ЗАЩИТА ИНФОРМАЦИИ И НАДЕЖНОСТЬ СИСТЕМ

INFORMATION PROTECTION AND SYSTEM RELIABILITY

УДК 004.832.519.6
https://doi.org/10.37661/1816-0301-2026-23-2-94-106

Поступила в редакцию | Received 22.04.2026
Подписана в печать | Accepted 11.05.2026
Опубликована | Published 30.06.2026

Квантовый блокчейн с интеграцией квантовой запутанности и алгоритма консенсуса

А. В. Сидоренко✉, И. А. Приходько
✉E-mail: sidorenkoa@yandex.by

Белорусский государственный университет,
пр. Независимости, 4, Минск, 220030, Беларусь

Аннотация

Цели. Целями работы являются разработка и программная реализация концептуальной модели квантово-защищенного блокчейна путем интеграции механизма квантового распределения ключей на основе протокола E91 в классическую архитектуру.

Методы. Рассмотрены вопросы уязвимости классических криптографических механизмов блокчейна к угрозам со стороны квантовых вычислений. Для создания устойчивой архитектуры предложено объединить свойства квантовой запутанности и классические криптографические методы. В качестве базы использован протокол квантового распределения ключей E91, основанный на квантовой запутанности и проверке неравенства Белла (CHSH-тест). Для связи блоков в цепочку введено новое поле E91 MAC, вычисляемое с помощью алгоритма HMAC от хеша предыдущего блока с использованием ключа, сгенерированного протоколом E91. В качестве механизма консенсуса выбран алгоритм DPoS (Delegated Proof of Stake).

Программная реализация включает симуляцию протокола E91 с использованием облачной платформы IBM Quantum и библиотеки Qiskit, а также развертывание одноранговой блокчейн-сети с CLI-интерфейсом на Python с помощью TCP-сокетов.

Результаты. Разработана концептуальная модель и реализован прототип квантово-защищенного блокчейна. Создана функциональная одноранговая сеть с алгоритмом консенсуса DPoS и механизмом распределенного голосования. Успешно выполнена симуляция протокола E91, подтверждающая возможность генерации и верификации квантового ключа. Доказана принципиальная осуществимость интеграции квантового механизма аутентификации (E91 MAC) в процесс создания и валидации блоков.

Заключение. Предложенная гибридная архитектура демонстрирует новый подход к безопасности блокчейна, основанный не только на вычислительной сложности, но и на фундаментальных законах квантовой механики. Интеграция протокола E91 и механизма DPoS обеспечивает потенциальную устойчивость к квантовым атакам и высокую энергоэффективность сети. Программный прототип подтверждает практическую реализуемость концепции для создания защищенных распределенных реестров нового поколения.

Ключевые слова: информация, защита, квантовый блокчейн, квантовая запутанность, распределение ключей, протокол E91, алгоритм DPoS, консенсус, квантовая криптография, средства разработки Qiskit

Для цитирования. Сидоренко, А. В. Квантовый блокчейн с интеграцией квантовой запутанности и алгоритма консенсуса / А. В. Сидоренко, И. А. Приходько // Информатика. – 2026. − Т. 23, № 2. – С. 94–106. – https://doi.org/10.37661/1816-0301-2026-23-2-94-106.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Quantum blockchain based on integration of quantum entanglement and consensus algorithm

Alevtina V. Sidorenko✉, Ivan A. Prikhodko
✉E-mail: sidorenkoa@yandex.by

Belarusian State University,
av. Nezavisimosti, 4, Minsk, 220030, Belarus

Abstract

Objectives. The aim of this work is to develop and implement a conceptual model of a quantum-secured blockchain by integrating a quantum key distribution mechanism based on the E91 protocol into a classical architecture.

Methods. The vulnerabilities of classical blockchain cryptographic mechanisms to threats posed by quantum computing are considered. To create a resilient architecture, it is proposed to combine the properties of quantum entanglement with classical cryptographic methods. The E91 quantum key distribution protocol, based on quantum entanglement and the Bell inequality test (CHSH test), is used as the foundation. A new field, E91 MAC, is introduced to link blocks in the chain, calculated using the HMAC algorithm from the hash of the previous block with a key generated by the E91 protocol. The Delegated Proof of Stake (DPoS) algorithm is chosen as the consensus mechanism.

The software implementation includes simulating the E91 protocol using the IBM Quantum cloud platform and the Qiskit library, as well as deploying a peer-to-peer blockchain network with a CLI interface in Python using TCP sockets.

