Технология блокчейн
#5

Алгоритмы консенсуса и майнинг блоков

Blockchain Center

Содержание

Blockchain Center

Содержание

Blockchain Center

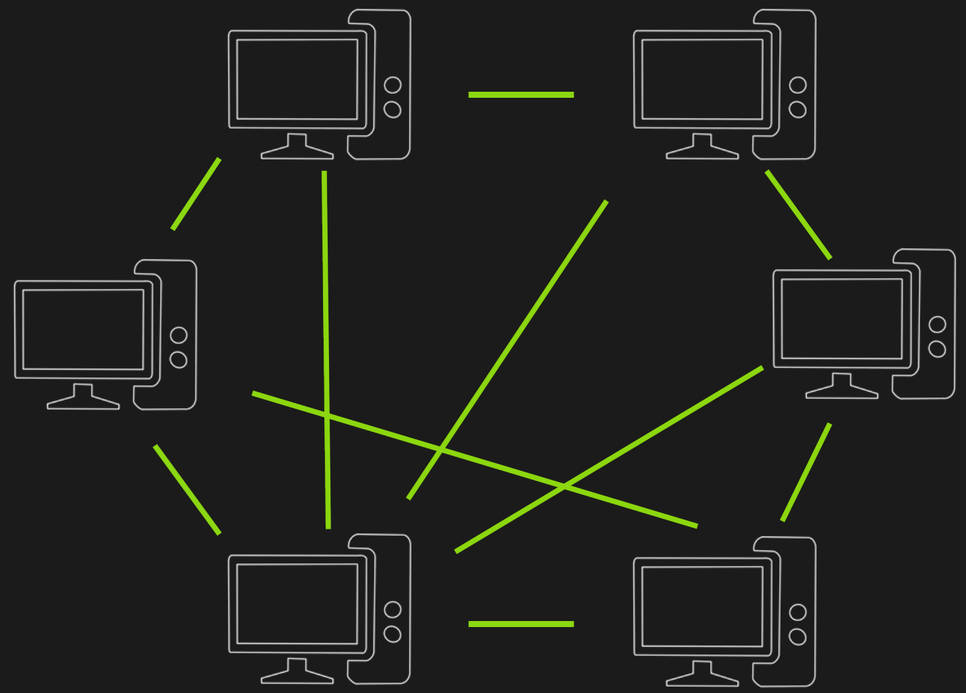
Содержание

Blockchain Center

Содержание

Peer-To-Peer сеть

Одноранговая сеть — это тип компьютерной сети, в которой два или более компьютеров совместно используют ресурсы без необходимости использования центрального сервера. Вместо того, чтобы полагаться на ***один центральный сервер*** *для управления и распространения данных, сети P2P позволяют компьютерам* ***общаться*** *и* ***обмениваться информацией*** *напрямую друг с другом.*

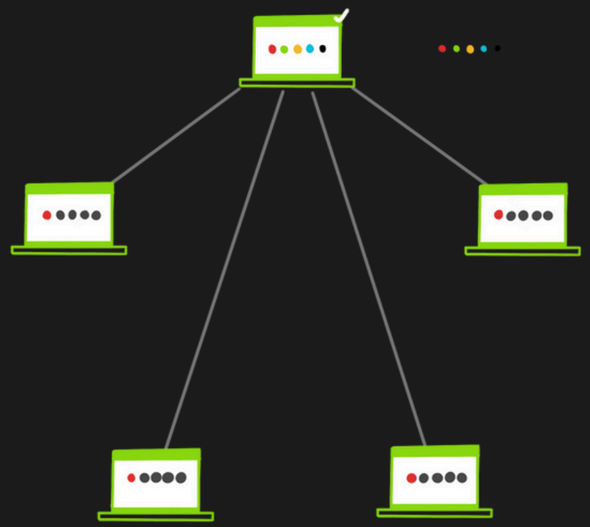


Blockchain Center

Отличия P2P от Клиент-Сервер

Клиент-Сервер

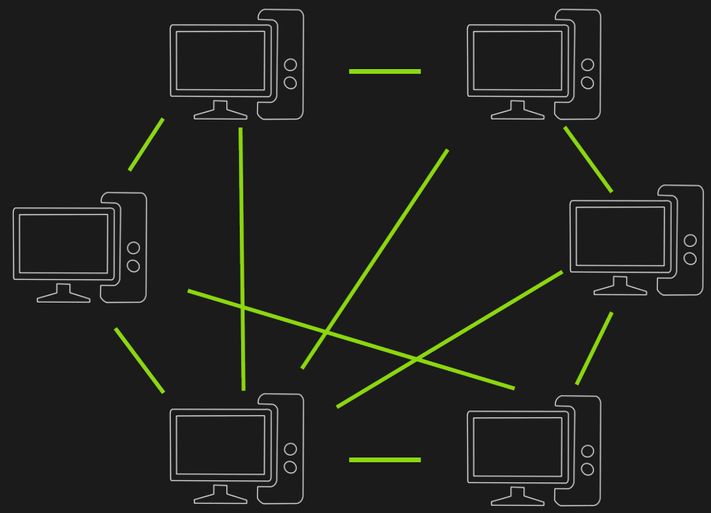
Архитектура



Клиент-Сервер - это тип сети, в которой один или несколько компьютеров, называемых "серверами", предоставляют ресурсы для остальных компьютеров, называемых "клиентами"

Peer-To-Peer (P2P)

