Технология блокчейн
#6

Понимание DLT, Bitcoin, Ethereum и BNB Chain

Обзор

1. Технология распределенного реестра (DLT)
2. DLT в сравнении с традиционными базами данных
3. Bitcoin и Реестр Bitcoin
4. Ethereum и Реестр Ethereum
5. BNB Chain

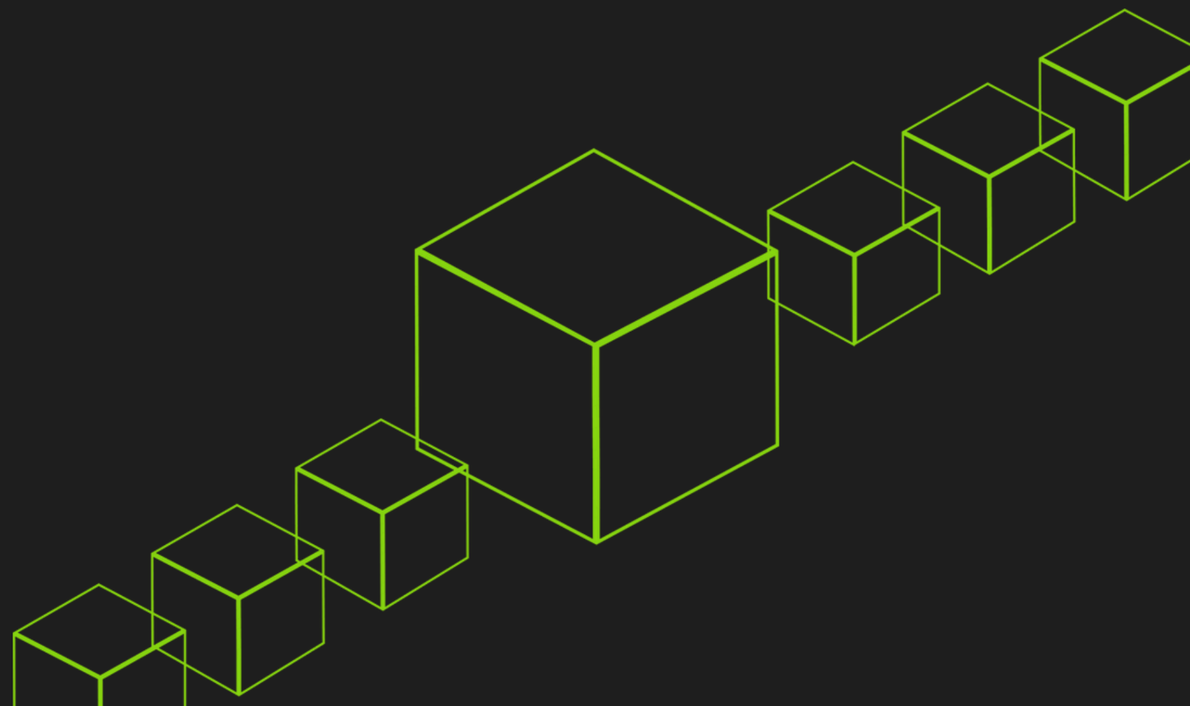
Blockchain Center

Модуль 1 - Технология распределенного реестра (DLT)

Blockchain Center

Технология Распределенного Реестра (DLT)