Results. A conceptual model was developed and a prototype of a quantum-secured blockchain was implemented. A functional peer-to-peer network with the DPoS consensus algorithm and a distributed voting mechanism was created. The successful simulation of the E91 protocol confirmed the possibility of generating and verifying a quantum key. The fundamental feasibility of integrating a quantum authentication mechanism (E91 MAC) into the block creation and validation process was demonstrated.

Conclusion. The proposed hybrid architecture demonstrates a novel approach to blockchain security, based not only on computational complexity but also on the fundamental laws of quantum mechanics. The integration of the E91 protocol and the DPoS mechanism provides potential resilience to quantum attacks and high network energy efficiency. The software prototype confirms the practical feasibility of the concept for creating secure next-generation distributed ledgers.

Keywords: information, security, quantum blockchain, quantum entanglement, key distribution, E91 protocol, DPoS algorithm, consensus, quantum cryptography, Qiskit development tools

For citation. Sidorenko A. V., Prikhodko I. A. *Quantum blockchain based on integration of quantum entanglement and consensus algorithm*. Informatika [*Informatics*], 2026, vol. 23, no. 2, pp. 94–106 (In Russ.). https://doi.org/10.37661/1816-0301-2026-23-2-94-106.

Conflict of interests. The authors declare of no conflict of interest.

Введение

Развитие информационных систем с использованием технологии блокчейна произвело революционный скачок в области хранения и передачи данных, предложив децентрализованные, прозрачные и в определенной степени неизменяемые реестры. Основой безопасности классических блокчейнов являются криптографические хеш-функции, объединяющие блоки в непрерывную цепочку, и механизмы консенсуса, обеспечивающие согласованность информационных данных между участниками сети [1, 2].

Конфиденциальность и целостность данных в блокчейне создают хеш-функции и алгоритмы консенсуса, что дает возможность функционировать целой распределенной платформе, построенной от ряда структур данных блокчейна. Каждый блок блочейна в формируемой цепочке содержит криптографический хеш, который определяется на основе содержания блока, включая хеш предварительного блока. Если данные в формируемом блоке не совпадают с хешем, то происходит изменение этого блока. Это указывает на махинацию (или нелегитимный доступ) и приводит к разрыву созданной цепочки блоков. Таким образом, свойства хеш-функции играют критическую роль в обеспечении секретности и интегрируемости структуры данных блокчейна. Алгоритмы консенсуса или смарт-контракты создают условия, при которых происходит формирование временной метки для периодического доступа делегатам, участвующим в создании блоков блокчейна. Среди используемых в блокчейне механизмов консенсуса выделяется DPoS, который не использует мощность компьютера в качестве решающего фактора и может поддерживать регламент в работе блокчейна [3–5].

Возникает необходимость перехода к новым методам криптографии, способным обеспечивать надежную защиту в квантовую эпоху [6]. Бурное развитие квантовых вычислений и компьютеров способствует разработке принципов квантовой криптографии, в основе которых лежит протокол квантового распределения ключей (Quantum Key Distribution, QKD) – инновационный протокол, использующий принцип суперпозиции и квантовой запутанности для безопасного распределения ключей шифрования.

В данной работе авторами предлагается новая концепция, заключающаяся в интеграции в архитектуру блокчейна механизма квантовой запутанности, лежащего в основе квантового распределения ключей, и обосновании «квантового» характера предложенной системы в контексте данной интеграции, причем речь идет о концептуальной модели и ее программной реализации.

Прежде чем перейти к описанию концепции и ее программной реализации, рассмотрим некоторые дополнительные аспекты.

Квантовое распределение ключей

При рассмотрении вопросов квантовой криптографии существенным являются понятия квантовой запутанности и квантовой суперпозиции.

Квантовой запутанностью могут обладать два или более кубита, и она выражается в особой корреляции между ними, которая может быть подтверждена с помощью нарушений неравенства Белла [7].

Квантовая суперпозиция – принцип, описывающий способность кубитов существовать в нескольких состояниях одновременно до момента измерения.

Квантовое распределение ключей как новое решение проблемы распределения в последнее время вызывает большой исследовательский интерес. Оно представляет собой метод безопасного распределения ключей шифрования, использующий свойства квантовой механики. Существует несколько различных протоколов для квантового распределения ключей, каждый из которых имеет свои преимущества и ограничения. Наиболее часто используемыми являются протоколы BB-84, B-92, E-91 и SARG-04. Протокол E-91 основан на квантовой запутанности между двумя сторонами [8].

