Технология блокчейн
#4

Как Работает Блокчейн?

Blockchain Center

Обзор

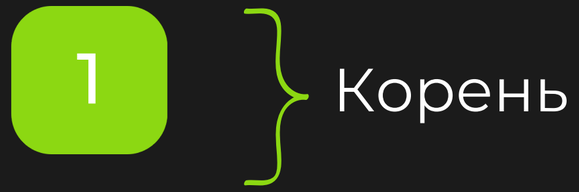
- Дерево Меркла
  - Двоичное дерево
  - Дерево Меркла
  - Корень Меркла
  - Как работает доказательство Меркла на блокчейне?
- Рабочий процесс блокчейна
  - Ноды
  - Блокчейн как рабочий процесс
  - Блокчейн форки
  - Типы транзакций блокчейна
- Практика

Двоичное дерево

Бинарное дерево - это древовидная структура данных, в котором каждый узел имеет не более двух дочерних элементов.

Бинарные деревья можно использовать для представления иерархических структур и для оценки математических выражений.

Они также могут иметь множество других применений, например, для реализации алгоритмов поиска.

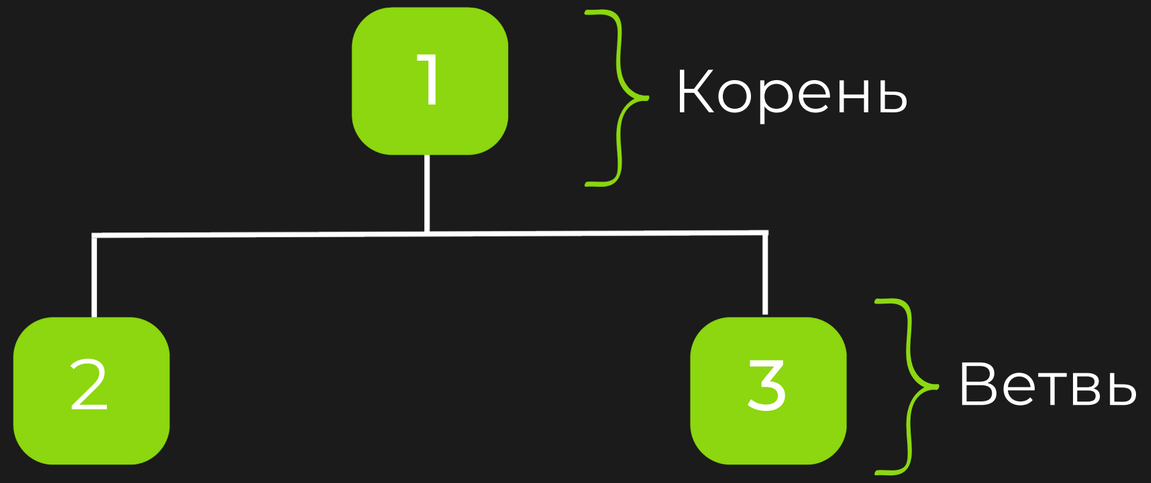


Двоичное дерево

Бинарное дерево - это древовидная структура данных, в которой каждый узел имеет не более двух дочерних элементов.

Бинарные деревья можно использовать для представления иерархических структур и для оценки математических выражений.

Они также могут иметь множество других применений, например, для реализации алгоритмов поиска.

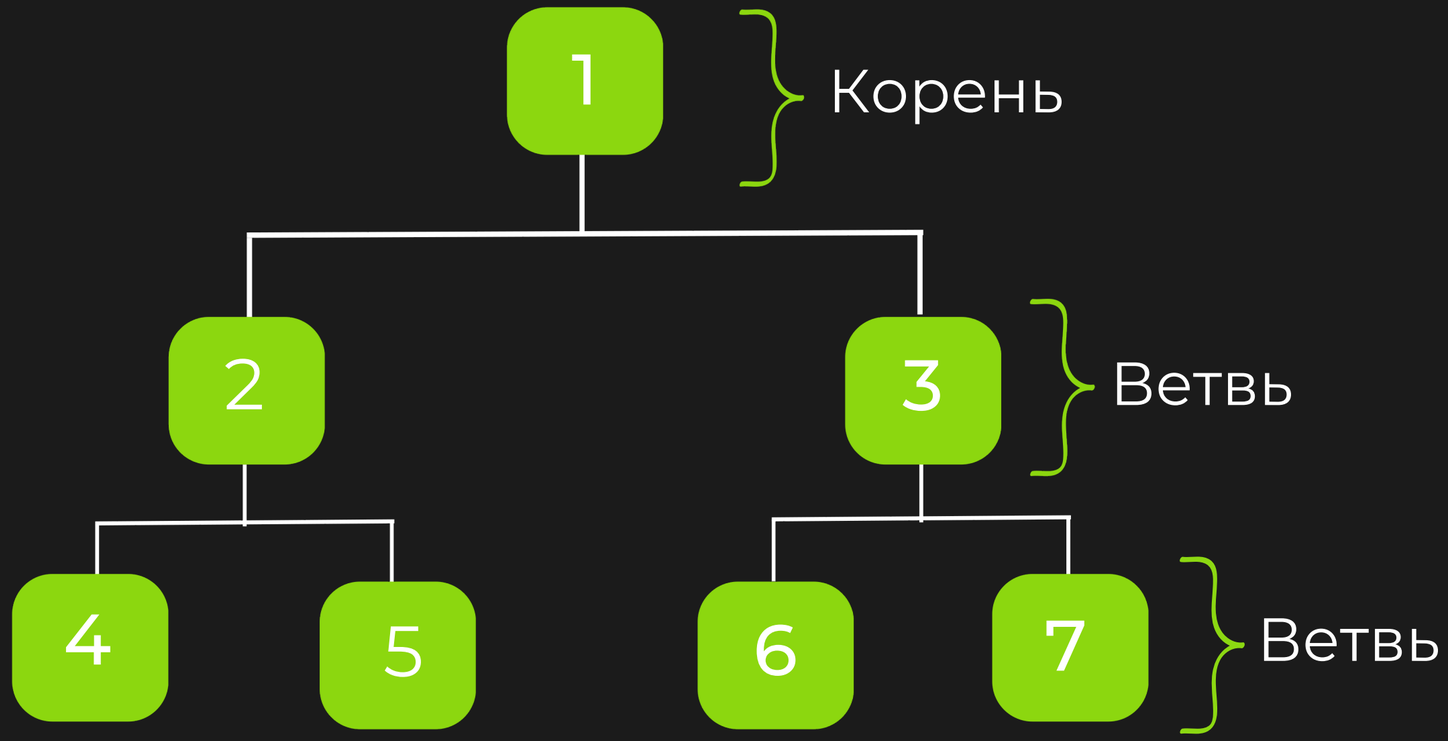


Двоичное дерево

Бинарное дерево - это древовидная структура данных, в которой каждый узел имеет не более двух дочерних элементов.

Бинарные деревья можно использовать для представления иерархических структур и для оценки математических выражений.

Они также могут иметь множество других применений, например, для реализации алгоритмов поиска.

