Технология блокчейн
#3

Ключевые термины — Криптография в Блокчейне

Обзор

1. Криптография в Блокчейне
2. Симметричное и Ассиметричное шифрование
3. Криптографические хэш функции

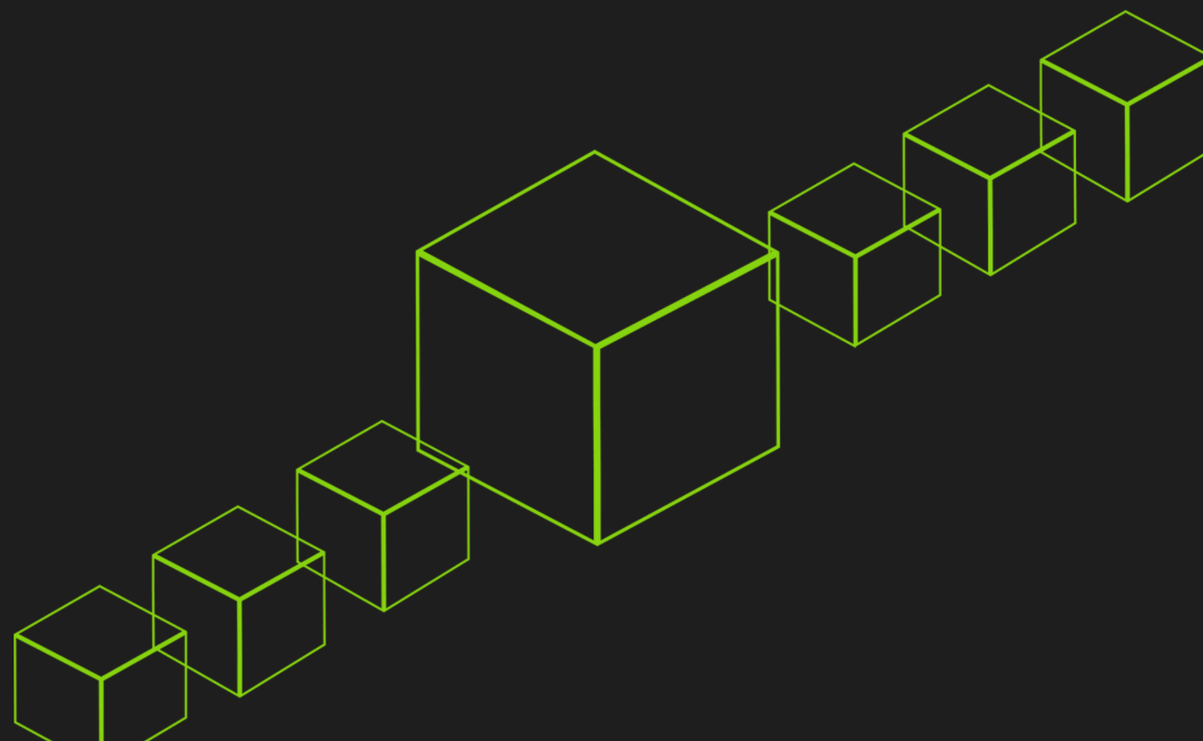
Blockchain Center

Модуль 1 - Криптография в Блокчейне

Blockchain Center

Криптография в Блокчейне

- Что подразумевается под **неизменностью данных**?
- Что такое **атака 51%**?
- Что такое **криптография**?
- Что такое **криптография в блокчейне** и как она **используется**?
- Криптографические **методы**, используемые в **блокчейне**



Blockchain Center

Что подразумевается под неизменностью данных?

Blockchain
Center

Что подразумевается под неизменностью данных?

Неизменность в блокчейне означает, что после записи данных они **не могут быть изменены** или **модифицированы**. Эта **функция достигается** за счет использования криптографических методов. Они позволяют проверять **целостность данных** и **поддерживать** ее.

Неизменность делает блокчейн **подходящей платформой** для **хранения** и **обмена важной информацией**, а также помогает **гарантировать**, что данным можно **доверять**, поскольку они **не могут быть изменены**.

Blockchain Center

Что подразумевается под неизменностью данных?

Неизменность в блокчейне означает, что после записи данных они **не могут быть изменены** или **модифицированы**. Эта **функция достигается** за счет использования криптографических методов. Они позволяют проверять **целостность данных** и **поддерживать** ее.

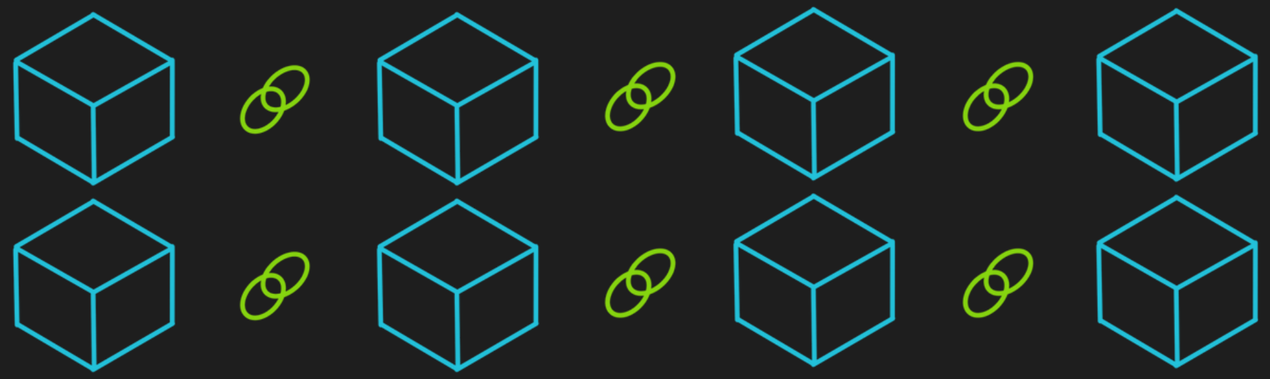
Неизменность делает блокчейн **подходящей платформой** для **хранения** и **обмена важной информацией**, а также помогает **гарантировать**, что данным можно **доверять**, поскольку они **не могут быть изменены**.

Blockchain Center

Что подразумевается под неизменностью данных?

Неизменность в блокчейне означает, что после записи данных они **не могут быть изменены** или **модифицированы**. Эта **функция достигается** за счет использования криптографических методов. Они позволяют проверять **целостность данных** и **поддерживать** ее.

Неизменность делает блокчейн **подходящей платформой** для **хранения** и **обмена важной информацией**, а также помогает **гарантировать**, что данным можно **доверять**, поскольку они **не могут быть изменены**.

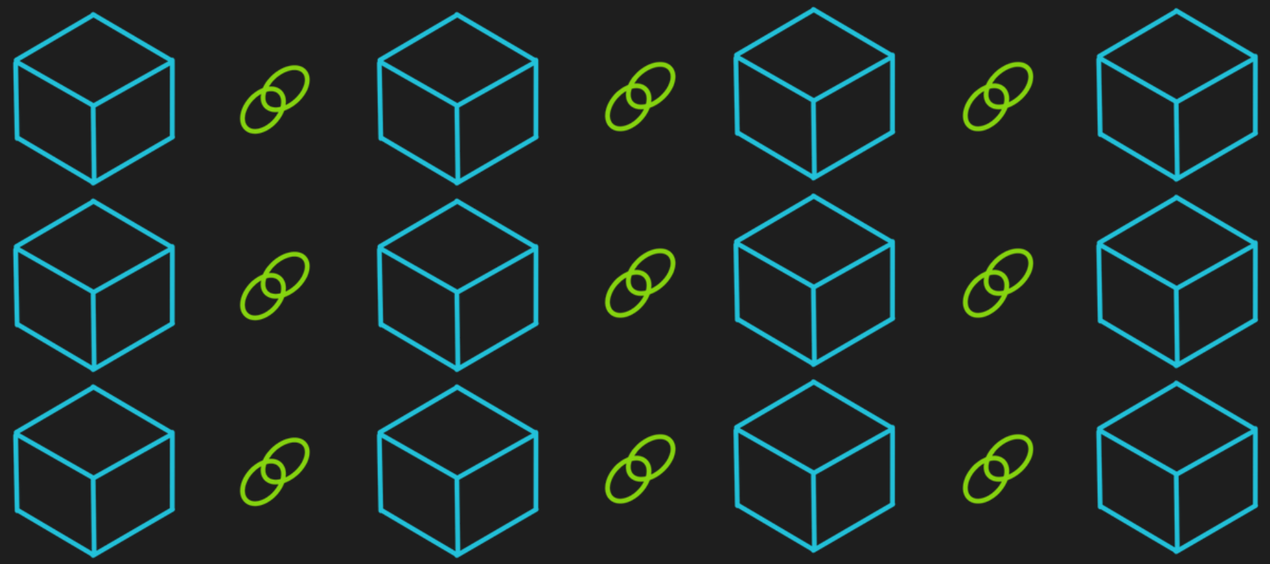


Blockchain Center

Что подразумевается под неизменностью данных?

Неизменность в блокчейне означает, что после записи данных они **не могут быть изменены** или **модифицированы**. Эта **функция достигается** за счет использования криптографических методов. Они позволяют проверять **целостность данных** и **поддерживать** ее.

Неизменность делает блокчейн **подходящей платформой** для **хранения** и **обмена важной информацией**, а также помогает **гарантировать**, что данным можно **доверять**, поскольку они **не могут быть изменены**.

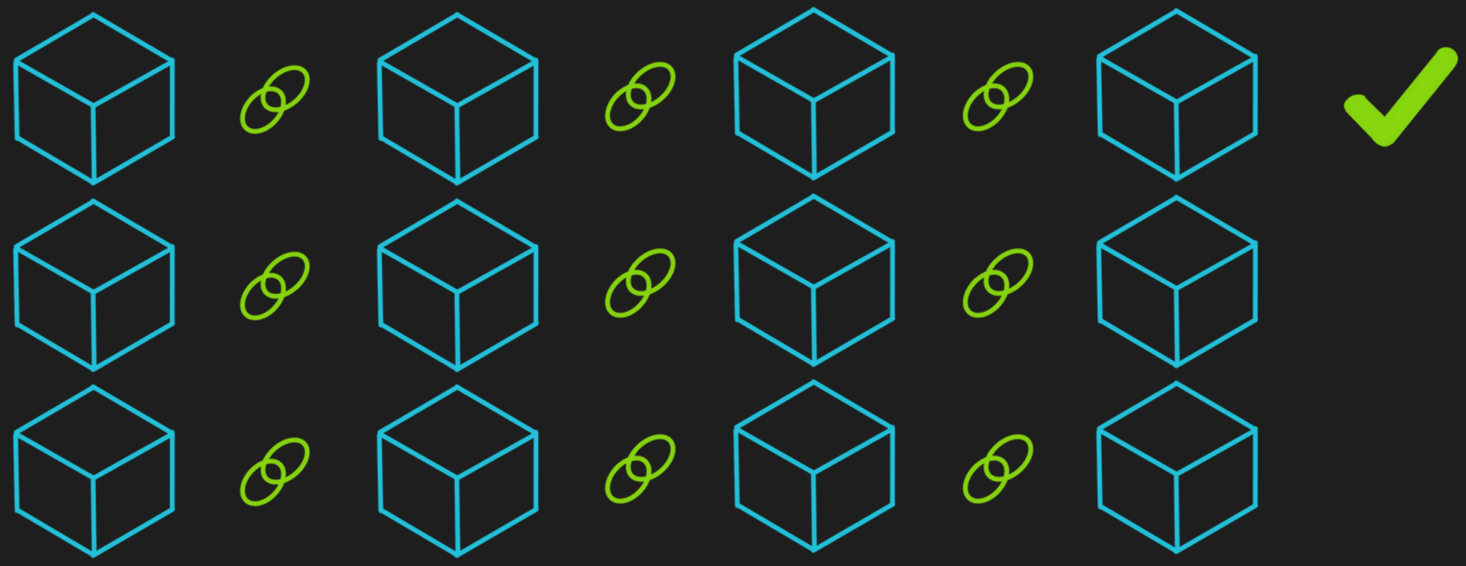


Blockchain Center

Что подразумевается под неизменностью данных?