Доверенным источником (условный *Charlie*) генерируется запутанная пара частиц, квантовое состояние которых характеризуется состояниями Белла, после чего одна частица отправляется по квантовом каналу Алисе, а другая – Бобу (рис. 1).

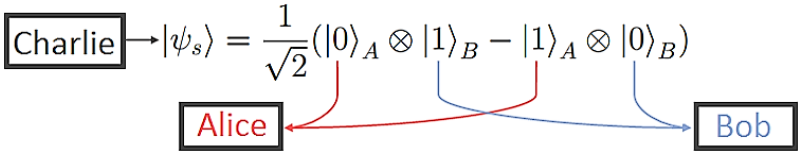

Рис. 1. Схема распределения частиц между Алисой и Бобом

Fig. 1. Diagram of particle distribution between Alice and Bob

Алиса и Боб генерируют строки $b = (b_1, \ldots, b_N)$ и $b' = (b'_1, \ldots, b'_N)$, где $b_i, b'_j = 1,2,3 \ldots$, и в соответствии с элементами этих строк проводят измерение проекции спинов полученных частиц на следующие направления (рис. 2):

$b_i = 1$: $\vec{a}_1 = (1,0,0)$ (X observable), $b'_j = 1$: $\vec{b}_1 = \left(\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)$ (W observable),

$b_i = 2$: $\vec{a}_2 = \left(\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)$ (W observable), $b'_j = 2$: $\vec{b}_2 = (0,0,1)$ (Z observable),

$b_i = 3$: $\vec{a}_3 = (0,0,1)$ (Z observable), $b'_j = 3$: $\vec{b}_3 = \left(-\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)$ (V observable).

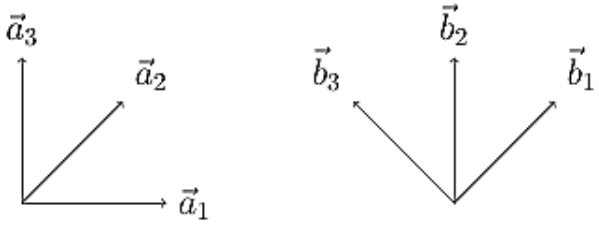

Рис. 2. Направления измерения проекций спинов в протоколе E-91

Fig. 2. Directions for measuring spin projections in the E-91 protocol

Из результатов измерений участники формируют строки $a = (a_1 \ldots a_N)$ и $a' = (a'_1 \ldots a'_N)$, где $a_i, a'_j = \pm 1$ (рис. 3).

Bit Number	1	2	3	4	5	6
Alice's random bases	×	×	+	+	×	+
Alice's observations	↗	↖	→	↑	↗	→
Bob's random bases	×	+	+	×	×	+
Bob's observations	↗	→	→	↗	↗	→

Рис. 3. Измерения Алисы и Боба в случайно выбранных ими базисах

Fig. 3. Alice and Bob's measurements in randomly chosen bases

Далее Алиса и Боб по классическому каналу связи сравнивают базисы, в которых проводили измерения состояний частиц, т. е. строки $b = (b_1 \dots b_N)$ и $b' = (b'_1 \dots b'_N)$ (рис. 4).

Bit Number	1	2	3	4	5	6
Alice's random bases	×	×	+	+	×	+
Public channel	⇳	⇳	⇳	⇳	⇳	⇳
Bob's random bases	×	+	+	×	×	+
Agree	✓		✓		✓	✓

Рис. 4. Сравнение по открытому каналу связи базисов измерений

Fig. 4. Comparison of measurement bases over an open communication channel

Из элементов строк a и a', полученных после измерения проекций спинов на одно и то же направление, Алиса и Боб получают ключ. Участники знают, что выполняется выражение (1) и уверены, что получают противоположные результаты измерений, т. е. $a_k = -a'_k$:

$$\langle (\vec{a} \cdot \vec{\sigma})_A \otimes \left(\vec{b} \cdot \vec{\sigma}\right)_B \rangle_{\rho_s} = -\vec{a} \cdot \vec{b}. \quad (1)$$

В отличие от протокола BB-84, результаты измерений проекций спинов частиц на разные направления используются для вычисления корреляционного значения, определяемого выражением

$$\langle X \otimes W \rangle_{\rho_s} - \langle X \otimes V \rangle_{\rho_s} + \langle Z \otimes W \rangle_{\rho_s} + \langle Z \otimes V \rangle_{\rho_s} = -2\sqrt{2}. \quad (2)$$

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.