- Что такое DLT?
- Примеры DLT
- Разные виды DLT
- Особенности DLT



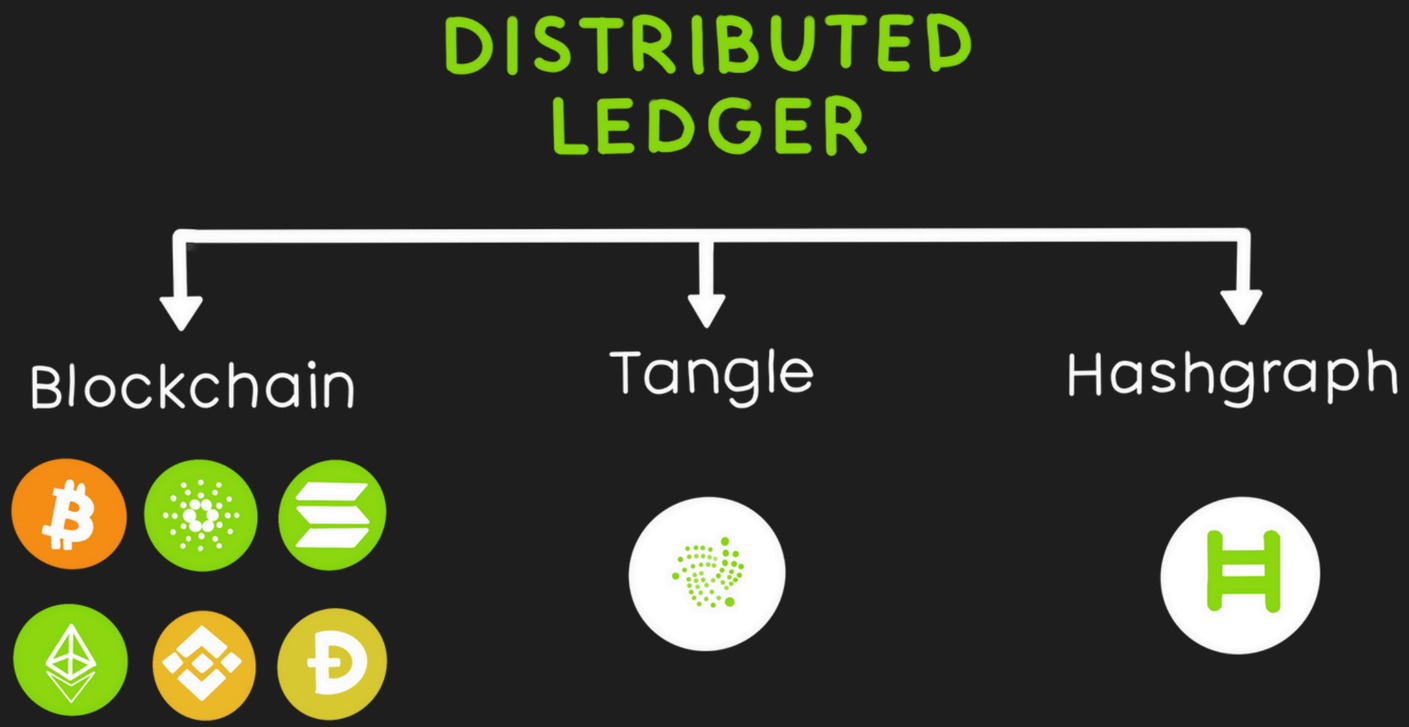
Blockchain Center

Что такое DLT?

- Распределенный реестр - это тип **базы данных**, которая совместно используется **сетью компьютеров**, позволяя всем участникам получить **доступ к одной и той же информации** и **обеспечивая прозрачное** и **безопасное внесение изменений** в реестр.
- DLT - это **системы**, использующие распределенные реестры для **хранения** и **отслеживания транзакций** или **других типов данных**.
- Блокчейн - один из примеров DLT, часто используемый для **создания** и **отслеживания** криптовалютных транзакций. Их **децентрализованный** и **прозрачный характер** делает DLT подходящими для использования в приложениях, где важны безопасность, доверие и отслеживание изменений.

Blockchain Center

Примеры DLT



Blockchain
Center

Разные виды DLT

- Каждый блокчейн работает на технологии **распределенных реестров**. Однако каждая криптовалюта может работать не на технологии блокчейн. Помимо технологии блокчейн, криптовалюта может работать на Tangle или Hashgraph. В отличие от блокчейна, **Tangle работает как структура Directed Acyclic Graph (DAG)**, где каждая транзакция **подтверждает** две предыдущие транзакции, что устраняет необходимость в майнерах и, таким образом, **обеспечивает масштабируемое решение** для высокоскоростных и недорогих транзакций.
- С другой стороны, Hashgraph - это **технология распределенных реестров** (DLT), которая использует **уникальный алгоритм консенсуса** для **подтверждения** транзакций и **поддержания целостности сети**. Он использует протокол "сплетни о сплетнях", позволяющий узлам сети **обмениваться информацией** и **достигать консенсуса быстрым** и **безопасным способом**.

Blockchain Center

Особенности DLT

DLT могут использоваться для хранения и отслеживания юридических документов, таких как контракты и акты. Поскольку DLT прозрачны и неизменяемы, они обеспечивают безопасный и защищенный от взлома способ хранения и управления юридическими документами.

Blockchain Center

Особенности DLT

DLT могут использоваться для хранения и отслеживания юридических документов, таких как контракты и акты. Поскольку DLT прозрачны и неизменяемы, они обеспечивают безопасный и защищенный от взлома способ хранения и управления юридическими документами.

DLT можно использовать для отслеживания движения товаров по цепочке поставок, от стадии сырья до конечного продукта. Это может помочь повысить эффективность, сократить отходы и повысить прозрачность цепочки поставок.