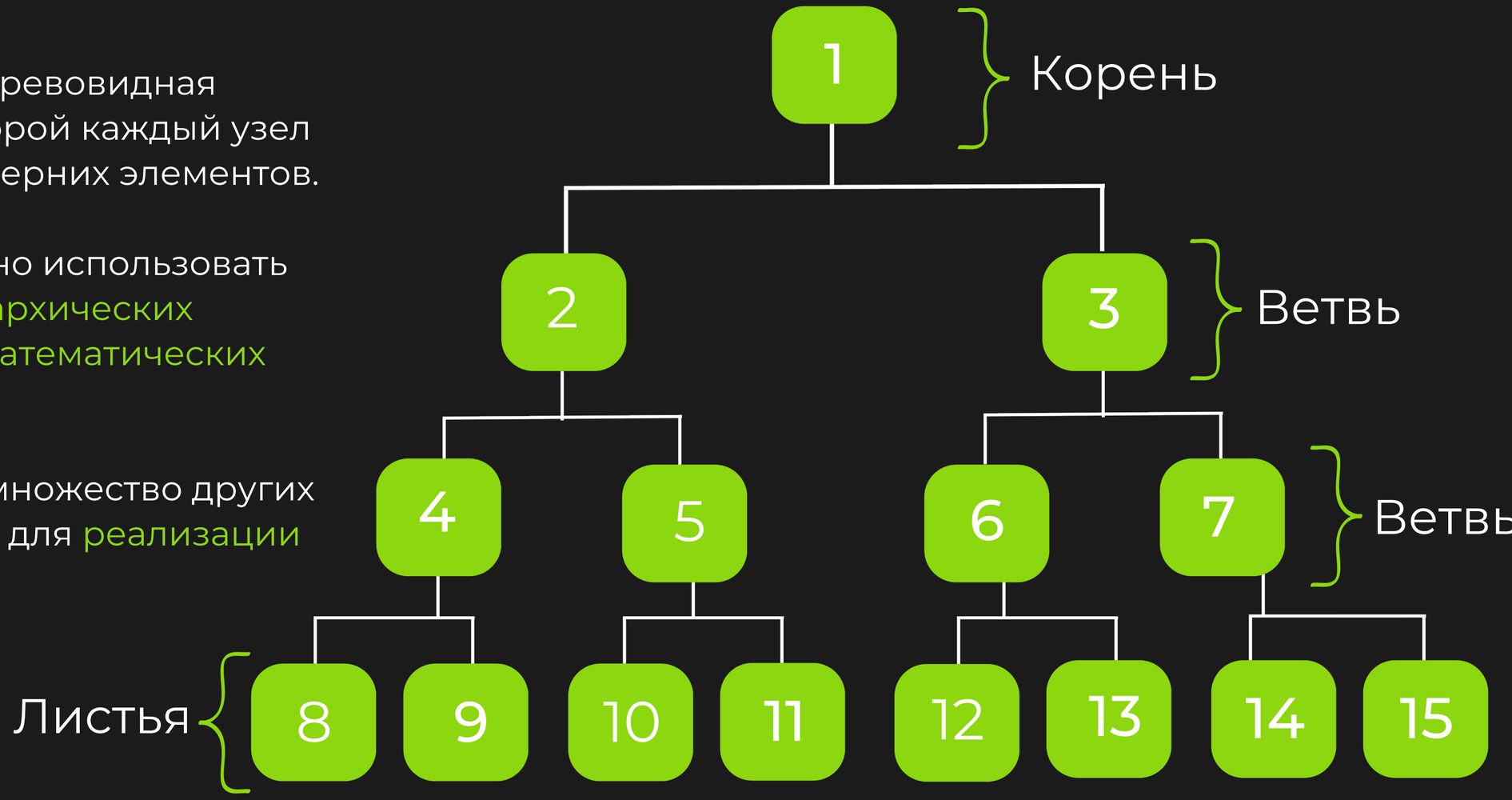


Двоичное дерево

Бинарное дерево - это древовидная структура данных, в которой каждый узел имеет не более двух дочерних элементов.

Бинарные деревья можно использовать для представления иерархических структур и для оценки математических выражений.

Они также могут иметь множество других применений, например, для реализации алгоритмов поиска.



Blockchain Center

Зачем нужна концепция двоичного дерева?

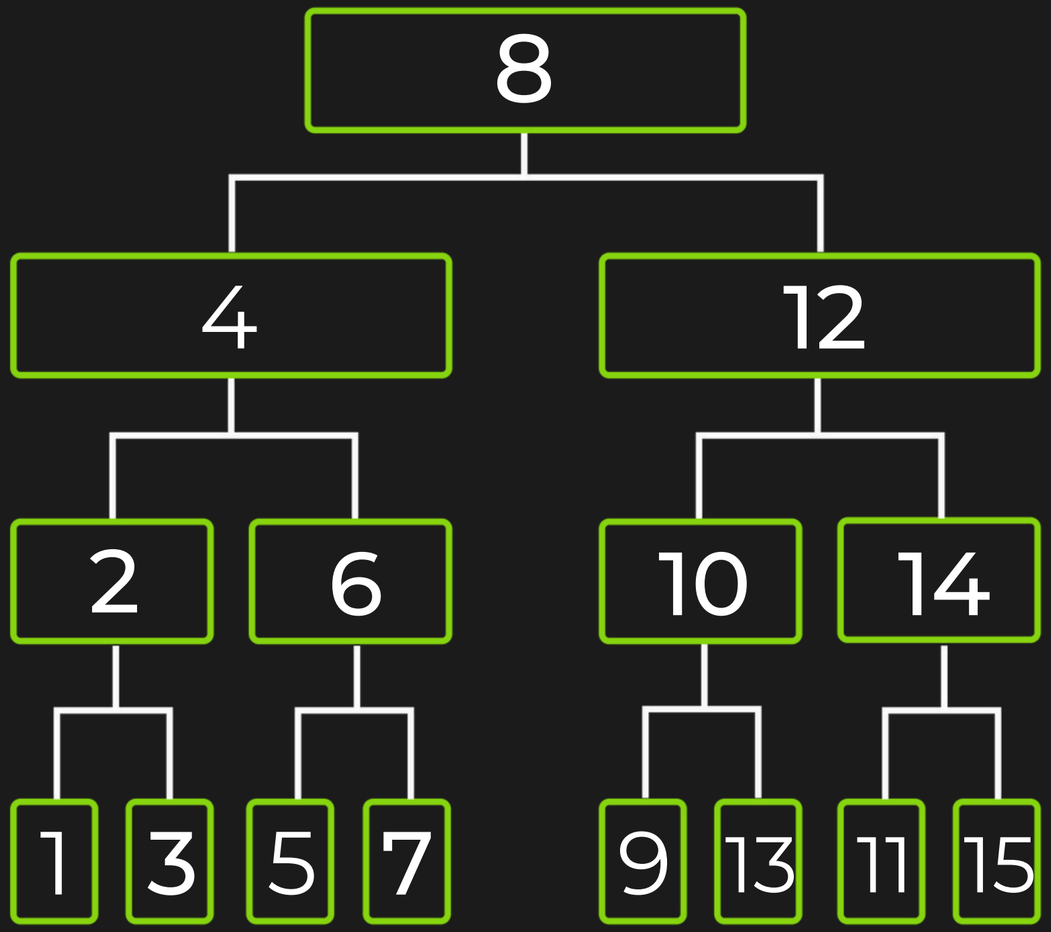
При поиске определенного элемента в списке необходимо просматривать каждый элемент по очереди, пока не будет найден нужный элемент. Это медленный процесс, особенно для больших списков, так как в худшем случае поиск должен просматривать каждый элемент.

{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25, 26, 27, 27, 28, 29, 30, 31, 32}

Дерево двоичного поиска

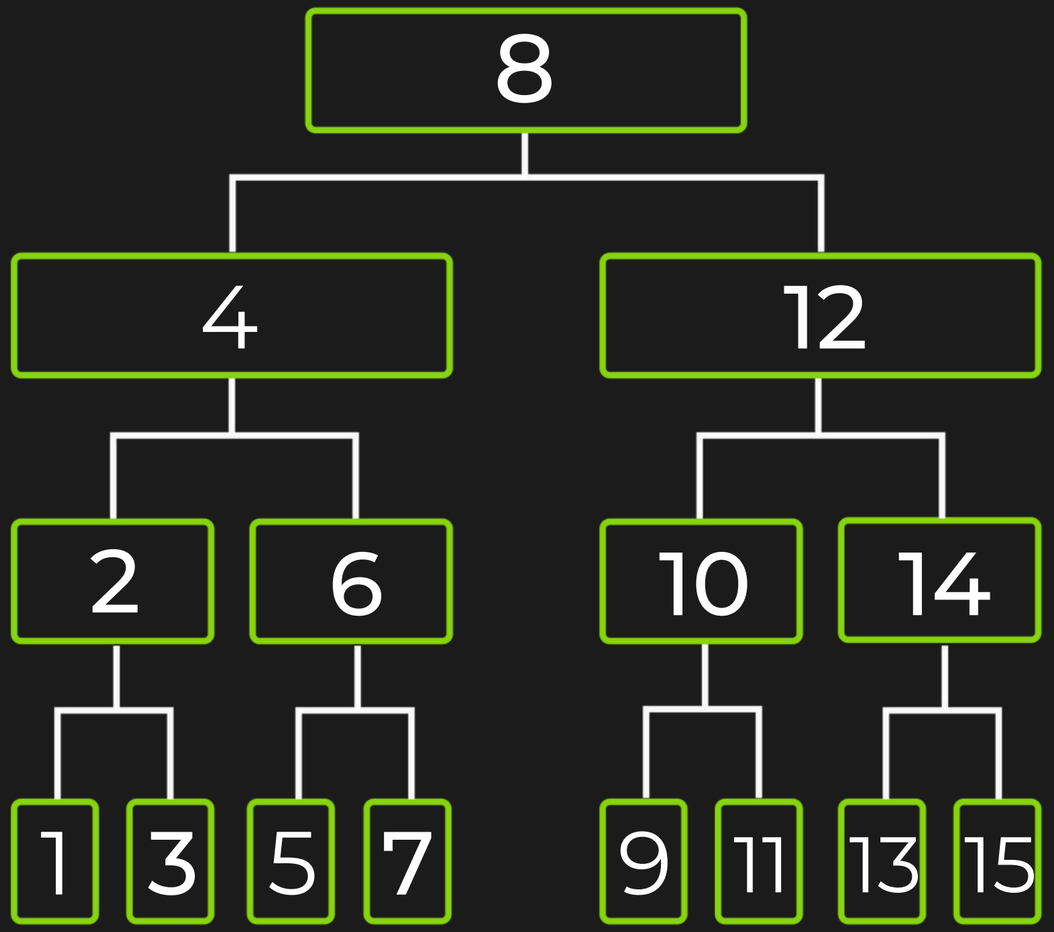
Дерево двоичного поиска - это дерево ,в котором левый дочерний узел имеет значение меньше, чем значение узла, а правый дочерний узел имеет значение больше, чем значения узла.