Одной из особенностей данного протокола является то, что источник запутанных пар частиц, который распределяет кубиты между Алисой и Бобом, может быть в распоряжении у третьей стороны, в том числе и необязательно доверенной. Таким образом, даже если оборудование, которое создает запутанные состояния, принадлежит злоумышленнику, это не даст последнему никаких преимуществ при подслушивании. Протокол рассматривается как перспективный с точки зрения повышения безопасности распределения ключей, поскольку позволяет не только генерировать секретный ключ, но и проводить внутреннюю проверку целостности канала связи.

Интеграция квантовой запутанности в архитектуру блокчейна

Блокчейн – это децентрализованная распределенная база данных, реализуемая в виде последовательной и криптографически связанной цепочки блоков. Каждый блок содержит записи транзакций и связан с предыдущим посредством криптографического хеш-функционала, что обеспечивает неизменяемость и верифицируемость всей истории данных. Формально структура блока в классической реализации включает следующие элементы [9]:

данные – полезная нагрузка блока, содержащая информацию о транзакциях или событиях;

временную метку – время создания блока;

хеш предыдущего блока (криптографический хеш блока (H(N–1))) – классический SHA-256-хеш блока (N–1), обеспечивающий базовую связность и обнаружение изменений;

E91 MAC – код аутентификации хеш-значения предыдущего блока.

Механизм E91 MAC является комбинацией метода криптографической аутентификации HMAC (Hash-based Message Autentification Code) и протокола квантового распределения ключей E-91. Для обеспечения целостности и конфиденциальности данных в блокчейне механизм генерации значения E91 MAC использует как криптографическую хеш-функцию, так и общий секретный ключ, сгенерированный посредством симуляции протокола квантового распределения ключей E91;

хеш текущего блока H(N) – классический SHA-256-хеш, вычисленный из совокупности всех остальных полей блока N, включая E-91 MAC.

Безопасность блокчейна определяется, с одной стороны, стойкостью применяемых криптографических алгоритмов (например, SHA-256, ECDSA), а с другой – надежностью используемых децентрализованных механизмов достижения консенсуса между узлами. Однако развитие квантовых вычислительных технологий создает потенциальные угрозы, которые могут существенно снизить эффективность и надежность данных компонентов. В связи с этим возникает необходимость в создании новых архитектур, где безопасность обеспечивается не только за счет математической сложности, но и за счет фундаментальных физических свойств квантовых систем. Одним из таких свойств является *квантовая запутанность* – явление, при котором квантовые состояния двух или более частиц оказываются неразрывно коррелированными независимо от расстояния между ними.

Разработанная концепция

В данной работе авторами предлагается новая концепция безопасной связи блоков, в рамках которой в классическую структуру блока добавляется дополнительное поле – E91 MAC. Это поле представляет собой результат выполнения алгоритма HMAC, примененного к хешу предыдущего блока. Принципиальной особенностью данного подхода является способ генерации ключа, используемого в HMAC [8, 10]. Ключ формируется не классическими средствами, а с помощью протокола квантового распределения ключей E91, основанного на механизме квантовой запутанности и проверке неравенства Белла в форме CHSH.

Таким образом, сообщением для HMAC служит условный SHA-256-хеш предыдущего блока H(N–1), а ключом – безопасно сгенерированный при помощи протокола E91 секретный ключ K. Ключ может быть использован для шифрования только в случае успешного прохождения CHSH-теста, подтверждающего наличие истинной квантовой запутанности и, следовательно, отсутствие прослушивания. Это позволит не только усилить доверие к корректности вычисленного значения E91 MAC, но и ввести новый уровень проверки подлинности и целостности. Валидаторы, обладающие доступом к тому же ключу K, могут независимо пересчитать и верифицировать значение E91 MAC, удостоверившись, что блок был создан авторизованной стороной и не был модифицирован.

Формирование целостной цепочки блоков

Определяется хеш предыдущего блока H(N–1):

1. Выполняется симуляция протокола квантового распределения ключей E91 для генерации уникального ключа K. Если генерация неуспешна (провалена проверка неравенства Белла в форме CHSH (11)), создание блока прерывается.

2. От хеш-значения предыдущего блока с применением секретного ключа K, сгенерированного на предыдущем этапе, вычисляется E91 MAC. Используется, например, стандартный HMAC-SHA256.

3. Проверяется, соответствует ли H(N–1) хешу реально существующего и валидного предыдущего блока.

4. Валидатор, имеющий безопасный доступ к ключу K, который был использован при создании этого блока, сравнивает исходное значение E91 MAC, хранящееся в блоке, с вычисленным лично.