Архитектура



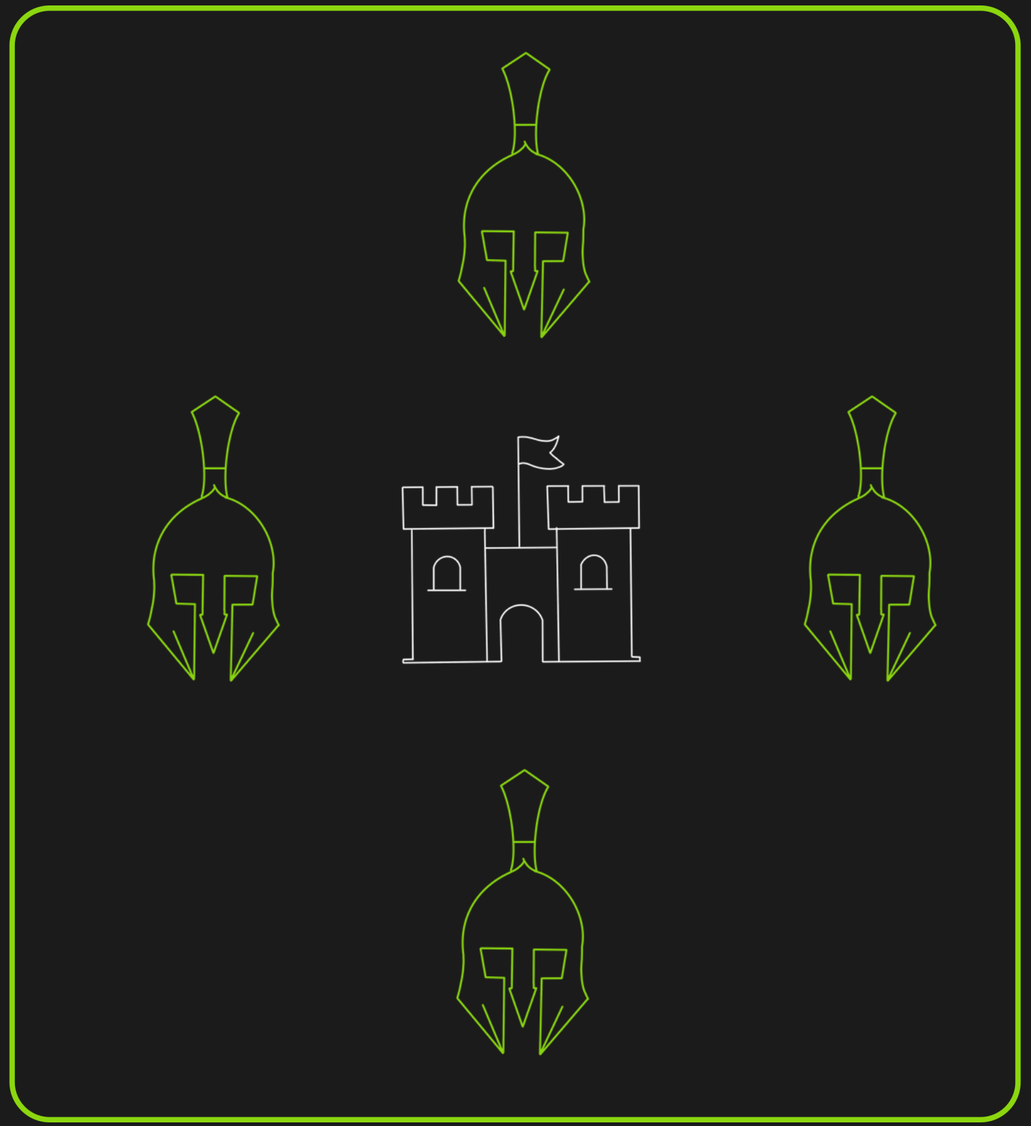
P2P сеть - это тип сети в которой соединены два и более компьютера, раздающие ресурсы без необходимости центрального сервера.

Сервер-Клиент VS P2P

Сервер-Клиент		P2P сеть
Централизована, один или несколько серверов предоставляют ресурсы клиентами.	**Архитектура**	Децентрализована, каждый участник одновременно является и клиентом и сервером.
Может потребовать дополнительные сервера для увеличения пропускной способности.	**Масштабируемость**	Может масштабироваться каждым участником сети без потребности в дополнительных серверах.
Более подвержена уязвимостям, так как существует центральный сервер на котором может быть сосредоточено внимание хакеров.	**Безопасность**	Безопаснее, нет центральной точки атаки для хакеров. При этом уязвимости возможны, так как каждый участник ответственен за безопасность хранения данных и ресурсов.
Более эффективна. Данные управляются единой централизованной системой.	**Эффективность**	Менее эффективна. Более длинный путь для получения данных по причине их хранения на множестве независимых источников.

Проблема Византийских генералов

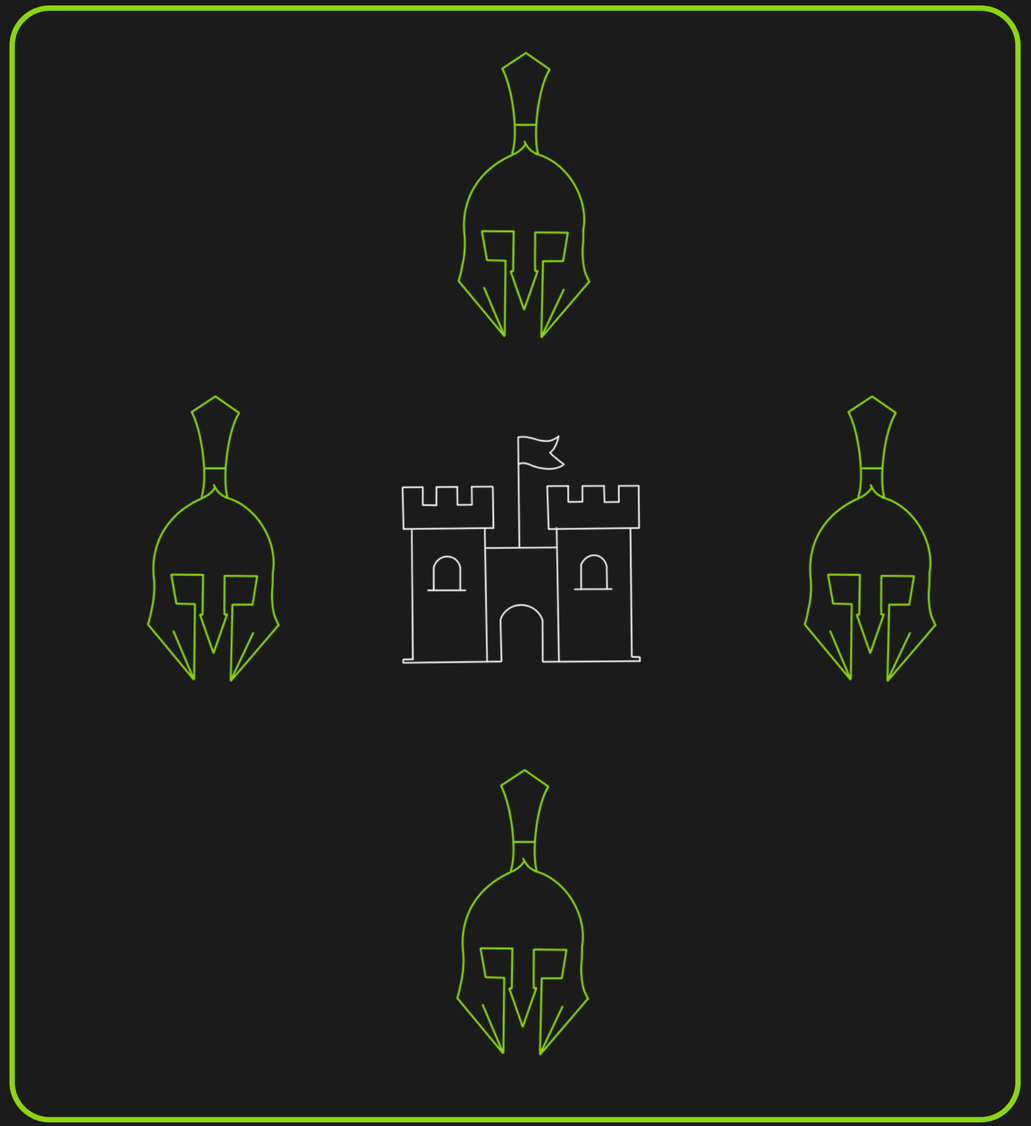
Проблема византийских генералов, также известная как проблема византийской отказоустойчивости (BFT), представляет собой гипотетический сценарий, демонстрирующий сложность достижения консенсуса в распределенной системе, когда некоторые узлы могут быть ненадежными.