Blockchain Center

Особенности DLT

DLT могут использоваться для хранения и отслеживания юридических документов, таких как контракты и акты. Поскольку DLT прозрачны и неизменяемы, они обеспечивают безопасный и защищенный от взлома способ хранения и управления юридическими документами.

DLT можно использовать для отслеживания движения товаров по цепочке поставок, от стадии сырья до конечного продукта. Это может помочь повысить эффективность, сократить отходы и повысить прозрачность цепочки поставок.

DLT можно использовать для хранения и отслеживания медицинских записей. Это поможет повысить точность и безопасность медицинских записей, а также упростит доступ и обмен важной информацией для медицинских работников.

Blockchain Center

Модуль 2 - DLT в сравнении с традиционными базами данных

Blockchain Center

DLT в сравнении с традиционными базами данных

Децентрализация:
Традиционная база данных обычно имеет централизованную реестр, контролируемую одним субъектом или организацией. В отличие от этого, DLT имеет децентрализованный реестр, распределенную по сети компьютеров и не контролируемую ни одной организацией. Эта децентрализация делает DLT более устойчивыми к взлому и цензуре.

Blockchain Center

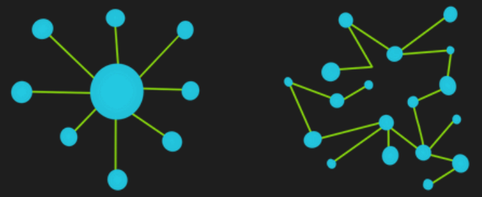
DLT в сравнении с традиционными базами данных

Децентрализация: Традиционная база данных обычно имеет централизованную реестр, контролируемую одним субъектом или организацией. В отличие от этого, DLT имеет децентрализованный реестр, распределенную по сети компьютеров и не контролируемую ни одной организацией. Эта децентрализация делает DLT более устойчивыми к взлому и цензуре.

Прозрачность: Все транзакции или другие типы данных, хранящиеся в бухгалтерской книге, видны всем участникам сети. В отличие от этого, традиционные базы данных часто имеют ограниченный доступ и не являются прозрачными в той же степени.

Blockchain Center

DLT в сравнении с традиционными базами данных



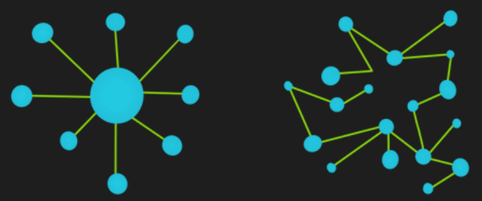
Децентрализация:
Традиционная база данных обычно имеет централизованную реестр, контролируемую одним субъектом или организацией. В отличие от этого, DLT имеет децентрализованный реестр, распределенную по сети компьютеров и не контролируемую ни одной организацией. Эта децентрализация делает DLT более устойчивыми к взлому и цензуре.

Прозрачность: Все транзакции или другие типы данных, хранящиеся в бухгалтерской книге, видны всем участникам сети. В отличие от этого, традиционные базы данных часто имеют ограниченный доступ и не являются прозрачными в той же степени.

Неизменность:
Как только данные внесены в бухгалтерскую книгу, они не могут быть изменены или удалены. Это делает DLT хорошо подходящими для использования в приложениях, где важно вести точный учет транзакций или других типов данных.

Blockchain Center

DLT в сравнении с традиционными базами данных



Децентрализация:
Традиционная база данных обычно имеет централизованную реестр, контролируемую одним субъектом или организацией. В отличие от этого, DLT имеет децентрализованный реестр, распределенную по сети компьютеров и не контролируемую ни одной организацией. Эта децентрализация делает DLT более устойчивыми к взлому и цензуре.

Прозрачность: Все транзакции или другие типы данных, хранящиеся в бухгалтерской книге, видны всем участникам сети. В отличие от этого, традиционные базы данных часто имеют ограниченный доступ и не являются прозрачными в той же степени.

Неизменность:
Как только данные внесены в бухгалтерскую книгу, они не могут быть изменены или удалены. Это делает DLT хорошо подходящими для использования в приложениях, где важно вести точный учет транзакций или других типов данных.

Механизм консенсуса:
Традиционные базы данных обычно используют централизованную систему для управления и проверки данных, в то время как DLT используют механизм консенсуса для проверки и регистрации транзакций. Это может быть алгоритм доказательства выполнения работы, как в блокчейне Bitcoin, или алгоритм доказательства ставки, как в блокчейне Ethereum.

Blockchain Center

Как блокчейн спользует DLT?

