

Технология блокчейн

#2

Основы Блокчейн Технологии

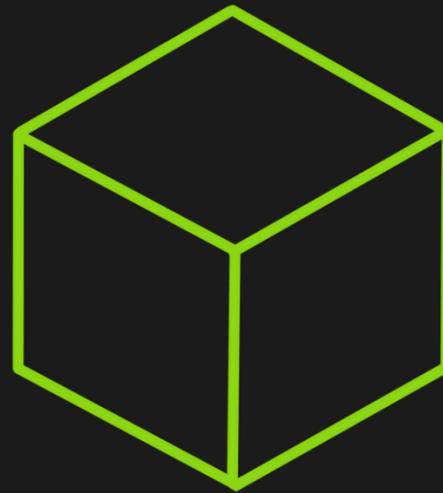
Обзор

- Что такое блок и его структура?
- Что такое Блокчейн? Как блоки соединяются вместе?
- Распределенный Реестр & Прозрачность Блокчейна
- База Данных vs Блокчейн
- Плюсы & Минусы Блокчейна

Что такое блок и его структура?

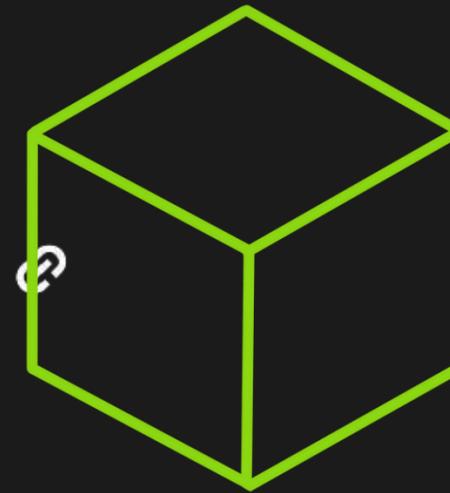
- Каждый блок имеет свой собственный хэш, который функционирует как уникальный идентификатор.
- Каждый новый блок должен использовать хэш (идентификатор) предыдущего блока.

Блок 1



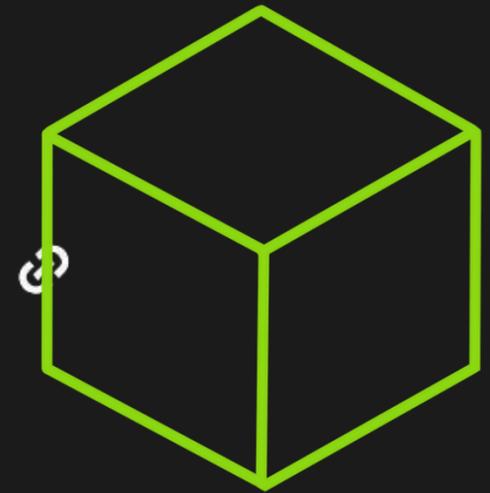
Хэш: 1BF1E
Предыдущий
хэш:
00000

Блок 2



Хэш: 6EBC7
Предыдущий
хэш:
1BF1E

Блок 3



Хэш: 138F2
Предыдущий
хэш:
6EBC7

Что такое блок и его структура? Элементы Блока

1. Размер блока

- Количество данных, которые может хранить блок

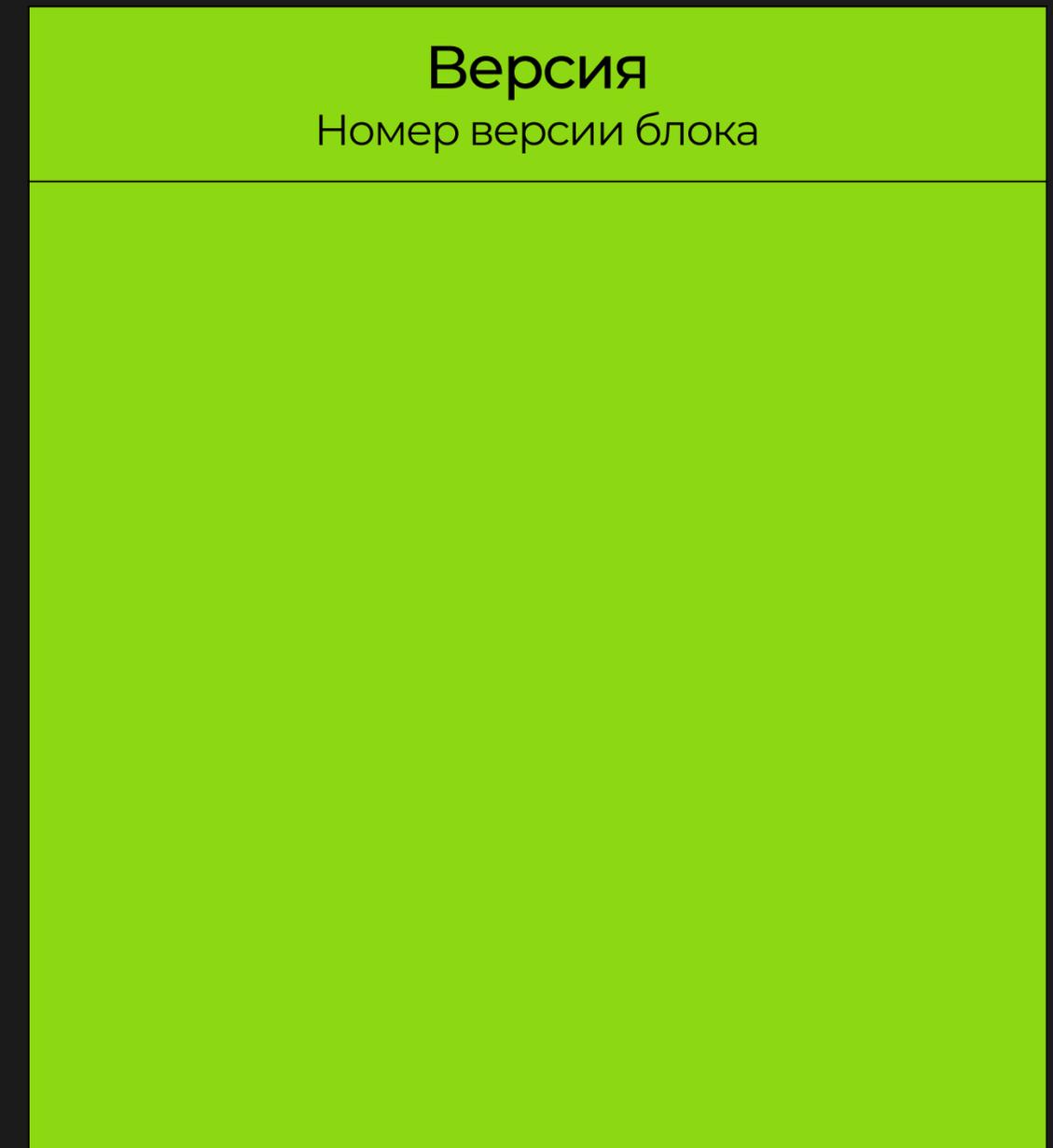
Что такое блок и его структура? Элементы Блока