Проблема Византийских генералов

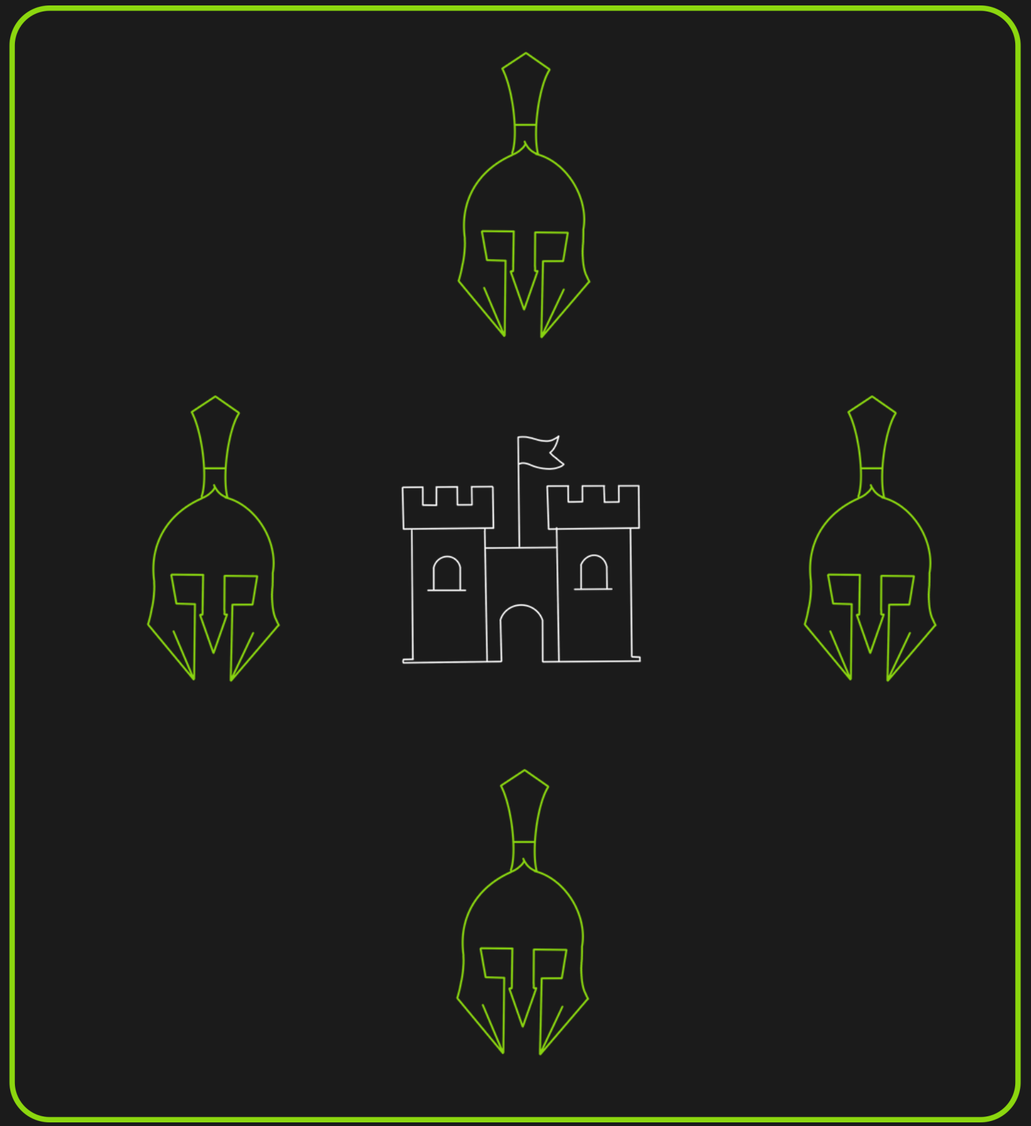
Проблема византийских генералов, также известная как проблема византийской отказоустойчивости (BFT), представляет собой гипотетический сценарий, демонстрирующий сложность достижения консенсуса в распределенной системе, когда некоторые узлы могут быть ненадежными.

Группа генералов вокруг вражеского города. Они должны выбрать стратегию нападения или отступления, и они должны коммуницировать друг с другом, чтобы прийти к консенсусу. Однако некоторые из генералов могут быть предателями, которые пытаются помешать лояльным генералам прийти к соглашению.



Проблема Византийских генералов

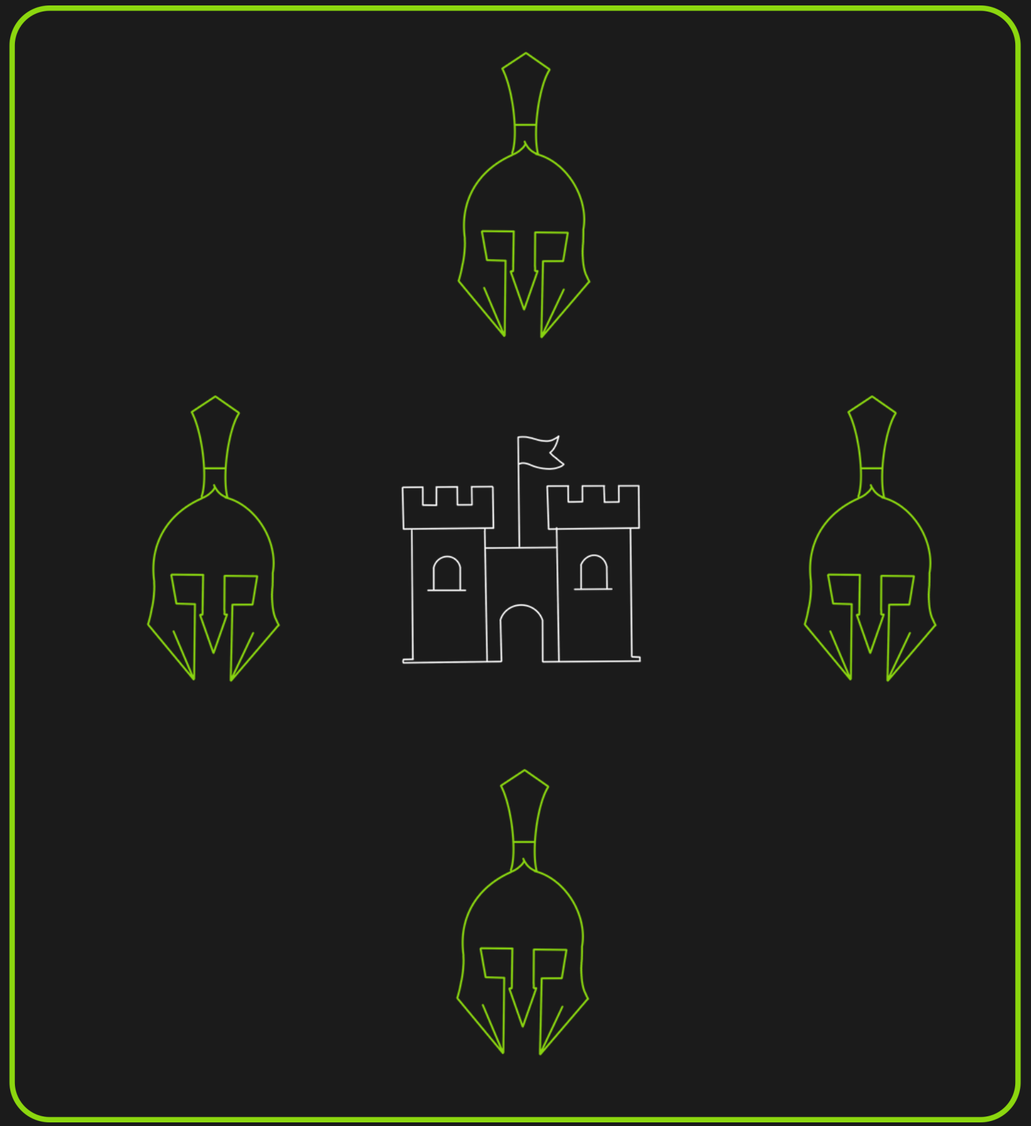
Проблема получила свое название от исторического события в Византийской империи, когда группа византийских генералов расположилась лагерем вокруг вражеского города и должна была общаться друг с другом.