5. Если “E91MAC_origin” = “E91MAC_calculated”, валидатор может быть уверен в следующем:

– целостность данных транзакции, хеша предыдущего блока H(N–1) и ключа K не нарушена;

– создание транзакции и блока инициировано тем, кто владеет ключом K (аутентификация).

6. Формируется тело блока, включающее:

– данные о транзакциях;

– временную метку;

– хеш предыдущего блока H(N–1);

– E91 MAC;

– хеш текущего блока H(N) от всего содержимого.

Роль квантовой запутанности в концепции

Безопасная связь блоков: в разработанной концепции аутентификация опирается не только на секретность ключа K, но и на гарантии безопасности самого процесса генерации этого ключа, основанные на запутанности. Попытка получить K через подслушивание была бы обнаружена благодаря свойствам запутанности (через CHSH-тест). Это отличает данный подход от использования ключей, распределенных классическими методами, которые могут быть уязвимы к подслушиванию без обнаружения, или асимметричными методами, уязвимыми к квантовым компьютерам.

Следовательно, хотя предложенный блокчейн является гибридной системой и использует симуляцию, его концептуальная основа безопасности в части связывания блоков непосредственно связана с квантовой запутанностью через протокол E91.

Важно четко определить, почему предложенная концепция может быть охарактеризована как «квантовая» несмотря на то, что основная структура и обработка данных выполняются на классических компьютерах в рамках симуляции.

Фундаментальная роль запутанности: «квантовая черта» концепции проистекает из интеграции симулированного протокола квантового распределения ключей E91 в ме-

ханизм обеспечения безопасности. Другими словами, безопасность ключа K, используемого для защиты связи между блоками, в протоколе E91 напрямую основана на квантовой запутанности.

Проверка неравенства Белла как индикатор запутанности: проверка нарушения неравенства CHSH, являющаяся неотъемлемой частью протокола E91 в предложенной концепции, – это прямой способ убедиться в наличии сильных квантовых корреляций, свойственных запутанности. Провал данного теста в симуляции интерпретируется как обнаружение атаки, предотвращая использование скомпрометированного ключа для защиты связи блоков.

Ключевые особенности концепции

Концептуальное усиление безопасности: добавляет дополнительный уровень защиты к хеш-цепочке, основанный на принципах квантового распределения ключей, устойчивых (теоретически) к подслушиванию.

Обнаружение вмешательства при генерации ключа: интегрированный (симулированный) тест CHSH позволяет обнаруживать попытки компрометации ключа K во время его генерации.

Перспективная устойчивость: хотя сам HMAC и хеш остаются классическими, безопасность ключа, используемого в E91 MAC, опирается на квантовые принципы, потенциально более устойчивые к будущим угрозам, чем классическое распределение ключей.

Алгоритмы консенсуса

Алгоритмы консенсуса блокчейна представляют собой совокупность принципов и правил, благодаря которым все участвующие в сети узлы (ноды) автоматически приходят к консенсусу, т. е. обеспечивается как безопасность сети, так и достоверность всех хранящихся в ней данных.

С учетом стремительного развития квантовых вычислений становится очевидным, что использование вычислительной мощности в качестве средства достижения консенсуса, как это реализовано, например, в алгоритме PoW (Proof of Work), представляется нецелесообразным для блокчейн-систем, устойчивых к квантовым атакам. У альтернативных механизмов консенсуса, не зависящих от ресурсоемких решений, можно выделить, например, DPoS, который представляет собой алгоритм, ориентированный на демократическое управление сетью и обеспечение высокой производительности без использования интенсивных вычислений [9]. Он является модификацией алгоритма PoS (Proof of Stake), в котором владельцы цифровых активов голосуют за делегатов (валидаторов), наделенных правом создания и верификации блоков. Алгоритм консенсуса DPoS устраняет необходимость решения сложных криптографических задач, что способствует снижению энергопотребления и повышению масштабируемости сети.

Алгоритм консенсуса DPoS, таким образом, обоснован как приоритетный для использования в защищенных распределенных реестрах нового поколения.

Разработанный алгоритм интеграции квантовой запутанности

Этапы разработанного алгоритма сводятся к следующему [10]:

1. Привести ключ, сгенерированный протоколом E91, к размеру блока соответствующей хеш-функции H.

2. Разбить сообщение M (в рассматриваемом случае хеш-значение предыдущего блока) на блоки размером b байт.

3. Склеить строку (последовательность байт) $K_0 \oplus opad$ с каждым блоком сообщения M:

opad (outer padding (внешний наполнитель): константа 0x5C, повторяемая до длины блока хеш-функции.

4. К строке, полученной на предыдущем шаге, применить хеш-функцию H.