1. Размер блока

- Количество данных, которые может хранить блок

2. Заголовок блока

- Содержит метаданные блока



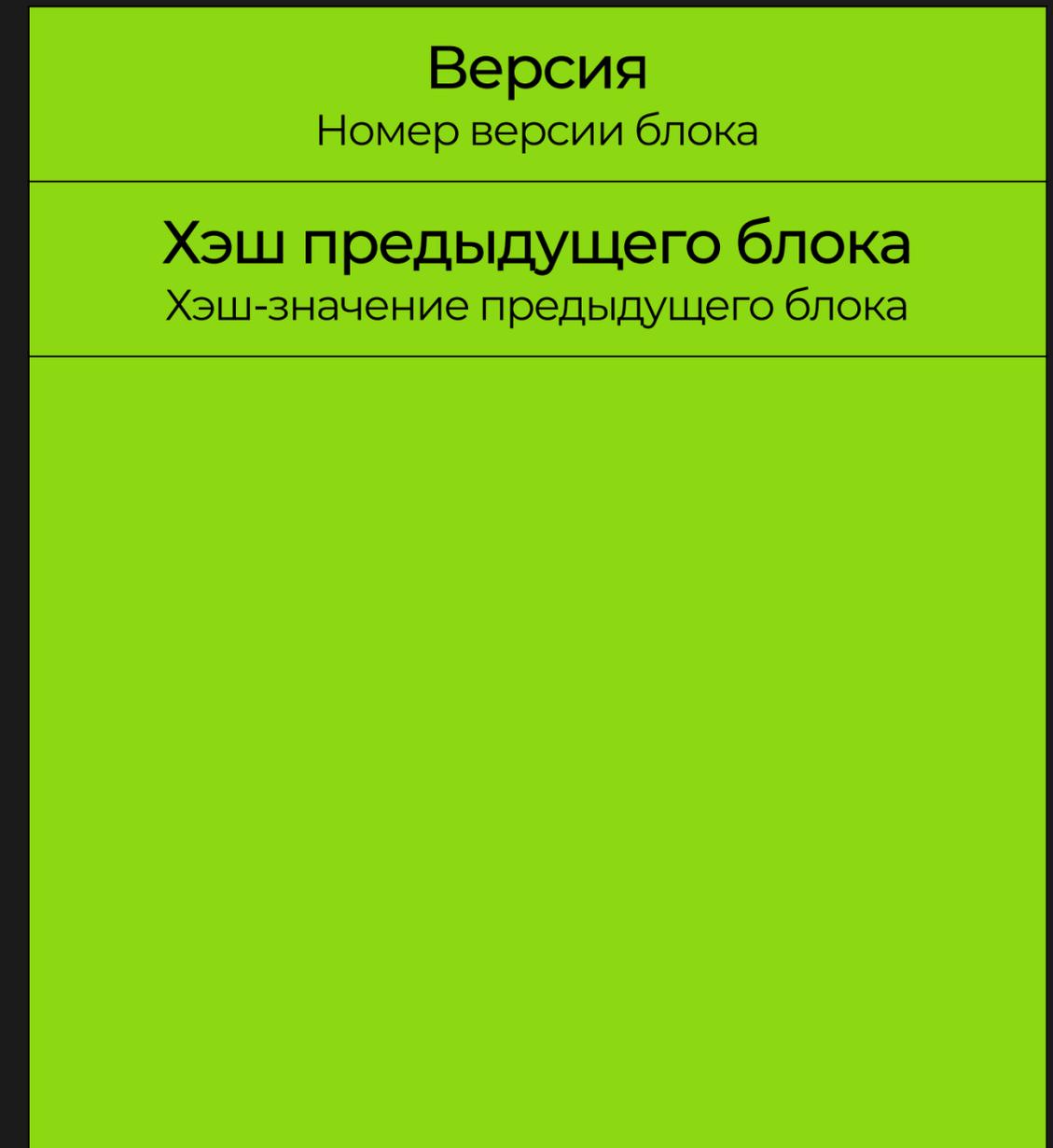
Что такое блок и его структура? Элементы Блока