- DLT - это **децентрализованная система**, которая **хранит** и **проверяет данные** в блоках, которые добавляются в бухгалтерскую книгу в линейном, хронологическом порядке. Каждый блок содержит **хэш предыдущего блока** и другие метаданные, **создавая цепочку блоков**, связанных между собой линейным образом.
- DLT устойчива к фальсификации и цензуре, поскольку она распределена по сети компьютеров и не контролируется каким-либо одним субъектом. Это затрудняет изменение данных в бухгалтерской книге без консенсуса сети.
- Существует множество различных **DLT-платформ**, включая Bitcoin, Ethereum и BNB Smart Chain. Эти платформы используются для **широкого спектра** приложений, включая финансовые операции, управление цепочками поставок и даже системы голосования.

Blockchain Center

Типы реестров:

- На базе транзакции
- На базе акаунтов

Blockchain
Center

Модуль 3 - Bitcoin и его тип реестра

Blockchain
Center

Про Bitcoin

Биткойн - это **децентрализованная криптовалюта**, использующая блокчейн для **отслеживания** и **проверки транзакций**. Это **первая** и **самая известная криптовалюта**, которая позволяет пользователям отправлять и получать платежи без центрального органа. Одним из главных **преимуществ биткоина** является его **децентрализация**, что делает его **устойчивым к взлому** и **цензуре**. Но есть и **некоторые недостатки**

Blockchain Center

Недостатки Bitcoin

Масштабируемость Блокчейн Биткойна имеет ограниченную мощность и может обрабатывать лишь небольшое количество транзакций в секунду. Это может сделать его медленным и дорогим в использовании использование, особенно в периоды высокого спроса.	**Потребление энергии** Процесс добычи новых биткойнов требует большого количества вычислительной мощности, что потребляет значительное количество энергии. Это вызывает обеспокоенность по поводу воздействия майнинга биткоинов на окружающую среду.	**Волатильность** Стоимость биткоина может быть очень неустойчивой, что затрудняет его использование в качестве стабильного хранилища стоимости или средства обмена.	**Отсутствие регулирования** Поскольку биткоин не контролируется центральным органом власти, он не подлежит регулированию, как традиционные финансовые учреждения. Это может затруднить защиту от мошенничества и других видов финансовых преступлений.

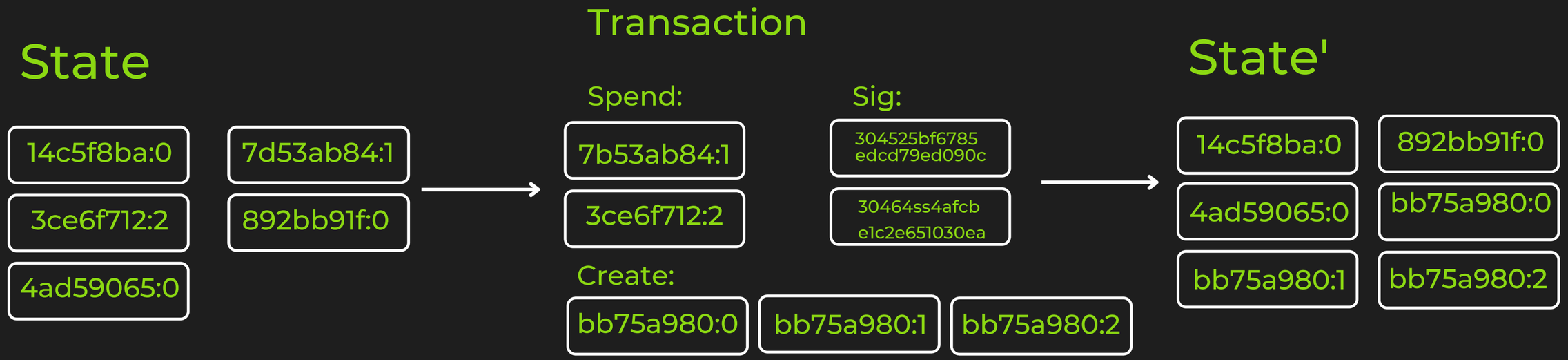
Blockchain Center

Какой реестр используется в bitcoin?