Неизменность в блокчейне означает, что после записи данных они **не могут быть изменены** или **модифицированы**. Эта **функция достигается** за счет использования криптографических методов. Они позволяют проверять **целостность данных** и **поддерживать** ее.

Неизменность делает блокчейн **подходящей платформой** для **хранения** и **обмена важной информацией**, а также помогает **гарантировать**, что данным можно **доверять**, поскольку они **не могут быть изменены**.

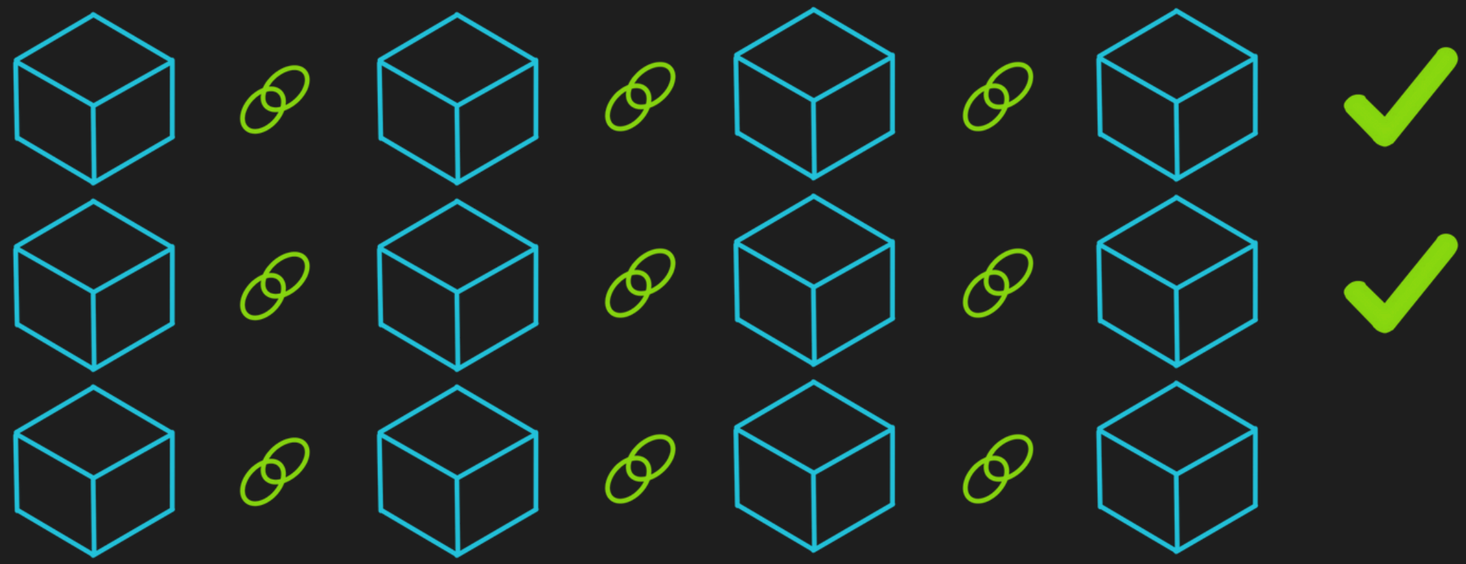


Blockchain Center

Что подразумевается под неизменностью данных?

Неизменность в блокчейне означает, что после записи данных они **не могут быть изменены** или **модифицированы**. Эта **функция достигается** за счет использования криптографических методов. Они позволяют проверять **целостность данных** и **поддерживать** ее.

Неизменность делает блокчейн **подходящей платформой** для **хранения** и **обмена важной информацией**, а также помогает **гарантировать**, что данным можно **доверять**, поскольку они **не могут быть изменены**.

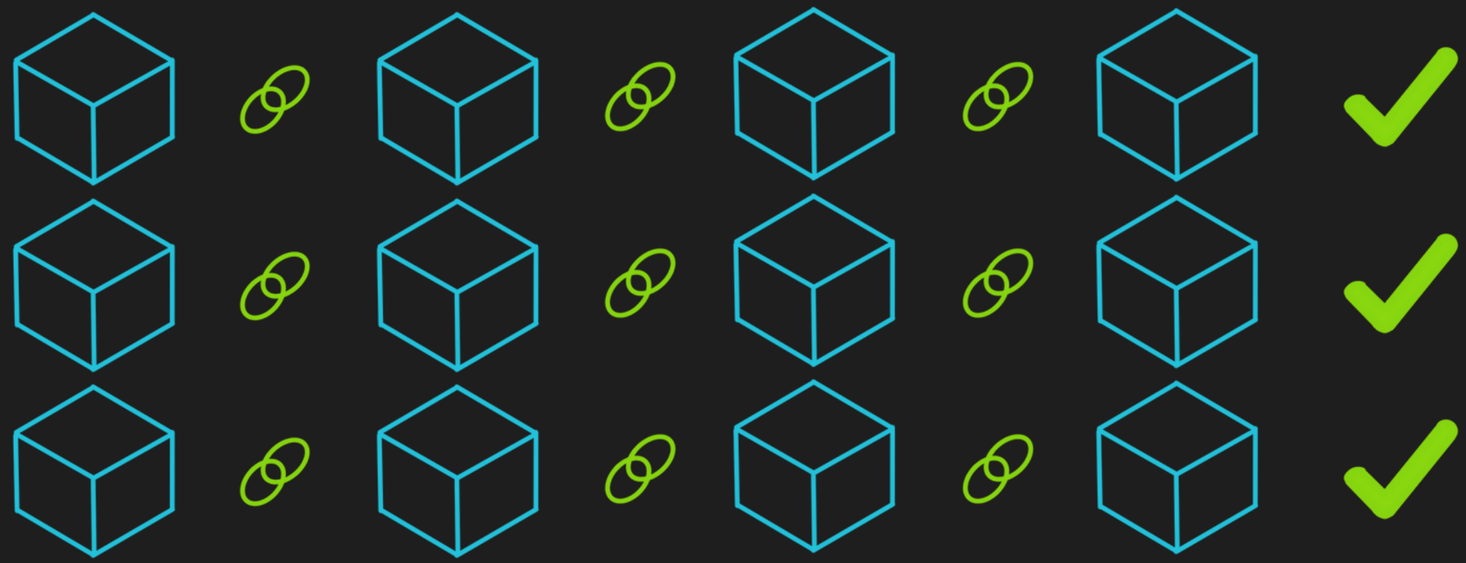


Blockchain Center

Что подразумевается под неизменностью данных?

Неизменность в блокчейне означает, что после записи данных они **не могут быть изменены** или **модифицированы**. Эта **функция достигается** за счет использования криптографических методов. Они позволяют проверять **целостность данных** и **поддерживать** ее.

Неизменность делает блокчейн **подходящей платформой** для **хранения** и **обмена важной информацией**, а также помогает **гарантировать**, что данным можно **доверять**, поскольку они **не могут быть изменены**.



Blockchain Center

Что если данные будут изменены на одном из компьютеров?

Blockchain
Center

Что если данные будут изменены на одном из компьютеров?

Если вы попытаетесь **изменить данные** на одном из компьютеров в сети блокчейн, это изменение **не будет принято** другими компьютерами в сети. Это происходит потому, что каждый компьютер в сети имеет **свою копию блокчейна**, и все они работают вместе, чтобы подтверждать новые **транзакции** и **поддерживать целостность данных.**

Blockchain Center

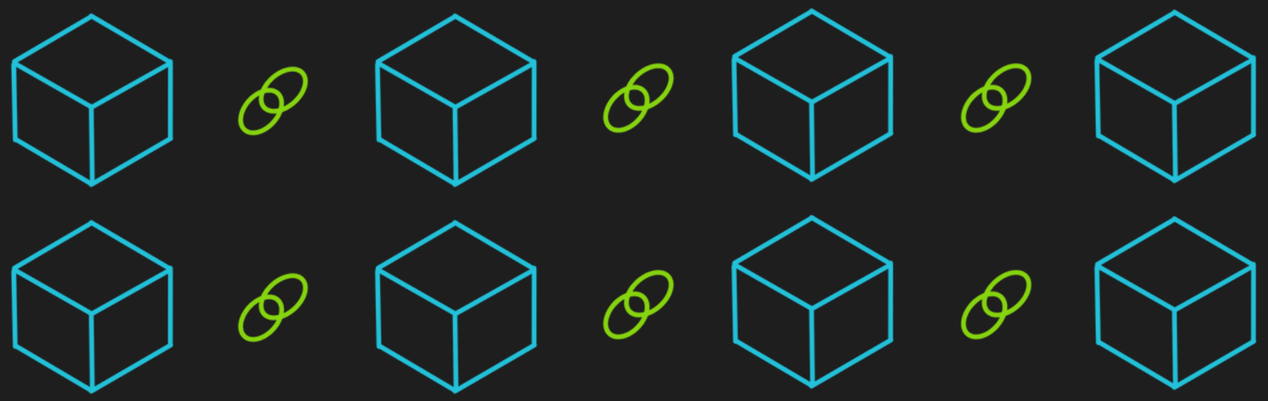
Что если данные будут изменены на одном из компьютеров?

Если вы попытаетесь **изменить данные** на одном из компьютеров в сети блокчейн, это изменение **не будет принято** другими компьютерами в сети. Это происходит потому, что каждый компьютер в сети имеет **свою копию блокчейна**, и все они работают вместе, чтобы подтверждать новые **транзакции** и **поддерживать целостность данных.**

Blockchain Center

Что если данные будут изменены на одном из компьютеров?

