УДК 004.021

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ И АЛГОРИТМЫ КОНСЕНСУСА ПРИ КВАНТОВОМ ШИФРОВАНИИ

А.В. Сидоренко, И.А. Приходько
Белорусский государственный университет, Минск, Республика

Аннотация. В работе приведены основные аспекты использования квантовых вычислений и блокчейна для обеспечения надежности и безопасности блокчейн сетей. Рассматриваются основные параметры протокола квантового распределения ключа и создания консенсуса в блокчейне. Представлены основные особенности, состав и характеристики разработанной реализации компьютерной программы прототипа блокчейн, полученные при использовании пакета QISKit.
Ключевые слова: квантовое шифрование; квантовый блокчейн; алгоритмы консенсуса; компьютерная программа

QUANTUM KEY DISTRIBUTION AND ALGORITHMS OF CONSENSUS FOR QUANTUM INFORMATION CODING

A.V. Sidorenko, I. A. Prihodko
Belarusian State University, Minsk, Belarus

Abstract. The main aspects of using quantum computation and blockchain for security, reliability and safety of blockchain networks, are presented. The based parameters of Quantum Distribution Keys, protocol of consensus are created for blockchain. The main features, structure and properties of created computer protocol of prototype blockchain are received by using QUISKit software package
Keywords: quantum encoding; quantum blockchain; algorithms of consensus; computer program

Введение

Интенсивное развитие новых технологий квантовых вычислений и блокчейна способствуют созданию более стойких криптографических методов при обеспечении

устойчивых к квантовым атакам алгоритмов шифрования. В данной работе исследованы возможности использования квантовых принципов при проектировании различных архитектур в технологии блокчейн

Рассматриваются вопросы квантового распределения ключей и алгоритмов консенсуса, которые обеспечивают надежность и безопасность блокчейн сетей.

Для обеспечения дополнительного уровня безопасности и уникальности блокчейна рассмотрена интеграция квантовой запутанности и алгоритмов консенсуса.

Целью работы является программная реализация архитектуры блокчейна с интегрированием квантового распределения ключа и алгоритма консенсуса Delegated Proof – of - Stake (DPoS).

Квантовое распределение ключей алгоритмы консенсуса

В основе квантовой криптографии лежит метод квантового распределения ключа (QKD). Применение принципа квантовой запутанности позволяет осуществить через оптический канал обмен информацией в кубитах при генерации скрытого ключа, устойчивого к атакам «прослушивание». Такая атака может производиться злоумышленниками в открытых каналах связи на электронные устройства, компьютеры и смартфоны. Квантовое распределение ключа использует комбинацию квантового канала и не секретность классического канала и позволяет надлежащим образом аутентифицировать распределение секретного ключа между двумя участниками. Фундаментальный принцип квантового распределения ключа основан на возмущении вызванного актом измерений квантовой системы, что позволяет немедленно обнаружить любой случай несанкционированного перехвата ключей.

Для квантового распределения ключей в настоящее время используется ряд протоколов: BB-84, B-92, E-91 и SARG-04, каждый из которых имеет отдельные преимущества и ограничения. Протокол E-91, выбранный нами для реализации компьютерной программы, основан на квантовой запутанности между двумя участниками. Доверенным источником генерируется запутанная пара частиц, квантовое состояние которых характеризуется состояниями Белла, после чего одна частица отправляется по квантовому каналу передающей стороне, другая – приемной стороне. Передающая сторона производит измерение проекции спинов полученных частиц на одно, случайно выбранное направление $\{0, \pi/8, \pi/4\}$, а приемная – на одно из $\{-\pi/8, 0, \pi/8\}$. Эти направления выбраны автором протокола для исполнения неравенств Белла. После чего по классическому каналу связи передающая и приемная стороны обмениваются базисами, в которых проводили измерения состояний частиц. Результаты измерений проекций спинов частиц на разные направления, используются для вычисления корреляционного значения. Если оно значительно отличается от $(-2\sqrt{2})$, то это значит, что запутанность состояний была нарушена либо шумами в квантовом канале, либо фактом прослушивания канала.