Проблема Византийских генералов

Проблема получила свое название от исторического события в Византийской империи, когда группа византийских генералов расположилась лагерем вокруг вражеского города и должна была общаться друг с другом.

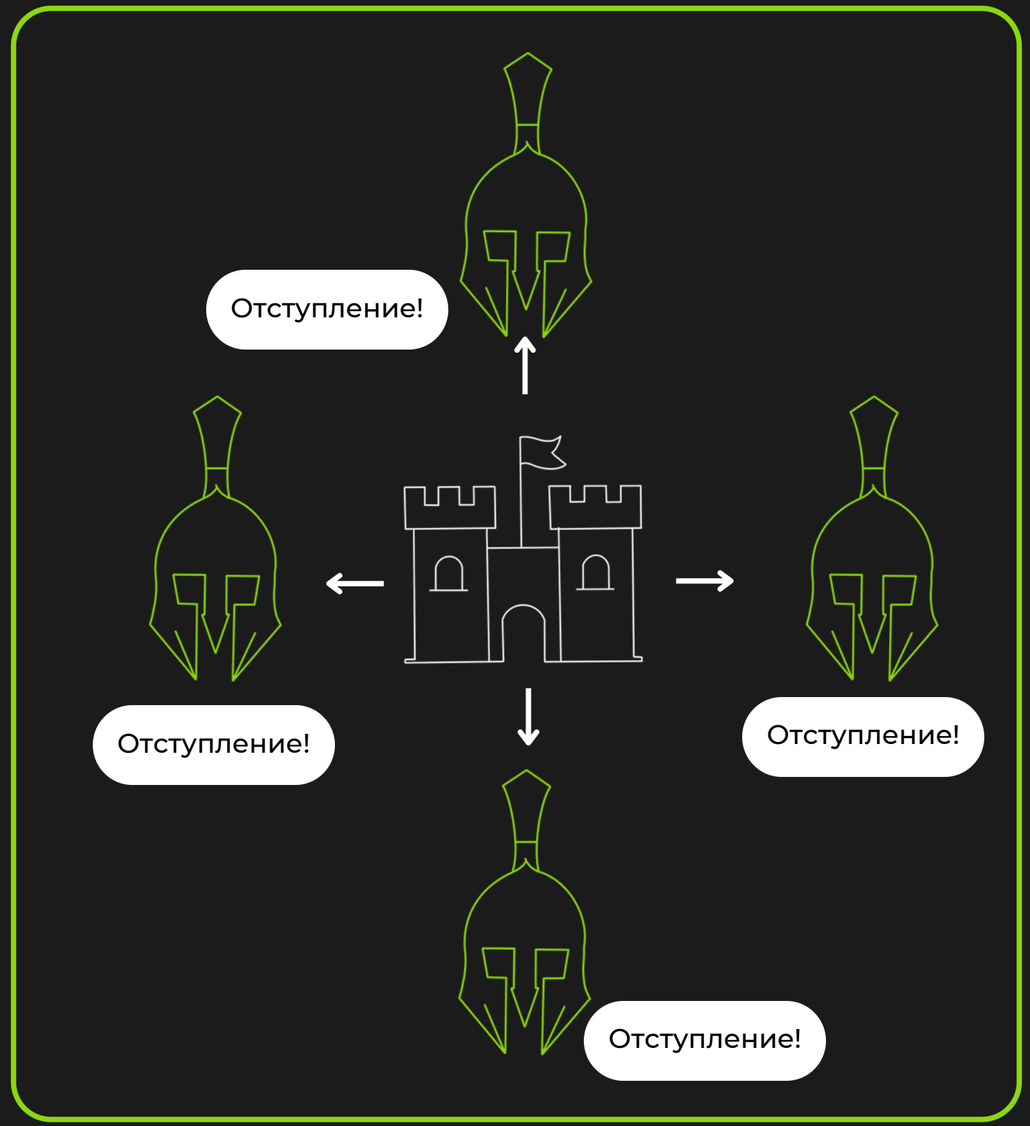
Эта проблема актуальна для алгоритмов консенсуса, поскольку она подчеркивает проблемы достижения консенсуса в распределенной системе. Алгоритмы консенсуса предназначены для решения проблемы византийских генералов, предоставляя узлам возможность достичь согласия по одному значению, несмотря на ненадежные узлы.



Проблема Византийских генералов

Проблема получила свое название от исторического события в Византийской империи, когда группа византийских генералов расположилась лагерем вокруг вражеского города и должна была общаться друг с другом.