5. Склеить строку $K_0 \oplus opad$ со строкой, полученной от хеш-функции H на предыдущем шаге:

ipad (inner padding, внутренний наполнитель): константа 0x36, повторяемая до длины блока хеш-функции (например, 64 байта для SHA-256).

6. К строке, полученной на предыдущем шаге, применить хеш-функцию H.

Полученное алгоритмом HMAC значение вносится как новое поле блока E91 MAC, создание которого и инициирует один из узлов.

Валидатор, имеющий безопасный доступ к ключу K, который был использован при создании этого блока, пересчитывает ожидаемое значение E91 MAC с помощью того же алгоритма. Если E91 MAC исходный совпадает с E91 MAC вычисленным, то валидатор может быть уверен в следующем:

– целостность данных транзакции хеш-значения предыдущего блока H(N–1) ключа K не нарушена;

– создание транзакции и блока инициировано тем, кто владеет ключом K (аутентификация).

Элементы программной реализации интеграции квантовой запутанности в архитектуру блокчейна

Программная реализация PoC (Proof of Concept) представляет собой доказательство осуществимости концепции, т. е. демонстрирует практическую осуществимость интеграции квантовой запутанности в прототип одноранговой (*peer-to-peer*) блокчейн-сети.

В данной работе архитектура блокчейна реализована на языке программирования Python с использованием TCP-сокетов, т. е. узлы сети обмениваются данными по локальной сети через соединения, установленные по протоколу TCP (Transmission Control Protocol). Протокол TCP отвечает за транспортировку и маршрутизацию данных через сетевую архитектуру и обеспечение их доставки определенным узлам, указанным IP. Реализованный прототип демонстрирует принципы децентрализованного взаимодействия узлов, автоматического восстановления сети и базовой реализации блокчейна.

В рамках расширения функциональности прототипа децентрализованной блокчейн-сети было принято решение внедрить механизм консенсуса DPoS.

Компьютерная программа организована следующим образом:

blockchain – управляет цепочкой блоков, включая добавление новых блоков и валидацию цепи;

transaction – описывает транзакцию между участниками сети;

server – отвечает за прием входящих соединений от клиентов и управление списком подключенных узлов;

client – обеспечивает подключение к серверу и взаимодействие пользователя с сетью;

superpeer – объединяет функциональность клиента и сервера, выступая в роли центрального узла при отсутствии других суперузлов;

peer – представляет обычный узел сети, функционирующий как клиент.

Для реализации сетевых соединений в проекте используются модули socket и hashlib для вычисления хешей при создании блоков и, следовательно, для обеспечения целостности данных.

Сеть функционирует по следующему алгоритму:

1. При запуске программа пытается подключиться к суперузлу, выполняющему функции как клиента, так и сервера, адрес которого хранится в файле *server_tracker.txt*.

2. Если подключение успешно, узел функционирует как клиент (peer).

3. Если подключение не удалось (например, суперузел недоступен), узел становится суперузлом (superpeer) и записывает свой адрес в *server_tracker.txt*, чтобы другие узлы могли к нему подключиться.

Обработка подключений: серверная часть каждого суперузла ожидает входящих соединений от клиентов. При подключении нового клиента сервер добавляет его в список активных узлов и рассылает обновленный список всем участникам сети. Это позволяет каждому узлу иметь актуальную информацию о структуре сети и поддерживать соединения с другими участниками.

Распространение данных: все данные, включая новые транзакции и блоки, передаются между узлами посредством обеспечения синхронизации состояния блокчейна между всеми участниками сети.

Такой подход обеспечивает децентрализацию и устойчивость сети: при отключении текущего суперузла один из клиентов автоматически берет на себя его роль, предотвращая остановку всей сети.

Программная реализация протокола E91

Реализация протокола E91 представляет собой компьютерное моделирование его выполнения на симуляторе квантовых вычислений и на квантовых устройствах компании IBM с использованием Qiskit (Quantum information software kit).

Qiskit – это набор средств разработки с открытым исходным кодом для работы с квантовыми устройствами облачной платформы IBM Q в OpenQASM-языке, созданном для взаимодействия с IBM Q и позволяющем экспериментировать с квантовыми схемами, в виде которых удобно представлять последовательность операций над *q*-битами.

