УДК 004.65

КВАНТОВЫЙ БЛОКЧЕЙН

Фёдоров С.О., студент гр. ПИб-181, I курс
Великий В.А., студент гр. ПИб-181, I курс
Кошкина Г.К., к.ф.-м.н., доцент
Кузбасский государственный технический университет имени Т. Ф. Горбачева
г. Кемерово

Согласно статистике компании Verizon злоумышленники тратят в среднем на взлом той или иной системы и на ее компрометацию всего несколько минут, в то время как специалисты по информационной безопасности обнаруживают факты взлома своих систем обычно в течение нескольких месяцев. Всё новые методы защиты быстро становятся уязвимы к взлому. Поэтому возникает потребность в создании такой системы, которую в принципе невозможно взломать. Одно из решений этой проблемы - создание квантового блокчейна.

Блокчейн – это цепочка связанных друг с другом блоков информации, выстроенная по определённым правилам. Эти блоки хранятся на компьютерах всех пользователей, обменивающихся данными в рамках блокчейна и каждый новый блок хранит в себе информацию о предыдущих. Поэтому что-то исправить или подделать в такой базе данных практически невозможно. Идея создания блокчейнов появилась около 30 лет назад. Первый раз такая система была использована при создании криптовалюты на её основе – биткоин. В будущем блокчейны могут найти применение для составления умных контрактов, хранения информации о правах интеллектуальной собственности и других данных.

В блокчейне может храниться база данных транзакций — описаний событий, когда один участник распределенной сети передает другому, например, некоторую сумму денег[1]. Транзакция считается завершённой и достоверной, когда проверены её формат и подписи и когда сама транзакция объединена в группу с несколькими другими и записана в специальную структуру — блок, в каждый из которых записан хэш информации. Для получения хэша используются достаточно сложные функции: если хотя бы один бит в данных транзакций поменяется, то сильно изменится и весь хэш.

Создание новых блоков в блокчейне - довольно непростая задача, занимающая определённое количество времени. И даже если злоумышленник сможет создать блок с поддельными транзакциями и попытается встроить его в блокчейн, то он просто не получит продолжения, так как транзакции в нем не будут подтверждены. Потом система отвергнет его[1].

Алгоритм защиты подобных систем построен по принципу асимметричного шифрования с открытым и закрытым ключом. Транзакция подписывается закрытым ключом, а ее истинность проверяется с помощью открытого ключа.

С использованием классических алгоритмов атаки практически невозможно найти закрытый ключ, зная открытый. Системы асимметричного шифрования, такие как RSA и подобные (DSA, DH и пр.), построены на том утверждении, что сложность разложения числа на простые множители растет экспоненциально от размера ключа. Однако, на квантовом компьютере становится возможным за полиномиальное время разложить число на простые множители и, таким образом, найти закрытый ключ, зная открытый. Эта опасность вряд ли приведет к мгновенному краху, например, биткоина, но позволит проводить нелегальные в рамках системы операции, в частности перенаправлять криптовалюту на другие кошельки[2].

Для того, чтобы обезопасить классические схемы от появления квантового компьютера, физики из Российского квантового центра впервые запустили квантовый блокчейн — инструмент для создания распределенной базы данных, в которой практически невозможно подделать записи[1]. Инструкции по его сборке были опубликованы в электронной библиотеке arXiv.org.

В то время как безопасность обычного блокчейна обеспечивается криптографией, в квантовом защищённость обеспечивается запутанными фотонами, причем даже в том случае, когда какая-то пара фотонов никогда не существовала одновременно. В результате потенциальный хакер не сможет подделать старый блок информации, так как кодировавший его фотон уже был поглощен одним из узлов сети[2].

Алексей Фёдоров из Российского квантового центра и его коллеги создали свой собственный блокчейн, позволяющий использовать квантовую криптографию и системы квантовой передачи данных для защиты подобных данных от взлома[3]. Технология была успешно протестирована, «злоумышленнику» не удалось внести ложные транзакции в базу данных.

Квантовый блокчейн позволит безопасно хранить записи обо всех транзакциях и валютных операциях, не опасаясь взлома. Это, как считают эксперты, позволит снизить расходы на защиту банков от взлома, решать судебные споры между игроками рынка в "автоматическом" порядке и другое. Поэтому подобные системы сегодня привлекают внимание финансистов и экспертов в области безопасности данных.

Однако сейчас говорить о возможности массового применения технологии квантового блокчейна весьма сложно, этому мешают ограничения, накладываемые самой технологией, и отсутствие необходимой для нее инфраструктуры в виде квантовых сетей[3].

Сначала необходимо создать квантовый интернет — глобальную многопользовательскую сеть, защищенную квантовой криптографией, а это потребует много времени и ресурсов. Спутники критически важны для его создания — без них межконтинентальные системы связи крайне сложно реализовать. Кто и как их контролирует — это тоже вопрос безопасности, для обеспечения которой необходим еще один уровень защиты. Поэтому вряд ли конечные пользователи смогут воспользоваться квантовым блокчейном в обозримом будущем[3].

Многим может показаться, что такая система сейчас не нужна обычному пользователю. Однако следует думать о будущем. Когда-нибудь уже используемые защищённые системы перестанут справляться со своей задачей, и тогда возникнет потребность в новых технологиях, таких, как квантовый блокчейн.

Список литературы:

1.В России запустили первый в мире квантовый блокчейн // NPLUS1.RU. 2015. URL : https://nplus1.ru/news/2017/05/26/quantum-blockchain (дата обращения: 26.05.2017)

2.Полностью квантовый блокчейн подобен машине времени // INDICATOR.RU : Интернет-издание. 2016. URL : https://indicator.ru/news/2018/04/25/kvantovyj-blokchejn-mashina-vremeni (дата обращения: 25.04.2018)

3.Квантовый блокчейн: как открытия физиков произведут революцию в IT // RIA.RU : МИА "Россия сегодня". 2014. URL: https://ria.ru/science/20180310/1515859987.html (дата обращения: 10.03.2018)