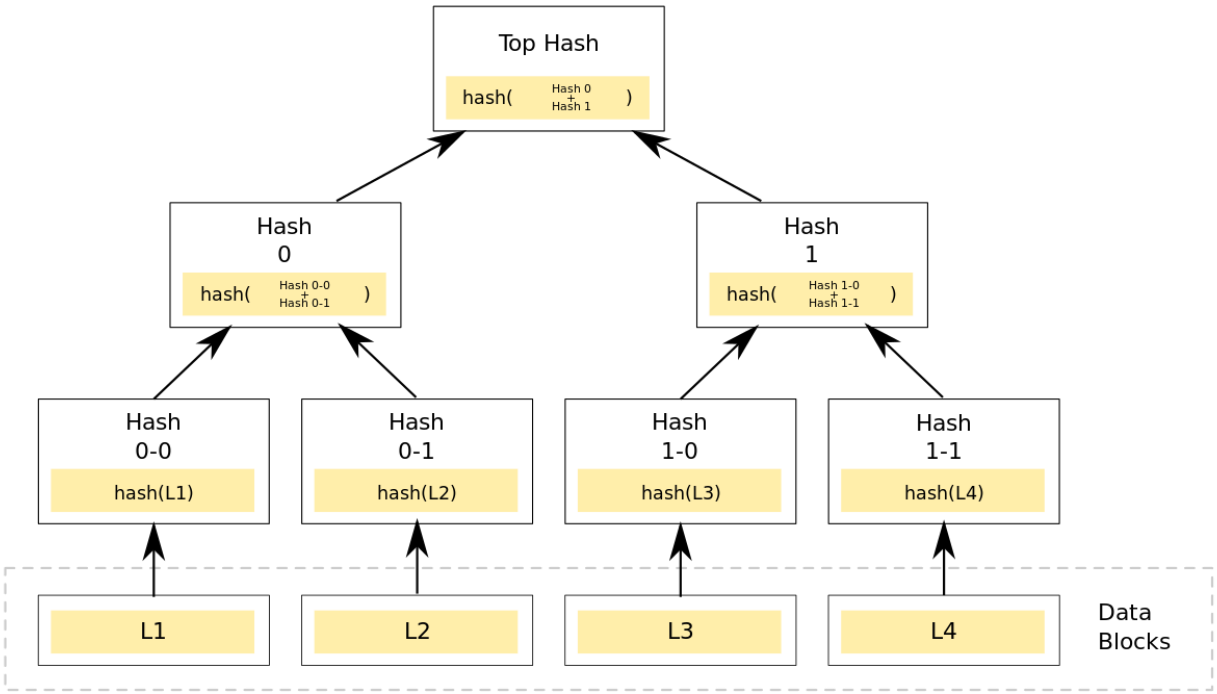

Рисунок 2 – Дерево Меркла из 4 блоков (Источник: https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D1%80%D0%B5%D0%B2%D0%BE_%D1%85%D0%B5%D1%88%D0%B5%D0%B9, дата обращения: 27.02.2024)

Большая часть блокчейнов обладает децентрализованной структурой, где функционирует множество независимых компьютеров, которые работают в сети, добавляя новые блоки к цепочке и обеспечивая её корректное функционирование. Для работы системы блокчейн каждый узел должен следовать определенным правилам алгоритма консенсуса. Алгоритм консенсуса блокчейна обеспечивает безопасность и достоверность данных в сети. 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. На рисунке 3 изображены некоторые наиболее распространенные из алгоритмов консенсуса, использующихся в блокчейне.