Это позволяет осуществлять быстрый поиск, так как на каждом шаге поиска можно исключить половину дерева, сравнивая ключ поиска со значением текущего узла.



Blockchain Center

Дерево двоичного поиска



Дерево Меркла

Дерево Меркла - это древовидная структура данных, используемая в криптографии для обеспечения безопасности с помощью проверки целостности больших объемов данных.

Дерево Меркла

Дерево Меркла - это древовидная структура данных, используемая в криптографии для обеспечения безопасности с помощью проверки целостности больших объемов данных.

Основное различие заключается в том, что мы используем хэши вместо чисел.

Дерево Меркла

Дерево Меркла - это древовидная структура данных, используемая в криптографии для обеспечения безопасности с помощью проверки целостности больших объемов данных.

Основное различие заключается в том, что мы используем хэши вместо чисел.

В блокчейне транзакции хэшируются в дерево Меркла, причем корневой хэш включается в заголовок блока.

Дерево Меркла

Дерево Меркла - это древовидная структура данных, используемая в криптографии для обеспечения безопасности с помощью проверки целостности больших объемов данных.

Основное различие заключается в том, что мы используем хэши вместо чисел.

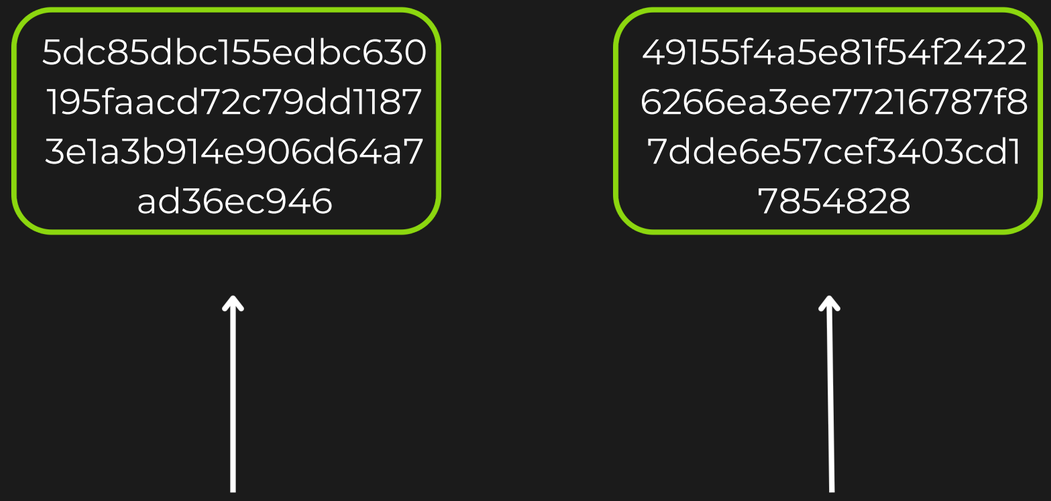
В блокчейне транзакции хэшируются в дерево Меркла, причем корневой хэш включается в заголовок блока.

Дерево Меркла

Дерево Меркла - это древовидная структура данных, используемая в криптографии для обеспечения безопасности с помощью проверки целостности больших объемов данных.

Основное различие заключается в том, что мы используем хэши вместо чисел.

В блокчейне транзакции хэшируются в дерево Меркла, причем корневой хэш включается в заголовок блока.

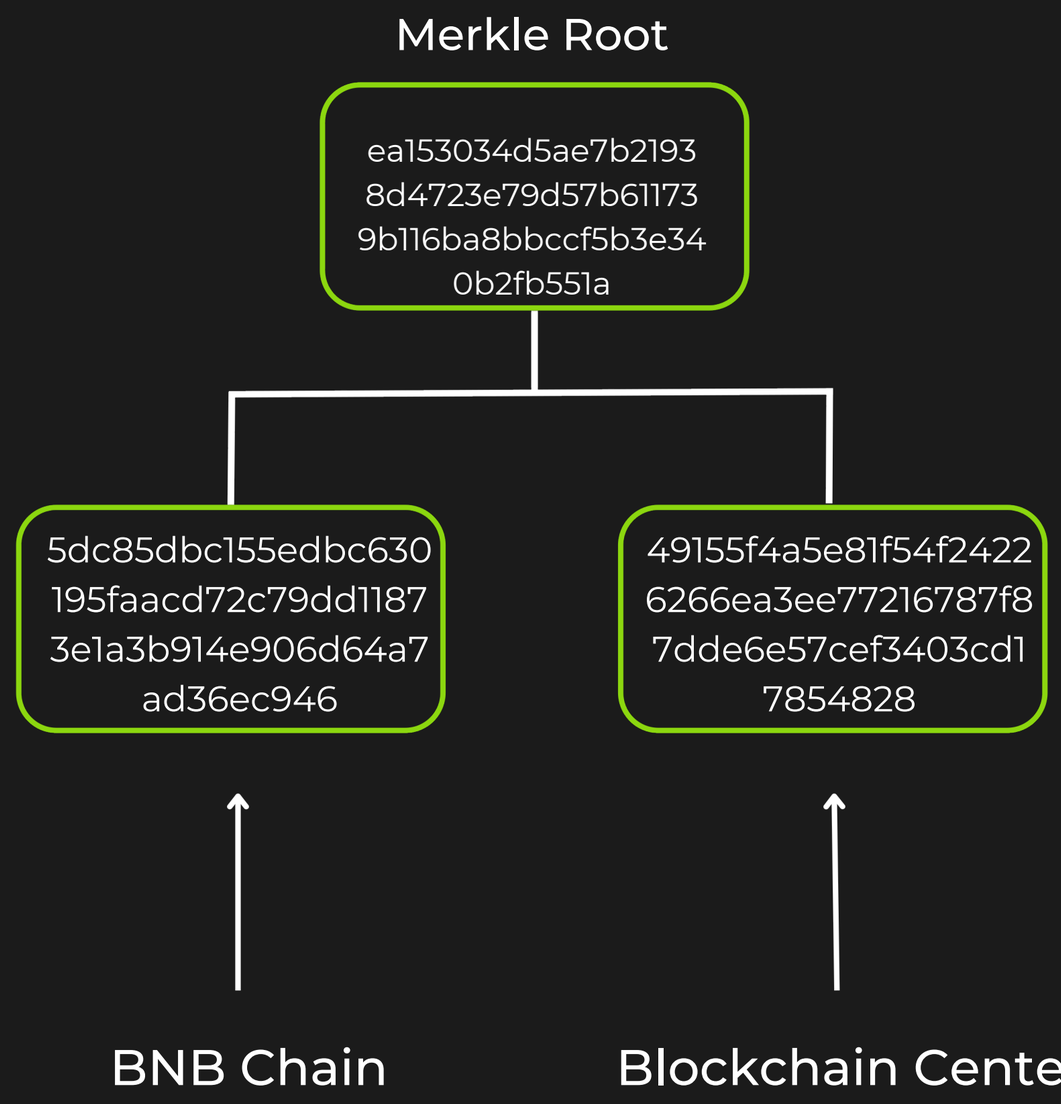


Дерево Меркла

Дерево Меркла - это древовидная структура данных, используемая в криптографии для обеспечения безопасности с помощью проверки целостности больших объемов данных.

Основное различие заключается в том, что мы используем хэши вместо чисел.

В блокчейне транзакции хэшируются в дерево Меркла, причем корневой хэш включается в заголовок блока.