Тип реестра использоемой в блокчейне bitcoin назывентся UTXO - Unspent Transaction Output или выход неизрасходованных транзакций

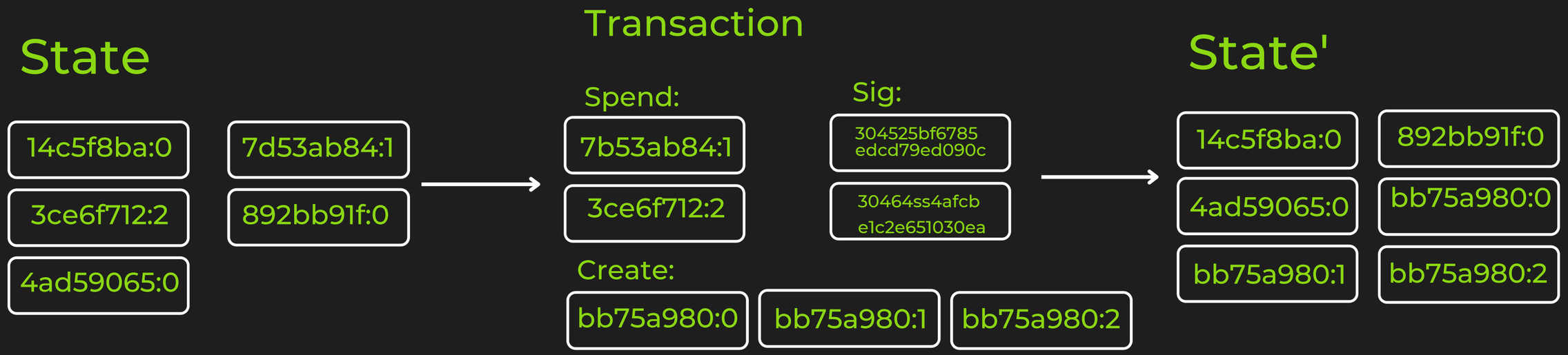
Blockchain Center

Тип реестра Bitcoin - UTXO



Blockchain Center

Тип реестра Bitcoin - UTXO



Функция перехода состояния APPLY(S,TX) -> S' может быть определена приблизительно следующим образом:

1. Для каждого ввода в TX:
    1.1. Если ссылаемый UTXO не находится в S, возвращается ошибка.
    1.2. Если предоставленная подпись не совпадает с владельцем UTXO, возвращается ошибка.
2. Если сумма номиналов всех входных UTXO меньше суммы номиналов всех выходных UTXO, возвращается ошибка.
3. Вернуть S с удаленными всеми входными UTXO и добавленными всеми выходными UTXO.

Blockchain Center

Транакции в Bitcoin реестре

КЛАССИЧЕСКИЕ ТРАНЗАКЦИИ

«У МЕНЯ ЕСТЬ 5 РУБЛЕЙ, ДЕРЖИ 3»

ТРАНЗАКЦИИ В БЛОКЧЕЙНЕ

«ДЕРЖИ 25 BTC, ИЗ КОТОРЫХ 5 МНЕ ДАЛ ВАНЯ, 12 МАКС, ..., И ВЕРНИ 3 BTC СДАЧИ»

Blockchain Center

Модуль 4 - Ethereum и его тип реестра

Blockchain Center

Что такое Ethereum?