1. Размер блока

- Количество данных, которые может хранить блок

2. Заголовок блока

- Содержит метаданные блока



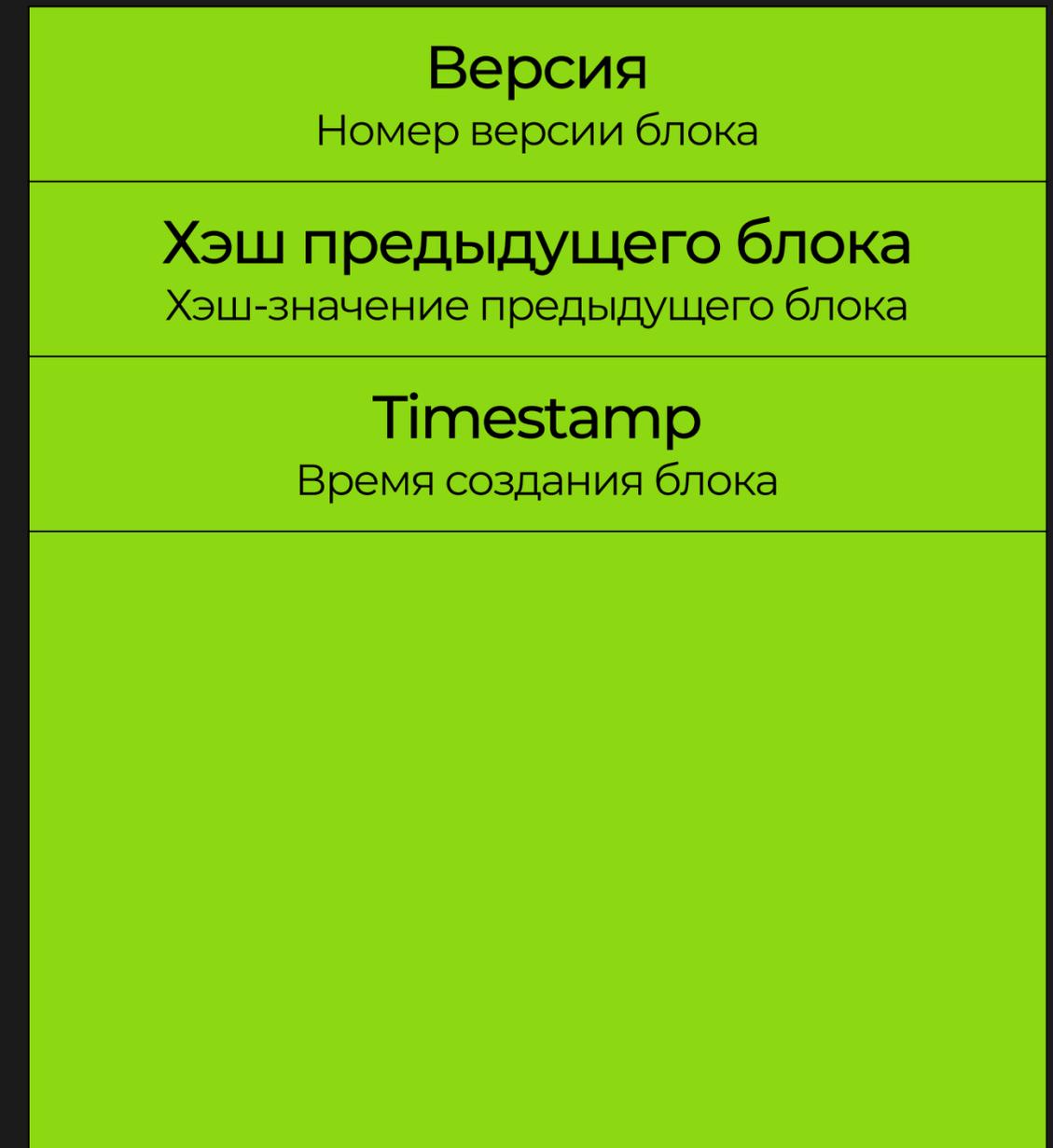
Что такое блок и его структура? Элементы Блока