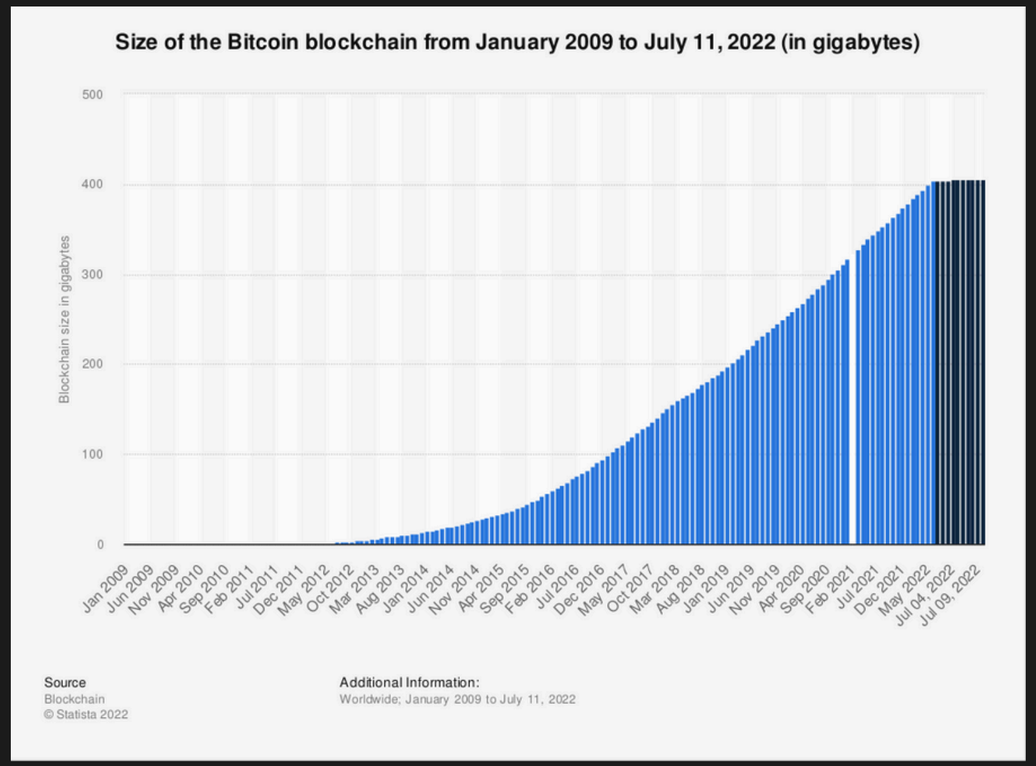


Зачем нам нужно Дерево Меркла?

Деревья Меркла используются в блокчейне биткоина для обеспечения надежного способа проверки целостности блоков транзакций.

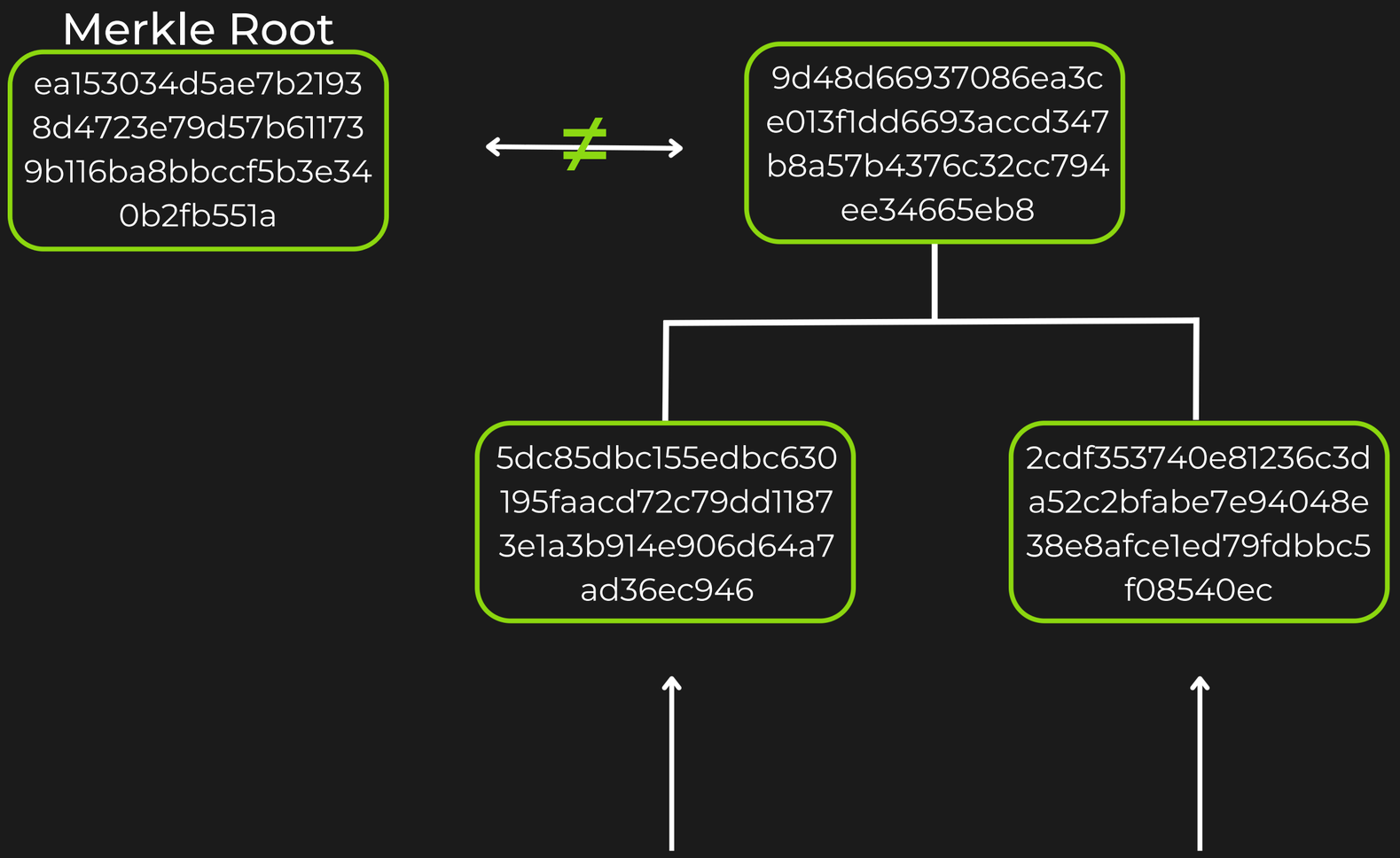
Без использования деревьев Меркла для проверки содержащихся в нем транзакций необходимо было бы передавать и хранить весь блок.

Это было бы неэффективно и потребовало бы большой пропускной способности и пронстранства для хранения, так как размер блокчейна биткойна в настоящее время превышает 400 ГБ.