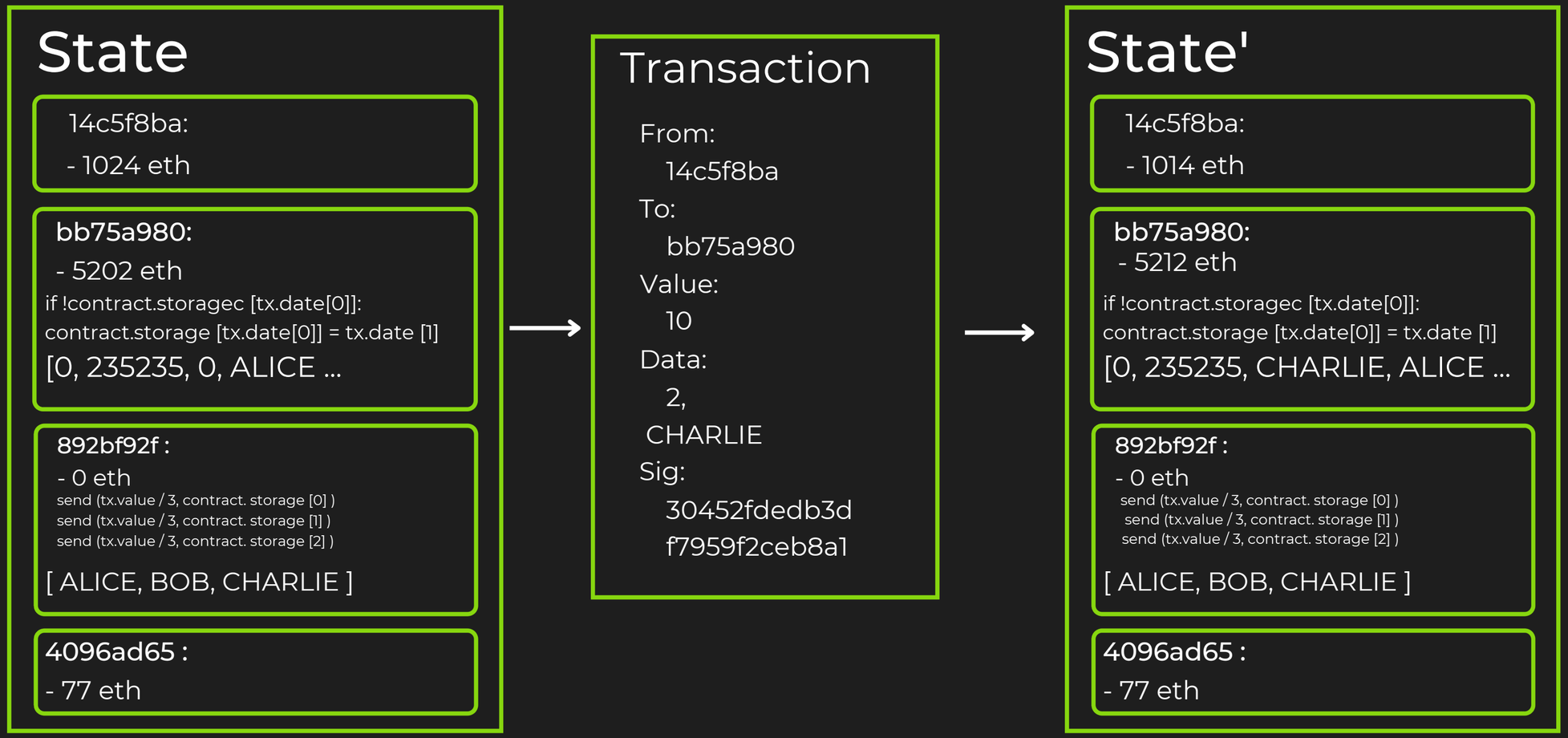
Эфириум (от англ. **Ethereum**) – это **децентрализованная вычислительная платформа**. Можете считать его своего рода ноутбуком или ПК, но с оговоркой на то, что данная система **не может функционировать лишь на одном устройстве**. Эфириум **одновременно работает на тысячах вычислительных машин по всему миру**, то есть у него **нет одного-единственного владельца**.

Эфириум, как и биткоин, и другие криптовалюты, служит для **перевода цифровых денег**. Однако возможности этой **сети гораздо шире** – вы можете **использовать** свой **собственный код** и **взаимодействовать** с приложениями, созданными другими пользователями. Благодаря **своей гибкости** эфириум **позволяет запускать** множество программ различной сложности.

Простыми словами, суть в том, что **разработчики** могут **создавать** и **запускать код** в **распределенной сети** вместо централизованного сервера.

Blockchain Center

Тип реестра Ethereum



Blockchain Center

Ethereum как state machine

Функция перехода состояния Ethereum, APPLY(S,TX) -> S', может быть определена следующим образом:

1. **Проверить, правильно ли сформирована транзакция** (т.е. имеет ли она нужное количество значений), действительна ли подпись, и совпадает ли nonce с nonce на счете отправителя. Если нет, возвращается ошибка.
2. **Рассчитайте комиссию за транзакцию как STARTGAS * GASPRICE и определите адрес отправителя из подписи**. Вычтите комиссию из баланса счета отправителя и увеличьте nonce отправителя. Если баланса недостаточно для расходования средств, верните ошибку.
3. **Инициализировать GAS = STARTGAS и снять определенное количество газа с каждого байта, чтобы оплатить байты в транзакции.**

Ethereum как state machine

Функция перехода состояния Ethereum, APPLY(S,TX) -> S', может быть определена следующим образом:

1. **Проверить, правильно ли сформирована транзакция** (т.е. имеет ли она нужное количество значений), действительна ли подпись, и совпадает ли nonce с nonce на счете отправителя. Если нет, возвращается ошибка.
2. **Рассчитайте комиссию за транзакцию как STARTGAS * GASPRICE и определите адрес отправителя из подписи**. Вычтите комиссию из баланса счета отправителя и увеличьте nonce отправителя. Если баланса недостаточно для расходования средств, верните ошибку.
3. **Инициализировать GAS = STARTGAS и снять определенное количество газа с каждого байта, чтобы оплатить байты в транзакции.**
4. **Перевести стоимость транзакции со счета отправителя на счет получателя.** Если счет-получатель еще не существует, создайте его. Если счет-получатель является контрактом, выполните код контракта либо до конца, либо пока в процессе выполнения не закончится газ.
5. Если передача ценности не удалась, потому что у отправителя не было достаточно денег, или в процессе выполнения кода закончился газ, верните все изменения состояния, кроме выплаты вознаграждения, и добавьте вознаграждение на счет майнера.
6. В противном случае верните отправителю плату за весь оставшийся газ, а плату за потребленный газ отправьте майнеру.