1. Размер блока

- Количество данных, которые может хранить блок

2. Заголовок блока

- Содержит метаданные блока



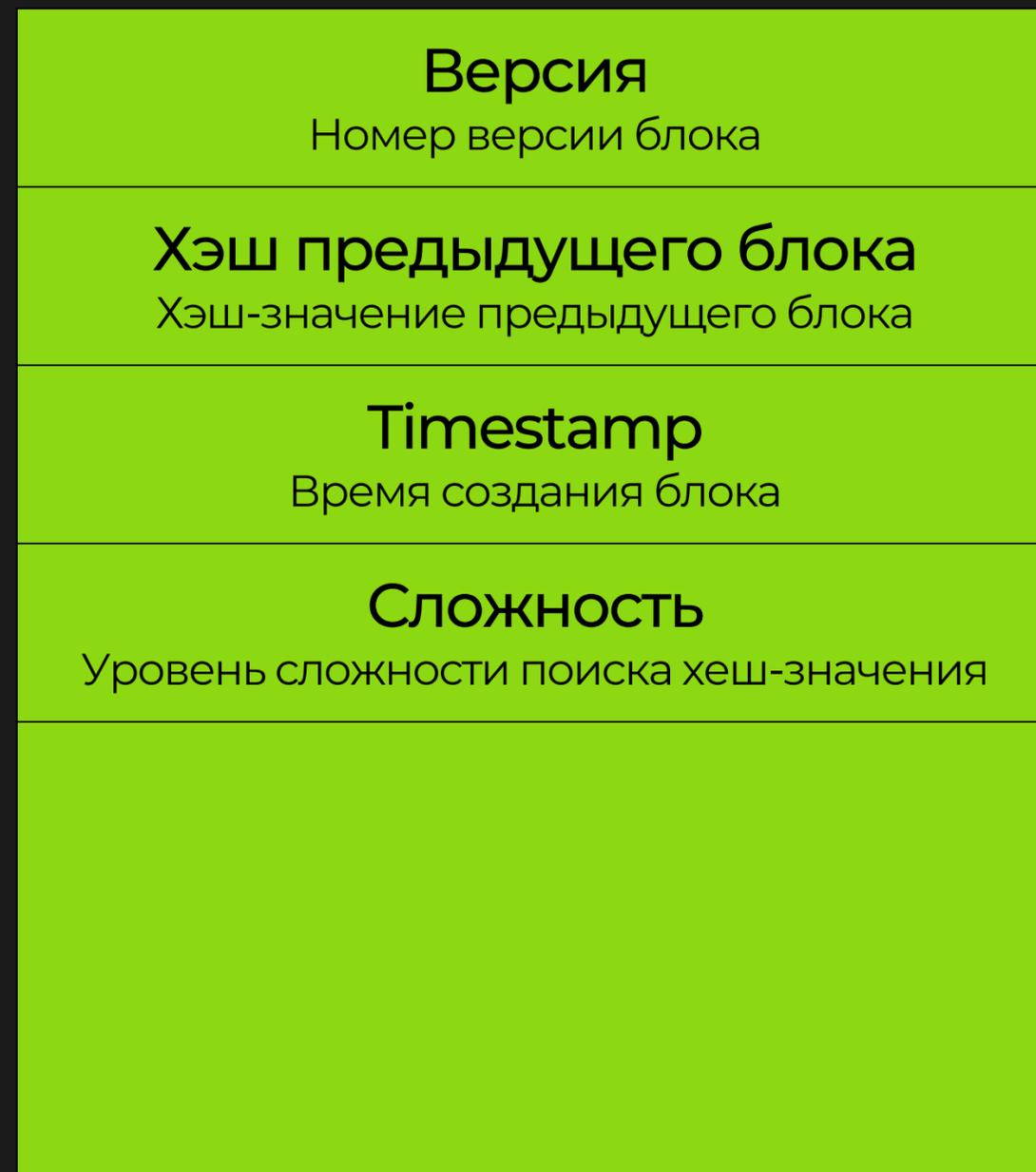
Что такое блок и его структура? Элементы Блока

1. Размер блока

- Количество данных, которые может хранить блок

2. Заголовок блока

- Содержит метаданные блока



Что такое блок и его структура? Элементы Блока

1. Размер блока

- Количество данных, которые может хранить блок

2. Заголовок блока

- Содержит метаданные блока



Версия Номер версии блока
Хэш предыдущего блока Хэш-значение предыдущего блока
Timestamp Время создания блока
Сложность Уровень сложности поиска хэш-значения
Nonce Значение, которое пытаются найти майнеры для достижения целевого хэша

Что такое блок и его структура? Элементы Блока

1. Размер блока

- Количество данных, которые может хранить блок

2. Заголовок блока

- Содержит метаданные блока



Версия Номер версии блока
Хэш предыдущего блока Хэш-значение предыдущего блока
Timestamp Время создания блока
Сложность Уровень сложности поиска хэш-значения
Nonce Значение, которое пытаются найти майнеры для достижения целевого хэша
Merkle root Значение, полученное после вычисления всех транзакция в дерево Меркла

Что такое блок и его структура? Элементы Блока

1. Размер блока

- Количество данных, которые может хранить блок

2. Заголовок блока

- Содержит метаданные блока

3. Transaction Counter

- Содержит количество транзакций, хранящихся в блоке



Версия Номер версии блока
Хэш предыдущего блока Хэш-значение предыдущего блока
Timestamp Время создания блока
Сложность Уровень сложности поиска хэш-значения
Nonce Значение, которое пытаются найти майнеры для достижения целевого хэша
Merkle root Значение, полученное после вычисления всех транзакция в дерево Меркла

Что такое блок и его структура? Элементы Блока

1. Размер блока

- Количество данных, которые может хранить блок

2. Заголовок блока

- Содержит метаданные блока

3. Transaction Counter

- Содержит количество транзакций, хранящихся в блоке

4. Транзакции

- Список транзакций внутри блока



Версия Номер версии блока
Хэш предыдущего блока Хэш-значение предыдущего блока
Timestamp Время создания блока
Сложность Уровень сложности поиска хэш-значения
Nonce Значение, которое пытаются найти майнеры для достижения целевого хэша
Merkle root Значение, полученное после вычисления всех транзакция в дерево Меркла

Что такое блок и его структура?

