УДК 004.93

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ШИФРОВАНИЯ, АУТЕНТИФИКАЦИИ И ПРИВАТНОСТИ В КОНТЕКСТЕ БЛОКЧЕЙН-ТЕХНОЛОГИЙ

Макаренко Е.Н.

студент,

Институт сферы обслуживания и предпринимательства (филиал) ДГТУ в г. Шахты,

Шахты, Россия

Клейменкин Д.В.

ассистент,

Институт сферы обслуживания и предпринимательства (филиал) ДГТУ в г. Шахты,

Шахты, Россия

Аннотация

Данная статья посвящена исследованию механизмов шифрования, аутентификации и приватности применения технологии блокчейн. Обеспечение безопасности и конфиденциальности данных, хранящихся в блокчейне является проблемой. Рассматриваются различные методы шифрования, такие как шифрование с симметричным ключом и шифрование с открытым ключом, их применение для защиты данных и т.д. Методы аутентификации также будут изучены для обеспечения целостности и подлинности транзакций. Уделяется внимание вопросам конфиденциальности, поскольку блокчейн делает транзакции и данные полностью прозрачными и доступными для всех пользователей сети. В технологиях блокчейна рассматривались различные методы анонимности.

Ключевые слова: блокчейн, шифрование, аутентификация, приватность, безопасность данных.

RESEARCH OF ENCRYPTION, AUTHENTICATION AND PRIVACY MECHANISMS IN THE CONTEXT OF BLOCKCHAIN TECHNOLOGIES

Makarenko E.N.
student,
Institute of Service and Entrepreneurship (branch) of DSTU in Shakhty,
Shakhty, Russia
Kleimenkin D.V.
assistant,
Institute of Service and Entrepreneurship (branch) of DSTU in Shakhty,
Shakhty, Russia

Abstract

This article is devoted to the study of the mechanisms of encryption, authentication and privacy of the use of blockchain technology. Ensuring the security and confidentiality of data stored in the blockchain is a problem. Various encryption methods are considered, such as symmetric key encryption and public key encryption, their use for data protection, etc. Authentication methods will also be studied to ensure the integrity and authenticity of transactions. Attention is paid to privacy issues, since blockchain makes transactions and data completely transparent and accessible to all network users. Various methods of anonymity have been considered in blockchain technologies.

Keywords: blockchain, encryption, authentication, privacy, data security.

Блокчейн – это децентрализованная база данных, являющаяся основой для криптовалют, смарт-контрактов, логистики, финансовых услуг и других различных областей его применения. Технология блокчейн основывается на шифровании, хранении данных и поддержании их целостности.

Шифрование блокчейна предотвращает попадание конфиденциальной информации в чужие руки или ее подделки.

В таблице 1 приведены механизмы, используемые для шифрования.

Таблица 1 – Механизмы шифрования

Метод	Использование
Криптография с открытым ключом или асимметричная криптография	Это область криптографических систем, которые применяют пару связанных криптографических ключей: – открытый ключ (можно открыто делиться); – закрытый ключ (находиться только у владельца).
Цифровая подпись	Создается с использованием криптографии с открытым ключом. Применяется для проверки подлинности и целостности данных. Цифровая подпись связывается с каждой транзакцией или блоком, с помощью чего блокчейн гарантирует, что отправитель является подлинным и данные не подделаны.
Хеш-функция	Математический алгоритм, преобразующий входные данные (сообщение) в выходные данные фиксированного размера. Применяется для защиты данных внутри блоков, так как каждый блок, включает в себя хеш-значение предыдущего блока и связывает их вместе. При любых изменениях данных внутри блоков произойдет изменение хеш-значения, это упрощает выявление несанкционированного доступа.
Дерево Меркла	Двоичное дерево, в качестве листьев которого выступают хеши транзакций, а внутренними вершинами являются хеши, полученные на основе объединения информации дочерних узлов. Применяется для проверки включена ли транзакция или фрагмент данных в блок. Обеспечивает быстрый и безопасный способ проверки больших объемов данных.
Симметричное шифрование	Предназначено для защиты сетевых подключений, связи узлами и хранения конфиденциальной информации. Для шифрования и дешифрования между отправителем и получателем использует общий ключ

Стоит отметить, что механизмы шифрования являются основой всего блокчейна и варьируются в зависимости от реализации блокчейна и используемого алгоритма. Исходя из потребностей различные платформы

имеют возможность использовать дополнительные или модифицированные методы шифрования.

