**Автономная некоммерческая общеобразовательная организация "Физтех-лицей"
(АНОО «Физтех-лицей» им. П.Л. Капицы)**

XX научно-практическая конференция

«Старт в инновации»

Криптовалюта в современном мире

Выполнили:
Бассэ. Владислав. 10-3-2
Руководитель:
Телешева. Наталия. Сергеевна

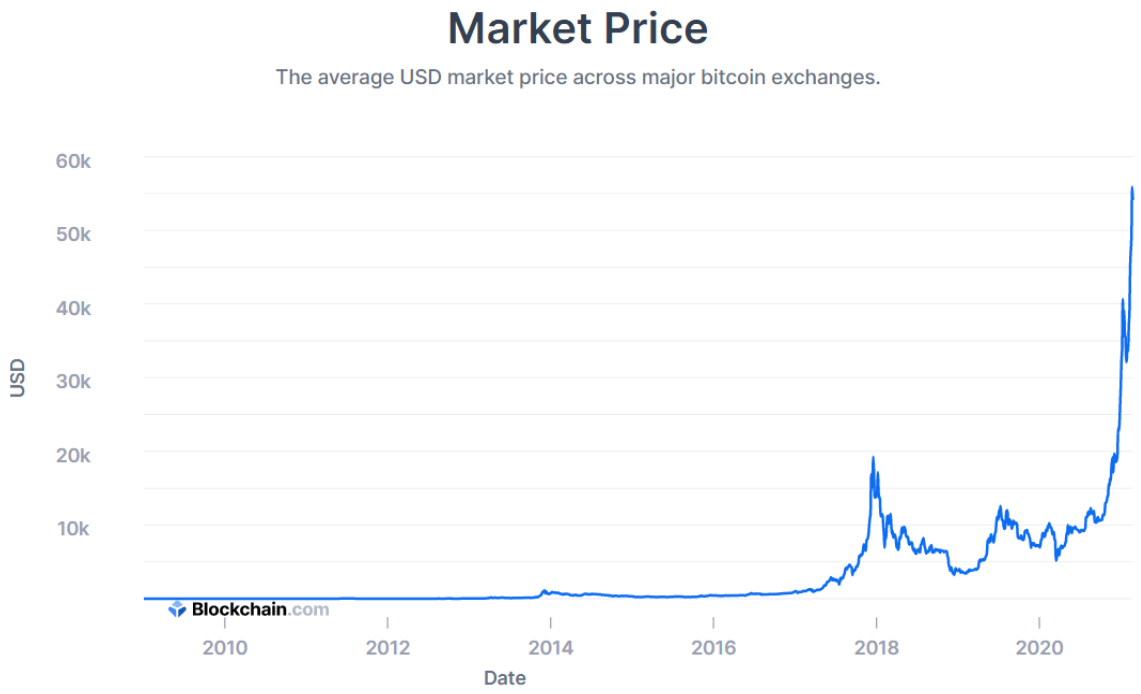
Московская область, г. Долгопрудный

2021 г.

Криптовалюта

Криптовалюта – это форма оплаты товаров и услуги в сети. Многие компании создали свои собственные валюты, часто называемыми токенами, которые обмениваются на товары или услуги предоставленные компаниями. Токены можно представить как фишки казино. Вы можете обменять настоящие деньги на криптовалюту, чтобы получить доступ к предоставленным товарам и услугам. Зашифрованные токены могут попасть под раздел крипто. Обычно криптовалюта делится на два типа: альтернативная криптовалюта (Альткоины) или токены.

Альткоины обычно относятся к криптовалютам которые не являются Биткоинами. Биткоин популярная цифровая валюта, в основе которой лежат вычислительные решения сложных математических задач . Это работает отдельно от центральных банков и казначейства.



Список некоторых альткоинов:

- Перкоин
- Лайткоин
- Доужкоин
- Ороракоин
- Нэймкоин

На самом деле, слово альткоин означает альтернатив Биткоину. Нэймкоин считается первым альткоином, созданный в 2011 году.