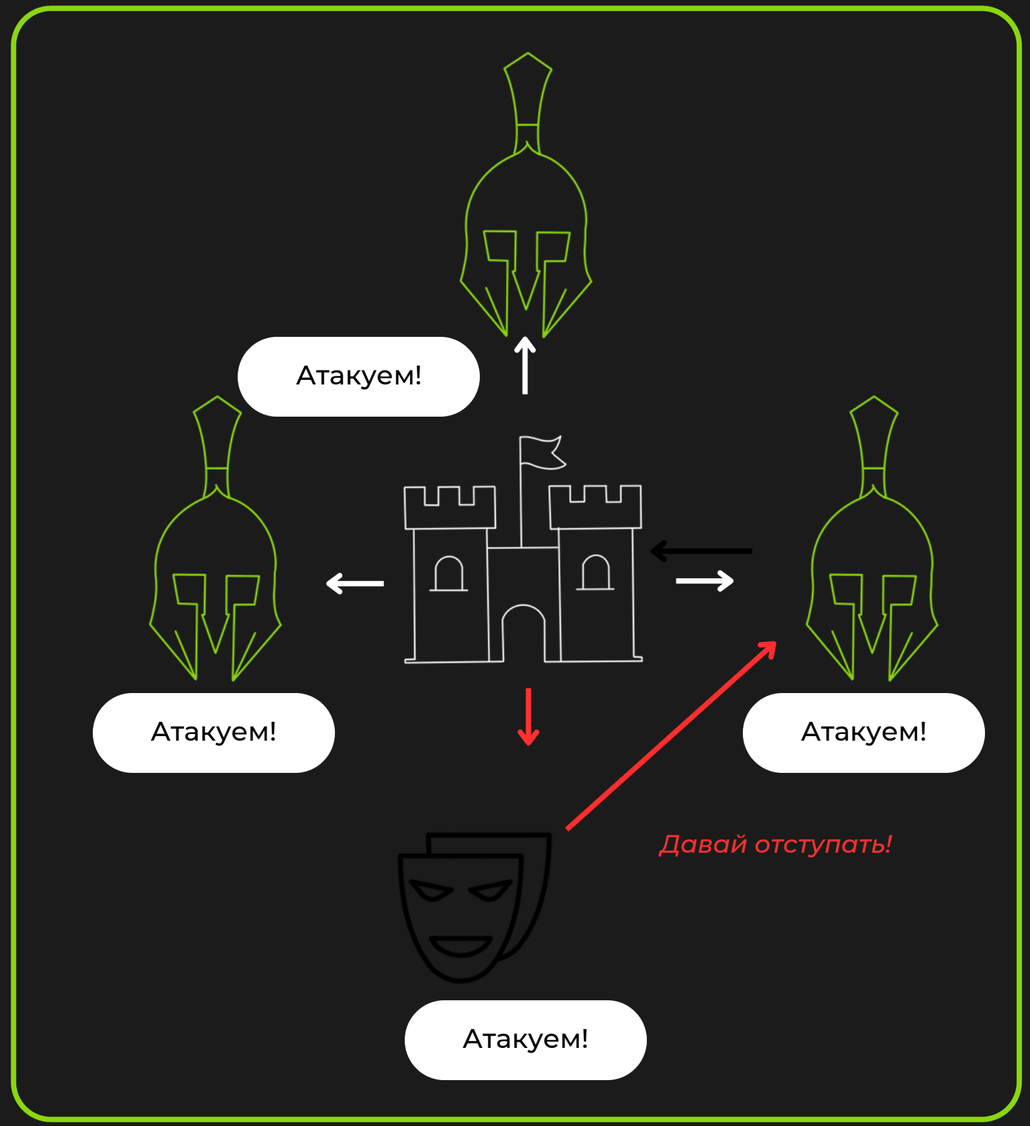
Эта проблема актуальна для алгоритмов консенсуса, поскольку она подчеркивает проблемы достижения консенсуса в распределенной системе. Алгоритмы консенсуса предназначены для решения проблемы византийских генералов, предоставляя узлам возможность достичь согласия по одному значению, несмотря на ненадежные узлы.



Проблема Византийских генералов

Проблема получила свое название от исторического события в Византийской империи, когда группа византийских генералов расположилась лагерем вокруг вражеского города и должна была общаться друг с другом.

Эта проблема актуальна для алгоритмов консенсуса, поскольку она подчеркивает проблемы достижения консенсуса в распределенной системе. Алгоритмы консенсуса предназначены для решения проблемы византийских генералов, предоставляя узлам возможность достичь согласия по одному значению, несмотря на ненадежные узлы.



Blockchain Center

Что такое Алгоритм консенсуса?

Алгоритмы консенсуса *— это протоколы или процессы, которые используются для достижения согласия по одному значению среди группы распределенных процессов или систем. Эти алгоритмы можно оценивать на основе нескольких атрибутов, включая отказоустойчивость, масштабируемость, безопасность и децентрализацию.*

Blockchain Center

Что такое Алгоритм консенсуса?

Алгоритмы консенсуса *— это протоколы или процессы, которые используются для достижения согласия по одному значению среди группы распределенных процессов или систем. Эти алгоритмы можно оценивать на основе нескольких атрибутов, включая отказоустойчивость, масштабируемость, безопасность и децентрализацию.*

Отказоустойчивый алгоритм консенсуса может достичь консенсуса, даже если некоторые узлы выходят из строя или ведут себя неправильно. Например, он может работать с недоступными или конфликтующими узлами.

Что такое Алгоритм консенсуса?

Алгоритмы консенсуса *— это протоколы или процессы, которые используются для достижения согласия по одному значению среди группы распределенных процессов или систем. Эти алгоритмы можно оценивать на основе нескольких атрибутов, включая отказоустойчивость, масштабируемость, безопасность и децентрализацию.*

Отказоустойчивый алгоритм консенсуса может достичь консенсуса, даже если некоторые узлы выходят из строя или ведут себя неправильно. Например, он может работать с недоступными или конфликтующими узлами.

Масштабируемость относится к способности алгоритма консенсуса справляться с увеличением количества узлов или объема транзакций. Масштабируемый алгоритм консенсуса должен иметь возможность продолжать эффективно достигать консенсуса по мере увеличения размера сети.

Blockchain Center

Что такое **Алгоритм консенсуса**?

Алгоритмы консенсуса *— это протоколы или процессы, которые используются для достижения согласия по одному значению среди группы распределенных процессов или систем. Эти алгоритмы можно оценивать на основе нескольких атрибутов, включая отказоустойчивость, масштабируемость, безопасность и децентрализацию.*

Отказоустойчивый алгоритм консенсуса может достичь консенсуса, даже если некоторые узлы выходят из строя или ведут себя неправильно. Например, он может работать с недоступными или конфликтующими узлами.

Масштабируемость относится к способности алгоритма консенсуса справляться с увеличением количества узлов или объема транзакций. Масштабируемый алгоритм консенсуса должен иметь возможность продолжать эффективно достигать консенсуса по мере увеличения размера сети.

Безопасность алгоритма консенсуса относится к его способности защищать от атак или других угроз. Например, безопасный алгоритм консенсуса может использовать криптографические методы, чтобы гарантировать, что транзакции безопасны и не могут быть изменены.

Что такое **Алгоритм консенсуса**?

Алгоритмы консенсуса *— это протоколы или процессы, которые используются для достижения согласия по одному значению среди группы распределенных процессов или систем. Эти алгоритмы можно оценивать на основе нескольких атрибутов, включая отказоустойчивость, масштабируемость, безопасность и децентрализацию.*

Отказоустойчивый алгоритм консенсуса может достичь консенсуса, даже если некоторые узлы выходят из строя или ведут себя неправильно. Например, он может работать с недоступными или конфликтующими узлами.

Масштабируемость относится к способности алгоритма консенсуса справляться с увеличением количества узлов или объема транзакций. Масштабируемый алгоритм консенсуса должен иметь возможность продолжать эффективно достигать консенсуса по мере увеличения размера сети.

Безопасность алгоритма консенсуса относится к его способности защищать от атак или других угроз. Например, безопасный алгоритм консенсуса может использовать криптографические методы, чтобы гарантировать, что транзакции безопасны и не могут быть изменены.

Децентрализация относится к распределению полномочий по контролю и принятию решений среди участвующих узлов в сети. Алгоритм децентрализованного консенсуса опирается на несколько узлов для достижения консенсуса, а не на один центральный орган.

Blockchain Center

Proof of Work Consensus Algorithm

The proof of work (PoW) механизм - это тип консенсусного алгоритма, который используется для достижения распредленного консенсуса в распределенной системе.

Proof of Work Consensus Algorithm

The proof of work (PoW) механизм - это тип консенсусного алгоритма, который используется для достижения распредленного консенсуса в распределенной системе.

Ключевые особенности Proof of Work

- Используется для достижения консенсуса в распределенных системах.