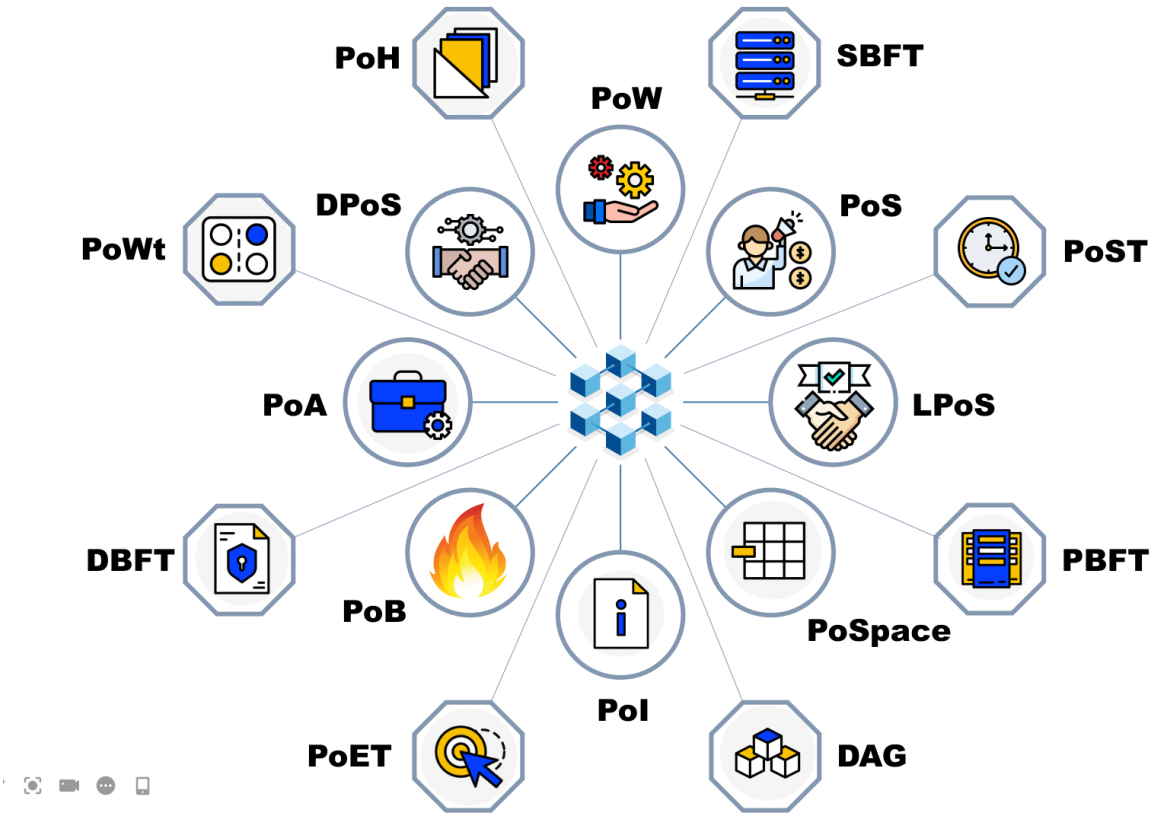

Рисунок 3– Разнообразие алгоритмов консенсуса (Источник: https://vc.ru/crypto/590486-algoritmy-konsensusa-chto-eto-i-kakie-byvayut, дата обращения: 27.02.2024)

Proof-of-Work (PoW)

Самый известный и один из наиболее распространенных алгоритмов консенсуса, который обеспечивает децентрализацию, безопасность, и стал основой для развития криптовалют. Но, несмотря на все преимущества, у него имеются следующие недостатки:

- **высокие затраты электроэнергии**;
- **низкая пропускная способность**;
- **высокие комиссии.**

Proof-of-Stake (PoS)

Алгоритм консенсуса, использующий замороженные объемы криптовалют для подтверждения транзакций PoS, применяется в таких блокчейнах, как Ethereum 2.0, BinanceSmartChain, Cardano, Tron. PoS не требует майнинга и специализированного оборудования, что снижает энергопотребление. Основной недостаток PoS – угроза централизации из-за риска консолидации крупных владельцев криптовалюты.

Delegated Proof-of-Stake (DPoS)

Это разновидность алгоритма PoS, который пытается избавиться от риска централизации путем делегирования права валидаторов держателям монет. Среди известных блокчейнов с применением алгоритма DPoS включаются такие проекты, как EOS, Tezos, и многие другие. Однако, как и в любой другой системе, DPoS имеет свои недостатки. Низкая активность участников сети может привести к тому, что DPoS станет похож на PoS, а также существует риск сговора между делегатами.

Proof-of-Authority (PoA)

Алгоритм PoA основывается на авторитете валидаторов, выбранных участниками сети путем голосования и использующих свою репутацию в качестве доказательства полномочий. Недостатком PoA является отсутствие стимулов и мотивации для участия валидаторов, поэтому этот алгоритм чаще используется в частных блокчейнах, где децентрализация не так важна.