Как и Биткоин, многие криптовалюты здесь перечисленные имеют ограниченное количество коинов – чтобы усилить воспринимаемую ценность. Существует фиксированное число Биткоинов – 21 миллион, как было решено создателем Биткоина, Единственный способ чтобы получить больше, это добавить протокол который это разрешит.

Несмотря на то, что многие альткоины построены по той же структуре что и Биткоин, многие утверждают что они лучшие версии Биткоина. Некоторые коины не работают с тем же самым протоколом, которым пользуется Биткоин. Например следующий список криптовалют создали свою собственную отдельную систему и протокол:

- Эфериум
- Рипл
- Омни
- Нкст
- Уэйвс
- Каунтерпарти

ICO (Initial Coin Offering)

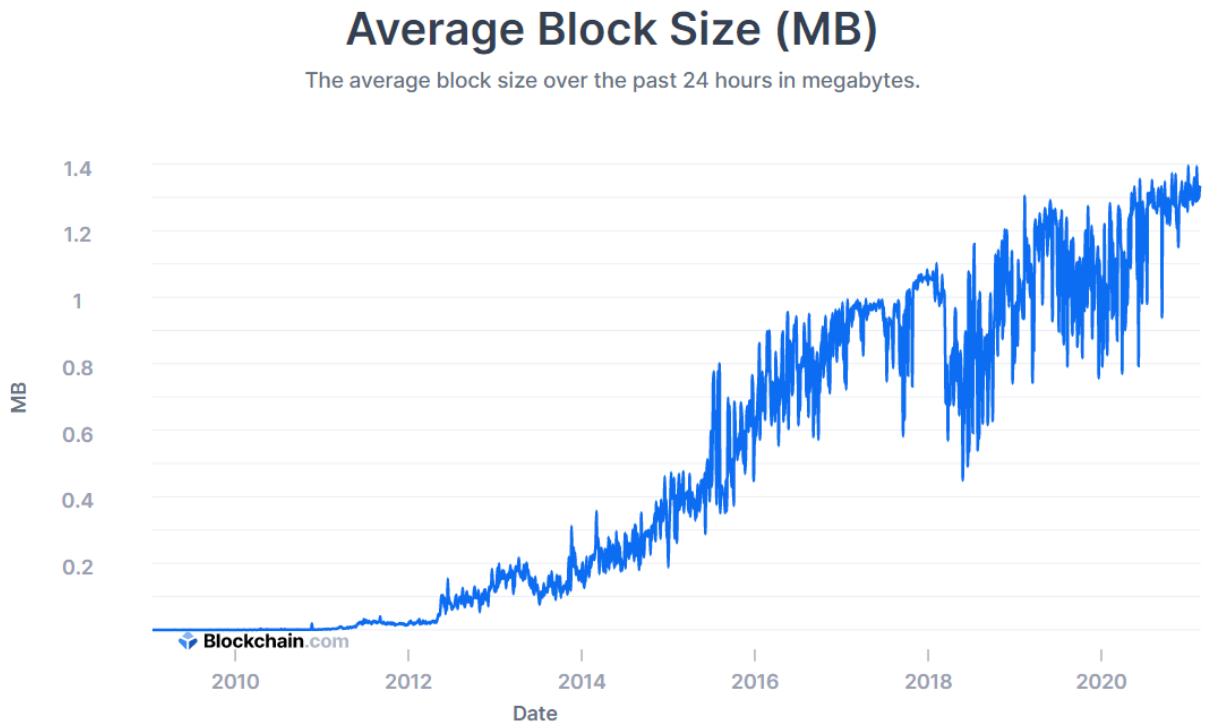
В отличие от алткоинов, токены созданы и выданы через ICO (Initial Coin Offering) или первоначальное предложение монет на русском. Они могут быть представлены как:

- Валютные токены (Биткоины)
- Токены безопасности (чтобы защитить вашу учетную запись)
- Утилитные токены (назначенные для специфичного использования)

Они не предназначены чтоб их использовали в качестве денег, так как они используются чтоб описать функцию. Как и Американские доллары, они представляют собой валюту, но сами никакой валюты не имеют. Токены - тип шифрования, конкретно относящийся к длинным строкам цифр и букв, представляющих криптографию, используемую в транзакции, такой как денежный перевод или оплата счета. Короче говоря, токены имеют много значений. Например, и Биткоин, и Эфир (от Эфириума) считаются крипто-токенами. Все криптовалюты работают с использованием технологии, называемой блокчейн.