Merkle Root

Это математическая структура данных, состоящая из хэшей различных блоков данных, которые суммируют все транзакции в блоке.

Что такое блок и его структура?

Merkle Root

Это математическая структура данных, состоящая из хэшей различных блоков данных, которые суммируют все транзакции в блоке.

Транзакции **'Leaf'** сначала группируются в пары.

Leaf
Транзакция 1

Leaf
Транзакция 2

Leaf
Транзакция 3

Leaf
Транзакция 4

Что такое блок и его структура?

Merkle Root

Это математическая структура данных, состоящая из хэшей различных блоков данных, которые суммируют все транзакции в блоке.

Хэш вычисляется для каждой пары транзакций с использованием хеш-функции, создавая 'Branch'.

Транзакции 'Leaf' сначала группируются в пары.



Что такое блок и его структура?

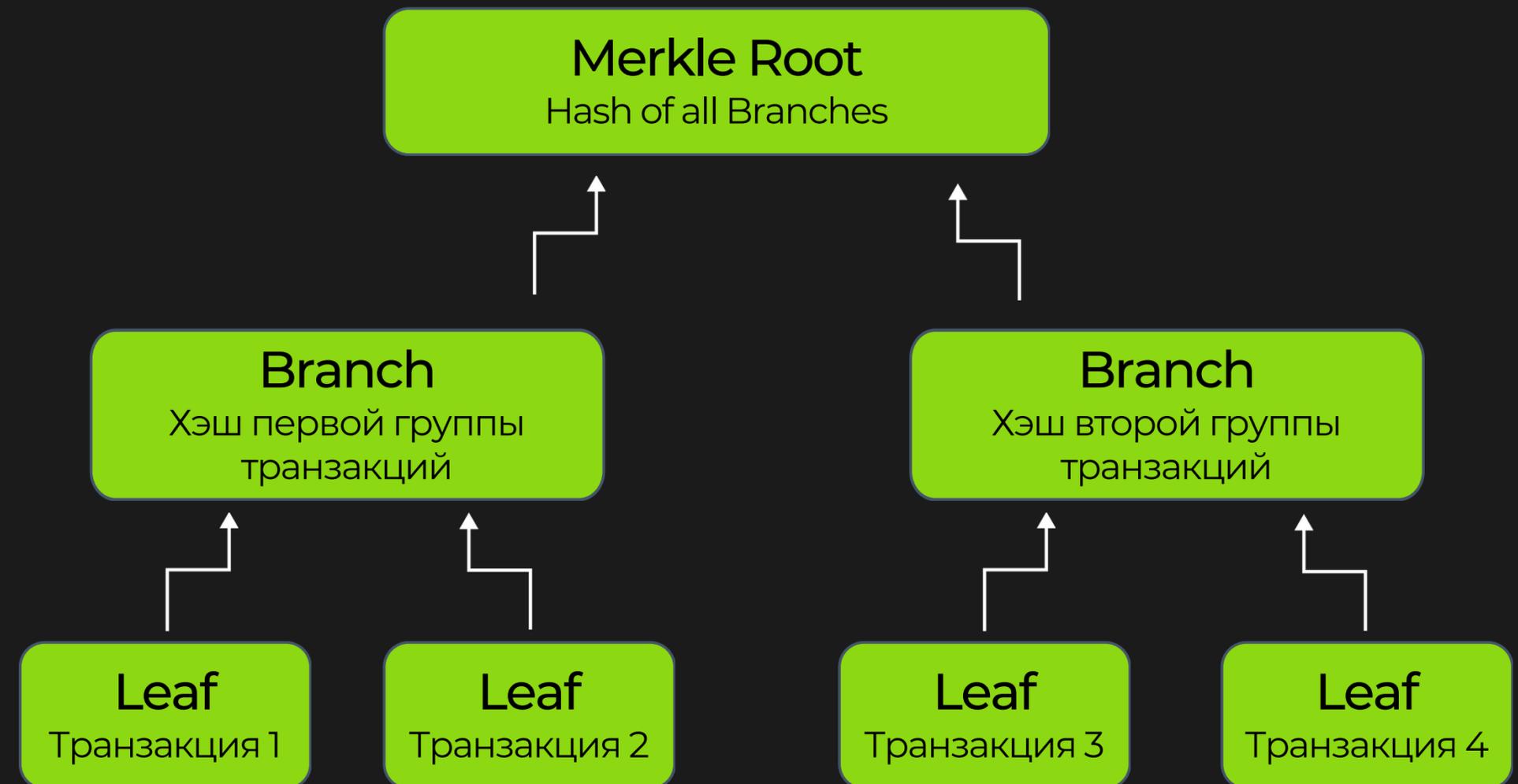
Merkle Root

Это математическая структура данных, состоящая из хэшей различных блоков данных, которые суммируют все транзакции в блоке.

Затем эти хэши группируются в пары и снова хэшируются, и процесс повторяется до тех пор, пока не останется только 'Root'.

Хэш вычисляется для каждой пары транзакций с использованием хеш-функции, создавая 'Branch'.

Транзакции 'Leaf' сначала группируются в пары.