Proof of Work Consensus Algorithm

The proof of work (PoW) механизм - это тип консенсусного алгоритма, который используется для достижения распредленного консенсуса в распределенной системе.

Ключевые особенности Proof of Work

- Используется для достижения консенсуса в распределенных системах.
- Необходимы майнеры для решения задач, необходимых для создания блока.

Proof of Work Consensus Algorithm

The proof of work (PoW) механизм - это тип консенсусного алгоритма, который используется для достижения распредленного консенсуса в распределенной системе.

Ключевые особенности Proof of Work

- Используется для достижения консенсуса в распределенных системах.
- Необходимы майнеры для решения задач, необходимых для создания блока.
- Майнер, который первый решил задачу внутри блока получает вознаграждение.

Proof of Work Consensus Algorithm

The proof of work (PoW) механизм - это тип консенсусного алгоритма, который используется для достижения распредленного консенсуса в распределенной системе.

Ключевые особенности Proof of Work

- Используется для достижения консенсуса в распределенных системах.
- Необходимы майнеры для решения задач, необходимых для создания блока.
- Майнер, который первый решил задачу внутри блока получает вознаграждение.
- Задача спроектирована так, что ее трудно решить, но легко проверить правильность правильность решения.

Blockchain Center

Proof of Work Consensus Algorithm

The proof of work (PoW) механизм - это тип консенсусного алгоритма, который используется для достижения распредленного консенсуса в распределенной системе.

Ключевые особенности Proof of Work

- Используется для достижения консенсуса в распределенных системах.
- Необходимы майнеры для решения задач, необходимых для создания блока.
- Майнер, который первый решил задачу внутри блока получает вознаграждение.
- Задача спроектирована так, что ее трудно решить, но легко проверить правильность правильность решения.
- Помогает защитить сеть, запрашивая значительные объемы вычислительной мощности для решения задач.

Blockchain Center

Proof of Work Consensus Algorithm

Чтобы скорость производства блоков оставалась ограниченной, майнеры должны решать головоломку для каждого блока. Эта головоломка о том, что хэш блока имеет определенный формат.

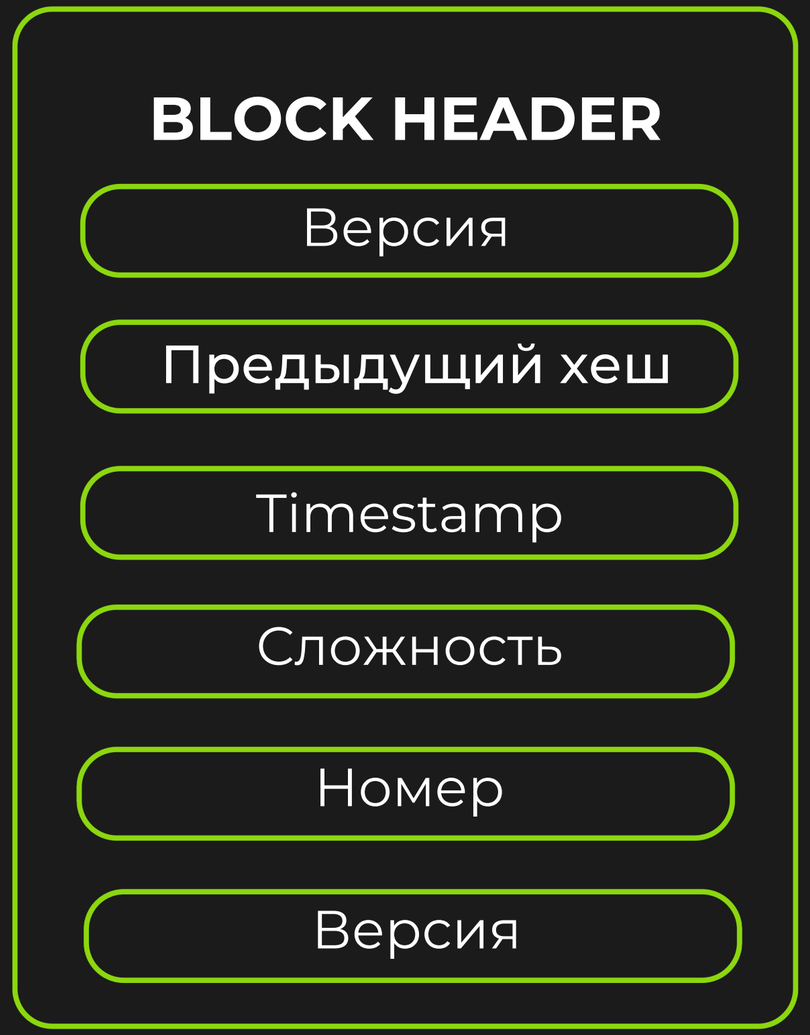
Например, майнеры должны получить hash значение, первые 4 цифры которого - 0

Пример: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdafd043c19

Таким образом, злоумышленники не могут создавать блоки один за другим.

Blockchain Center

Что такое Алгоритм консенсуса?



Blockchain Center

Что такое Алгоритм консенсуса?

BLOCK HEADER

- Версия
- Предыдущий хеш
- Timestamp
- Сложность
- Nonce
- Версия

Хеш блока

3655adf12498c56fee3e3ac60a18ec0d991ca165cc1aeb22048466b98580a7e4

Что такое Алгоритм консенсуса?

