Казанцева Т.И.
Математическая основа биткойна

*Уральский федеральный университет имени первого Президента России Б.Н. Ельцина
(Россия, Екатеринбург)*

doi:10.18411/lj-04-2018-140

idsp: 000001:lj-04-2018-140

Аннотация

Работа посвящена описанию математических принципов защиты биткойн-системы. В частности, рассмотрены основы эллиптических кривых и конечных полей.

Ключевые слова: блокчейн, конечное поле, эллиптическая кривая, биткойн

Abstract

The work is devoted to the analysis of Bitcoin protection on mathematical bases, in particular, elliptic curves and finite fields.

Keywords: block, finite field, elliptic curve, Bitcoin

Ни для кого не секрет, что на сегодняшний день, криптовалюта является одним из легких и общедоступных способов оплаты чего угодно, не тратя при этом много времени. Но почему-то многих сбивает с толку тот факт, что биткойн нарушает привычное понятие собственности, т.е. не принадлежит какому-то конкретному лицу. По этой причине большинство людей «боится» пользоваться криптовалютой.

Целью статьи: показать, что безопасность криптовалюты, в частности биткойна, закреплена простой математикой.

Нельзя сказать, что биткойном кто-то управляет, так как биткойны существуют лишь как записи в блокчейне [1]. Блокчейн – база данных, которая хранит информацию обо всех транзакциях участников системы. Под системой понимается добровольная сеть подключенных компьютеров. Если вы «владеете» биткойном значит вы просто имеете возможность передать контроль над этими записями кому-то еще, зафиксировав факт этой передачи на блокчейне. Эту способность дает вам эксклюзивный доступ к паре ключей ECDSA: секретному и публичному [2].

Разберемся, что же такое ECDSA. ECDSA – это акроним для Алгоритма Цифровой Подписи с Эллиптическими Кривыми. Данный алгоритм использует эллиптические кривые и конечные поля, чтобы «подписать» данные таким образом, чтоб третьи лица смогли легко проверить подлинность подписи, но при этом сам «подписывающий» оставлял за собой эксклюзивную возможность создавать подписи. В случае биткойна «данные», которые подписываются – это транзакция, которая передает право собственности на биткойны.

ECDSA имеет две отдельные процедуры для подписи и ее проверки. Каждая процедура представляет собой алгоритм, состоящий из нескольких арифметических операций. Алгоритм подписи использует секретный ключ, а алгоритм проверки использует только открытый ключ. Оба этих алгоритма основаны на эллиптической криптографии [3].

Чтобы продвинуться дальше, для начала познакомимся поближе с эллиптическими кривыми и конечными полями.

В эллиптических кривых нет ничего сложного. Каждая такая кривая представляется уравнением вида: $y^2 = x^3 + ax + b$. Конкретно для биткойна используется уравнение с параметрами: $a = 0$ и $b = 7$.

Эллиптические кривые имеют некоторые полезные свойства:

- перпендикулярная прямая к оси абсцисс, пересекающая кривую в двух точках, обязательно пересечет кривую в третьей точке, лежащей на кривой;
- перпендикулярная прямая к оси абсцисс, которая является касательной к кривой, обязательно пересечет кривую ровно в одной точке.

Эти свойства используются, чтобы определить две операции над точками, составляющими кривую: сложение точек и удвоение.

Сложение точек $A + B = D$ основано на первом свойстве. Мы проводим через точки A и B прямую, которая, пересекает кривую в некоторой третьей точке C . Затем мы находим точку на кривой, симметричную точке C относительно оси абсцисс. Именно эта точка D и будет являться суммой A и B .

Чтобы удвоить точку A , воспользуемся вторым свойством. При удвоении мы проводим прямую, касательную к данной кривой в точке A , которая, должна пересекать ее еще в одной точке C . Точка B , симметричная относительно оси абсцисс, будет являться результатом удвоения точки A .

С помощью этих операций мы можем определить операцию скалярного умножения, $B = aA$.

Теперь мы знаем об эллиптических кривых все, что о них стоит знать.

Конечное поле, в контексте ECDSA, можно рассматривать как заданный диапазон положительных чисел. Любые операции могут осуществляться в рамках этого диапазона. Если же результат операции выходит за пределы этого диапазона, то мы просто по окончании диапазона возвращаемся к его началу и продолжаем считать, как ни в чем ни бывало. Результат, как ни крути, останется внутри нашего диапазона, как бы он ни хотел из него выбраться [4].