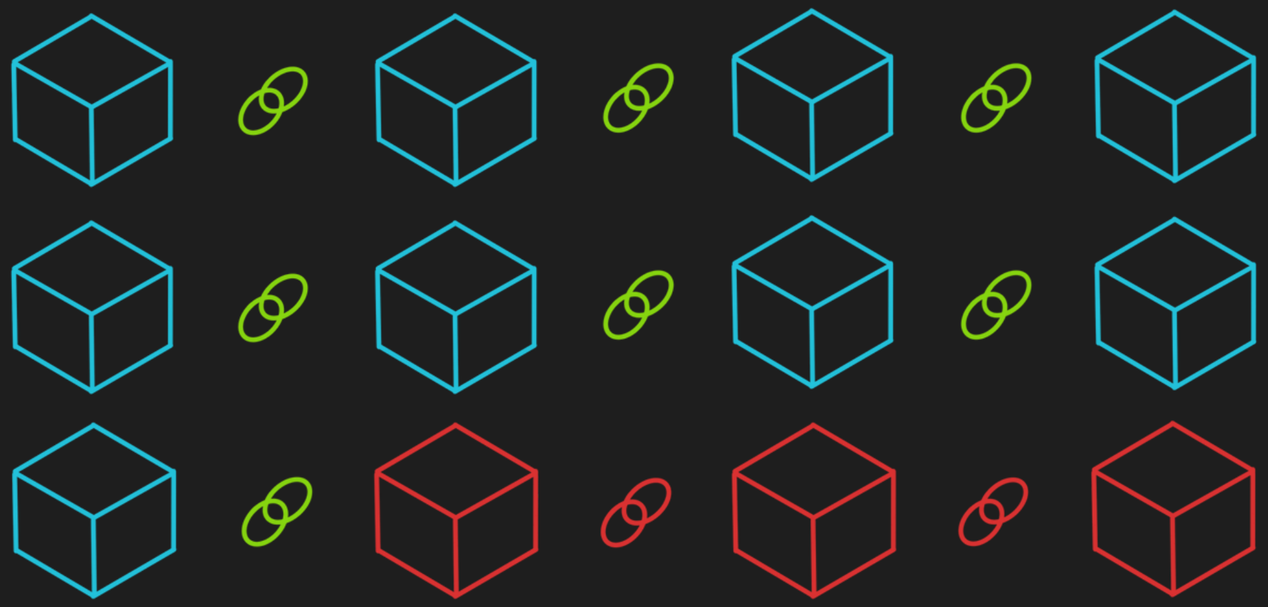
Если вы попытаетесь **изменить данные** на одном из компьютеров в сети блокчейн, это изменение **не будет принято** другими компьютерами в сети. Это происходит потому, что каждый компьютер в сети имеет **свою копию блокчейна**, и все они работают вместе, чтобы подтверждать новые **транзакции** и **поддерживать целостность данных.**



Blockchain Center

Что если данные будут изменены на одном из компьютеров?

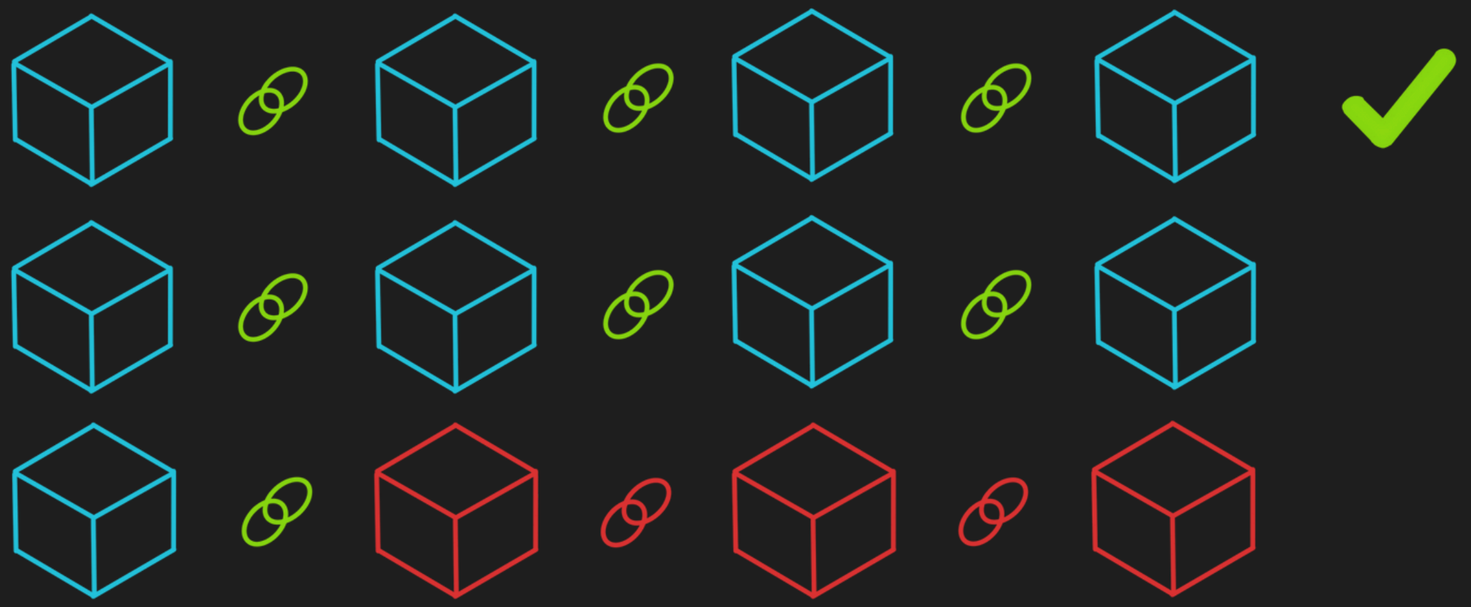
Если вы попытаетесь **изменить данные** на одном из компьютеров в сети блокчейн, это изменение **не будет принято** другими компьютерами в сети. Это происходит потому, что каждый компьютер в сети имеет **свою копию блокчейна**, и все они работают вместе, чтобы подтверждать новые **транзакции** и **поддерживать целостность данных.**



Blockchain Center

Что если данные будут изменены на одном из компьютеров?

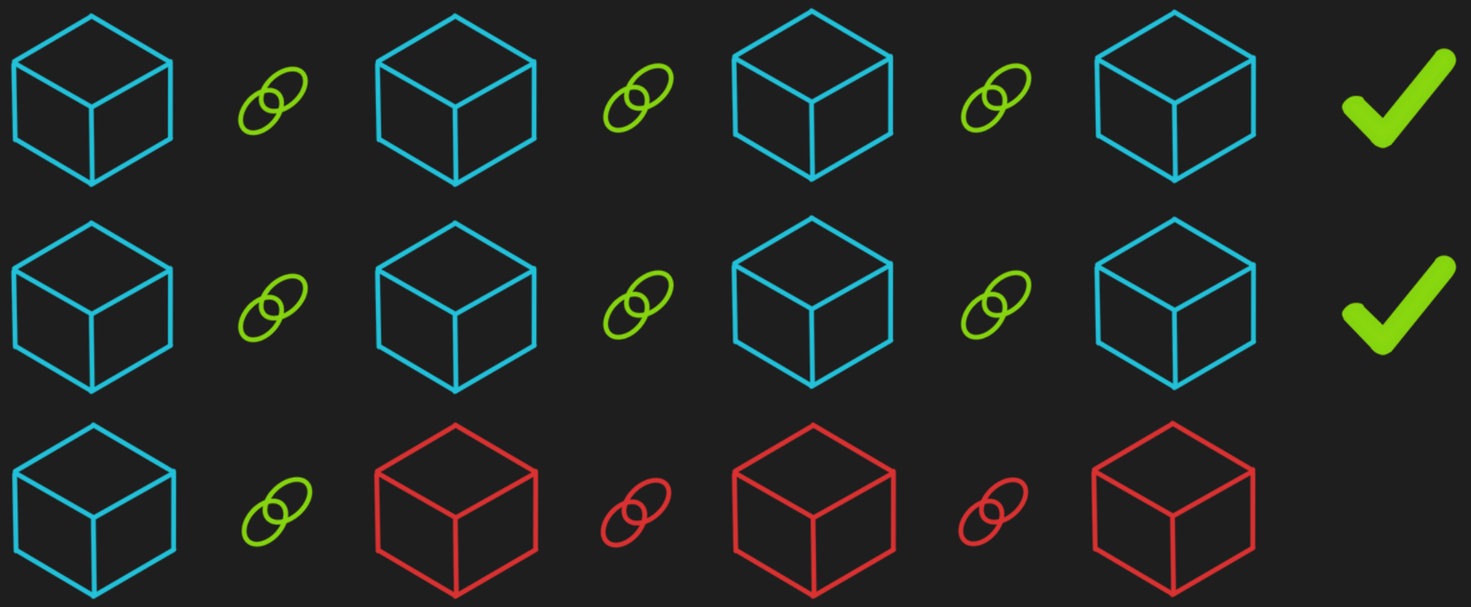
Если вы попытаетесь **изменить данные** на одном из компьютеров в сети блокчейн, это изменение **не будет принято** другими компьютерами в сети. Это происходит потому, что каждый компьютер в сети имеет **свою копию блокчейна**, и все они работают вместе, чтобы подтверждать новые **транзакции** и **поддерживать целостность данных.**



Blockchain Center

Что если данные будут изменены на одном из компьютеров?

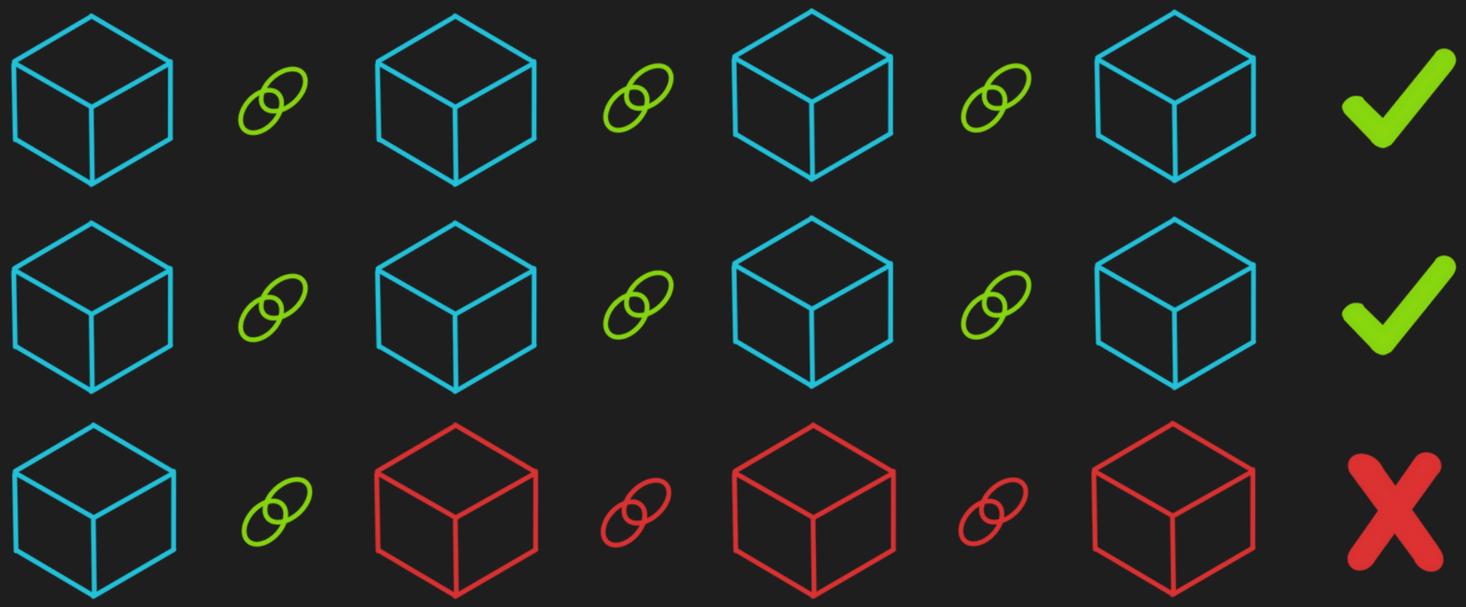
Если вы попытаетесь **изменить данные** на одном из компьютеров в сети блокчейн, это изменение **не будет принято** другими компьютерами в сети. Это происходит потому, что каждый компьютер в сети имеет **свою копию блокчейна**, и все они работают вместе, чтобы подтверждать новые **транзакции** и **поддерживать целостность данных.**



Blockchain Center

Что если данные будут изменены на одном из компьютеров?