Блокчейн, в отличие от обычной базы данных, администрируемой централизованно, представляет собой одноранговую децентрализованную сеть, с которой может взаимодействовать любой участник. Классический блокчейн представляет из себя последовательную цепочку блоков данных. Блоки записываются один за другим, и, в зависимости от того, каким образом они записываются в цепочку, блокчейн обладает теми или иными определенными базовыми свойствами. Для того, чтобы система работала и, учитывала, что узлы блокчейна не зависят друг от друга, используются алгоритмы консенсуса блокчейна.

Алгоритмы консенсуса представляют собой совокупность принципов и правил, благодаря которым все участвующие в сети узлы автоматически приходят к консенсусу

о текущем состоянии сети. Это позволяет гарантировать безопасность сети, то есть достоверность всех хранящихся в ней данных. К наиболее распространенным алгоритмам консенсуса относятся: Proof – of - Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), YAC (Yet Another Consensus).

Алгоритм консенсуса Delegated Proof of Stake (DPoS, делегирование полномочий одному участнику), выбранный нами для использования в компьютерной программе, представляет собой разновидность алгоритма PoS. В алгоритме консенсуса DPoS право валидаторов одобрять транзакции декларируется им узлами, владеющими ресурсами сети, при этом они голосуют за того или иного валидатора. Любой участник сети, обладающий определенным объемом ресурсов, может стать валидатором, но также в любой момент голоса за этого валидатора могут быть отозваны в пользу другого. Риск при использовании этого алгоритма консенсуса представляет низкая активность участников, не исключен также сговор делегатов.

Программная реализация

Программная реализация разработанной авторами компьютерной программы проводилась с использованием симулятора квантовых вычислений и на квантовых устройствах компании IBM с применением QISKit (Quantum Information Software Kit), представляющих собой набор средств разработки с открытым исходным кодом для работы с квантовыми устройствами облачной платформы IBM Q [1]. В данной разработке также применена облачная платформа (IBM Quantum Platform), которая дает возможность работы на квантовом компьютере.

Реализация протокола E-91 производилась компьютерным моделированием на симуляторе квантовых вычислений и квантовых устройствах с использованием QISKit.

В реализации структуры блокчейна был использован язык программирования Phyton. Определяющая структуру программы платформа “Flask” позволяет при помощи HTTP- запросов взаимодействовать с блокчейном в сети, регистрируя новые связанные узлы сети, тем самым делая его полноценной децентрализованной системой. Запустив исходный код программы, мы запускаем сервер. С помощью GET-запроса "http://localhost:5000/mine"формируется единый узел в нашем блокчейне.

Заключение

Разработана компьютерная реализация прототипа блокчейна с использованием языка программирования Python. Архитектура поддерживает генерацию и использование квантовых ключей для шифрования транзакций, а также включает классические механизмы консенсуса, такие как DPoS. Компьютерная программа квантового распределения ключа E-91, моделирующая выполнение и тестирование этого протокола, выполнена на симуляторе квантовых вычислений, встроенном в пакете QISKit. и входит в состав разработанной программы.

Список использованных источников

1. IBM Quantum Platform [Электронный ресурс]. Режим доступа: IBM Quantum Platform. Дата доступа: 24.12.2024.

References

1. IBM Quantum Platform[Электронный ресурс]. Режим доступа: IBM Quantum Platform. Дата доступа: 24.12.2024.

Сведения об авторах

Сидоренко А.В., д.-р техн. наук, проф., профессор кафедры физики и аэрокосмических технологий, Белорусский государственный университет, e-mail: sidorenkoA@yandex.by.
Приходько И.А. студент факультета радиофизики и компьютерных технологий, Белорусский государственный университет.

Information about the authors

Sidorenko A., Dr. Sci. (Tech.), Professor, Professor of Department of Radiophysics and Computer Technologies, Belarusian State University, sidorenkoA@yandex.by.
Prihodko I. A. Dr. student of Department of Radiophysics and Computer Technologies, Belarusian State University.