IBM Quantum Platform – облачная платформа, которая предоставляет возможность работы на квантовом компьютере. Устройства построены на сверхпроводящих *q*-битах, работа которых основана на эффекте Джозефсона: между сверхпроводниками, разделенными тонким слоем диэлектрика, течет ток. С помощью этого набора можно писать, компилировать и запускать программы на различных устройствах и симуляторах. Кроме того, в Qiskit встроен симулятор, которым можно пользоваться без подключения к облачной платформе IMB Q. Он позволяет моделировать выполнение квантовых вычислений с присутствием шумов, которые возникают при работе реальных устройств. Qiskit служит связующим звеном между пользователем и квантовыми устройствами IBM Q. Набор

использует язык Python. Это значит, что пользователь может манипулировать реальными или симулированными *q*-битами и при этом применять все возможности языка Python для каких-либо промежуточных вычислений и операций.

Заключение

В исследовании разработана и программно реализована концептуальная модель квантово-защищенного блокчейна, в которой в классическую архитектуру интегрирован механизм квантового распределения ключей на основе протокола E91.

Принципиальным отличием предложенной модели является включение в классическую структуру блока поля E91 MAC, вычисляемого от хеш-значения предыдущего блока с помощью ключа, полученного протоколом E91, и алгоритма HMAC. Комбинация этого алгоритма и проверки неравенств Белла (CHSH) для генерации и аутентификации секретного ключа обеспечивает криптографическую проверку подлинности. Такая интеграция дает дополнительный уровень безопасности – не основанный на вычислительной сложности, а вытекающий из физических законов квантовой механики.

В работе обоснован выбор и предложен механизм консенсуса DPoS, реализованный в рамках одноранговой блокчейн-сети на языке программирования Python с использованием TCP-сокетов. Пользователю предоставляется CLI-интерфейс, позволяющий проводить транзакции, участвовать в голосовании за делегатов и инициировать создание блоков. Каждый блок содержит не только данные транзакций и хеши, но и поле E91 MAC, подтверждающее подлинность предыдущего блока на основе квантово-сгенерированного ключа.

Программная реализация симуляции протокола E91 с использованием облачной платформы IBM Quantum Platform и библиотеки Qiskit и интеграция DPoS в архитектуру блокчейна с CLI-интерфейсом и функционалом распределенного голосования продемонстрировали принципиальную осуществимость концепции.

Вклад авторов. *А. В. Сидоренко* осуществила сбор, анализ и оформление результатов работы и подготовила окончательный вариант статьи. *И. А. Приходько* предложил концепцию работы и реализовал компьютерную программу, объединив свойства квантовой запутанности и классических компьютерных методов.

Список использованных источников

1. Звозникова, Г. А. Обзор алгоритмов технологии блокчейн / Г. А. Звозникова // Теория и практика современной науки. – 2020. – № 5 (59). – С. 187–190.

2. Сидоренко, А. В. Алгоритм хеширования на основе SHA-3 с использованием хаотических отображений / А. В. Сидоренко, М. С. Шишко // Информатика. – 2020. − Т. 17, № 1. – С. 109–118. – https://doi.org/10.37661/1816-0301-2020-17-1-109-118.

3. Quantum-secured blockchain / E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev [et al.]. – 2018. – URL: https://arxiv.org/pdf/1705.09258 (date of access: 13.03.2026).

4. Belkhir, M. Quantum vs classic computing: a comparative analysis / M. Belkhir, H. Benkaouha, E. Benkhelifa // Proc. of Seventh Intern. Conf. on Fog and Mobile Edge Computing (FMEC), Paris, France, 12–15 Dec. 2022. – Paris, 2022. – P. 1–8. – https://doi.org/10.1109/FMEC57183.2022.10062753.

5. Сидоренко, А. В. Квантовое распределение ключа в квантовой криптографии / А. В. Сидоренко, И. А. Приходько // Военная безопасность государства в современных условиях : тез. докл. Междунар.

воен.-науч. конф. учреждения образования «Военная академия Республики Беларусь», Минск, 24–25 апр. 2024 г. – Мн. : Военная академия Республики Беларусь, 2024. – С. 535.

6. Nguyen, G. T. A survey about consensus algorithm used in Blockchain / G. T. Nguyen, K. Kim // Journal of Information Processing Systems. – 2018. – Vol. 14. – P. 101–128.

7. The Physics of Quantum Information: Quantum Criptography, Quantum Teleportation, Quantum Computation / ed.: D. Bouwmeetster [et al.]. – Berlin : Springer, 2000. – 350 p.

8. Artur, K. A quantum cryptography based on Bell's theorem / K. Artur, A. Ekert // Physical Review. – 1991. – Vol. 67. – P. 661–663.