Если вы попытаетесь **изменить данные** на одном из компьютеров в сети блокчейн, это изменение **не будет принято** другими компьютерами в сети. Это происходит потому, что каждый компьютер в сети имеет **свою копию блокчейна**, и все они работают вместе, чтобы подтверждать новые **транзакции** и **поддерживать целостность данных.**



Blockchain Center

Атака 51%

Blockchain
Center

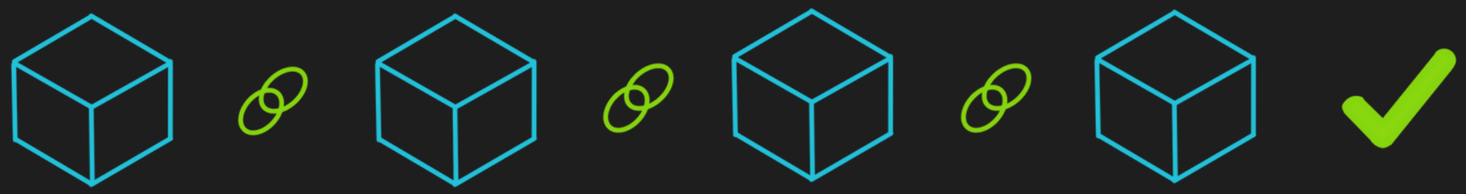
Атака 51%

Если бы злоумышленники смогли взять под контроль большинство компьютеров в сети блокчейн, они потенциально могли бы манипулировать сетью различными способами. Это известно как "атака 51%", поскольку для осуществления такой атаки злоумышленникам потребуется контролировать **более 50%** вычислительной мощности сети.

Blockchain
Center

Атака 51%

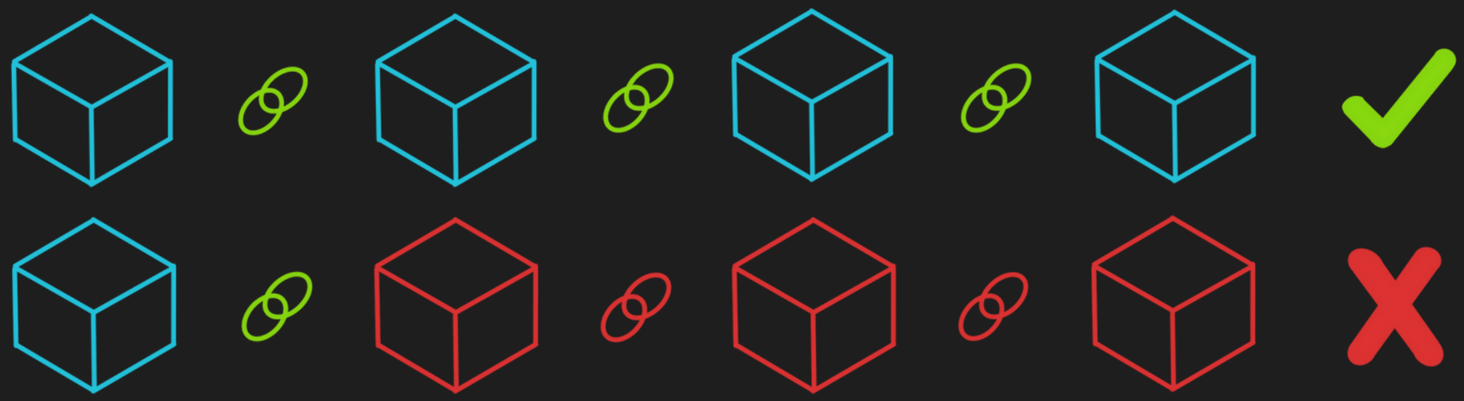
Если бы злоумышленники смогли взять под контроль большинство компьютеров в сети блокчейн, они потенциально могли бы манипулировать сетью различными способами. Это известно как "атака 51%", поскольку для осуществления такой атаки злоумышленникам потребуется контролировать **более 50%** вычислительной мощности сети.



Blockchain Center

Атака 51%

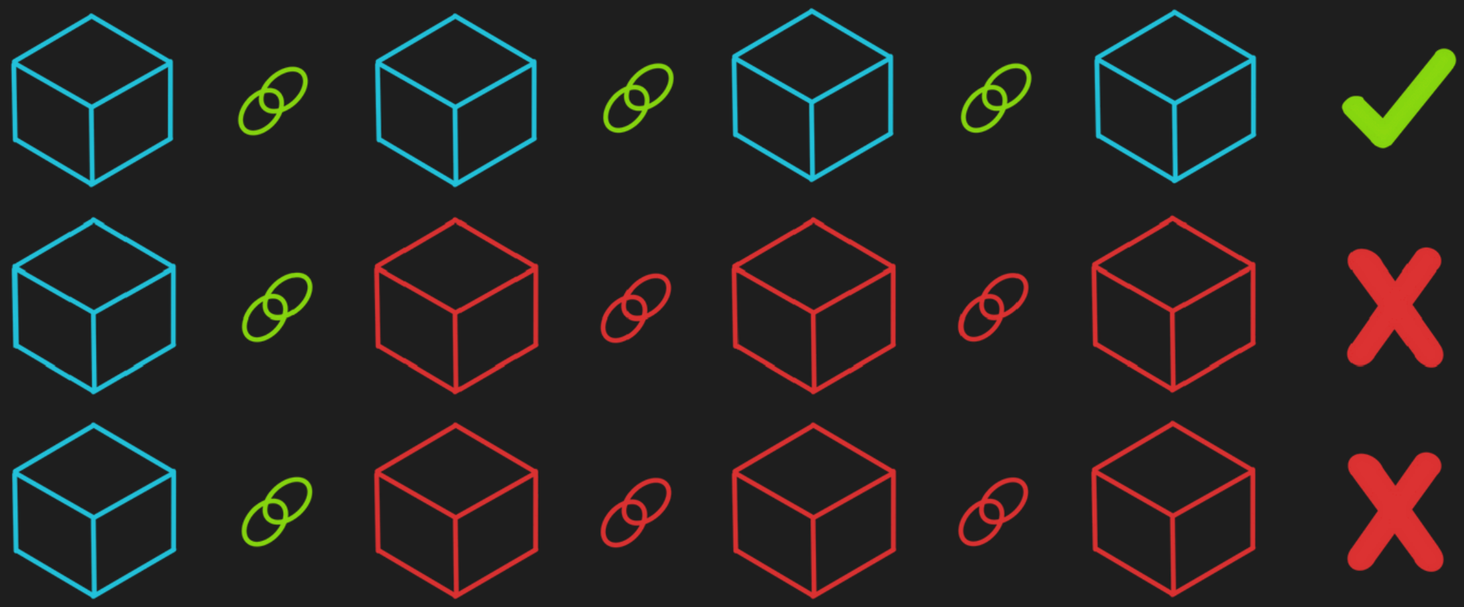
Если бы злоумышленники смогли взять под контроль большинство компьютеров в сети блокчейн, они потенциально могли бы манипулировать сетью различными способами. Это известно как "атака 51%", поскольку для осуществления такой атаки злоумышленникам потребуется контролировать **более 50%** вычислительной мощности сети.



Blockchain Center

Атака 51%

Если бы злоумышленники смогли взять под контроль большинство компьютеров в сети блокчейн, они потенциально могли бы манипулировать сетью различными способами. Это известно как "атака 51%", поскольку для осуществления такой атаки злоумышленникам потребуется контролировать **более 50%** вычислительной мощности сети.



Blockchain Center

Что такое криптография?

Blockchain
Center

Что такое криптография?

Криптография - это практика создания и использования кодов и шифров для защиты информации от несанкционированного доступа или манипуляций.

Blockchain Center

Что такое криптография?

Криптография - это практика создания и использования кодов и шифров для защиты информации от несанкционированного доступа или манипуляций.

Она предполагает использование математических алгоритмов и методов для шифрования и дешифрования данных, гарантируя, что доступ к ним или их изменение могут получить только те, у кого есть соответствующий ключ или знания.

Blockchain Center

Что такое криптография?

Криптография - это практика создания и использования кодов и шифров для защиты информации от несанкционированного доступа или манипуляций.

Криптография - это практика, которая имеет долгую историю, восходящую к древним цивилизациям. Она предполагает использование кодов и шифров для защиты информации от несанкционированного доступа или манипуляций.

Она предполагает использование математических алгоритмов и методов для шифрования и дешифрования данных, гарантируя, что доступ к ним или их изменение могут получить только те, у кого есть соответствующий ключ или знания.

Blockchain Center

Что такое криптография?

Криптография - это практика создания и использования кодов и шифров для защиты информации от несанкционированного доступа или манипуляций.

Криптография - это практика, которая имеет долгую историю, восходящую к древним цивилизациям. Она предполагает использование кодов и шифров для защиты информации от несанкционированного доступа или манипуляций.

Она предполагает использование математических алгоритмов и методов для шифрования и дешифрования данных, гарантируя, что доступ к ним или их изменение могут получить только те, у кого есть соответствующий ключ или знания.

На протяжении всей истории криптография использовалась для многих целей, таких как обеспечение безопасности военной и дипломатической связи, проверка финансовых операций и сохранение конфиденциальности в электронной коммуникации.

Blockchain Center

Пример криптографии в истории

Blockchain
Center

Пример криптографии в истории

- Шифр Цезаря использовался Юлием Цезарем для шифрования своих сообщений. Он отправлял сообщения своим чиновникам с помощью этого шифра, чтобы защитить передаваемое от перехвата и понимания врагами.

Blockchain Center

Пример криптографии в истории

- Шифр Цезаря использовался Юлием Цезарем для шифрования своих сообщений. Он отправлял сообщения своим чиновникам с помощью этого шифра, чтобы защитить передаваемое от перехвата и понимания врагами.