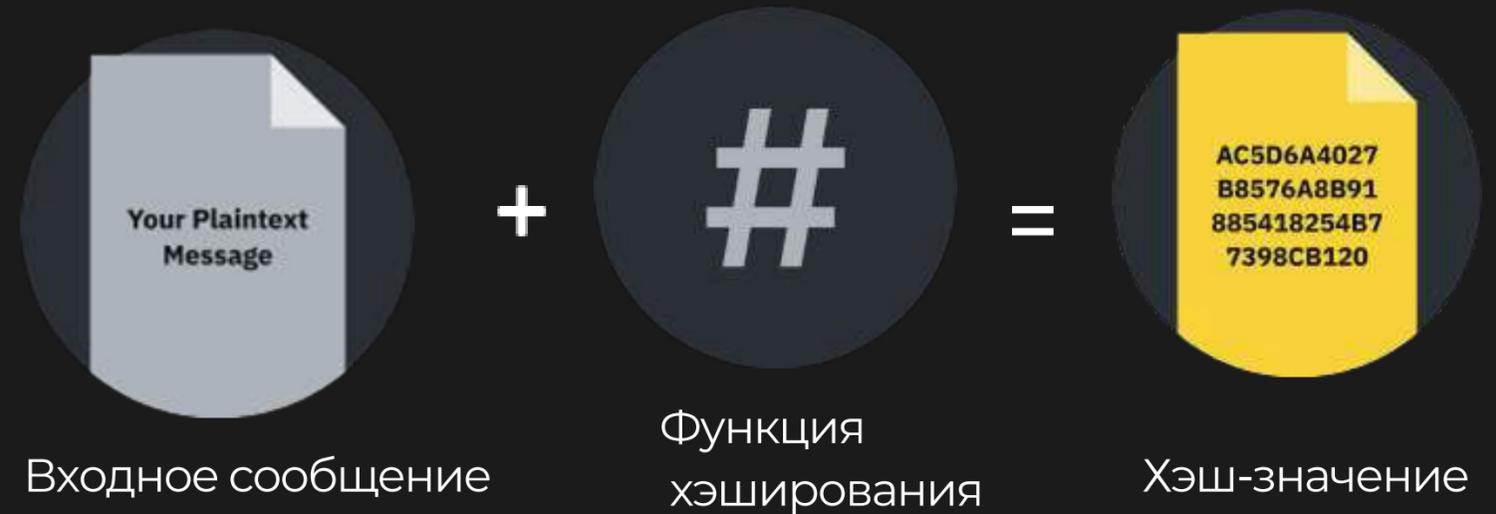


Что такое блок и его структура? **Хэш Блока**

Хэширование

- ◆ Процесс использования входных данных для создания строки определенного размера, которая также называется выходом
- ◆ Выполнено с использованием хэш-функций
- ◆ Примеры ввода: текст, изображения, видео

Пример хэш-функции:



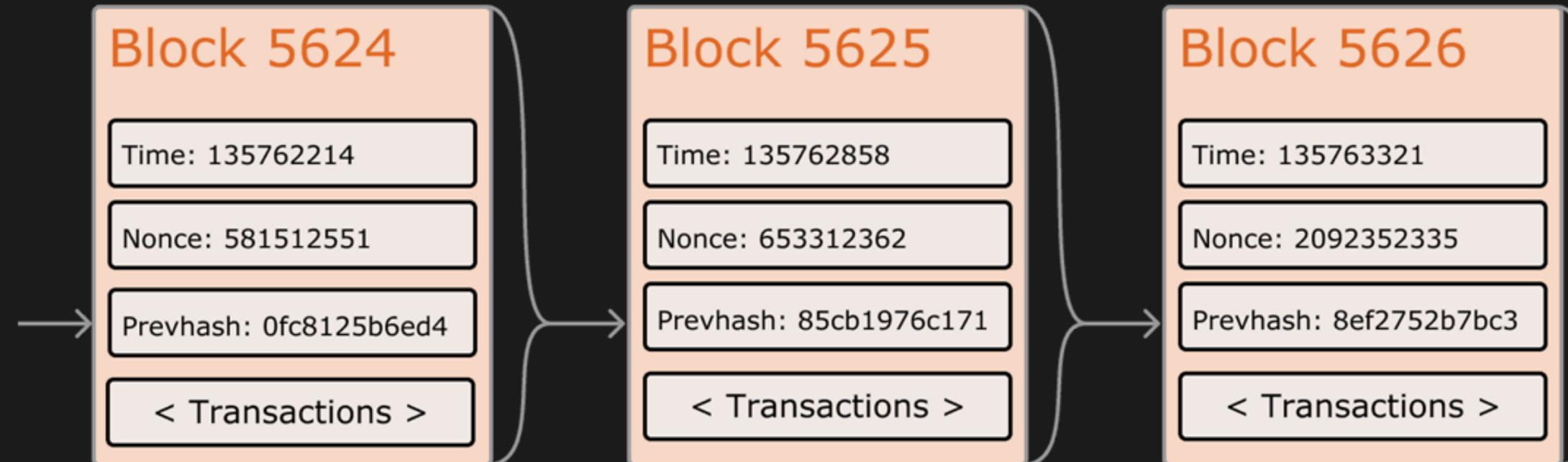
Что такое Блокчейн? Как блоки соединяются вместе?

Блокчейн это криптографически защищенная цепочка блоков, в которой один блок ссылается на предыдущий блок, и так до первого блока

1. Чтобы добавить новый блок в цепочку, нужно решить сложную проблему (нахождение **nonce**)

2. Нахождение такого числа, чтобы полученный хэш был равен X ведущим нулям.