Есть очень простой способ проиллюстрировать выше сказанное. Остаток от целочисленного деления, или оператор по модулю (MOD). Например, $11/6$ дает 1 с остатком 5:

$$11 \text{ MOD } 6 = 5$$

В нашем случае конечное поле от 0 до 5, и все операции по модулю 6, над любым числом, дадут результат, который попадет в этот диапазон.

ECDSA использует не просто эллиптические кривые, а эллиптические кривые в контексте конечного поля, что значительно меняет их внешний вид.

Чтобы пользователи могли друг с другом договариваться, такой протокол как биткойн должен зафиксировать набор параметров для эллиптической кривой и ее конечного поля. Этими параметрами являются: **базовая точка, значение модуля поля, уравнение кривой, порядок базовой точки**.

Для всех этих параметров биткойн использует невообразимо большие числа. Это важно! Ведь безопасность этого алгоритма опирается на то, что эти значения слишком большие, чтобы подобрать что-то простым перебором [5].

Значения, которые использует биткойн:

Уравнение эллиптической кривой: $y^2 = x^3 + 7$

Простой модуль = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF

Базовая точка = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB
2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448
A6855419 9C47D08F FB10D4B8

Порядок = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF BAAEDCE6 AF48A03B
BFD25E8C D0364141

Данная конкретная реализация ECDSA известна как **secp256k1** [6] является частью семейства стандартов, предлагаемых для использования в криптографии.

В результате вооружившись всеми этими базовыми знаниями, становится понятно, что отвечает за безопасность криптовалюты и, что происходит в недрах биткойн-клиента, когда мы пытаемся что-нибудь оплатить.

1. Генкин А. Блокчейн: Как это работает и что ждет нас завтра / Артем Генкин, Алексей Михеев. — М.: Альпина Паблицер, 2018.
2. Саломеа А. Криптография с открытым ключом. — М.: Мир, 1995. — 318 с.
3. Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию. — М.: КомКнига, 2006. — 280 с.
4. Журавлев Ю. И., Флеров Ю. А., Вялый М. Н. Дискретный анализ. Основы высшей алгебры. — 2-е изд. — М.: МЗ Пресс, 2007. — 224 с.
5. Пол Винья и Майкл Кейси. Эпоха криптовалют. Как биткоин и блокчейн меняют мировой экономический порядок — М.: Манн, Иванов и Фербер, 2017. — 432 с.
6. What does the curve used in Bitcoin, secp256k1, look like? [Электронный ресурс] URL: <https://bitcoin.stackexchange.com/questions/21907/what-does-the-curve-used-in-bitcoin-secp256k1-look-like> (дата обращения: 16.04.2018)

Майданов Д.А.

Удаленная on-line диагностика технического состояния транспортных средств и грузов

ГУУ

doi:10.18411/lj-04-2018-141

idsp: 000001:lj-04-2018-141

Аннотация

В данной статье описывается возможно дальнейшее развитие диагностики автомобиля с использованием on-line и дальнейшим ремонтом автомобиля удаленно. Также поднимаются все известные на данный момент системы, взаимодействующие с автомобилем удаленно.

Ключевые слова: логистика; автомобиль; грузоперевозки; сеть Интернет; on-line; ремонт; диагностика; транспортное средство; удаленный доступ; техническое состояние автомобиля

В составляющих структурах, элементах, звеньях, цепей поставок, логистических систем на национальном, региональном, международном уровне экономического и социального развития во времени и пространстве особо важное и главное место занимает качественное и надежное перемещение, перевозка товарных грузов и пассажиров [1-3] разными видами и типами транспортных средств по различным маршрутам и направлениям воздушным, сухопутным, водным [4,5] с использованием правильного установление места его обслуживания национального транспорта на международных рынках где постоянно используются инновационные технологии, в том числе и автомобильным транспортом, на котором автор сосредоточил свое основное внимание [6,7].

С тех времен, когда человек изобрел свой первый автомобиль для осуществления поездок, он начал долгий и длительный путь по его совершенствованию. Добавлялись новые более технологично-правильные, качественные детали, инженеры стали задумываться об аэродинамике и использовать для обводов корпуса аэродинамические трубы, менялись технологии процессов преобразования энергии и появлялись все более совершенные модели с минимальным негативным влиянием на экологию и окружающую среду. Человек не может стоять на месте, ему нужно совершенствование всего.

Это можно с уверенностью можно назвать современным качественным подходом к «жизни» и любой деятельности. И вот, перед нами то, что мы имеем на сегодняшний день