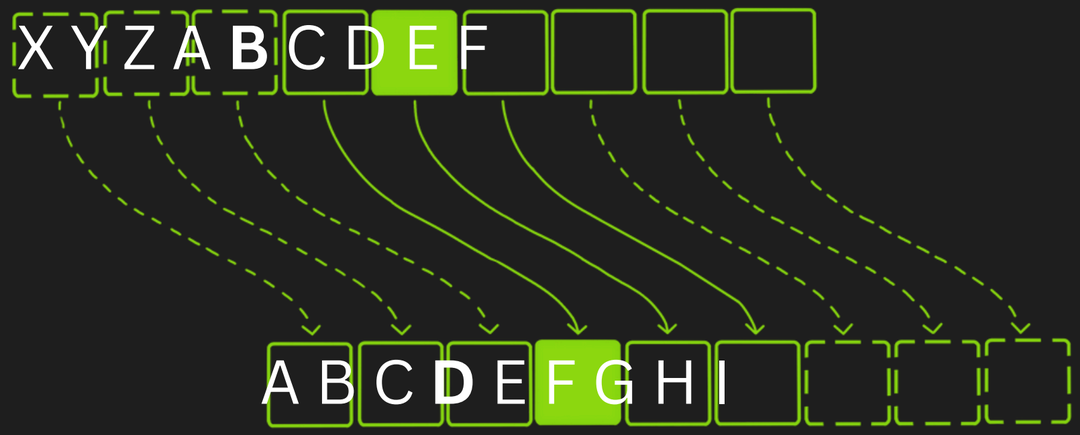
- Чтобы использовать шифр Цезаря, Цезарь выбирал значение сдвига (например, 3), а затем сдвигал каждую букву в сообщении на это количество позиций. Например, если значение сдвига было равно 3, то буква "A" заменялась на "D", "B" - на "E" и так далее.

Blockchain Center

Пример криптографии в истории

- Шифр Цезаря использовался Юлием Цезарем для шифрования своих сообщений. Он отправлял сообщения своим чиновникам с помощью этого шифра, чтобы защитить передаваемое от перехвата и понимания врагами.

- Чтобы использовать шифр Цезаря, Цезарь выбирал значение сдвига (например, 3), а затем сдвигал каждую букву в сообщении на это количество позиций. Например, если значение сдвига было равно 3, то буква "A" заменялась на "D", "B" - на "E" и так далее.



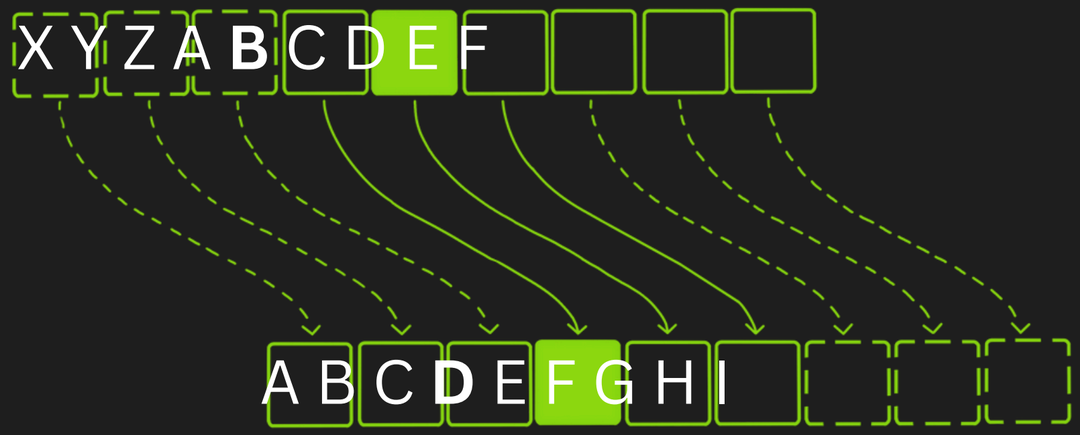
Blockchain Center

Пример криптографии в истории

- Шифр Цезаря использовался Юлием Цезарем для кодирования своих сообщений. Он отправлял сообщения своим чиновникам с помощью этого шифра, чтобы защитить передаваемое от перехвата и понимания врагами.

- Чтобы использовать шифр Цезаря, Цезарь выбирал значение сдвига (например, 3), а затем сдвигал каждую букву в сообщении на это количество позиций. Например, если значение сдвига было равно 3, то буква "A" заменялась на "D", "B" - на "E" и так далее.

- Чтобы расшифровать сообщение, получатель сдвигает каждую букву в зашифрованном сообщении назад на одинаковое количество позиций.



Blockchain Center

Криптография в блокчейне и ее применение

Blockchain Center

Криптография в блокчейне и ее применение

Криптография является фундаментальным аспектом технологии блокчейн и используется для обеспечения безопасности и защиты данных, хранящихся в блокчейне.

Blockchain Center

Криптография в блокчейне и ее применение

Криптография является фундаментальным аспектом технологии блокчейн и используется для обеспечения безопасности и защиты данных, хранящихся в блокчейне.

Она предполагает применение математических алгоритмов и методов для кодирования и декодирования данных, гарантируя, что доступ к ним или их изменение могут получить только те, кто обладает необходимым ключом или знаниями.

Blockchain Center

Криптография в блокчейне и ее применение

Криптография является фундаментальным аспектом технологии блокчейн и используется для обеспечения безопасности и защиты данных, хранящихся в блокчейне.

Она предполагает применение математических алгоритмов и методов для кодирования и декодирования данных, гарантируя, что доступ к ним или их изменение могут получить только те, кто обладает необходимым ключом или знаниями.

Криптография выполняет ряд важнейших функций в работе блокчейна, включая проверку подлинности и целостности транзакций, защиту данных от несанкционированного доступа и сохранение конфиденциальности пользователей.

Blockchain Center

Криптографические методы используемые в блокчейне

Существует несколько криптографических методов, используемых в технологии блокчейн для обеспечения безопасности и защиты данных, хранящихся в блокчейне. Некоторые из наиболее часто используемых методов включают:

Blockchain Center

Криптографические методы используемые в блокчейне

Существует несколько криптографических методов, используемых в технологии блокчейн для обеспечения безопасности и защиты данных, хранящихся в блокчейне. Некоторые из наиболее часто используемых методов включают:

Хеширование
Это предполагает использование математической функции для преобразования данных в строку символов фиксированной длины, известную как "хэш". Этот хэш можно использовать для проверки целостности данных, поскольку любое изменение данных приведет к созданию другого хэша.

Blockchain Center

Криптографические методы используемые в блокчейне

Существует несколько криптографических методов, используемых в технологии блокчейн для обеспечения безопасности и защиты данных, хранящихся в блокчейне. Некоторые из наиболее часто используемых методов включают:

Хеширование

Это предполагает использование математической функции для преобразования данных в строку символов фиксированной длины, известную как "хэш". Этот хэш можно использовать для проверки целостности данных, поскольку любое изменение данных приведет к созданию другого хэша.

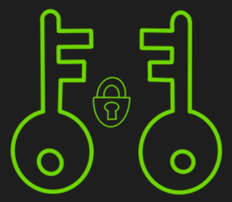
Цифровые подписи

Они используются для проверки подлинности транзакций в блокчейне и гарантируют, что они не могут быть изменены. Цифровые подписи используют пару ключей (открытый ключ и закрытый ключ) для создания уникальной подписи, которая может быть использована для проверки личности отправителя.

Blockchain Center

Криптографические методы используемые в блокчейне

Существует несколько криптографических методов, используемых в технологии блокчейн для обеспечения безопасности и защиты данных, хранящихся в блокчейне. Некоторые из наиболее часто используемых методов включают:

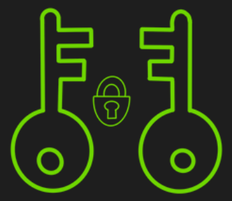


Криптография с открытым ключом
Это тип криптографии, который использует пару ключей (открытый ключ и закрытый ключ) для защиты связи. Открытый ключ используется для шифрования данных, а закрытый ключ - для их расшифровки.

Blockchain Center

Криптографические методы используемые в блокчейне

Существует несколько криптографических методов, используемых в технологии блокчейн для обеспечения безопасности и защиты данных, хранящихся в блокчейне. Некоторые из наиболее часто используемых методов включают:



Криптография с открытым ключом
Это тип криптографии, который использует пару ключей (открытый ключ и закрытый ключ) для защиты связи. Открытый ключ используется для шифрования данных, а закрытый ключ - для их расшифровки.

Криптография с симметричным ключом
Это тип криптографии, в котором используется один ключ для шифрования и расшифровки данных. Ключ должен храниться в секрете, чтобы обеспечить безопасность данных.

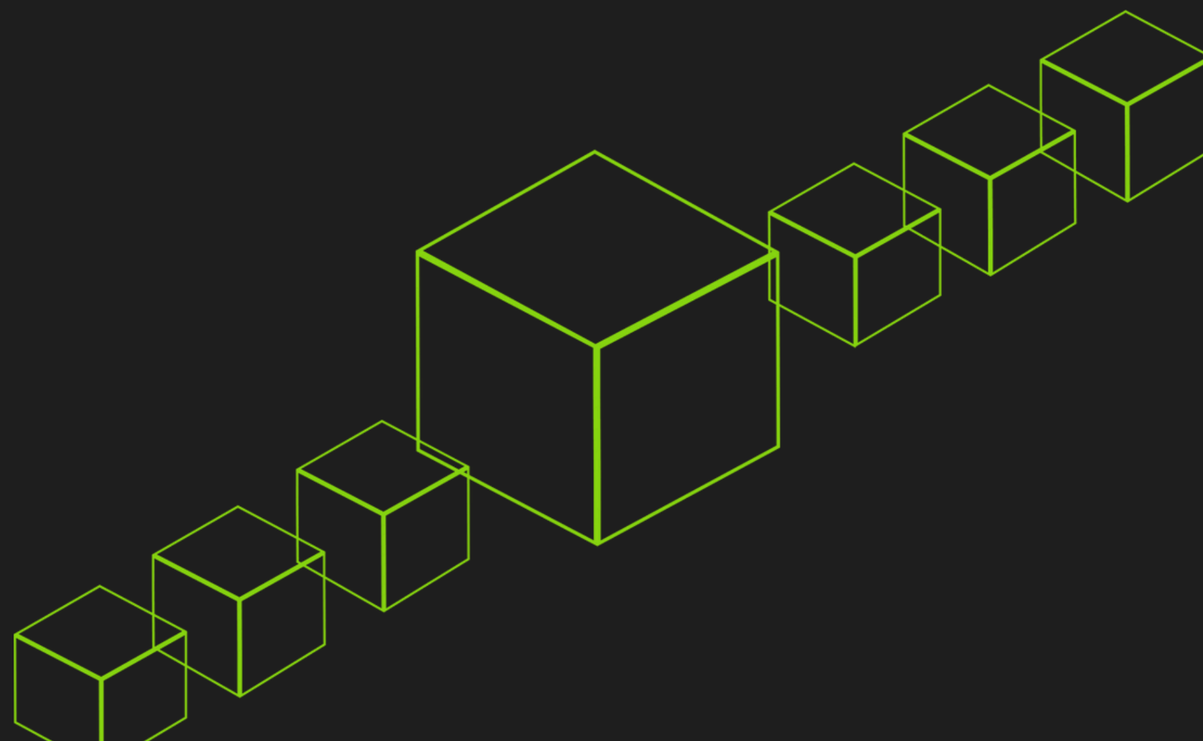
Blockchain Center

Модуль 2 - Симметричное и Ассиметричное шифрование

Blockchain Center

Симметричное и Ассиметричное шифрование

- Криптографические термины
- Симметричное шифрование
- Плюсы симметричного шифрования
- Минусы симметричного шифрования
- Асимметричное шифрование
- Плюсы асимметричного шифрования
- Минусы асимметричного шифрования



Blockchain Center

Термины криптографии

Blockchain
Center

Термины криптографии

Шифр
это метод кодирования сообщения для сохранения его конфиденциальности.
Он предполагает превращение сообщения в секретный код (шифротекст) и его обратное декодирование в исходное сообщение по определенным правилам. Существуют различные типы шифров, и они используются для защиты сообщений в различных контекстах, например, на компьютерах или при хранении информации.