9. Приходько, И. А. Компьютерная программа для квантового распределения ключей / И. А. Приходько // Материалы XIII Межвуз. науч.-техн. конф. курсантов и магистрантов факультета связи и автоматизированных систем управления, Минск, 22 мая 2024 г. – Мн. : Военная академия Республики Беларусь, 2024. – С. 22.

10. Сидоренко, А. В. Квантовое распределение ключей и алгоритмы консенсуса при квантовом шифровании / А. В. Сидоренко, И. А. Приходько // Технические средства защиты информации : материалы XXIII Междунар. науч.-техн. конф., Минск, 8 июня 2025 г. – Мн. : БГУИР, 2025. – С. 289–292.

References

1. Zvoznikova G. A. *Survey of technology algorithms blockchain*. Teorija i praktika sovremennoj nauki [*The Theory and Practice of Modern Science*], 2020, no. 5 (59), pp. 187–190 (In Russ.).

2. Sidorenko A. V., Shishko M. S. Hashing technique based on SHA-3 using chaotic maps. *Informatics*, 2020, vol. 17, no. 1, pp. 109–118 (In Russ.). http://doi.org/10.37661/1816-0301-2020-17-1-109-118.

3. Kiktenko E. O., N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, …, Fedorov A. K. *Quantum-secured blockchain*, 2018. Available at: https://arxiv.org/pdf/1705.09258 (accessed 13.03.2026).

4. Belkhir M., Benkaouha H., Benkhelifa E. Quantum vs classic computing: a comparative analysis. *Proceedings of Seventh International Conference on Fog and Mobile Edge Computing (FMEC), Paris, France,* 12–15 December 2022. Paris, 2022. https://doi.org/10.1109/FMEC57183.2022.10062753.

5. Sidorenko A. V., Prihodko I. A. *The quantum of distribution keys in quantum cryptography*. Voennaja bezopasnost' gosudarstva v sovremennyh uslovijah: tezisy dokladov Mezhdunarodnoj voenno-nauchnoj konferencii uchrezhdenija obrazovanija «Voennaja akademija Respubliki Belarus'», Minsk, 24–25 aprelja 2024 g. [*The Military of State Safety in Modern Conditions: Abstracts of Reports of International Military-sciensies Conference of "Military Academy of Belarus", Minsk, 24–25 April 2024*]. Minsk, Voennaja akademija Respubliki Belarus', 2024, p. 535 (In Russ.).

6. Nguyen G. T., Kim K. A survey about consensus algorithm used in Blockchain. *Journal of Information Processing Systems*, 2018, vol. 14, pp. 101–128.

7. Bouwmeetster D., Ekert A., Zeilinger A. (eds.). *The Physics of Quantum Information: Quantum Criptography, Quantum Teleportation, Quantum Computation*. Berlin, Springer, 2000, 350 p.

8. Artur K., Ekert A. A quantum cryptography based on Bell's theorem. *Physical Review*, 1991, vol. 67, pp. 661–663.

9. Prihodko I. A. *The computer program for quantum of distribution keys*. Materialy XIII Mezhvuzovskoj nauchno-tehnicheskoj konferencii kursantov i magistrantov fakul'teta svjazi i avtomatizirovannyh sistem upravlenija, Minsk, 22 maja 2024 g. [*The Materials of XIII Young Science-technical Conference of Military Students and Magistrants of Connection and Automatic System of Management Faculty, Minsk, 22 May 2024*]. Minsk, Voennaja akademija Respubliki Belarus', 2024, p. 22 (In Russ.).

10. Sidorenko A. V., Prihodko I. A. *The quantum of distribution keys and algorithms of consensus for quantum encryption*. Tehnicheskie sredstva zashhity informacii: materialy XXIII Mezhdunarodnoj nauchno-tehnicheskoj konferencii, Minsk, 8 ijunja 2025 g. [*The Technical Means of Information Defence: Materials of XXIII International Science-technical Conference, Minsk, 8 July 2025*]. Minsk, Belorusskij gosudarstvennyj universitet informatiki i radiojelektroniki, 2025, p. 289–292 (In Russ.).

Информация об авторах

Сидоренко Алевтина Васильевна, доктор технических наук, профессор, Белорусский государственный университет.
E-mail: sidorenkoa@yandex.by

Приходько Иван Андреевич, студент, Белорусский государственный университет.
E-mail: prikhodko@bsu.by

Information about the authors

Alevtina V. Sidorenko, Dr. Sci. (Eng.), Prof., Belarusian State University.
E-mail: sidorenkoa@yandex.by

Ivan A. Prikhodko, Student, Belarusian State University.
E-mail: prikhodko@bsu.by