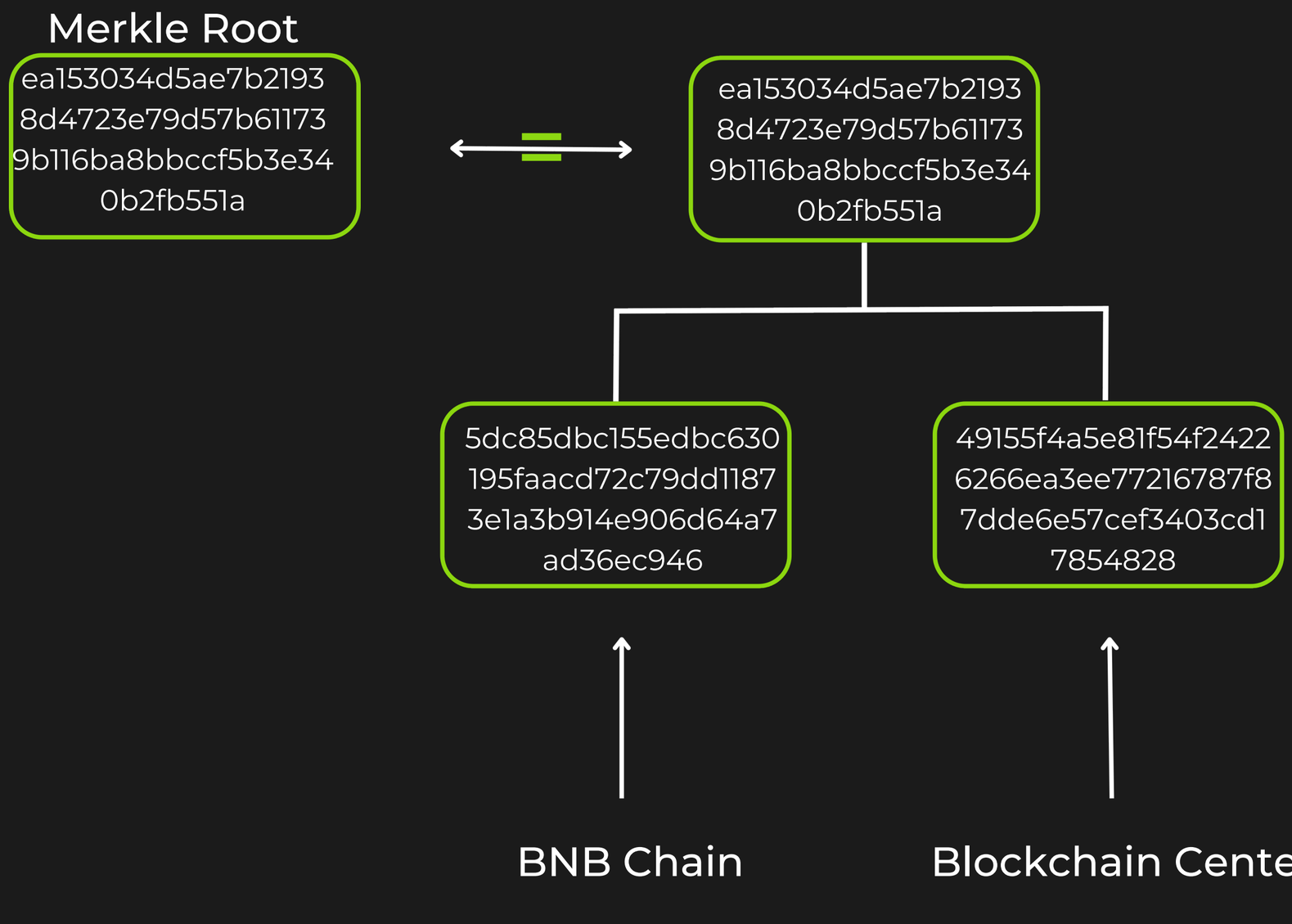


source: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

Корень Меркла



Корень Меркла



Как блокчейн использует дерево Меркла?

- В блокчейне каждый блок транзакций хэшируется, и хэши размещаются в древовидной структуре, называемой merkle tree.
- корневой хэш этого дерева затем включается в заголовок блока, позволяя проверить целостность транзакций в блоке без необходимости передавать весь блок.
- при добавлении нового блока в цепочку корневой хэш предыдущих блоков дерева Merkle включается в заголовок нового блока.
- это создает цепочку корневых хешей, причем корневой хеш каждого блока зависит от корневых хешей предшествующих блоков.
- с помощью деревьев merkle можно эффективно проверять целостность транзакций в блоке и весь блокчейн, так как необходимо только сравнить корневые хэши блоков.

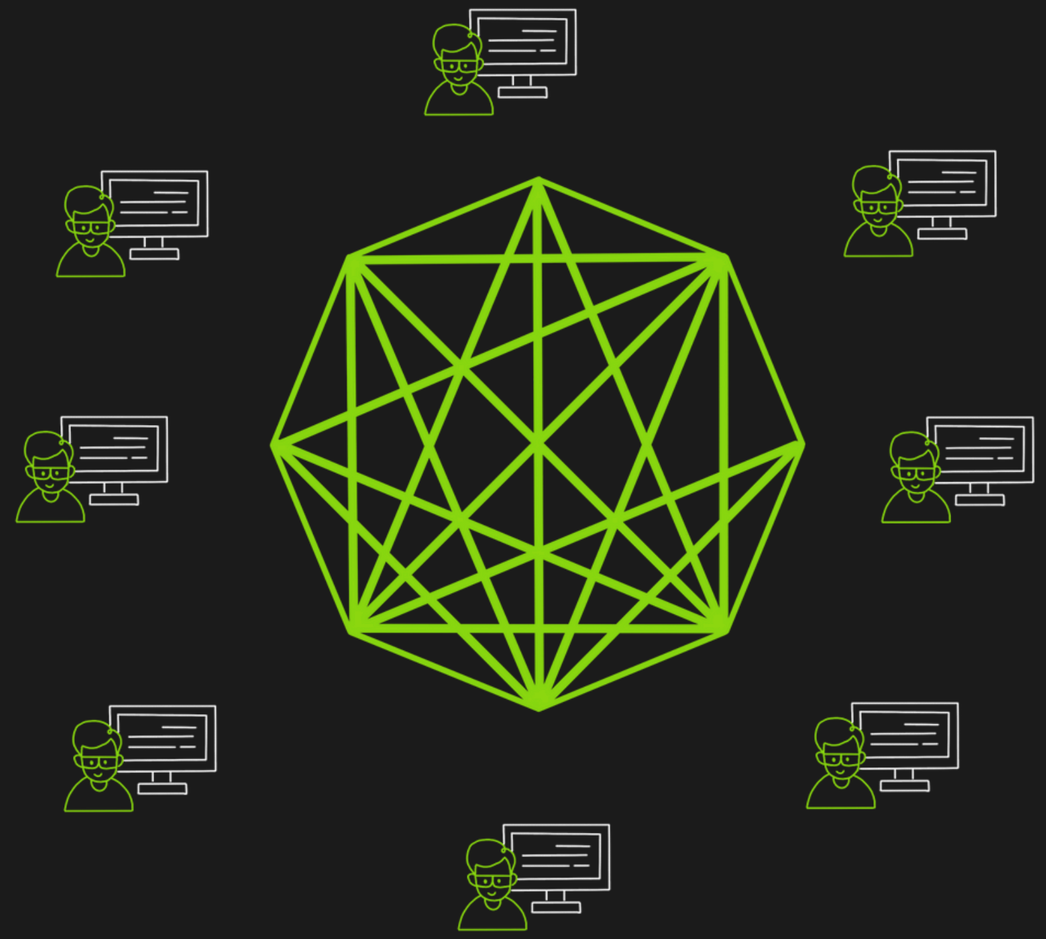
Как работает merkle proof на блокчейне?

Blockchain Center

Когда узел хочетподтвердить, что конкретная транзакция является частью блока, он может запросить подтверждение Merkle у другого узла.

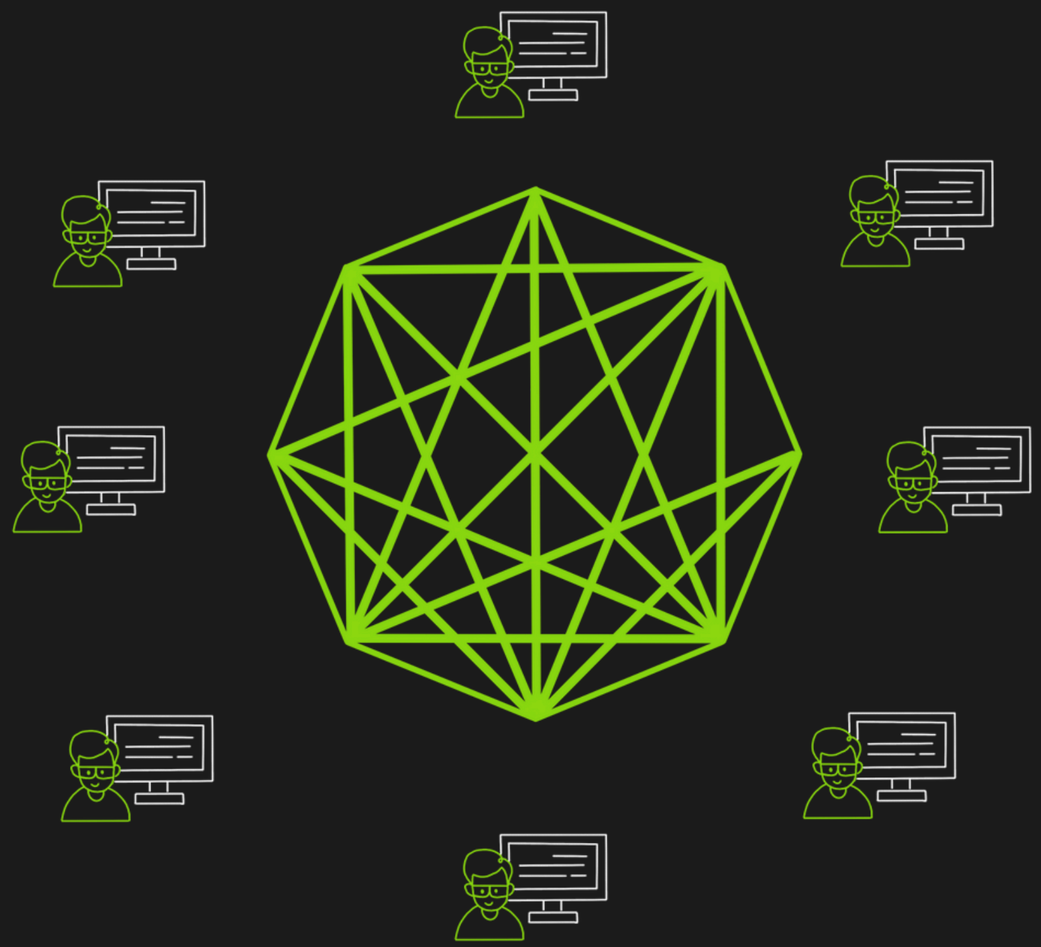
Это доказательство представляет собой ряд хэшей, которые образуют путь от корня дерева Меркла вплоть до рассматриваемой транзакции.