Аутентификация в технологии блокчейн – это безопасный метод проверки пользователей в сети. Она повышает безопасность и прозрачность транзакций, используя криптографические ключи и цифровые подписи.

Примеры аутентификации на блокчейне:

– финансовые транзакции;

– здравоохранение;

– кибербезопасность;

– цепочка поставок;

– личная идентификация.

Принцип работы заключается в следующем. При подтверждении личности пользователю приходится генерировать пару ключей. Закрытый ключ используется для подписи транзакций и находится в секрете, а открытый ключ является доступным для остальных.

Когда пользователю нужно получить доступ к сервису или выполнить транзакцию, он ставит подпись своим закрытым ключом. Создается уникальная цифровая подпись для данного пользователя и транзакции. Далее транзакция транслируется в сеть.

Транзакция проверяется сетью узлов в сети блокчейн путем проверки цифровой подписи с использованием открытого ключа. После проверки подпись действительна значит узел добавит транзакцию в новый блок, каждый новый блок связан с предыдущим, создавая цепочку блоков. Блокчейн-аутентификация защищена и устойчива ко взлому и мошенничеству, так как историю транзакций подделать довольно трудно.

Двухфакторная аутентификация обеспечивает дополнительный уровень безопасности путем добавления еще одного уровня безопасности к уже существующему.

Предполагается, что пользователь вводит имя и пароль, и вместо того, чтобы сразу получить доступ к своей учетной записи, пользователю потребуется ввести еще некоторую информацию: данные карты, аппаратный токен, секретный вопрос, PIN-код или биометрические данные.

Двухфакторная аутентификация выполняется на следующих этапах:

1. Введите имя пользователя и пароль: на этом шаге пользователю предлагается ввести имя пользователя и пароль
2. Проверка имени пользователя и пароля: Имя пользователя и пароль проверяются сервером аутентификации, и если учетные данные верны, то пользователь имеет право на аутентификацию второго фактора.
3. Аутентификация со вторым фактором: на этом этапе пользователь введет данные в соответствии с выбранным вторым механизмом аутентификации.
4. Проверка аутентификации второго фактора: сервер аутентификации проверит дополнительную информацию аутентификации, предоставленную устройством второго фактора, и подтвердит личность пользователя.

Аутентификация на блокчейне является лучшим решением для удовлетворения растущей потребности в безопасных, прозрачных и эффективных транзакциях в современном цифровом мире.

Конфиденциальность в блокчейн-техологиях является важнейшей проблемой, потому что блокчейн предназначен для прозрачности и неизменности. Он использует криптографию для защиты транзакций и гарантирует, что защита конфиденциальности обеспечена.

Блокчейн использует псевдонимы, что означает, что участники идентифицируются по криптографическим адресам, а не по их реальным личностям. Это обеспечивает уровень конфиденциальности, уменьшая напрямую связь между отдельными лицами и их транзакциями.

Для повышения конфиденциальности в блокчейне разрабатываются и внедряются различные методы, такие как кольцевые подписи и доказательства

с нулевым разглашением, что позволяет проверять транзакции без раскрытия фактических данных.

Некоторые приложения для обработки транзакций или данных используют автономные решения, что снижает видимость конфиденциальной информации в основном блокчейне.

Для того, чтобы ограничить воздействие в блокчейне должна находиться только необходимая информация, а все остальные конфиденциальные данные могут храниться вне цепочки.

Достижение конфиденциальности в блокчейн-технологиях является весьма сложной задач. Для решения этой проблемы предпринимаются усилия по разработке новых методов и решений.

Таким образом, были исследованы механизмы шифрования; рассмотрены принципы работы аутентификации и приведены ее примеры на блокчейне; проанализирована важность конфиденциальности в блокчейн-технологиях.

Библиографический список:

1. Генкин А.С. Блокчейн. Как это работает и что ждет нас завтра / А. С. Генкин. – М.: Альпина Паблишер. – 2018. - 874 с.

2. Лелу Лоран. Блокчейн от А до Я. Все о технологии десятилетия / Лоран Лелу. – М.: Эксмо, 2017. – 556 с.

3. Молдовян Н.А. Криптография: от примитивов к синтезу алгоритмов / Н. А. Молдовян, А. А. Молдовян, М. А. Еремеев. – М.: СПб: БХВ, 2004. – 448 с.

4. Рассел Джесси Единая система идентификации и аутентификации / Джесси Рассел. – М.: VSD, 2013. – 950 с.

5. Фурасов В. Д. Задачи гарантированной идентификации / В. Д. Фурасов. – Москва: Гостехиздат, 2005. – 152 с.

Оригинальность 75%