BLOCK HEADER

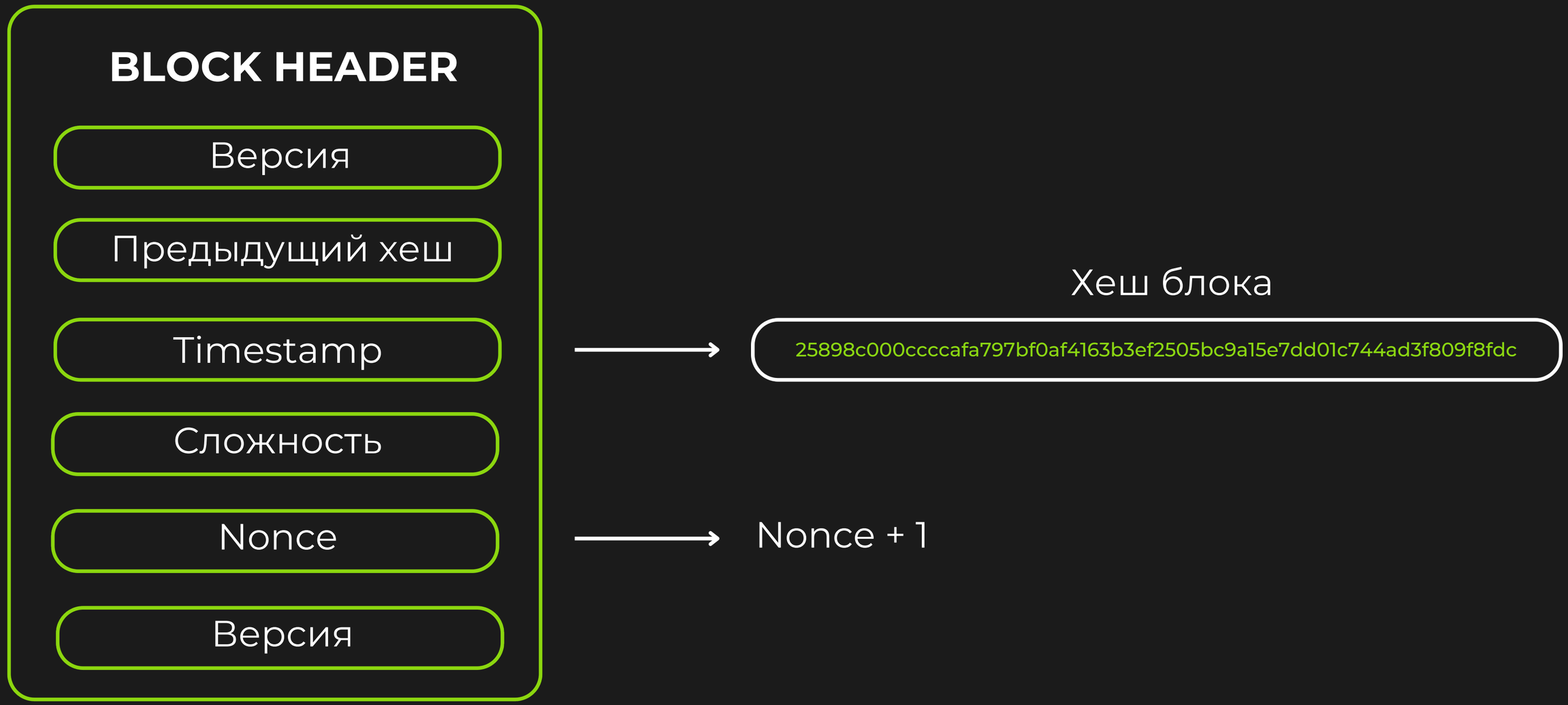
- Версия
- Предыдущий хеш
- Timestamp
- Сложность
- Nonce
- Версия

Timestamp → Хеш блока: 3655adf12498c56fee3e3ac60a18ec0d991ca165cc1aeb22048466b98580a7e4

Nonce → Nonce + 1

Blockchain Center

Что такое Алгоритм консенсуса?



Blockchain Center

Что такое Алгоритм консенсуса?

BLOCK HEADER

- Версия
- Предыдущий хеш
- Timestamp
- Сложность
- Nonce
- Версия

Хеш блока

0000dbce42b61ebb8a459bed02782aca0f733314cfe4896c6c907d00d0c1a0f2

Альтернативные варианты алгоритма консенсуса

Blockchain Center

Содержание

Blockchain Center

Proof Of Stake Consensus Algorithm

1

Валидаторы заносят в стейкинг часть своих монет, чтобы получить вознаграждение за добавление нового блока транзакций.

Proof Of Stake Consensus Algorithm

1

Валидаторы заносят в стейкинг часть своих монет, чтобы получить вознаграждение за добавление нового блока транзакций.

Джо

Рейчел

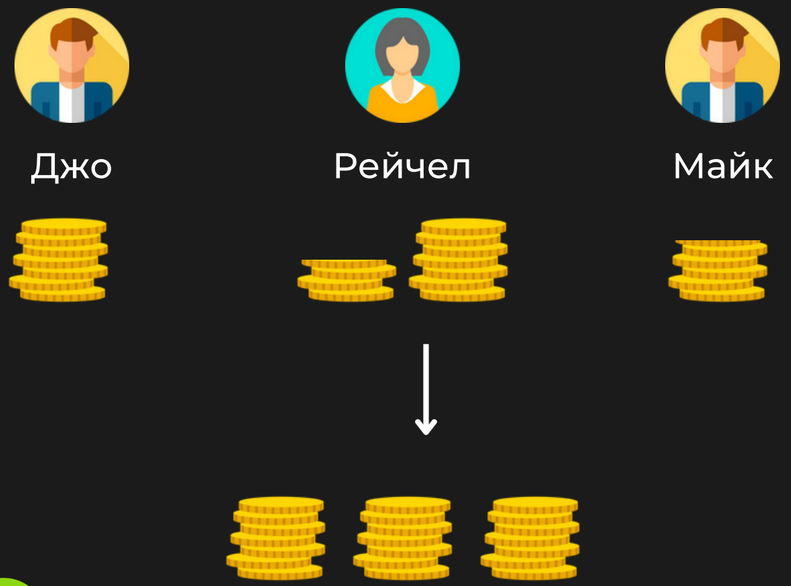
Майк

Blockchain Center

Proof Of Stake Consensus Algorithm

1

Валидаторы заносят в стейкинг часть своих монет, чтобы получить вознаграждение за добавление нового блока транзакций.

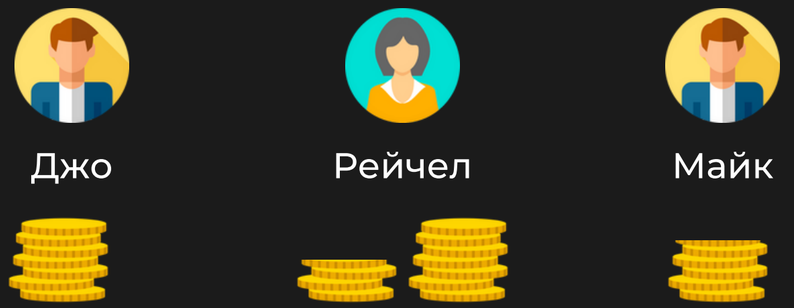


2

Монеты в «Стейкинге» на счете условного депонирования

Proof Of Stake Consensus Algorithm

1. Валидаторы заносят в стейкинг часть своих монет, чтобы получить вознаграждение за добавление нового блока транзакций.



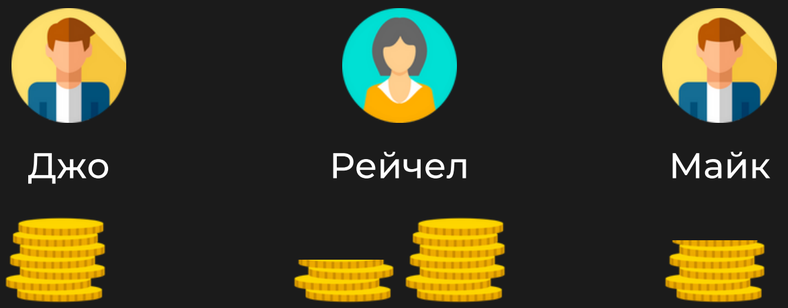
2. Монеты в «Стейкинге» на счете условного депонирования

3. Функция выбирающая рандомный валидатор

4. Джо выбран для добавления нового блока

Proof Of Stake Consensus Algorithm

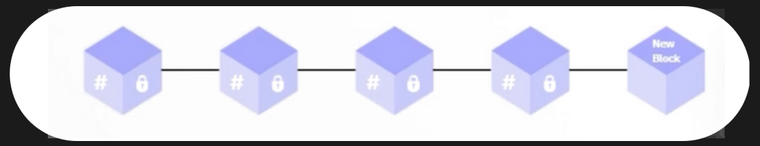
1 Валидаторы заносят в стейкинг часть своих монет, чтобы получить вознаграждение за добавление нового блока транзакций.