Затем узел может использовать эти хэши для воссоздания дерева Merkle блока и проверки необходимости включения в него транзакции.



Если транзакция включена, корневой хэш реконструированного дерева будет соответствовать корневому хэшу, сохраненному в заголовке блока.

Это позволяет узлу проверить транзакцию в блоке без необходимости передачи всего блока.



Применение дерева Меркла

- Large 100,000+ token airdrops
- Bitcoin транзакции
- Inter Planetary File Systems - IPFS (distributed storage protocol)
- Git (distributed version control system)

Blockchain Center

Рабочий процесс блокчейна

В блокчейн-сети узлы - это компьютеры или устройства, которые помогают поддерживать распределенный реестр (distributed ledger) и обеспечивать целостность сети. Они проверяют и записывают транзакции и обеспечивают безопасность блокчейна.

Узлы помогают децентрализовать блокчейн и сделать его устойчивым к подделке или цензуре, участвуя в сети и работая вместе для проверки и записи новых транзакций, обеспечивая точность и актуальный статус распределённого реестра.

Blockchain Center

Full Nodes (Полные узлы):

Полные узлы имеют полную копию блокчейна и отвечают за проверку новых транзакций и блоков. Они играют важнейшую роль в поддержании целостности блокчейна.

Mining Nodes (Узлы для майнинга) :

В PoW блокчейне, таком как биткоин, узлы майнинга отвечают за решение сложных математических задач, чтобы создавать новые блоки и зарабатывать вознаграждения.

Lightweight Nodes (Облегченные узлы):

Облегченные узлы (узлы упрощенной проверки платежей) не имеют полной копии блокчейна. Вместо этого они полагаются на полные узлы для предоставления им необходимой информации для проверки транзакций.

Validator Nodes (Проверочные узлы):

Узлы валидатора отвечают за создание новых блоков в интеллектуальной цепочке BNB. Они выбираются посредством процесса, называемого «объединением», в котором пользователи могут выставлять свои маркеры, чтобы получить право на участие в качестве средства проверки.

Узлы: как выполняются транзакции?

Кошелек хранит ключи и позволяет отправлять и получать цифровую валюту. При отправке транзакции кошелек подключается к узлу и транслирует транзакцию. Транзакция добавляется в блокчейн после проверки.
Узел, к которому подключена транзакция, **помогает обеспечить безопасность** и **целостность блокчейна**, записывая транзакцию и делая ее доступной для других узлов.

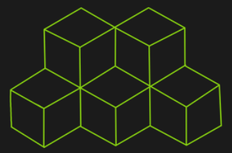
Кто-то запрашивает транзакцию

Транзакция запроса передается по P2P сети компьютеров, называемых узлами.

Проверка

криптовалюта, контракты, записи

После проверки транзакции он добавляется в группу других транзакций из нового блока.

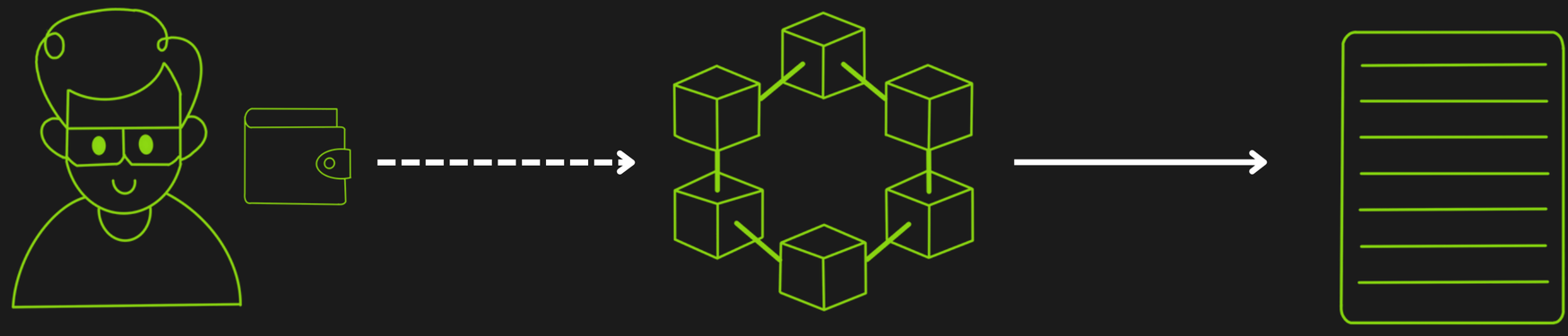


Новый блок, содержащий подтвержденную транзакцию, навсегда добавляется в существующий блокчейн и не может быть изменен.

Сделка завершена

Рабочий процесс: пул транзакций

Транзакции, транслируемые в блокчейн, временно хранятся в пуле транзакций, также известном как «пул памяти» или «mempool». Это набор неподтвержденных транзакций, ожидающих включения в следующий блок Когда транзакция передается в сеть, узлы получают ее и помещают в пул транзакций. Затем как транзакция добавилась в блок, а блок - в блокечейн, транзакция будет считаться подтвержденной.



Блокчейн

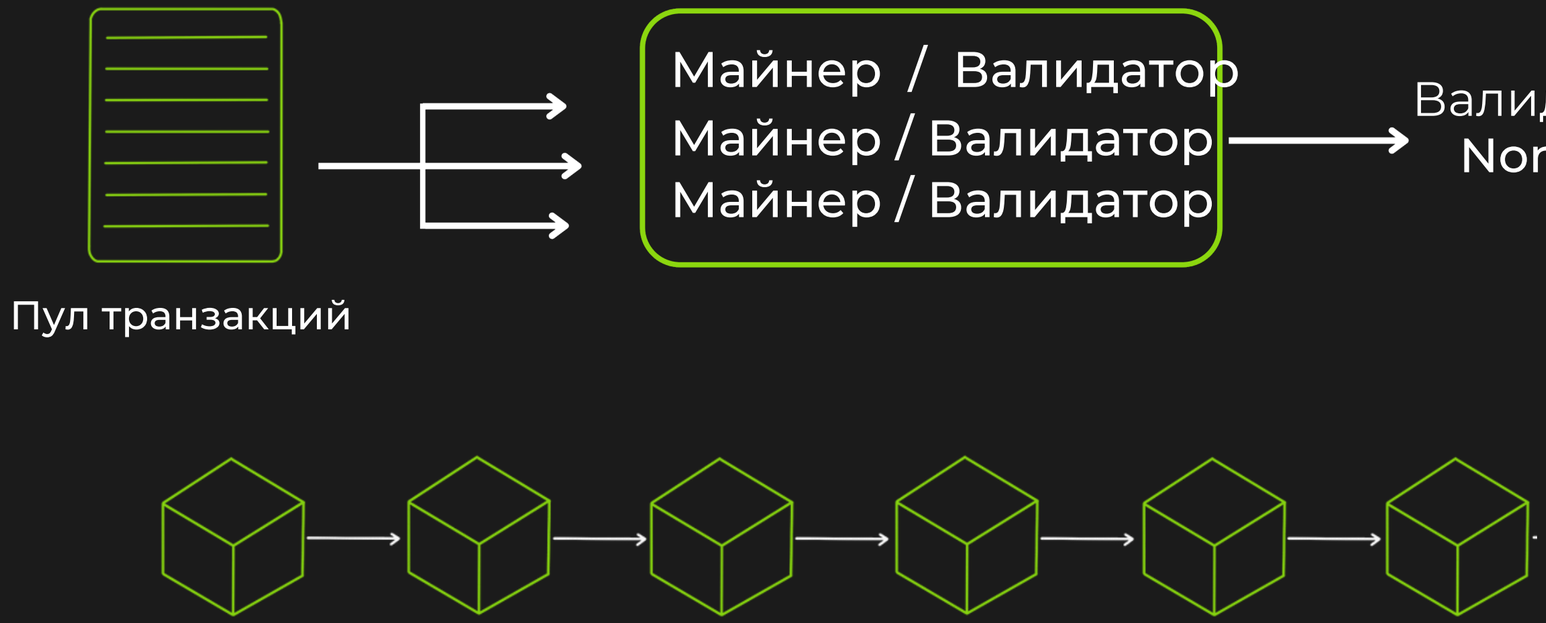
Пул транзакций

Майнинг

Транзакции в блокчейн-сети временно сохраняются в пуле транзакций до тех пор, пока они не будут добавлены в блок майнерами. Это помогает обеспечить **целостность** и **безопасность** блокчейна.