Blockchain Center

Термины криптографии

Шифр
это метод кодирования сообщения для сохранения его конфиденциальности.
Он предполагает превращение сообщения в секретный код (шифротекст) и его обратное декодирование в исходное сообщение по определенным правилам. Существуют различные типы шифров, и они используются для защиты сообщений в различных контекстах, например, на компьютерах или при хранении информации.

Секретный ключ
это часть информации, которая используется вместе с шифром для шифрования и дешифрования сообщения. Он является важной частью процесса шифрования и используется для скремблирования и дешифрования сообщения таким образом, что любому, у кого нет ключа, трудно его изменить.

Blockchain Center

Термины криптографии

Шифр
это метод кодирования сообщения для сохранения его конфиденциальности.
Он предполагает превращение сообщения в секретный код (шифротекст) и его обратное декодирование в исходное сообщение по определенным правилам. Существуют различные типы шифров, и они используются для защиты сообщений в различных контекстах, например, на компьютерах или при хранении информации.

Секретный ключ
это часть информации, которая используется вместе с шифром для шифрования и дешифрования сообщения. Он является важной частью процесса шифрования и используется для скремблирования и дешифрования сообщения таким образом, что любому, у кого нет ключа, трудно его изменить.

Открытый текст
Под открытым текстом понимается исходное, незашифрованное сообщение или данные. Его называют "открытым текстом", поскольку он находится в читаемой, незашифрованной форме, которая может быть легко понята человеком.

Blockchain Center

Термины криптографии

Шифротекст
это зашифрованная форма сообщения. Это результат применения шифра, или алгоритма шифрования, к открытому тексту. Шифротекст выглядит как случайная строка символов, и его трудно понять без секретного ключа, который использовался для его шифрования.

Blockchain Center

Термины криптографии

Шифротекст
это зашифрованная форма сообщения. Это результат применения шифра, или алгоритма шифрования, к открытому тексту. Шифротекст выглядит как случайная строка символов, и его трудно понять без секретного ключа, который использовался для его шифрования.

Шифрование
Шифрование - это процесс преобразования открытого текста в зашифрованный с помощью шифра и секретного ключа. Оно используется для обеспечения конфиденциальности сообщения и защиты его от перехвата и прочтения неавторизованными лицами.

Blockchain Center

Термины криптографии

Шифротекст

это зашифрованная форма сообщения. Это результат применения шифра, или алгоритма шифрования, к открытому тексту. Шифротекст выглядит как случайная строка символов, и его трудно понять без секретного ключа, который использовался для его шифрования.

Шифрование

Шифрование - это процесс преобразования открытого текста в зашифрованный с помощью шифра и секретного ключа. Оно используется для обеспечения конфиденциальности сообщения и защиты его от перехвата и прочтения неавторизованными лицами.

Дешифрование

Дешифрование - это процесс преобразования шифротекста обратно в исходный открытый текст с помощью шифра и секретного ключа. Это обратный процесс шифрования, который используется для раскрытия исходного сообщения, которое было зашифровано.

Blockchain Center

Симметричное шифрование

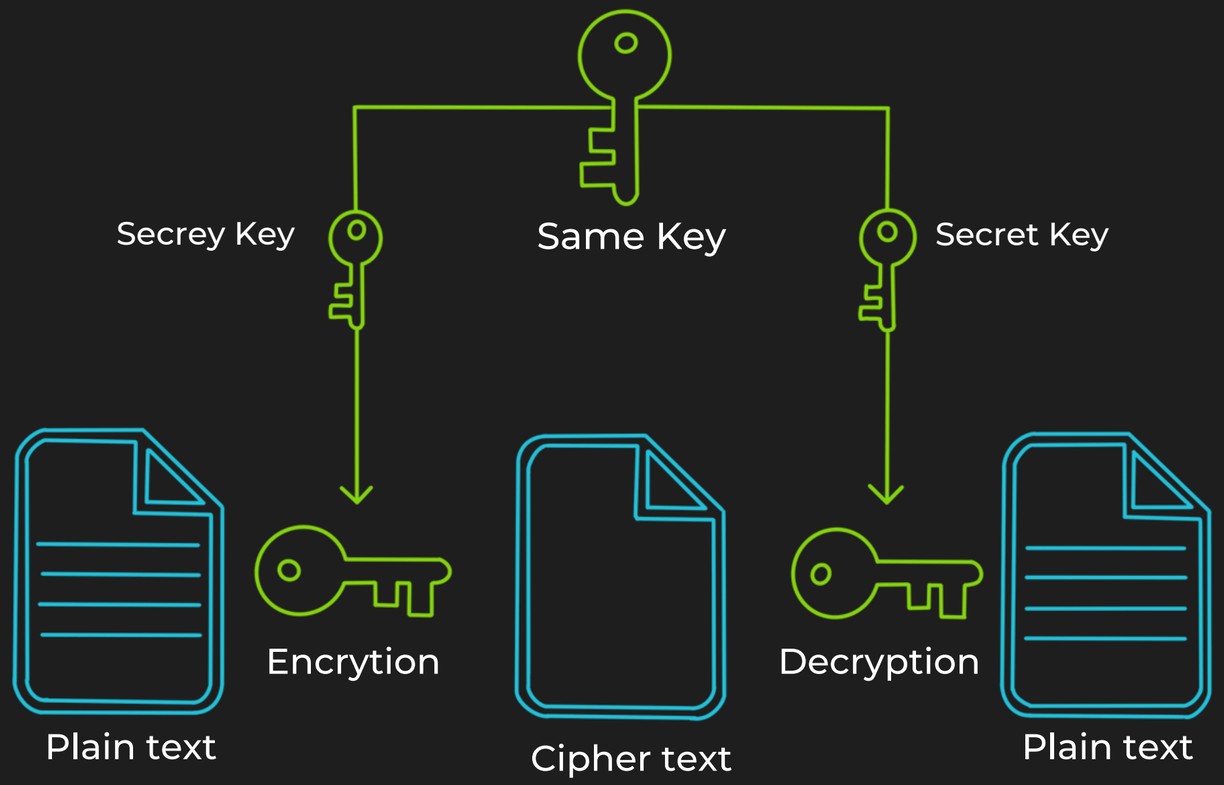
Симметричное шифрование

Симметричное шифрование - это тип шифрования, который использует один и тот же секретный ключ для процессов шифрования и расшифровки.

Blockchain
Center

Симметричное шифрование

Симметричное шифрование - это тип шифрования, который использует один и тот же секретный ключ для процессов шифрования и расшифровки.



Blockchain Center

Симметричное шифрование:

Шифр Цезаря

Blockchain
Center

Симметричное шифрование:

Шифр Цезаря

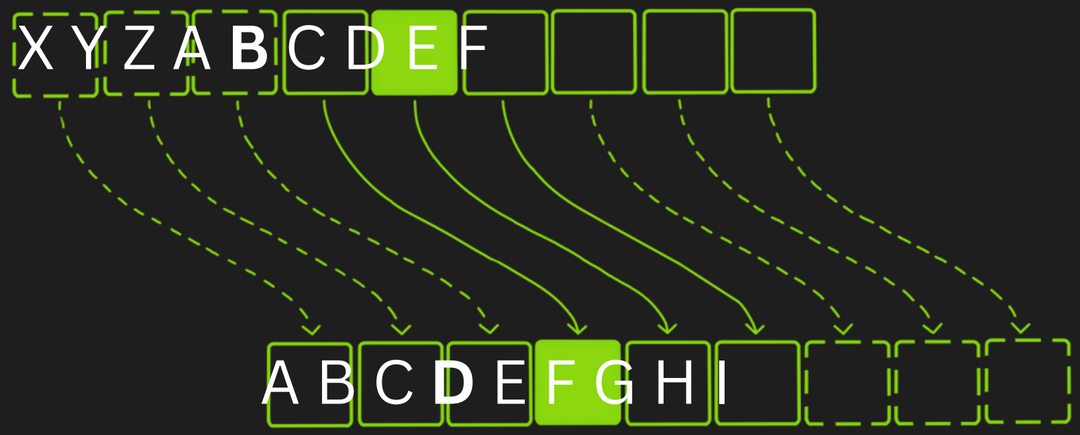
Шифр Цезаря, также известный как шифр со сдвигом, - это простой шифр с подстановкой, который заменяет каждую букву в открытом тексте на букву, расположенную на фиксированное число позиций ниже по алфавиту. Например, при сдвиге на 3 буквы A заменяются на D, B - на E и так далее. Шифр Цезаря - это моноалфавитный шифр, то есть каждая буква в открытом тексте всегда заменяется одной и той же буквой в шифрованном тексте.

Blockchain Center

Симметричное шифрование:

Шифр Цезаря

Шифр Цезаря, также известный как шифр со сдвигом, - это простой шифр с подстановкой, который заменяет каждую букву в открытом тексте на букву, расположенную на фиксированное число позиций ниже по алфавиту. Например, при сдвиге на 3 буквы A заменяются на D, B - на E и так далее. Шифр Цезаря - это моноалфавитный шифр, то есть каждая буква в открытом тексте всегда заменяется одной и той же буквой в шифрованном тексте.



Blockchain Center

Пример симметричного шифрования:

Шифр Цезаря

Blockchain
Center

Пример симметричного шифрования:

Шифр Цезаря

Алиса и Боб могут договориться использовать секретный ключ "3" для шифрования и дешифрования своих сообщений с помощью шифра Цезаря. Алиса может использовать этот секретный ключ вместе с шифром Цезаря, чтобы зашифровать сообщение (Привет, Боб!) и отправить его Бобу. Затем Боб может использовать тот же секретный ключ и шифр, чтобы расшифровать сообщение и прочитать его исходное содержание.

Blockchain Center

Пример симметричного шифрования:
Шифр Цезаря

- Секретный ключ: "3"

Blockchain
Center

Пример симметричного шифрования:
Шифр Цезаря

- Секретный ключ: "3"
- Шифр: "шифр Цезаря".