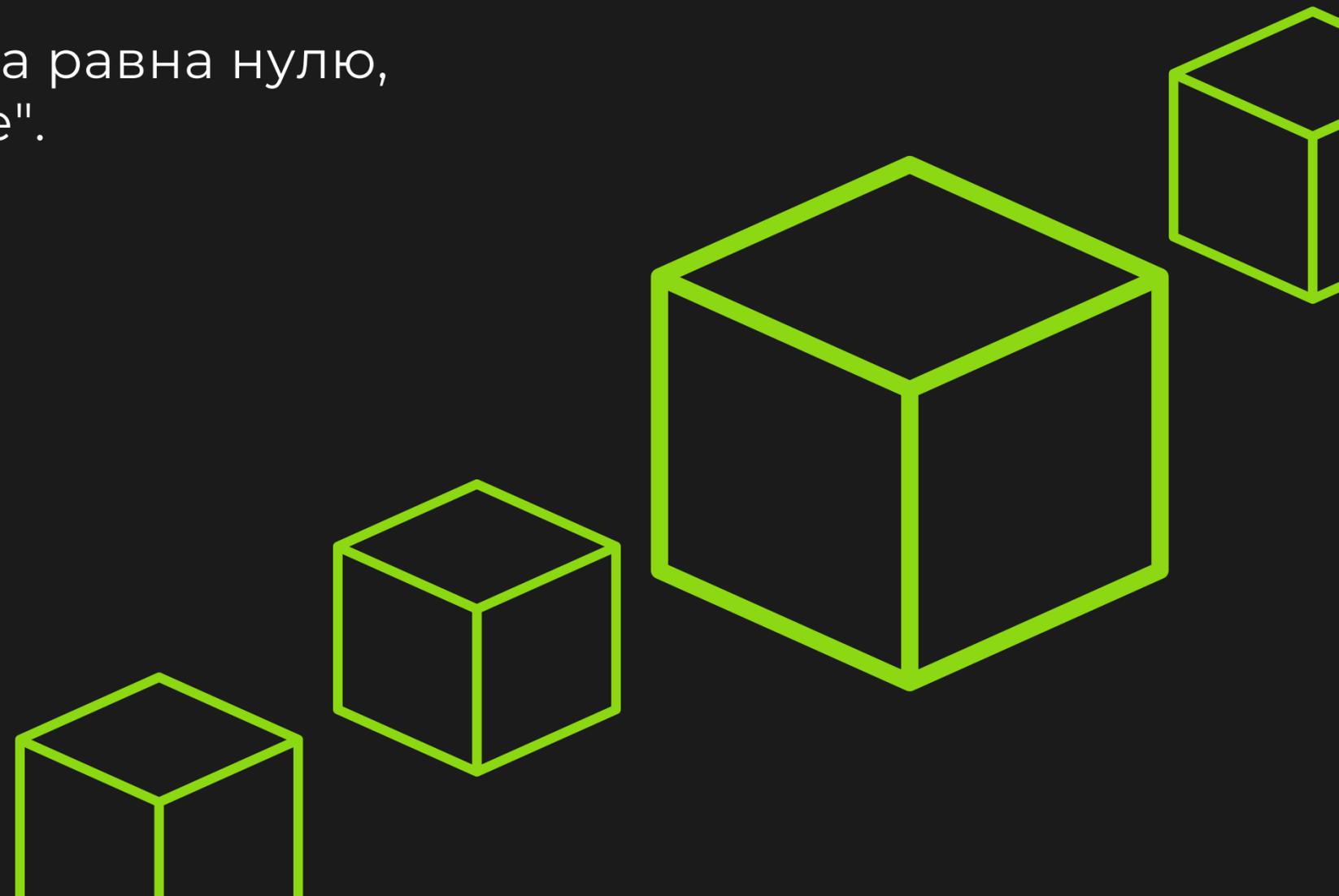
3. Синхронизироваться через алгоритм консенсуса



Генезис Блок

Самый первый блок в сети. Помимо этого главного различия, этот блок также отличается от остальных блоков, поскольку он в основном содержит конфигурации и правила для плавной работы blockchain.

Обратите внимание, что высота этого блока равна нулю, так как в цепи нет ничего перед или "выше".



Высота Блока

Как и любая другая структура данных, существует индекс или, скорее, "серийный номер", присвоенный каждому блоку, который в этом контексте называется высотой блока и его соотношением с блоком генезиса.

Например, высота блока 74638-го блока в цепи составляла бы 74638.

