МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОВАЛЮТ

С.А. Прохожий
Витебск, ВГУ имени П.М. Машерова

Человеческое общество всегда невозможно было представить без денег. Деньги – это специфический товар максимальной ликвидности, который является универсальным эквивалентом стоимости других услуг или товаров. История развития денег тесно связана с развитием человеческой цивилизации. Товары, продукты и оружие, монеты различных видов (от костяных до золотых), акции, бумажные банкноты – это всего лишь часть того, что раньше использовалось человеком и до настоящего времени используется в качестве денег. С развитием информационных технологий современный мир вступил в эпоху «электронных денег», которые не выпускаются национальными центральными банками. Монеты и банкноты постепенно стали заменяться пластиковыми платежными картами, а в сети Интернет появилось множество платежных систем, изначально созданных только для электронных платежей, таких как Яндекс. Деньги, PayPal, WebMoney. Сегодня мы наблюдаем рост криптовалют – нового платежного средства XXI века, которое имеет ряд существенных отличий от других видов электронных денег [1]. Прогресс не стоит на месте, и в наше время криптовалютами пользуется множество людей во всем мире.

Целью данной работы является изучение математических принципов, на которых основана работа криптовалют, на примере биткоина.

Материал и методы. При написании статьи проанализированы различные источники по криптографии и шифрованию, криптовалютам, алгебре конечных полей, а также материалы из глобальной сети Интернет.

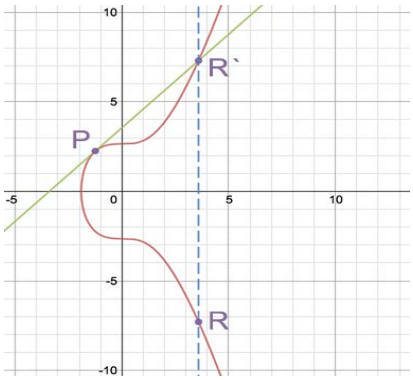
Результаты и их обсуждение. Рассмотрим математические принципы работы криптовалют на примере биткоина, который сегодня обладает самой разветвленной и обширной сетью и является наиболее ликвидной криптовалютой. Биткоин нематериален и не обладает привязкой к каким-либо государственным валютам, драгоценным металлам или природным ресурсам. Его курс чрезвычайно подвижен и определяется исключительно балансом спроса и предложения. Оборот этой валюты не контролируется какими-либо органами, ведомствами или организациями и осуществляется исключительно между криптокошельками участников сети. Отмена транзакции монет невозможна.

Сами по себе биткоины не хранятся ни централизованно, ни локально – и поэтому нельзя сказать, кто отвечает за их доверенное хранение. Биткоины существуют лишь как записи в распределенной бухгалтерской книге, называемой *блокчейном*, копии которой распределены среди добровольной сети подключенных компьютеров. Быть «владельцем» биткоинов просто означает иметь возможность передать контроль над этими записями кому-то еще, зафиксировав факт этой передачи на блокчейне. Что же дает эту способность? Эксклюзивный доступ к паре ключей ECDSA: секретному и публичному [2].

ECDSA (Elliptic Curve Digital Signature Algorithm) – алгоритм с открытым ключом для создания цифровой подписи, определённый в группе точек эллиптической кривой [3]. Это процесс, который использует эллиптические кривые и конечные поля, чтобы «подписать» данные таким образом, что третьи лица могут легко проверить подлинность подписи, но при этом сам подписывающий оставляет за собой эксклюзивную возможность создавать подписи. 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.

Эллиптические кривые – графики функции, уравнение которой имеет вид
$y^2 = x^3 + ax + b$ [4].

Для работы биткоина принимается $a = 0$ и $b = 7$. График соответствующей эллиптической кривой, а также соответствующее этой кривой правило удвоения точки изображены на рисунке.



Конечным полем называется конечное множество элементов, замкнутое по отношению к двум заданным в нем операциям комбинирования элементов [5]. Под замкнутостью понимается тот факт, что результаты операций не выходят за пределы конечного множества введенных элементов.

Чтобы использовать ECDSA, такой протокол биткоина должен зафиксировать набор параметров для эллиптической кривой и ее конечного поля, чтобы эти параметры знали и применяли все пользователи протокола. Иначе каждый будет решать свои собственные уравнения, которые не будут сходиться друг с другом, и они никогда ни о чем не договорятся.

Эти зафиксированные параметры включают в себя *уравнение кривой*, значение *модуля поля* и *базовую точку*, которая лежит на кривой. Последним параметром является *порядок* базовой точки, который в графическом виде можно представить себе как количество раз, которое базовая точка может быть прибавлена к себе до тех пор, пока ее касательная кривая не станет вертикальной. Этот параметр подбирается таким образом, чтобы он являлся очень большим простым числом.

Заключение. В наши дни криптовалюты продолжают свое развитие, число пользователей новыми платежными средствами постоянно растет. Популярность биткоина стимулирует создание других криптовалют, которые развиваются параллельно, но их возможности и популярность пока еще намного меньше. Однако вместе с тем следует отметить, что каждая из них основана на различных математических принципах, хотя идеология блокчейна (выстроенной по определённым правилам непрерывной последовательной цепочки блоков, содержащих всю полную информацию, копии которых хранятся независимо друг от друга на множестве разных компьютеров) присутствует в любой из них.

1. Свон, М. Блокчейн. Схема новой экономики / М. Свон – М.: Олимп-Бизнес, 2017. – 240с.
2. Филиппов, Е. Криптовалюта от А до Я / Е. Филиппов. – 2017. – 50с.
3. Алгоритм ECDSA / Википедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/?oldid=90242139 (дата обращения: 12.01.2018).
4. Эллиптическая кривая / Википедия [Электронный ресурс]. – Режим доступа http://ru.wikipedia.org/?oldid=90075838 (дата обращения: 05.01.2018).
5. Биткоин / Википедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/?oldid=90310153 (дата обращения: 15.01.2018).

ВЫБОР И ОПТИМИЗАЦИЯ АЛГОРИТМА СОРТИРОВКИ ДЛЯ ДОСТИЖЕНИЯ МАКСИМАЛЬНОГО БЫСТРОДЕЙСТВИЯ

Д.Ю. Романцов
Орша, Оршанский колледж ВГУ имени П.М. Машерова

Сортировка данных одна из самых распространённых задач. На данный момент существует около 40 видов сортировок [1]. Практически для всех определена временная сложность O, на основе которой можно определить их скорость. Однако из-за того, что это достаточно обобщённая характеристика, то сказать однозначно, какой алгоритм быстрее нельзя.

Целью исследования является выявление наиболее оптимального алгоритма сортировки массива данных эмпирическим способом.