Блокчейн

Блокчейн - это децентрализованная технология, распространенная на многих компьютерах, которая контролирует и записывает транзакции. Многих привлекает эта технология связи с её безопасностью.



Что такое блокчейн?

Блокчейн кажется сложным, но его основная концепция на самом деле довольно проста. Блокчейн - это тип базы данных. Чтобы понять что такое блокчейн, нужно сначала понять, что такое база данных на самом деле.

База данных - это сбор информации, который хранится в компьютерной системе. Информация или данные в базах данных обычно структурируются в табличном формате, чтобы облегчить поиск и фильтрацию конкретной информации. В чем разница между тем, кто использует электронную таблицу для хранения информации, а не базу данных? Электронные таблицы предназначены для одного человека или небольшой группы людей, чтобы хранить и получать доступ к ограниченным объемам информации. В отличие от электронных таблиц, база данных предназначена для размещения значительно больших объемов информации, которые могут быть фильтрованы и обработаны значительно быстрее и легче любым количеством пользователей одновременно. Большие базы данных достигают этого, размещая данные на серверах, которые сделаны из мощных компьютеров. Эти серверы иногда могут быть построены с использованием сотен или тысяч компьютеров, чтобы иметь вычислительную мощность и емкость памяти, необходимые для одновременного доступа многих пользователей к базе

данных. Хотя электронная таблица или база данных могут быть доступны многими людьми, они часто принадлежат бизнесу и управляются назначенным лицом, которое имеет полный контроль над тем, как она работает и какие данные в ней хранятся.

Так чем же блокчейн отличается от базы данных?

Блокчейн отличается от базы данных структурой хранения. Одним из ключевых различий между типичной базой данных и блокчейном является способ структурирования данных. Блокчейн собирает информацию в группы - блоки. Блоки имеют определенные емкости хранения и, когда они заполняются, они присоединяются к ранее заполненному блоку, образуя цепочку данных, известную как “блокчейн”. Вся новая информация, которая следует за этим недавно добавленным блоком, компилируется во вновь сформированный блок, который затем также будет добавлен в цепочку после заполнения.

Proof-of-work

Доказательство работы (Proof-of-work) - это алгоритм, который защищает многие криптовалюты, включая Биткойн и Эфириум. Большинство цифровых валют имеют центрального лидера, который отслеживает каждого пользователя и сколько у него денег. Но нет такого лидера, отвечающего за криптовалюты, как Биткойн. Доказательство работы необходимо, чтобы заставить онлайн-валюту работать без компании или правительства. Более конкретно, доказательство работы (Proof-of-work) решает “проблему двойных расходов”, которую сложнее решить без руководителя. Если пользователи могут тратить свои монеты дважды, это обесценивает монеты всех остальных и делает валюту непредсказуемой и бесполезной. Двойные расходы - проблема для онлайн - транзакций, потому что цифровые действия очень легко воспроизвести, что делает тривиальным копирование и вставку файла или отправку электронной почты более чем одному человеку. Доказательство работы (Proof-of-work) делает удвоение цифровых денег очень трудным. Это и есть “доказательство” того, что кто-то сделал значительное количество вычислений.

Как работает доказательство работы (Proof-of-work)

Биткоин - это блокчейн, который представляет собой общую бухгалтерскую книгу, содержащую историю каждой Биткоин транзакции, которая когда-либо имела место. Этот блокчейн, как следует из названия, состоит из блоков. В каждом блоке хранятся последние транзакции.

Доказательство работы (Proof-of-work) - это необходимая часть добавления новых блоков в блокчейн Биткоина. Блоки появляются с помощью майнеров, игроками в экосистеме, которые выполняют доказательство работы. Новый блок принимается сетью каждый раз, когда майнер придумывает новое выигрышное доказательство работы (Proof-of-work), что происходит примерно каждые 10 минут. Найти выигрышное доказательство работы

(Proof-of-work) настолько сложно, что единственный способ обеспечить работу майнеров, необходимую для добычи Биткоина, - это использовать дорогие специализированные компьютеры. Майнеры будут зарабатывать Биткоины, если они будут угадывать соответствующие вычисления. Чем больше вычислений они производят, тем больше Биткоинов они заработают.