Blocks 🔥 Fees Burnt: 152,041.85 BNB

Block #25573096 to #25573120 (Total of 25,573,121 blocks) First < Page 1 of 1022925 > Last

Block	Age	Txn	Validator	Gas Used	Gas Limit	Reward	Fees Burnt
25573120	7 secs ago	103	0xb4dd66d7c2c7e57f62...	8,837,124 (6.38%)	138,361,556	0.05525 BNB	0.00552 BNB
25573119	10 secs ago	89	Validator: Alan Turing	14,377,953 (10.35%)	138,904,149	0.07262 BNB	0.00726 BNB
25573118	13 secs ago	93	Validator: Avengers	9,615,395 (6.90%)	139,448,870	0.04295 BNB	0.00429 BNB
25573117	16 secs ago	98	Validator: Legend III	13,178,193 (9.41%)	139,995,727	0.06789 BNB	0.00678 BNB
25573116	19 secs ago	99	Validator: Fuji	19,709,072 (14.13%)	139,450,998	0.1025 BNB	0.01025 BNB
25573115	22 secs ago	92	0x73564052d8e469ed07...	10,884,120 (7.84%)	138,908,389	0.05682 BNB	0.00568 BNB
25573114	25 secs ago	120	Validator: BNB48 Club	26,226,316 (18.81%)	139,453,126	0.10899 BNB	0.01089 BNB
25573113	28 secs ago	142	Validator: BscScan	15,331,928 (10.95%)	140,000,000	0.07937 BNB	0.00793 BNB
25573112	31 secs ago	81	0x61dd481a114a2e761c...	6,716,180 (4.80%)	140,000,000	0.03814 BNB	0.00381 BNB
25573111	34 secs ago	93	Validator: Legend II	8,075,847 (5.77%)	140,000,000	0.04429 BNB	0.00442 BNB
25573110	37 secs ago	65	Validator: NodeReal	8,442,844 (6.03%)	140,000,000	0.07791 BNB	0.00779 BNB

Вознаграждение за блок

Этот термин применим в случаях, когда майнеры получают вознаграждение за ресурсы и энергию, которые они тратят на добычу и позволяют сети достичь консенсуса.

Базовым вознаграждением за блок является coinbase награда

6.25 BTC

Coinbase
Reward

b76fca4...	0.000912 BTC
701aa0c...	0.000897 BTC
210fd8...	0.000846 BTC
a123bbc...	0.000721 BTC
abc420d...	0.000694 BTC
a1b2c3d...	0.000563 BTC

Transaction
Fees

Распределенный Реестр & Прозрачность Блокчейна

Распределенный реестр — это база данных, которая хранится, совместно используется и синхронизируется в сети компьютеров. Технология блокчейн позволяет нескольким сторонам записывать транзакции и обмениваться записями друг с другом прозрачно и безопасно.

Распределенный Реестр & Прозрачность Блокчейна

Распределенный реестр — это база данных, которая хранится, совместно используется и синхронизируется в сети компьютеров. Технология блокчейн позволяет нескольким сторонам записывать транзакции и обмениваться записями друг с другом прозрачно и безопасно.



Распределенный Реестр & Прозрачность Блокчейна

Распределенный реестр — это база данных, которая хранится, совместно используется и синхронизируется в сети компьютеров. Технология блокчейн позволяет нескольким сторонам записывать транзакции и обмениваться записями друг с другом прозрачно и безопасно.



База Данных vs Блокчейн

База Данных

Блокчейн

База Данных vs Блокчейн

База Данных

Блокчейн

Централизованный



Децентрализованный

База Данных vs Блокчейн

База Данных

Централизованный

Быстрый

Блокчейн

Децентрализованный

Медленный



База Данных vs Блокчейн

База Данных

Централизованный

Быстрый

Непостоянное

Блокчейн

Децентрализованный

Медленный

Неизменное



Плюсы и Минусы Блокчейна

Плюсы и Минусы Блокчейна

Плюсы

Безопасность

Плюсы и Минусы Блокчейна

Плюсы

Безопасность

Прозрачность

Плюсы и Минусы Блокчейна

Плюсы

Безопасность

Прозрачность

Доступность

Плюсы и Минусы Блокчейна

Плюсы

Безопасность

Прозрачность

Доступность

Децентрализованный

Плюсы и Минусы Блокчейна

Плюсы

Безопасность

Прозрачность

Доступность

Децентрализованный

Минусы

Неэффективность

Плюсы и Минусы Блокчейна

Плюсы

Безопасность

Прозрачность

Доступность

Децентрализованный

Минусы

Неэффективность

Сложность

Плюсы и Минусы Блокчейна

Плюсы

Безопасность

Прозрачность

Доступность

Децентрализованный

Минусы

Неэффективность

Сложность

Контроль

Плюсы и Минусы Блокчейна

Плюсы

Безопасность

Прозрачность

Доступность

Децентрализованный

Минусы

Неэффективность

Сложность

Контроль

Скорость транзакций

Типы Блокчейна: Публичный vs Приватный

Типы Блокчейна: Публичный vs Приватный

Публичный

Любой может участвовать в качестве валидатора или пользователя.

Приватный

Имеет ограниченный доступ

Типы Блокчейна: Публичный vs Приватный

Публичный

Любой может участвовать в качестве валидатора или пользователя.

Любой имеет право на чтение, запись или проверку транзакций.

Приватный

Имеет ограниченный доступ

Только авторизованным сторонам разрешаются проверка транзакций и получение доступ к данным в сети.

Типы Блокчейна: Публичный vs Приватный

Публичный

Любой может участвовать в качестве валидатора или пользователя.

Любой имеет право на чтение, запись или проверку транзакций.

Децентрализованный

Приватный

Имеет ограниченный доступ

Только авторизованным сторонам разрешаются проверка транзакций и получение доступ к данным в сети.

Частично децентрализованный.

Практика: Работа с тестовым блокчейном

- Создание web3 кошелька
- Переключение между EVM сетями
- Получение тестовых коинов (test BNB) из крана
- Совершить транзакцию в блокчейне
- Отследить транзакцию в блокчейне