

# Квантовый переход и безопасность блокчейнов

Александр Подобных, эксперт КОСАтка, член АРСИБ



**К**вантовые компьютеры — мощные машины, которые могут решать сложные уравнения гораздо быстрее, чем обычные. Эксперты полагают, что квантовые компьютеры способны взламывать системы шифрования за считанные минуты, в то время как обычным на это потребовалось бы несколько тысяч лет. Если эти предположения верны, то под угрозой находится большая часть современной инфраструктуры цифровой безопасности, включая криптографию, лежащую в основе биткоина и криптовалюты в целом.

измениться с развитием новых вычислительных систем, таких как квантовые компьютеры.

## Квантовые вычисления

По оценкам, классической вычислительной системе понадобится тысячелетия, чтобы подобрать соответствующий 55-битный ключ. При этом минимальный рекомендуемый размер ключа, используемого в биткоине, составляет 128 бит, а во многих других реализациях кошелька — 256 бит. Из этого следует, что классические вычислительные системы не представляют угрозы для асимметричного шифрования, используемого в криптовалюте и инфраструктуре Интернета.

В классических компьютерах бит используется для отображения информации и может иметь два состояния: 0 или 1. Квантовые компьютеры работают с квантовыми битами, или кубитами. Кубит — это основная единица измерения информации в квантовом компьютере. Так же, как и бит, кубит может быть в двух состояниях. Однако благодаря особенностям квантово-механических явлений состояние кубита может быть как 0, так и 1 в одно и то же время.

Это побудило многие университеты и частные компании начать вкладывать ресурсы в научные исследования и разработки такой новой и захватывающей области, как квантовые вычисления. Технология квантовых вычислений основана на абстрактной теории и практических инженерных задачах. В глобальном смысле ее появление — это достижение для всего человечества.

## Риски и угрозы, связанные с квантовыми вычислениями

К сожалению, побочным эффектом таких квантовых компьютеров будет то, что алгоритмы, лежащие в основе асимметричной криптографии, станут простыми для решения, таким образом фун-

даментально разрушая системы, которые полагаются на данный тип шифрования.

Рассмотрим пример взлома 4-битного ключа. Теоретически 4-кубитный компьютер может принимать все 16 состояний (комбинаций) одновременно в рамках одной вычислительной задачи. Вероятность нахождения правильного ключа составит 100% при выполнении этих вычислений.

Появление технологии квантовых вычислений может подорвать принцип работы криптографии, который лежит в основе большей части современной цифровой инфраструктуры, включая криптовалюты.

Это поставит под угрозу безопасность и коммуникацию всего мира, от правительств и транснациональных корпораций до отдельных пользователей. Неудивительно, что значительный объем исследований направлен на изучение и разработку мер защиты. Криптографические алгоритмы, которые защищены от угрозы квантовых компьютеров, известны как квантово-устойчивые алгоритмы.

На базовом уровне предполагается, что риск, связанный с квантовыми компьютерами, можно уменьшить с помощью криптографии с симметричным ключом путем простого увеличения длины ключа. Эта область криптографии была ограничена криптографией с асимметричным ключом в связи с проблемой использования общего секретного ключа через открытый канал.

Проблема с безопасным обменом общего ключа через открытый канал может найти решение в квантовой криптографии. В настоящее время многие криптографы делают успехи в разработке контрмер против перехвата информации. Прослушка на общем канале может быть обнаружена с помощью применения тех же принципов, которые необходимы для разработки квантовых компьютеров. Это позволило бы полу-

## Асимметричная криптография

Асимметричная криптография (также известная, как криптография с открытым ключом) — важнейший компонент в экосистеме криптовалюты и большей части инфраструктуры Интернета. В ней используется пара ключей для шифрования и дешифрования информации, а именно открытый (публичный) ключ для шифрования и закрытый (приватный) ключ для дешифрования. При этом криптография с симметричным ключом использует только один ключ для шифрования и дешифрования данных.

Одно из основных преимуществ асимметричной криптографии — возможность обмена информацией без совместного использования общего ключа с помощью ненадежного канала связи. Без этой решающей особенности информационная безопасность в Интернете была бы невозможной. Например, сложно представить себе банковские онлайн-сервисы без безопасного шифрования информации сторон, у которых отсутствует доверие друг к другу.

Некоторые аспекты безопасности асимметричной криптографии основаны на том, что алгоритм, генерирующий пару ключей, делает невероятно трудным вычисление приватного ключа из публичного, в то время как обратное вычисление является простым. В математике это называют односторонней функцией с потайным входом, поскольку произвести расчет чисел в одном направлении гораздо проще, чем в другом.

Для решения таких функций не подходит ни один из современных компьютеров, поскольку даже для самых мощных устройств вычисление подходящего значения займет огромное количество времени. Тем не менее все может вскоре