Какие именно вычисления делают майнеры? В биткойне майнеры выплевывают так называемый “хэш”, который превращает входные данные в произвольно выглядящую строку букв и цифр.

Цель майнеров - создать хэш, соответствующий текущей “цели " Биткойна.” Они должны создать хэш с достаточным количеством нулей впереди. Вероятность получить несколько нулей подряд очень мала. Но майнеры по всему миру делают триллионы таких вычислений в секунду, поэтому им требуется в среднем около 10 минут, чтобы достичь этой цели.

Тот, кто достигнет цели первым, выиграет партию криптовалюты биткойн. Затем протокол биткойна создает новое значение, которое майнеры должны хэшировать, и майнеры снова начинают гонку за поиском выигрышного доказательства работы.

Что Такое Хэшинг?

Хэш-это функция, которая преобразует ввод букв и цифр в зашифрованный вывод фиксированной длины. Хэш создается с помощью алгоритма и имеет важное значение для управления блокчейном в криптовалюте.

КЛЮЧЕВЫЕ МОМЕНТЫ

• Хэш-это функция, которая удовлетворяет зашифрованным требованиям, необходимым для решения блокчейн-вычислений.

• Хеш, как и nonce или решение, является основой блокчейн-сети.

• Хэши имеют фиксированную длину, так как это делает почти невозможным угадать длину хэша, если кто-то пытался взломать блокчейн.

• Хэш разрабатывается на основе информации, содержащейся в заголовке блока.

Основой криптовалюты является блокчейн, представляющий собой глобальную бухгалтерскую книгу, образованную путем объединения отдельных блоков транзакционных данных. Блокчейн содержит только проверенные транзакции, что предотвращает мошеннические транзакции и двойное расходование валюты. Полученное зашифрованное значение представляет собой ряд цифр и букв, которые не похожи на исходные данные и называются хэшем. Майнинг криптовалют предполагает работу с этим хэшем.

Хеширование требует обработки данных из блока с помощью математической функции, что приводит к выходу фиксированной длины. Использование вывода фиксированной

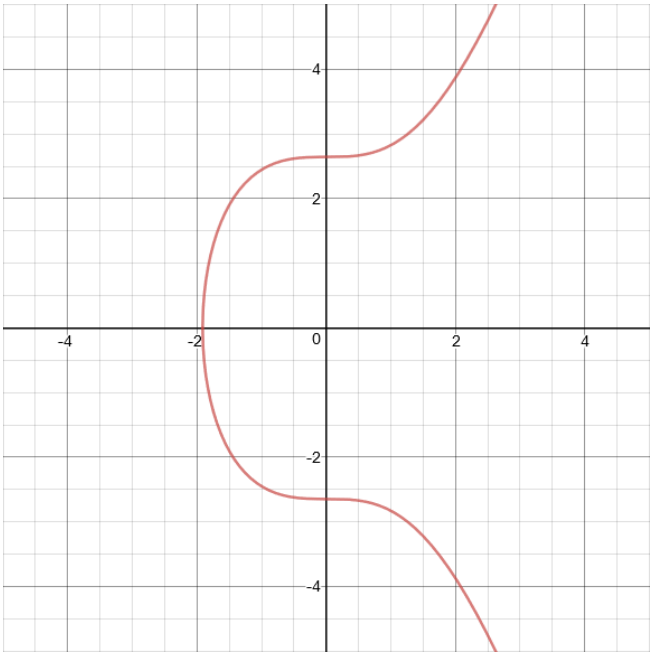
длины повышает безопасность, так как любой, кто пытается расшифровать хэш, не сможет определить, насколько длинный или короткий ввод, просто посмотрев на длину вывода.

Майнер фокусируется на случайное число, последовательность цифр. Это число добавляется к хэшированному содержимому предыдущего блока, которое затем хэшируется. Если этот новый хэш меньше или равен целевому хэшу, то он принимается в качестве решения, майнеру дается вознаграждение, и блок добавляется в блокчейн.