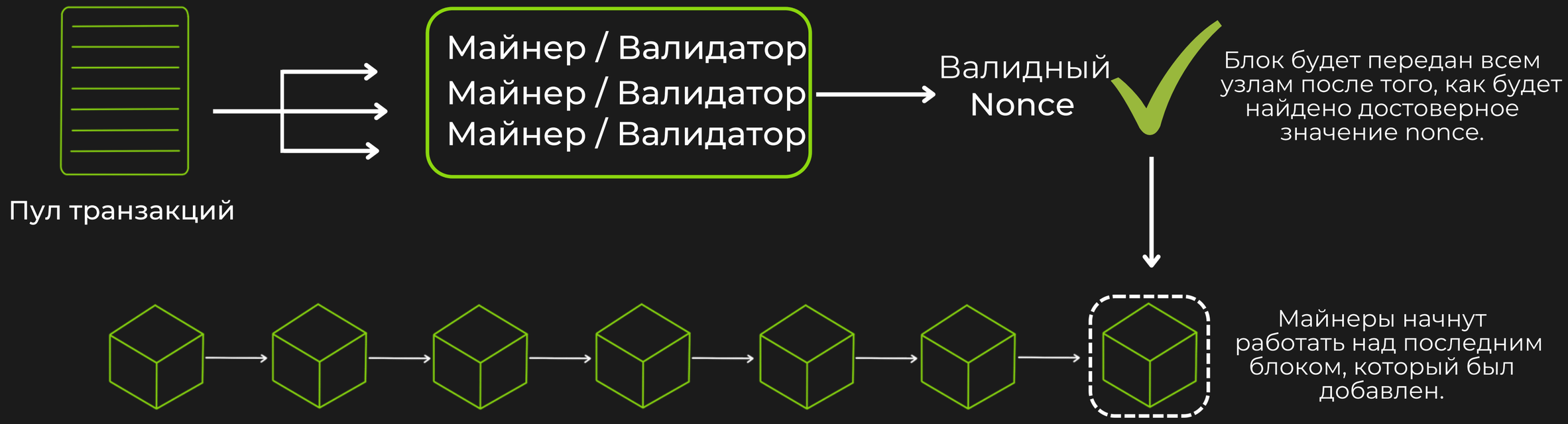
Майнинг

Транзакции в блокчейн-сети временно сохраняются в пуле транзакций до тех пор, пока они не будут добавлены в блок майнерами. Это помогает обеспечить **целостность** и **безопасность** блокчейна.



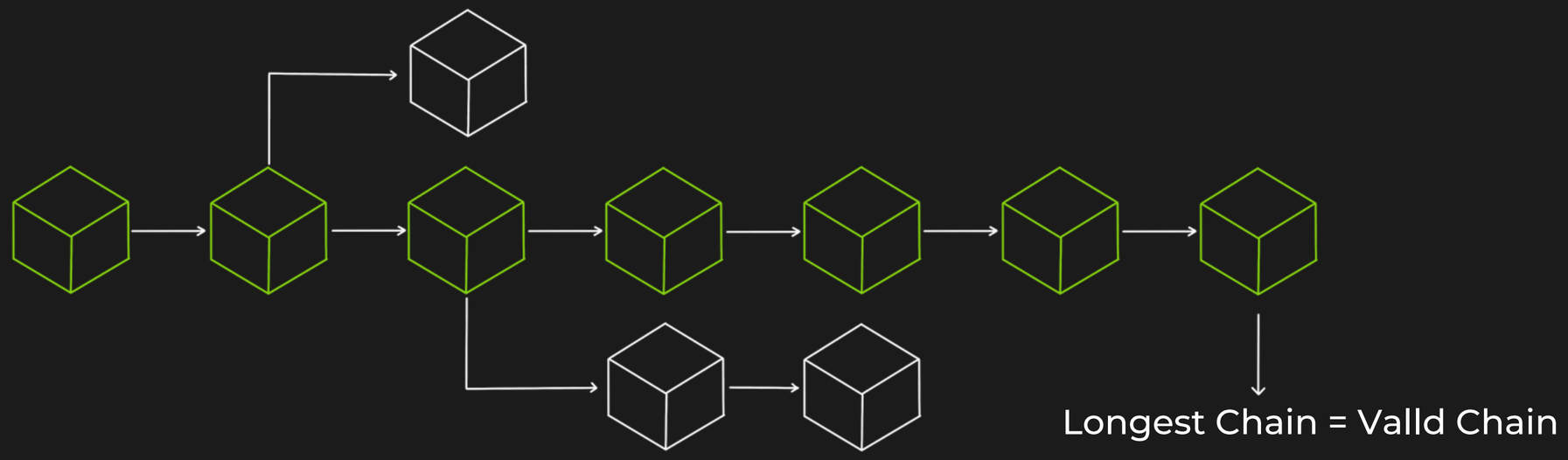
Майнинг

Транзакции в блокчейн-сети временно сохраняются в пуле транзакций до тех пор, пока они не будут добавлены в блок майнерами. Это помогает обеспечить **целостность** и **безопасность** блокчейна.



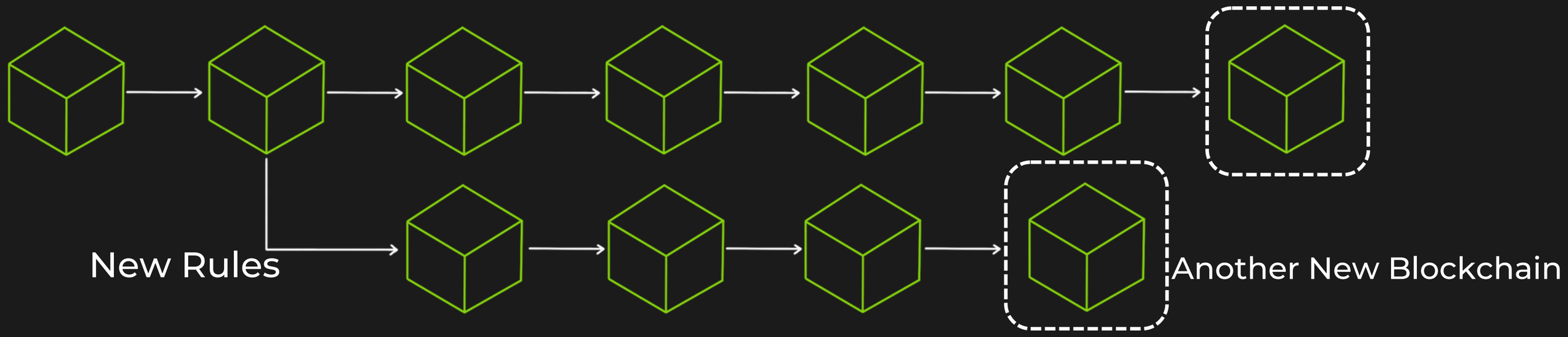
Блокчейн-вилки: временная вилка

Временная вилка может возникать, когда одновременно получают **два хеш-значения** или **два аналогичных** хеш-значения. Это может произойти, когда **два майнера** одновременно решают головоломку **PoW** и создают **конкурирующие** блоки.
Сеть разрешает вилку, выбирая самую **длинную цепочку**, которая, как предполагается, представляет наибольшую работу и является наиболее **заслуживающей доверия**, и отбрасывая другую. Это **гарантирует**, что в блокчейн будут добавлены только действительные блоки и поможет сохранить его целостность и безопасность.



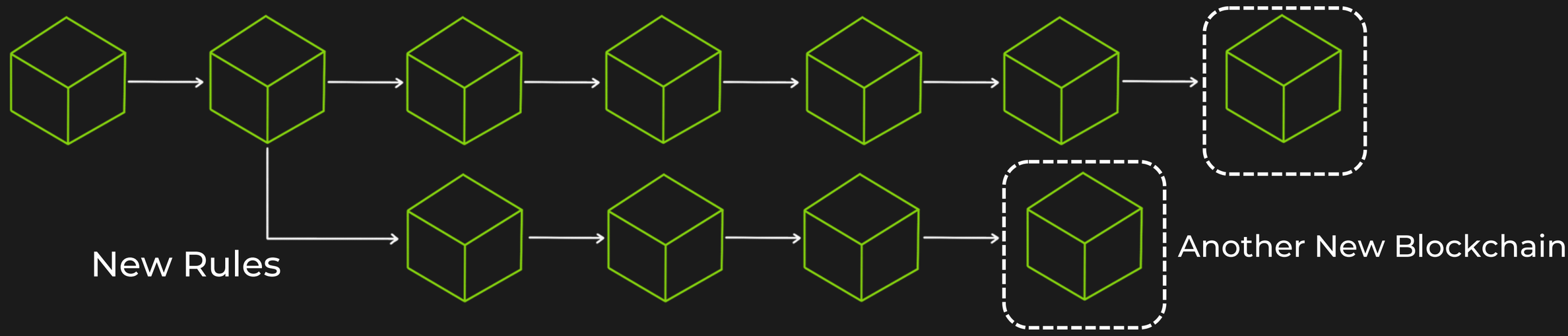
Блокчейн-вилки: жёсткая вилка

Жёсткая вилка - это обновление до блокчейн-сети, создающей новый блокчейн с другими **правилами**, чем у оригинала. Это может произойти, когда есть **разногласия внутри** сети или желание ввести в сеть **новые функции**. Во время **жёсткой вилки** сеть разделяется на **две отдельные блокчейн-сети**: исходную сеть и новую сеть. Каждая сеть имеет свой **собственный набор** правил и **работает независимо** от другой.