Blockchain Center

Ethereum как state machine

Предположим, что хранилище контракта начинается пустым, и посылается транзакция, содержащая 10 эфиров, 2000 газа, 0,001 цены газа эфира и 64 байта данных, где байты 0-31 представляют число 2, а байты 32-63 - строку CHARLIE. Процесс для функции перехода состояния в этом случае выглядит следующим образом:

1. Проверьте, что **транзакция действительна** и **правильно оформлена**.
2. Проверьте, есть ли у отправителя транзакции не менее 2000 * 0,001 = 2 эфира. Если это так, то вычтите 2 эфира из счета отправителя.
3. Инициализируйте газ = 2000; предполагая, что длина транзакции 170 байт, а байт-штраф равен 5, вычтите 850, чтобы осталось 1150 газа.

Ethereum как state machine

Предположим, что хранилище контракта начинается пустым, и посылается транзакция, содержащая 10 эфиров, 2000 газа, 0,001 цены газа эфира и 64 байта данных, где байты 0-31 представляют число 2, а байты 32-63 - строку CHARLIE. Процесс для функции перехода состояния в этом случае выглядит следующим образом:

1. Проверьте, что **транзакция действительна** и **правильно оформлена**.
2. Проверьте, есть ли у отправителя транзакции не менее 2000 * 0,001 = 2 эфира. Если это так, то вычтите 2 эфира из счета отправителя.
3. Инициализируйте газ = 2000; предполагая, что длина транзакции 170 байт, а байт-штраф равен 5, вычтите 850, чтобы осталось 1150 газа.
4. **Вычтите еще 10 эфиров** со счета отправителя и добавьте их на счет контракта.
5. **Запустите код**. В данном случае все просто: он проверяет, используется ли хранилище контракта с индексом 2, замечает, что нет, и устанавливает хранилище с индексом 2 в значение CHARLIE. Предположим, что на это уходит 187 газа, поэтому оставшееся количество газа равно 1150 - 187 = 963
6. Добавьте 963 * 0.001 = 0.963 эфира обратно на счет отправителя и верните полученное состояние.

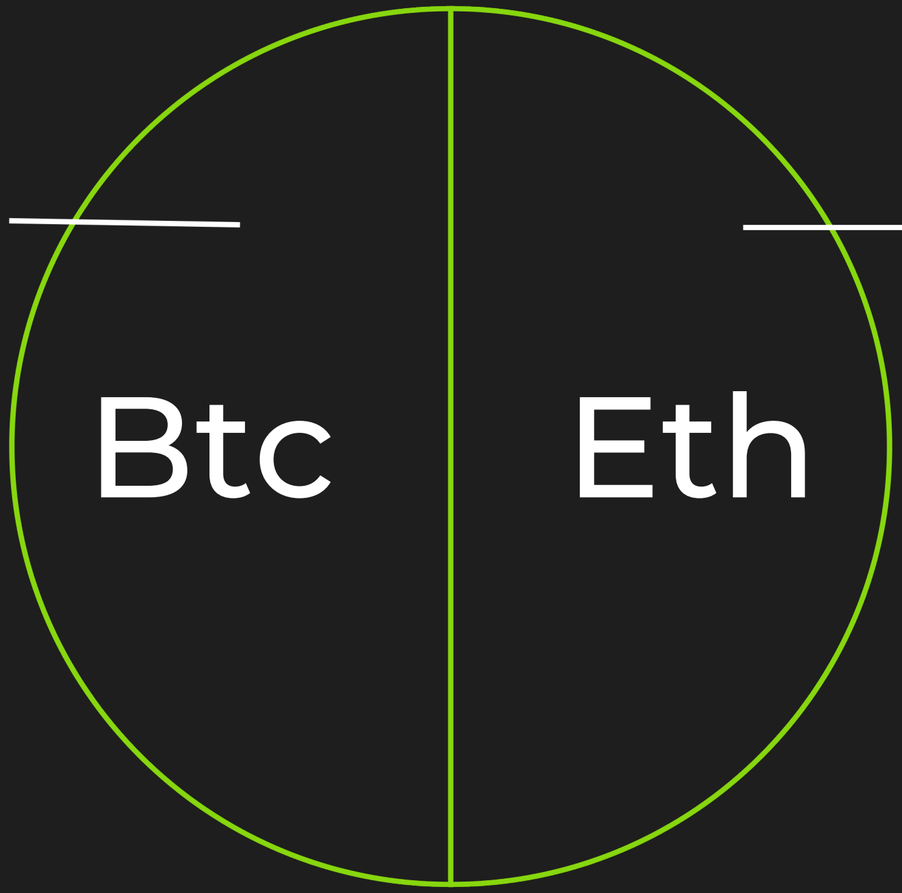
Если бы на стороне получателя транзакции не было контракта, то общая плата за транзакцию была бы просто равна предоставленной GASPRICE, умноженной на длину транзакции в байтах, а данные, отправленные вместе с транзакцией, не имели бы значения.