Процесс валидации блокчейн-транзакций основан на шифровании данных с помощью алгоритмического хеширования.

Решение хэша требует, чтобы майнер определил, какую строку использовать в качестве nonce, что само по себе требует значительного количества проб и ошибок. Это происходит потому, что nonce-это случайная строка. Крайне маловероятно, что майнер успешно придумает правильный nonce с первой попытки, а это означает, что майнер потенциально может протестировать большое количество вариантов nonce, прежде чем получить его правильно. Чем больше сложность—мера того, насколько трудно создать хэш, соответствующий требованиям целевого хэша,—тем больше времени, вероятно, потребуется для создания решения.

Пример функции хэша



Хеширование слова “привет” приведет к выходу, который будет иметь ту же длину, что и хэш для “Я иду в магазин.” Функция, используемая для генерации хэша, является детерминированной, то есть она будет давать один и тот же результат каждый раз, когда используется один и тот же входной сигнал. Он может эффективно генерировать хэшированные входные данные; он также затрудняет определение входных данных (что приводит к майнингу), а также вносит небольшие изменения во входные данные, приводящие к неузнаваемому, совершенно другому хэшу.

Обработка хэш-функций, необходимых для шифрования новых блоков, требует значительных вычислительных мощностей, что может быть дорогостоящим. Чтобы побудить частных лиц и компании, называемые майнерами, инвестировать в необходимую технологию, криптовалютные сети вознаграждают их как новыми криптовалютными токенами, так и комиссией за транзакцию. Майнеры получают компенсацию только в том случае, если они первыми создают хэш, соответствующий требованиям, изложенным в целевом хэше.

Когда кто-то отправляет вам биткойн, он отправляет его на ваш адрес. Если вы хотите потратить любой из биткоинов, отправленных на ваш адрес, вы создаете транзакцию и указываете, куда должен пойти ваш биткоин. Такая сделка может выглядеть так:

Конечно, любой может создать транзакцию, похожую на описанную выше, так что если бы она была добавлена в блокчейн как есть и без проблем, то вы получили бы $30 000+, нравится вам это или нет. К счастью, такая транзакция не входит в блокчейн, потому что в ней отсутствует действительная цифровая подпись. Добавив цифровую подпись, вы можете доказать, что знаете закрытый ключ, соответствующий адресу 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfN. Если вы не знаете соответствующего закрытого ключа, то вам, вероятно, не следовало говорить людям, чтобы они отправляли вам биткойн по этому адресу, так как вы не можете потратить ни одного из отправленных туда биткойнов!

Когда вы создаете биткойн-адрес для себя (или адрес/учетную запись для любой другой криптовалюты), вы сначала генерируете закрытый ключ. Из закрытого ключа вы вычисляете соответствующий открытый ключ и, хешируя этот открытый ключ, получаете свой адрес. Надеюсь, вы не можете сначала выбрать адрес, а затем определить закрытый ключ из него, иначе вы могли бы определить закрытый ключ для любого адреса, используя тот же метод. Еще раз, какой адрес у Сатоши?

Криптография с открытым ключом

Открытые ключи, закрытые ключи и цифровые подписи являются основными компонентами криптографии с открытым ключом. Независимо от того, какая математическая основа используется для реализации криптографической системы с открытым ключом, она должна удовлетворять следующим требованиям, по крайней мере для наших целей:

1. Вычислительно невозможно получить закрытый ключ, соответствующий данному открытому ключу.

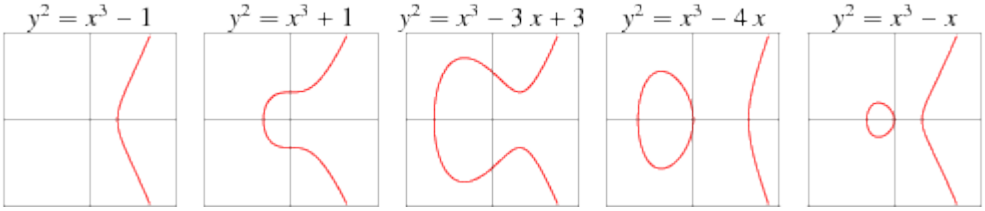
2. Можно доказать, что человек знает закрытый ключ, соответствующий открытому ключу, не раскрывая при этом никакой полезной информации о закрытом ключе. Кроме того, такое доказательство может быть построено таким образом, что оно требует проверки конкретного сообщения. Таким образом, доказательство формирует цифровую подпись для этого сообщения.