Отличия приватного и публичного блокчейна

Приватные блокчейны чаще используют компании и корпорации. Так они упрощают аудит, бухгалтерский учет и другие процессы. Компаниям позволяется контролировать доступ к данным и определять права участников.

Один из самых больших минусов такой сети также является и преимуществом – ее легко взломать. Так как контролирует всю информацию один или несколько людей, злоумышленнику достаточно получить доступ к компьютеру одного из руководителей, что позволяет анализировать возможные попытки атаки на одну организацию. А в публичном блокчейне вероятность взлома сведена к минимуму из-за равных прав каждого участника сети и большого количества пользователей. Даже если злоумышленник получит доступ к компьютеру одного из участников, изменить блокчейн он не сможет. Но если участвует группа злоумышленников с большими ресурсами, это позволяет им провести атаку 51%, то есть захватить распределенную сеть и вносить свои изменения.

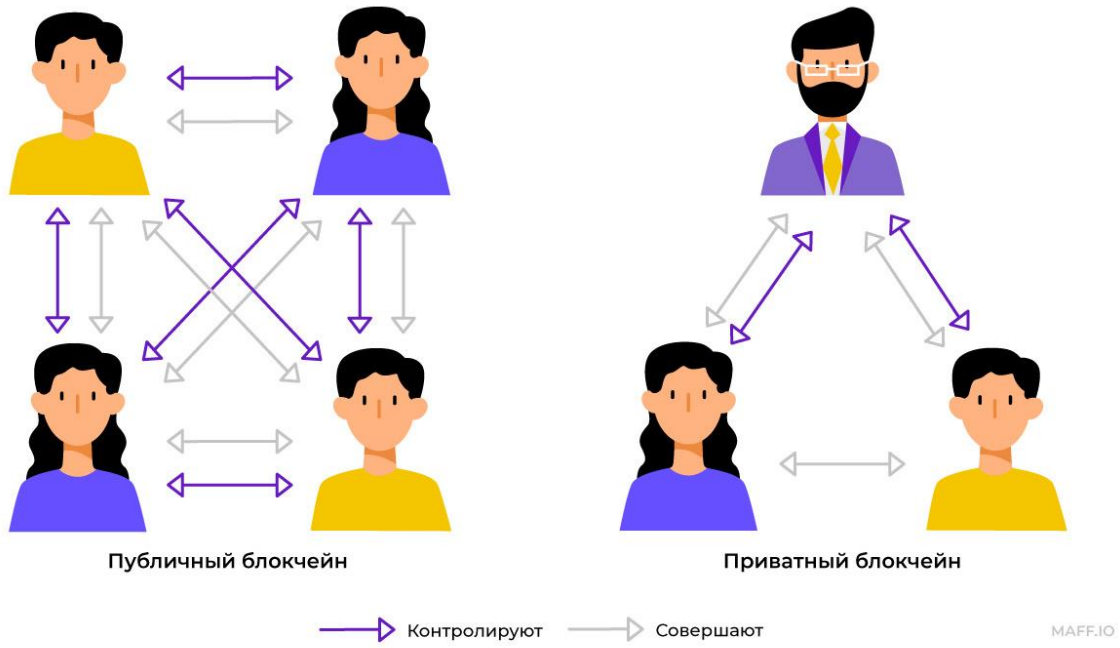

Рисунок 4– Отличие публичного и приватного блокчейна (Источник: https://maff.io/media/wp-content/uploads/2021/11/public_blockchain_info1.jpg, дата обращения: 27.02.2024)

Если частная блокчейн-сеть предназначена для использования только одной компанией, то доступ к управлению процессами имеют лишь избранные сотрудники — например, администраторы системы и управленческий персонал. Эти люди контролируют, кто имеет доступ к данным и право создавать новые блоки. Для доступа к системе необходимо получить авторизацию, которую выдает только высшее руководство. А в отличие от этого в открытую блокчейн-сеть может присоединиться любой желающий без ограничений. [7]

Процессы в закрытых блокчейнах в разы более быстрые, чем в открытых блокчейнах, так как в них участвует гораздо меньше узлов. Это позволяет избежать необходимости передавать информацию сразу на тысячи компьютеров, что обычно замедляет процесс и делает его более затратным. В результате транзакции в публичных блокчейнах обычно проходят медленнее и стоят дороже.[7]

Отличие от централизованной сети

Приватный блокчейн напоминает централизованную сеть, но с рядом особенностей децентрализованной сети:

- Неизменяемость. Как только данные внесли в блокчейн, их видят все участники, у которых есть доступ. Информация останется в блокчейне навсегда и будет неизменной. В обычной централизованной сети такого нет: информацию можно менять после публикации.[7]
- Цифровые подписи. Они облегчают сделку для двух сторон, потому что не нужно привлекать посредников и юристов.