Blockchain
Center

Пример симметричного шифрования:

Шифр Цезаря

- Секретный ключ: "3"
- Шифр: "шифр Цезаря".
- Открытое сообщение: "Hello, Bob!"

Blockchain
Center

Пример симметричного шифрования:

Шифр Цезаря

- Секретный ключ: "3"
- Шифр: "шифр Цезаря".
- Открытое сообщение: "Hello, Bob!"
- Шифротекст: "Khoor, Ere!"

Blockchain
Center

Пример симметричного шифрования:

Шифр Цезаря

- Секретный ключ: "3"
- Шифр: "шифр Цезаря".
- Открытое сообщение: "Hello, Bob!"
- Шифротекст: "Khoor, Ere!"

- Шифрование: Алиса использует секретный ключ "3" и шифр "Шифр Цезаря" для шифрования сообщения "Hello, Bob!" в шифротекст "Khoor, Ere!".

Blockchain Center

Пример симметричного шифрования:

Шифр Цезаря

- Секретный ключ: "3"
- Шифр: "шифр Цезаря".
- Открытое сообщение: "Hello, Bob!"
- Шифротекст: "Khoor, Ere!"

- Шифрование: Алиса использует секретный ключ "3" и шифр "Шифр Цезаря" для шифрования сообщения "Hello, Bob!" в шифротекст "Khoor, Ere!". Дешифрование: Боб
- использует секретный ключ "3" и шифр "шифр Цезаря" для расшифровки шифротекста "Khoor, Ere!" и чтения исходного сообщения "Hello, Bob!".

Blockchain Center

Пример симметричного шифрования:

Шифр Цезаря

- Секретный ключ: "3"
- Шифр: "шифр Цезаря".
- Открытое сообщение: "Hello, Bob!"
- Шифротекст: "Khoor, Ere!"

- Шифрование: Алиса использует секретный ключ "3" и шифр "Шифр Цезаря" для шифрования сообщения "Hello, Bob!" в шифротекст "Khoor, Ere!". Дешифрование: Боб
- использует секретный ключ "3" и шифр "шифр Цезаря" для расшифровки шифротекста "Khoor, Ere!" и чтения исходного сообщения "Hello, Bob!".

Примечание: Шифр Цезаря является очень слабым алгоритмом шифрования и может быть легко взломан криптоаналитиком. Он использовался в основном Юлием Цезарем для общения со своими генералами и не рекомендуется для использования в современной криптографии

Blockchain Center

Плюсы симметричного шифрования

Blockchain
Center

Плюсы симметричного шифрования

Симметричное шифрование - это тип шифрования, который использует один и тот же секретный ключ для процессов шифрования и дешифрования.

Blockchain Center

Плюсы симметричного шифрования

Симметричное шифрование - это тип шифрования, который использует один и тот же секретный ключ для процессов шифрования и дешифрования.

Оно обычно быстрее, чем другие типы шифрования, такие как асимметричное шифрование.

Blockchain Center

Плюсы симметричного шифрования

Симметричное шифрование - это тип шифрования, который использует один и тот же секретный ключ для процессов шифрования и дешифрования.

Оно обычно быстрее, чем другие типы шифрования, такие как асимметричное шифрование.

Оно хорошо подходит для шифрования больших объемов данных, таких как файлы или целые дисковые накопители.

Blockchain Center

Плюсы симметричного шифрования

Симметричное шифрование - это тип шифрования, который использует один и тот же секретный ключ для процессов шифрования и дешифрования.

Оно обычно быстрее, чем другие типы шифрования, такие как асимметричное шифрование.

Оно хорошо подходит для шифрования больших объемов данных, таких как файлы или целые дисковые накопители.

Его легко реализовать, но он требует надежного обмена ключами между отправителем и получателем.

Blockchain Center

Плюсы симметричного шифрования

Симметричное шифрование - это тип шифрования, который использует один и тот же секретный ключ для процессов шифрования и дешифрования.

Оно обычно быстрее, чем другие типы шифрования, такие как асимметричное шифрование.

Оно хорошо подходит для шифрования больших объемов данных, таких как файлы или целые дисковые накопители.

Его легко реализовать, но он требует надежного обмена ключами между отправителем и получателем.

Оно может быть очень надежным, если секретный ключ хранится в безопасности, но оно уязвимо для атак, если ключ скомпрометирован или украден.

Blockchain Center

Минусы симметричного шифрования

Blockchain
Center

Минусы симметричного шифрования

Симметричное шифрование требует безопасного метода обмена секретным ключом между отправителем и получателем. Если ключ перехвачен или скомпрометирован в процессе обмена, шифрование может быть легко нарушено.

Blockchain Center

Минусы симметричного шифрования

Симметричное шифрование требует безопасного метода обмена секретным ключом между отправителем и получателем. Если ключ перехвачен или скомпрометирован в процессе обмена, шифрование может быть легко нарушено.

Симметричное шифрование уязвимо для атак, таких как «человек посередине», которые могут поставить под угрозу безопасность шифрования.

Blockchain Center

Минусы симметричного шифрования

Симметричное шифрование требует безопасного метода обмена секретным ключом между отправителем и получателем. Если ключ перехвачен или скомпрометирован в процессе обмена, шифрование может быть легко нарушено.

Симметричное шифрование уязвимо для атак, таких как «человек посередине», которые могут поставить под угрозу безопасность шифрования.

Каждая сторона должна сгенерировать новый общий ключ для связи. Это затрудняет обращение с обоими этими ключами и их защиту.

Blockchain Center

Асимметричное шифрование - криптография с открытым ключом

Blockchain Center

Асимметричное шифрование - криптография с открытым ключом

Асимметричное шифрование, или шифрование с открытым ключом, предполагает использование двух различных ключей: открытого и закрытого.

Blockchain Center

Асимметричное шифрование - криптография с открытым ключом

Асимметричное шифрование, или шифрование с открытым ключом, предполагает использование двух различных ключей: открытого и закрытого.

Открытый ключ используется для шифрования данных, а закрытый - для их расшифровки. Это означает, что только владелец закрытого ключа может расшифровать сообщение, зашифрованное соответствующим открытым ключом.

Blockchain Center

Асимметричное шифрование - криптография с открытым ключом

Асимметричное шифрование, или шифрование с открытым ключом, предполагает использование двух различных ключей: открытого и закрытого.

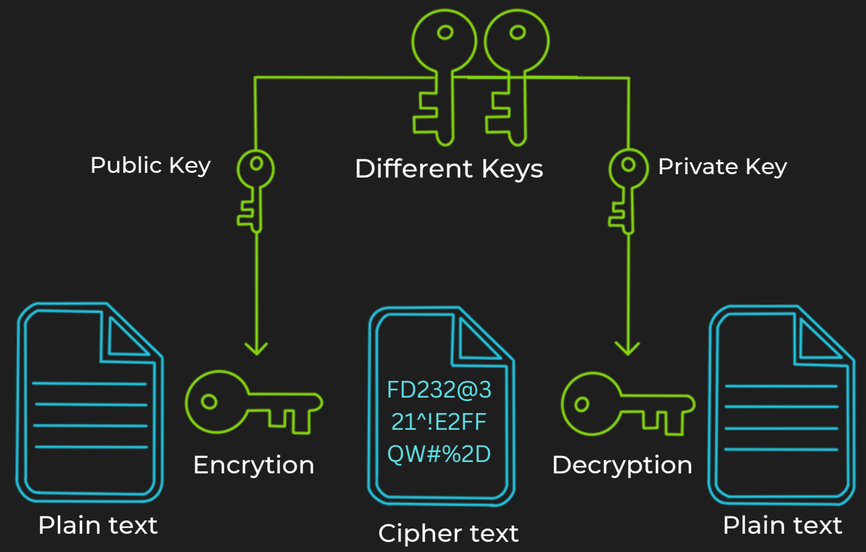
Открытый ключ используется для шифрования данных, а закрытый - для их расшифровки. Это означает, что только владелец закрытого ключа может расшифровать сообщение, зашифрованное соответствующим открытым ключом.

Асимметричное шифрование используется для безопасной связи и, как правило, является более медленным и требует больших вычислительных затрат, чем симметричное шифрование.

Blockchain Center

Асимметричное шифрование - криптография с открытым ключом

Асимметричное шифрование, или шифрование с открытым ключом, предполагает использование двух различных ключей: открытого и закрытого.



Открытый ключ используется для шифрования данных, а закрытый - для их расшифровки. Это означает, что только владелец закрытого ключа может расшифровать сообщение, зашифрованное соответствующим открытым ключом.

Асимметричное шифрование используется для безопасной связи и, как правило, является более медленным и требует больших вычислительных затрат, чем симметричное шифрование.

Blockchain Center

Плюсы асимметричного шифрования

- Асимметричное шифрование обеспечивает безопасную связь без необходимости предварительного обмена секретным ключом.

Blockchain Center

Плюсы асимметричного шифрования

- Асимметричное шифрование обеспечивает безопасную связь без необходимости предварительного обмена секретным ключом.
- Устойчив к атакам, направленным на перехват и изменение связи между отправителем и получателем.

Blockchain Center

Плюсы асимметричного шифрования

- Асимметричное шифрование обеспечивает безопасную связь без необходимости предварительного обмена секретным ключом.
- Устойчив к атакам, направленным на перехват и изменение связи между отправителем и получателем.
- Может использоваться для проверки подлинности электронных документов с помощью цифровых подписей.

Blockchain Center

Плюсы асимметричного шифрования

- Асимметричное шифрование обеспечивает безопасную связь без необходимости предварительного обмена секретным ключом.
- Устойчив к атакам, направленным на перехват и изменение связи между отправителем и получателем.
- Может использоваться для проверки подлинности электронных документов с помощью цифровых подписей.
- Шифрование широко используется и поддерживается, многие приложения и протоколы полагаются на него для обеспечения безопасности связи.

Плюсы асимметричного шифрования

- Асимметричное шифрование обеспечивает безопасную связь без необходимости предварительного обмена секретным ключом.
- Устойчив к атакам, направленным на перехват и изменение связи между отправителем и получателем.
- Может использоваться для проверки подлинности электронных документов с помощью цифровых подписей.
- Шифрование широко используется и поддерживается, многие приложения и протоколы полагаются на него для обеспечения безопасности связи.
- Асимметричное шифрование обычно медленнее и требует больших вычислительных затрат, чем симметричное шифрование.

Минусы асимметричного шифрования

- Асимметричное шифрование может не подойти для расшифровки больших объемов данных из-за более низкой скорости обработки по сравнению с симметричным шифрованием.

Blockchain Center

Минусы асимметричного шифрования

- Асимметричное шифрование может не подойти для расшифровки больших объемов данных из-за более низкой скорости обработки по сравнению с симметричным шифрованием.
- Потеря закрытого ключа может привести к невозможности расшифровки сообщений.