Один из способов криптографии с открытым ключом-это эллиптические кривые. Другой способ-это RSA, который вращается вокруг простых чисел. Большинство криптовалют — включая биткойн и Эфириум — используют эллиптические кривые, потому что 256-битный закрытый ключ эллиптической кривой так же безопасен, как и 3072-битный закрытый ключ RSA.

Криптография эллиптических кривых

Что такое эллиптическая кривая? Эллиптическая кривая состоит из всех точек, удовлетворяющих уравнению следующего вида:

y2 = x3+ax+b,



где 4a3+27b2 ≠ 0 (это необходимо, чтобы избежать особых точек).

Вот несколько примеров эллиптических кривых:

Обратите внимание, что все эллиптические кривые выше симметричны относительно оси x. Это верно для каждой эллиптической кривой, потому что уравнение для эллиптической кривой:

y2 = x3+ax+b

А если взять квадратный корень из обеих сторон, то получится:

y = ± √x3+ax+b

Таким образом, если a=27 и b=2 и вы подключаете x=2, вы получите y=±8, что приведет к точкам (2, -8) и (2, 8).

Эллиптическая кривая, используемая Биткоином, Эфириумом и многими другими криптовалютами, называется secp256k1. Уравнение для кривой secp256k1 имеет вид y2 = x3+7. Эта кривая выглядит так:

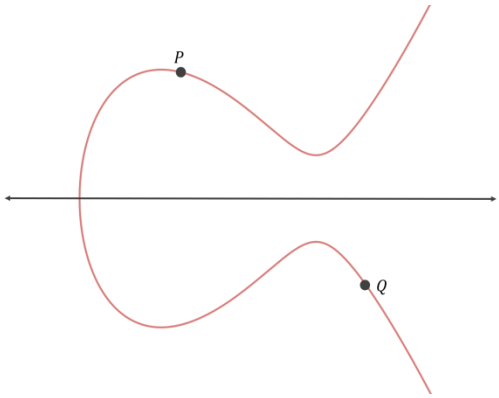
Сатоши выбрал secp256k1 без особой причины.

Пункт дополнение

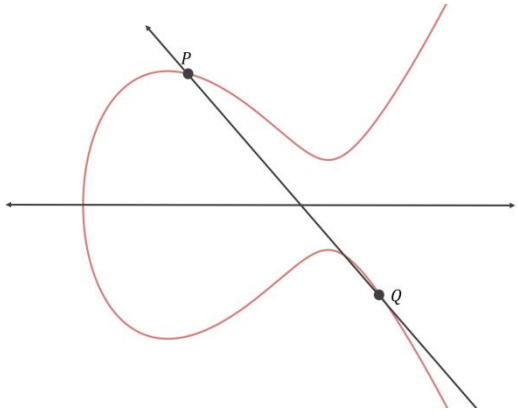
Вы знаете, как можно сложить два числа вместе, чтобы получить третье? Вы можете сложить две точки на эллиптической кривой вместе, чтобы получить третью точку на кривой.

Чтобы сложить две точки на эллиптической кривой вместе, вы сначала находите линию, которая проходит через эти две точки. Затем вы определяете, где эта линия пересекает кривую в третьей точке. Затем вы отражаете эту третью точку поперек оси x (то есть умножаете координату y на -1), и любая точка, которую вы получаете из нее, является результатом сложения первых двух точек вместе.