Blockchain
Center

Разница между распределнными реестрами Bitcoin и Ethetereum

Transaction based

Coins are stored as a lsit of unspent transaction or UTXOs.



Account based

Coins are represented as a balance within an account.

What about tokens?

Blockchain Center

Модуль 3 - BNB Chain

Blockchain
Center

Блокчейны экосистемы BNB Chain

Состоит из BNB Beacon Chain и **BNB Chain**

BNB Beacon Chain был запущен компанией Binance в **апреле 2019 года**. Его **главная задача** — содействовать **быстрой децентрализованной** (или некастодиальной) торговле. В результате крупнейшим децентрализованным приложением (DApp) на этом блокчейне является децентрализованная биржа Binance DEX.

BNB Smart Chain (BNB Chain) — это **блокчейн**, который **работает параллельно** BNB Beacon Chain. BNB Chain **обеспечивает функциональность** смарт-контрактов и совместимость с виртуальной машиной Ethereum (EVM). Его **цель — сохранить высокую пропускную способность** BNB Beacon Chain и при этом внедрить в экосистему смарт-контракты. BNB Chain не является решением второго уровня или офчейн-решением для масштабирования.

Blockchain Center

Как работает BNB Smart Chain

Консенсус

Время **создания блока** в BNB Smart Chain достигает **примерно трех секунд** благодаря **алгоритму консенсуса Proof of Stake**. В частности, сеть использует алгоритм Proof of Staked Authority (PoSA), в рамках которого участники вносят BNB в стейкинг, чтобы стать валидаторами. Если они предложат действительный блок, то получат включенные в него комиссии за транзакции.

Кроссчейн-совместимость

Сеть BNB Smart Chain была задумана как **независимое дополнение** к существующей BNB Chain. Ее архитектура двойного чейна позволяет беспрепятственно переводить активы с одного блокчейна на другой. Таким образом, на BNB Chain можно осуществлять **быструю торговлю**, а на BSC — создавать **мощные децентрализованные приложения**. Такая совместимость предоставляет пользователям доступ к **обширной экосистеме**, способной **выполнять множество задач**.

Blockchain Center

Особенности BNB Chain

BNB Smart Chain была запущена в **сентябре 2020 года** как **высокопроизводительная блокчейн-сеть** для децентрализованных приложений. Она **разработана** для **обеспечения высокой скорости транзакций** и **низких комиссий за транзакции**, что делает ее **привлекательным вариантом** для разработчиков, желающих создать новые приложения.

Одна из особенностей высокая производительность:
BNB Smart Chain может обрабатывать **до 100 транзакций в секунду**, что делает ее одной из **самых быстрых блокчейн-сетей**, доступных в настоящее время.

Blockchain
Center

Особенности BNB Chain

Низкие тарифы:

Транзакции в **BNB Smart Chain** обычно стоят менее $0,03, что делает ее **доступным** вариантом для **разработчиков** и **пользователей.**

Межцепочечная совместимость:

BNB Smart Chain (BSC) способна **взаимодействовать** с другими блокчейн-сетями, такими как Ethereum, благодаря реализации межцепочечных коммуникационных протоколов. Это позволяет передавать активы и информацию между BSC и другими сетями блокчейн.

Совместимость с EVM:

BNB Smart Chain (BSC) оснащена совместимостью с виртуальной машиной Ethereum (EVM), что позволяет разрабатывать смарт-контракты и децентрализованные приложения с использованием языка программирования Solidity.

Стейкинг:

Механизм стейкинга BNB Smart Chain позволяет держателям BNB "стейкать" или блокировать свои токены, чтобы помочь обеспечить безопасность сети и получить взамен вознаграждение.

Blockchain Center

Blockchain Center

Спасибо за внимание