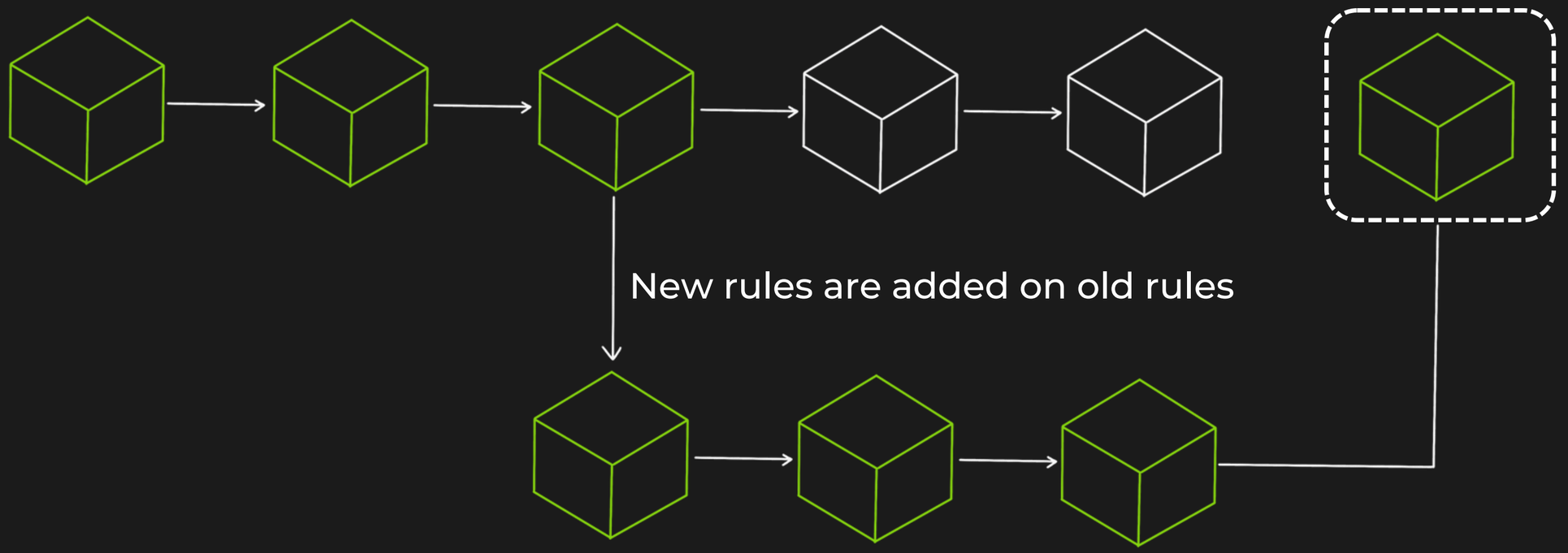
Блокчейн-вилки: жёсткая вилка

Примеры Hard Fork
1.Bitcoin Gold
2.Bitcoin Cash
3.Ethereum Classic
4.Ethereum PoW



Блокчейн-вилки: мягкая вилка

Мягкая вилка - это обратно совместимое обновление **блокчейн-сети**. Он используется для введения **новых функций** или **внесения незначительных** изменений в сеть. Это **не приводит** к созданию отдельного, несовместимого блокчейна. Узлы, которые еще не обновлены, могут по-прежнему участвовать в сети во время программной работы.

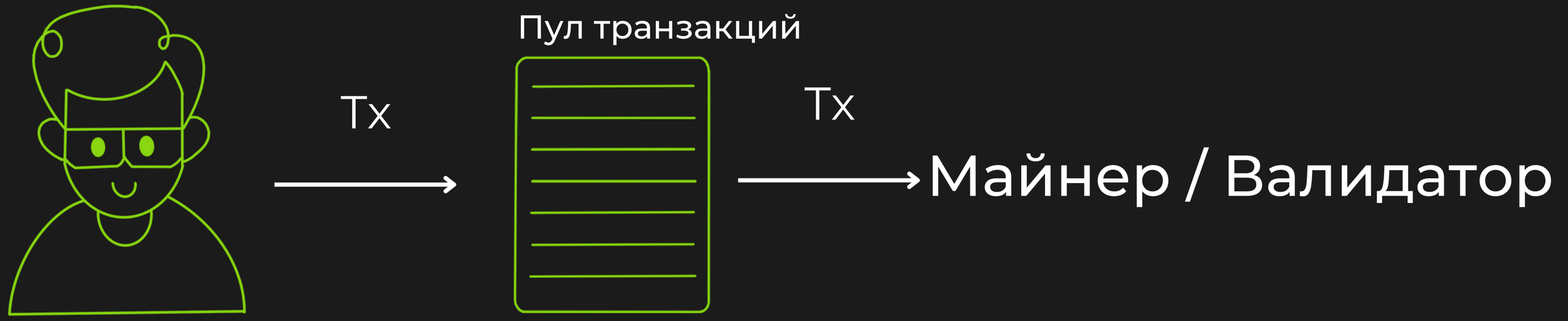


Blockchain Center

Тип блокчейн-транзакций:

Публичные транзакции

Публичные транзакции хранятся в пуле транзакций некоторое время и ожидают подтверждения.



Тип блокчейн-транзакций:

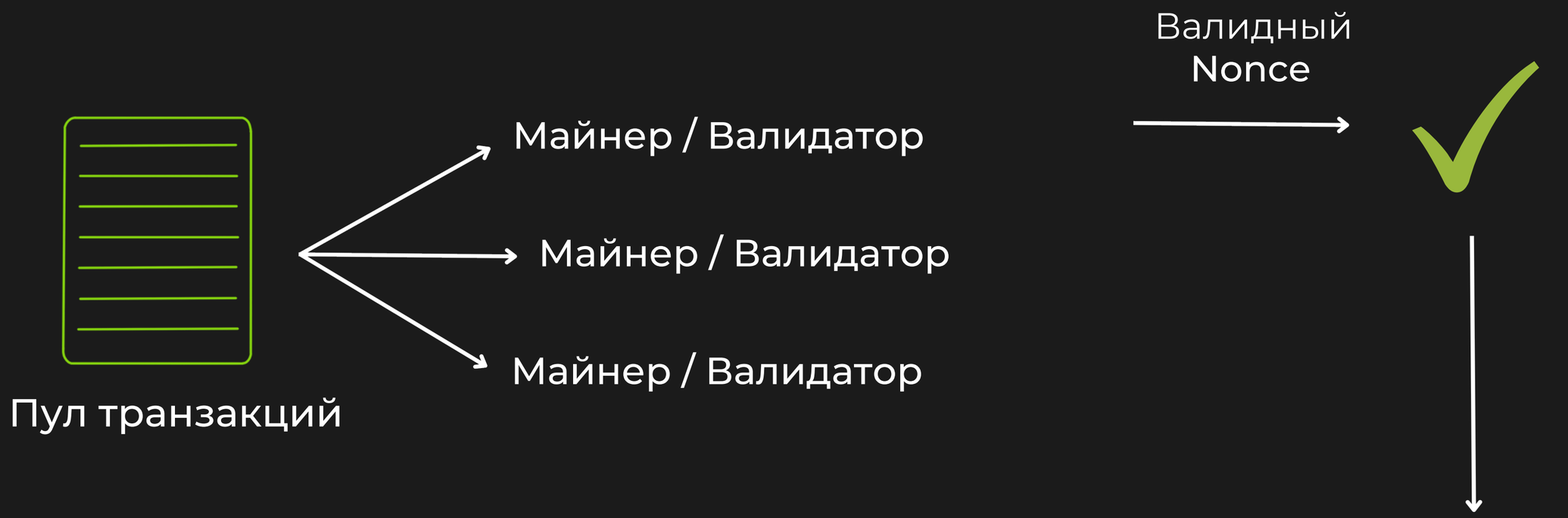
Частные транзакции

Частные транзакции отправляются непосредственно в устройство обработки/проверки без сохранения в пуле транзакций.

Tx

Майнер / Валидатор

Практика


Валидный
Nonce
Майнер / Валидатор
Майнер / Валидатор
Майнер / Валидатор
Пул транзакций
Блок
Блок
Блок
Блок
Блок
Блок
Блок