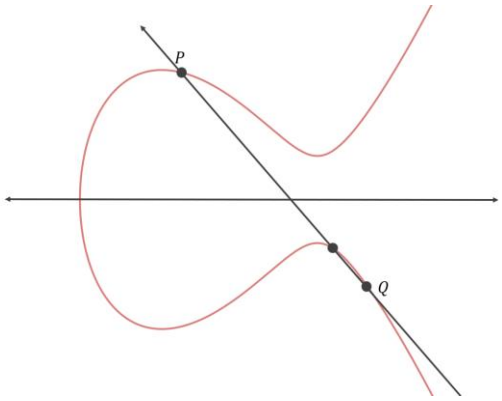
Давайте рассмотрим пример этого. Допустим, вы хотите сложить вместе следующие два пункта:



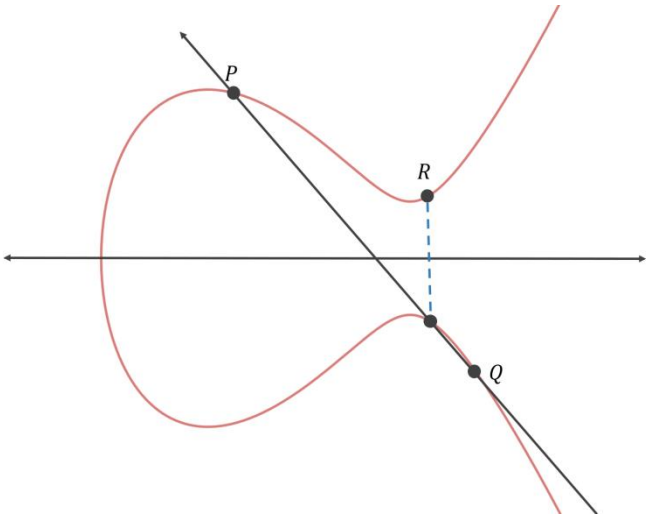
Во-первых, вы находите линию, которая проходит через две точки:



Затем вы находите третью точку на кривой, которую пересекает линия:



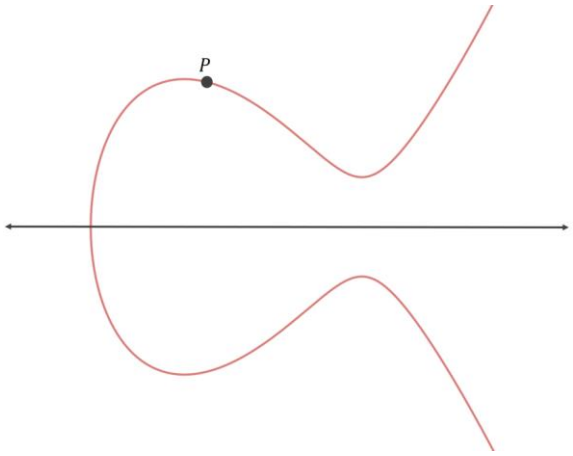
Тогда вы отражаете этот момент по оси X:



Следовательно, P+Q=R.

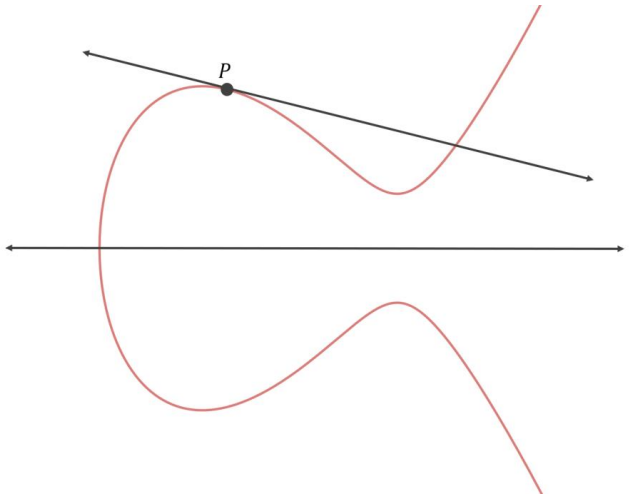
Чтобы правильно выполнять криптографию эллиптических кривых, вместо того чтобы складывать две произвольные точки вместе, мы указываем базовую точку на кривой и добавляем только эту точку к себе.