На рисунке 5 можно заметить разницу между блокчейном и централизованной сетью. В сеть внесли документ с неправильными данными. В блокчейне его нельзя изменить или удалить: нужно внести новый исправленный документ. В централизованной сети можно просто изменить тот же документ

Рисунок 5 – Отличие блокчейна от централизованной сети (Источник: https://maff.io/media/wp-content/uploads/2021/12/%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%8B.jpg, дата обращения: 27.02.2024)

Преимуществом приватного блокчейна является его использование фирмами и корпорациями для оптимизации процессов аудита, учета и документооборота. Он контролируется группой доверенных лиц, определяющих, кто имеет доступ к платформе. Управляющие обладают правом создавать блоки, в то время как другие участники могут лишь просматривать или совершать транзакции. Приватный блокчейн отличается от публичного ограниченным доступом, частичной децентрализацией и быстрыми транзакциями. Наиболее важная особенность – неизменяемость записей в блокчейне, что гарантирует их надежность и сохранность на протяжении всего срока хранения. [7]

Заключение

В заключение: создание цифровой валюты с использованием консенсуса Proof-of-stake, proof-of-authority, приватного блокчейна и смарт-контрактов, а также дерева Меркла представляет собой важный шаг в обеспечении безопасности, прозрачности и эффективности финансовых операций. Эти технологии позволяют обеспечить высокую степень надежности и неподдельности данных, а также снизить риски мошенничества и коррупции. Реализация подобной цифровой валюты способствует развитию экономики и облегчает обмен ценностями между участниками, делая процесс более простым и удобным.

С точки криптографии необходимо применять хэш-функции, как SHA-256 и ассиметричные алгоритмы шифрования с публичным и приватным ключами. В итоге криптографическая правда приносит стабильность, точность и прозрачность в наши

вычисления и записи. Зная, что программный код будет исполнен верно и что исторические данные защищены от вмешательства, мы можем строить социальные и экономические отношения на основе истины на более высоком уровне. Существование надежного основания правды способствует развитию экономики и укреплению социального согласия, что является идеалом для всех. Поэтому важно создавать и внедрять технологии блокчейна и оракулов, утверждающие криптографическую правду во всем взаимодействии нашего общества.

Список использованных источников

1. Что такое криптография? - .- URL: https://www.iso.org/ru/information-security/what-is-cryptography#:~:text=%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F%20%2D%20%D1%8D%D1%82%D0%BE%20%D0%B2%D0%B0%D0%B6%D0%BD%D1%8B%D0%B9%20%D0%B8%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BC%D0%B5%D0%BD%D1%82%20%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%BE%D0%B9,%D0%B8%D0%BB%D0%B8%20%D0%B2%D0%BC%D0%B5%D1%88%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE%20%D0%B2%20%D0%B8%D1%85%20%D1%86%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C. (дата обращения: 27.02.2024). Текст: электронный.
2. Биткоин (BTC) цены и статистика - .- URL: https://bitinfocharts.com/ru/bitcoin/ (дата обращения 27.02.2024). Текст: электронный.
3. Что такое дерево Меркла? - .- URL: https://forklog.com/cryptorium/chto-takoe-derevo-merkla (дата обращения: 27.02.2024). Текст: электронный.
4. Что такое криптография? - .- URL: https://standard.kz/ru/post/cto-takoe-kriptografiya(дата обращения: 27.02.2024). Текст: электронный.
5. Криптография и будущее децентрализованных вычислений - .- URL: https://habr.com/ru/articles/680650/(дата обращения: 27.02.2024). Текст: электронный.
6. Криптография и основы блокчейна - .- URL: https://vc.ru/crypto/571604-3-kriptografiya-i-osnovy-blokcheyna(дата обращения: 27.02.2024). Текст: электронный.
7. Что такое приватный блокчейн и где используется - .- URL: https://Maff.io/private_blockchain_foil/(дата обращения: 27.02.2024). Текст: электронный.