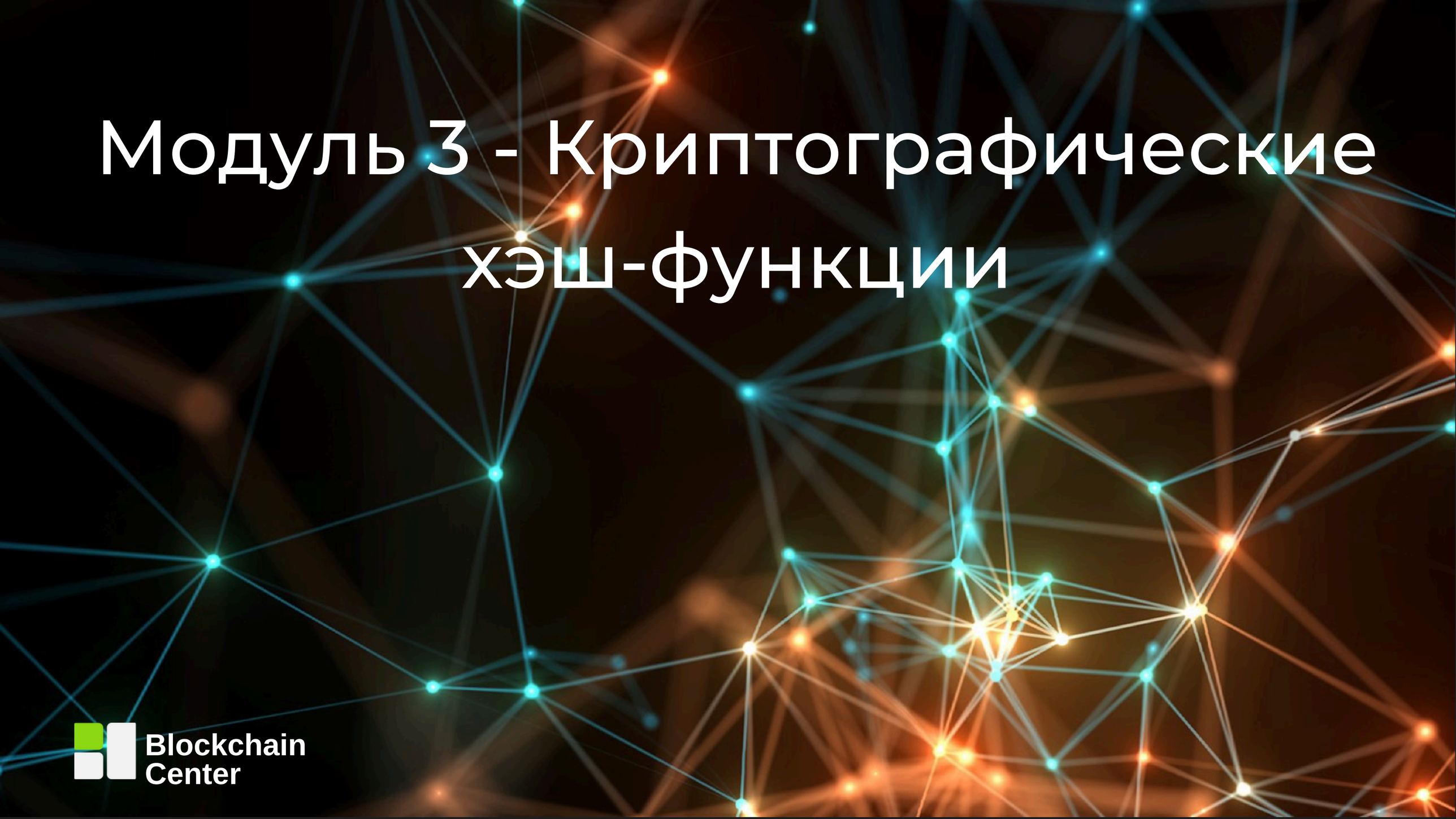
Blockchain Center

Минусы асимметричного шифрования

- Асимметричное шифрование может не подойти для расшифровки больших объемов данных из-за более низкой скорости обработки по сравнению с симметричным шифрованием.
- Потеря закрытого ключа может привести к невозможности расшифровки сообщений.
- Если закрытый ключ скомпрометирован, злоумышленник может получить доступ к зашифрованному сообщению.

Blockchain Center

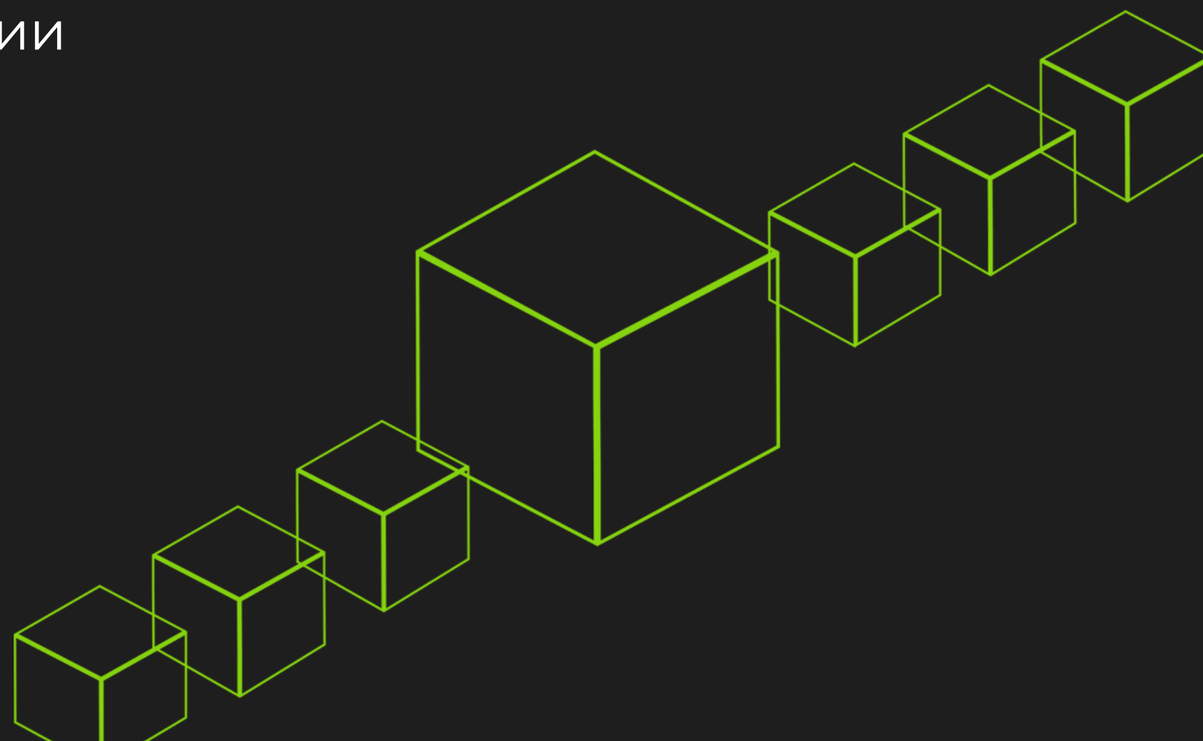
Модуль 3 - Криптографические хэш-функции



Blockchain Center

Криптографические хэш-функции

- Что такое криптографические хэш-функции?
- Свойства криптографических хэш-функции



Blockchain Center

Что такое криптографические хэш-функции?

Blockchain
Center

Что такое криптографические хэш-функции?

- Криптографические хэш-функции - это математические функции, которые принимают входные данные (или "сообщение") и возвращают строку символов фиксированного размера, уникальную для входных данных. Двумя примерами криптографических хэш-функций являются MD5 и SHA-256. SHA-256 обычно считается более безопасной, чем MD5, и широко используется в различных приложениях, включая блокчейн.

Blockchain Center

Что такое криптографические хэш-функции?

- Криптографические хэш-функции - это математические функции, которые принимают входные данные (или "сообщение") и возвращают строку символов фиксированного размера, уникальную для входных данных. Двумя примерами криптографических хэш-функций являются MD5 и SHA-256. SHA-256 обычно считается более безопасной, чем MD5, и широко используется в различных приложениях, включая блокчейн.

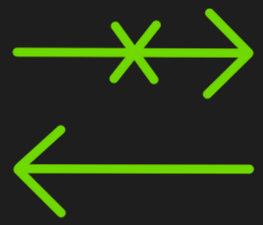
- С помощью SHA-256 можно хэшировать данные, изображения, и видео. Криптографические хэш-функции можно применять к любому типу данных, независимо от их формата или содержания. Например, вы можете хэшировать текстовый файл, файл изображения, документ PDF или видеофайл с помощью SHA-256. Хеш-функция принимает данные на вход и производит выходной результат фиксированного размера (256 бит), уникальный для входных данных.

Blockchain Center

Свойства криптографических хэш-функций

Blockchain Center

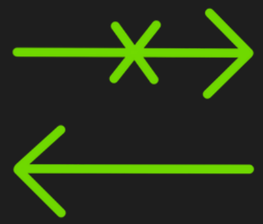
Свойства криптографических хэш-функций



Односторонний
Вычислительно невыполнимо определить исходный ввод по хэш-значению. Например, трудно определить исходное сообщение или данные по хэш-значению.

Blockchain Center

Свойства криптографических хэш-функций

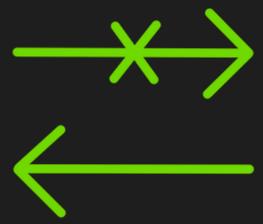


Односторонний
Вычислительно невыполнимо определить исходный ввод по хэш-значению. Например, трудно определить исходное сообщение или данные по хэш-значению.

Детерминированный
Один и тот же ввод всегда будет давать один и тот же вывод. Например, если хэшировать сообщение "Hello, world!" несколько раз, то всегда будет получаться одно и то же хэш-значение.

Blockchain Center

Свойства криптографических хэш-функций



Односторонний

Вычислительно невыполнимо определить исходный ввод по хэш-значению. Например, трудно определить исходное сообщение или данные по хэш-значению.

Детерминированный

Один и тот же вход всегда будет давать один и тот же выход. Например, если хэшировать сообщение "Hello, world!" несколько раз, то всегда будет получаться одно и то же хэш-значение.

Быстрый

Генерация хэш-значения из входных данных должна быть эффективной. Например, для генерации хэш-значения сообщения или данных должно требоваться всего несколько миллисекунд.

Blockchain Center

Свойства криптографических хэш-функций

Устойчивый к коллизиям

Должно быть трудно найти два входа, которые дают одинаковый выход. Это гарантирует, что каждый входной сигнал уникален и отличим от других.

Blockchain Center

Свойства криптографических хэш-функций

Устойчивый к коллизиям

Должно быть трудно найти два входа, которые дают одинаковый выход. Это гарантирует, что каждый входной сигнал уникален и отличим от других.

Лавинный эффект

Небольшое изменение на входе должно приводить к значительному изменению на выходе. Например, изменение одной буквы во фразе "Hello, world!" должно дать совсем другое хэш-значение.

Blockchain Center

Ссылки

https://testnet.bscscan.com/

https://chainstack.com/how-do-ethereum-and-solana-generate-public-and-private-keys/

Blockchain Center