Например, предположим, что у нас есть следующая кривая с базовой точкой P:

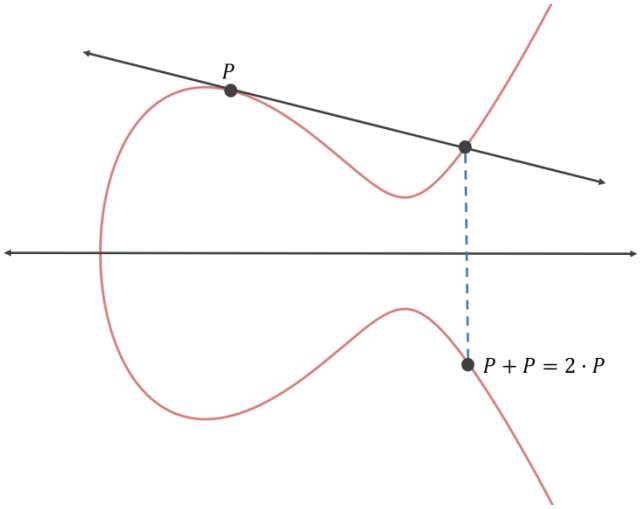


Изначально у нас есть P, или 1•P.

Теперь давайте добавим P к самому себе. Во-первых, мы должны найти уравнение прямой, проходящей через P и P. Таких линий бесконечное множество! В этом частном случае мы выбираем касательную линию.

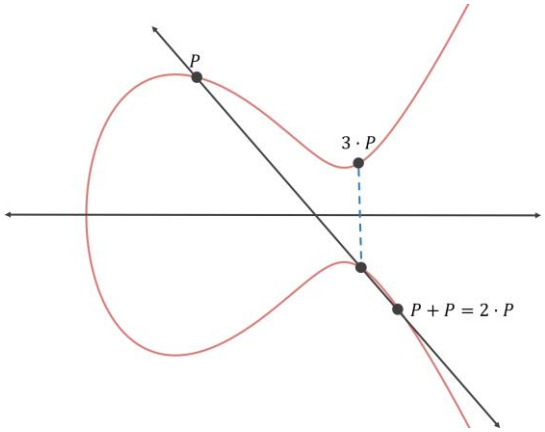


Теперь мы находим “третью” точку, которую пересекает эта линия, и отражаем ее поперек оси x.



Таким образом, P, добавленное к самому себе, или P+P, равно 2•P.

Если мы снова добавим P к себе, мы будем вычислять P, добавленное к себе, добавленное к себе, или P+P+P. В результате получится 3•П. Чтобы вычислить 3•P, мы можем просто сложить P и 2•P вместе.



Мы можем продолжать добавлять P к себе, чтобы вычислить 4•P и 5•P и так далее.

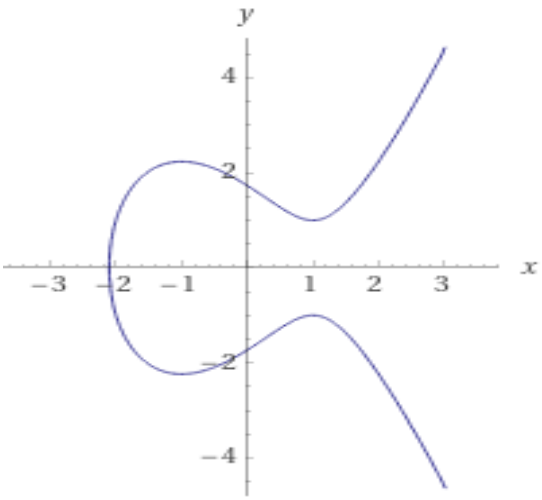
Базовая точка, используемая кривой secp256k1, имеет следующие координаты x и y:

x-координата:
55066263022277343669578718895168534326250603453777594175500187360389116729240

y-координата:

32670510020758816978083085130507043184471273380659243275938904335757337482424

В приведенных выше примерах используется другая базовая точка, так что все операции сложения точек помещаются в маленькое окно.



Выводы:

- В данной работе был разработан **собственный алгоритм** для нахождения и создания хэша
- Изучен **сегодняшний рынок** криптовалют и **принцип работы** блокчейна.
- Исследованы различные способы **шифрования** для безопасности криптовалюты.