2 Монеты в «Стейкинге» на счете условного депонирования

3 Функция выбирающая рандомный валидатор

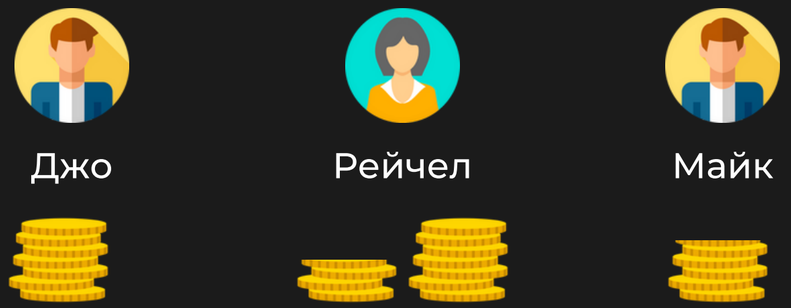
4 Джо выбран для добавления нового блока



5 Новый блок проверяется валидаторами

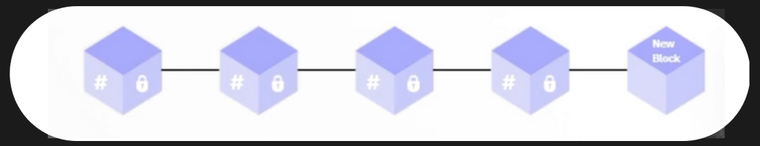
Proof Of Stake Consensus Algorithm

1 Валидаторы заносят в стейкинг часть своих монет, чтобы получить вознаграждение за добавление нового блока транзакций.



2 Монеты в «Стейкинге» на счете условного депонирования

3 Функция выбирающая рандомный валидатор



4 Джо выбран для добавления нового блока

5 Новый блок проверяется валидаторами

Корректно

Джо получил вознаграждение

Некорректно

Джо потерял свои средства в сети

Blockchain Center

Proof Of Stake Consensus Algorithm

Некоторое количество монет необходимо внести в стейкинг для того, чтобы стать валидатором.

Blockchain Center

Proof Of Stake Consensus Algorithm

Некоторое количество монет необходимо внести в стейкинг для того, чтобы стать валидатором.

Генератор блоков выбирается случайным образом с учетом таких параметров, как продолжительность ставки и количество поставленных монет.

Blockchain Center

Proof Of Stake Consensus Algorithm

Некоторое количество монет необходимо внести в стейкинг для того, чтобы стать валидатором.

Генератор блоков выбирается случайным образом с учетом таких параметров, как продолжительность ставки и количество поставленных монет.

Низкое потребление энергии в сравнении с PoW

Blockchain Center

Delegated Proof of Stake Consensus Algorithm

Это вариант алгоритма Proof of Stake

Blockchain Center

Delegated Proof of Stake Consensus Algorithm

Это вариант алгоритма Proof of Stake

Вы (как делегатор) ставите монеты на условное депонирование валидатору. Если валидатор выиграет право на создание блока и заработает монеты, вы получите долю вознаграждения в зависимости от вашего депозита.

Blockchain Center

Delegated Proof of Stake Consensus Algorithm

Это вариант алгоритма Proof of Stake

Вы (как делегатор) ставите монеты на условное депонирование валидатору. Если валидатор выиграет право на создание блока и заработает монеты, вы получите долю вознаграждения в зависимости от вашего депозита.

Процесс выбора валидаторов аналогичен PoS

Blockchain Center

Delegated Proof of Stake Consensus Algorithm

Это вариант алгоритма Proof of Stake

Вы (как делегатор) ставите монеты на условное депонирование валидатору. Если валидатор выиграет право на создание блока и заработает монеты, вы получите долю вознаграждения в зависимости от вашего депозита.

Процесс выбора валидаторов аналогичен PoS

Затем выбранные валидаторы несут ответственность за проверку транзакций и добавление их в блокчейн.

Blockchain Center

Proof of Authority Consensus Algorithm

Список валидаторов ограничен

Blockchain Center

Proof of Authority Consensus Algorithm

Список валидаторов ограничен

Очень высокая масштабируемость

Blockchain Center

Proof of Authority Consensus Algorithm

Список валидаторов ограничен

Очень высокая масштабируемость

Децентрализация утеряна

Blockchain Center

Proof of Authority Consensus Algorithm

Список валидаторов ограничен

Очень высокая масштабируемость

Децентрализация утеряна

Основана на доверии

Proof of Stake Authority (PoSA) Consensus Algorithm

PoA

В PoA права на создание новых блоков предоставляются узлам, которые доказали свои полномочия на это. Чтобы получить эти полномочия и право генерировать новые блоки, узел должен пройти предварительную аутентификацию.

Blockchain Center

Proof of Stake Authority (PoSA) Consensus Algorithm

PoA

В PoA права на создание новых блоков предоставляются узлам, которые доказали свои полномочия на это. Чтобы получить эти полномочия и право генерировать новые блоки, узел должен пройти предварительную аутентификацию.

PoS

Владельцы валюты стейкают монеты, чтобы получить возможность определить блок

Blockchain Center

Proof of Stake Authority (PoSA) Consensus Algorithm

PoA

В PoA права на создание новых блоков предоставляются узлам, которые доказали свои полномочия на это. Чтобы получить эти полномочия и право генерировать новые блоки, узел должен пройти предварительную аутентификацию.

PoS

Владельцы валюты стейкают монеты, чтобы получить возможность определить блок

PoSA

PoSA представляет собой комбинацию PoA и PoS. Блоки производятся ограниченным набором валидаторов, они избираются и избираются на основе управления, основанного на стейкинге.

Альтернативные алгоритмы консенсуса

Proof of capacity

Тип доказательства, требующий от участника предоставить доказательство того, что он выделил определенный объем дискового пространства для сети.

Альтернативные алгоритмы консенсуса

Proof of capacity

Тип доказательства, требующий от участника предоставить доказательство того, что он выделил определенный объем дискового пространства для сети.

Proof of Elapsed Time

Тип подтверждения, требующий от участника предоставления доказательства того, что для участия в сети прошло определенное количество времени.

Blockchain Center

Альтернативные алгоритмы консенсуса

Proof of capacity

Тип доказательства, требующий от участника предоставить доказательство того, что он выделил определенный объем дискового пространства для сети.

Proof of Elapsed Time

Тип подтверждения, требующий от участника предоставления доказательства того, что для участия в сети прошло определенное количество времени.

Proof of Identify

Тип доказательства, который требует от участника предъявить подтверждение своей личности для участия в сети.

Blockchain Center

Альтернативные алгоритмы консенсуса

Proof of capacity

Тип доказательства, требующий от участника предоставить доказательство того, что он выделил определенный объем дискового пространства для сети.

Proof of Elapsed Time

Тип подтверждения, требующий от участника предоставления доказательства того, что для участия в сети прошло определенное количество времени.

Proof of Identify

Тип доказательства, который требует от участника предъявить подтверждение своей личности для участия в сети.

Proof of Activity

Тип подтверждения, который требует от участника демонстрации доказательств своей деятельности, например выполнения задачи или участия в сети.

Blockchain Center

Спасибо за внимание