УДК 004.056.5;004.75

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИСПОЛЬЗУЕМЫЕ В ТЕХНОЛОГИИ БЛОКЧЕЙН

А.Н. Гайдук

Белорусский государственный университет,
пр. Независимости, 4, 220030, г. Минск, Беларусь, gaidukan@bsu.by

Представлены криптографические методы защиты информации, используемые в технологии блокчейн, являющиеся фундаментальной основой его безопасности. Указаны перспективные направления криптографических исследований в области технологии блокчейн.

***Ключевые слова*:** Блокчейн; криптография; криптографические методы защиты информации.

CRYPTOGRAPHIC METHODS OF INFORMATION PROTECTION USED IN BLOCKCHAIN TECHNOLOGY

A.N. Gaiduk

Belarusian State University, 4 Niezalieznasci Avenue, Minsk 220030, Belarus,
gaidukan@bsu.by

Cryptographic methods of information protection used in blockchain technology, which are the fundamental basis of its security, are presented. Promising areas of cryptographic research in the field of blockchain technology are indicated.

***Keywords*:** Blockchain; cryptography; cryptographic methods of information protection.

Введение

С момента своего появления технология блокчейн привлекла большое внимание как со стороны научных кругов, правительства, так и бизнеса [1]. Распределенный и децентрализованный характер технологии блокчейна обеспечивает устойчивый к несанкционированному доступу контроль над общим регистром данных. Сегодня технология блокчейн находит широкий спектр применения в различных областях, помимо криптовалют (см., например, [2]). При этом возникает много исследовательских проблем касающихся как безопасности технологии блокчейн, так и ее масштабируемости, и эффективности. Эти проблемы возникают из-за структуры сети и лежащих в ее основе механизмов консенсуса, а также используемых криптографических методов защиты информации.

Поскольку криптография – это обширная область исследований, всегда есть возможность найти новые криптографические методы, чтобы улучшить существующие решения в технологии блокчейн. В данной работе выделены основные методы криптографической защиты информации, используемые в технологии блокчейн, а также указаны перспективные направления криптографических исследований в области технологии блокчейн.

1. Методология исследования / теоретические основы

В последние годы количество публикаций, связанных с технологией блокчейна стремительно растет. Для того чтобы определить множество допустимых статей для анализа была использована методология исследования, которая определяет стратегию поиска соответствующих публикаций, процедуру первичного отбора, критерии включения и исключения, и метод сбора данных для накопления соответствующих публикаций. Чтобы найти соответствующие публикации для нашего исследования, были использованы следующие строки поиска (cryptography) AND (blockchain), (криптография) AND (блокчейн). Поиск осуществлялся через поисковые системы Google и Яндекс. Также проводился поиск в базах данных: 1) Архив eprint IACR, 2) IEEE Xplore, 3) ACM Digital Library 4) ScienceDirect 5) Springer Link.

После процедуры первичного отбора к публикациям применялись критерии включения и исключения, которые определяли соответствие публикации данному исследованию.

2. Результаты и их обсуждение

Структура данных блокчейна представляет собой связанный список, в котором в качестве указателя используется хэш-указатель. Структурной единицей такого списка является блок, который содержит «хэш-указатель» на предыдущий блок и некоторые «данные». Последовательность таких блоков образует цепочку (список), где каждый блок содержит хэш-указатель на предыдущий блок. Хэш-значение предыдущего заголовка блока включается в следующий блок в качестве ссылки, и поэтому изменение даже одного символа в одной из транзакций сделает ссылку недействительной. Данная цепочка (список) и называется блокчейном. Основное различие между блокчейном и связанным списком заключается в том, что ссылки в блокчейне криптографически защищены. Напротив, указатели в связанном списке могут быть изменены в любое время без нарушения целостности данных и, следовательно, может быть изменен по-

рядок следования записей в связанном списке. В блокчейне защищенные ссылки устанавливают порядок следования блоков друг за другом и фактически делают блокчейн структурой данных только для добавления в конец цепочки (списка), т.е. новые данные могут быть добавлены только с новыми блоками. Первый или начальный блок называется блоком генезиса.

Основными криптографическими методами защиты информации, используемыми в технологии блокчейн, являются: хэш-функция, электронная цифровая подпись (ЭЦП), криптографические протоколы доказательства с нулевым разглашением, протоколы конфиденциального вычисления, проверяемая случайная функция. Далее приведем краткое описание применения данных методов криптографической защиты информации в технологии блокчейн.

Определение 1. Хэш-функцией или функцией хэширование называется отображение множества слов произвольной длины в множество слов фиксированной длины:

$$hash: \ \{0,1\}^* \to \{0,1\}^n, \ n \in \mathrm{N}.$$

Используемые в криптографии хэш-функции должны иметь полиномиальную от длины входного слова сложность. В технологии блокчейн хэш-функции используются

- для контроля целостности блоков и транзакций;
- при вычислении адресов участников сети;
- в модели консенсуса;
- при генерации псевдослучайных чисел;
- в алгоритмах ЭЦП.

При конструировании хэш-функций важно учитывать критерии безопасности, которым она должна удовлетворять. Классическими для хэш-функций требованиями являются: стойкость к коллизиям, стойкость к нахождению прообраза, стойкость к нахождению второго прообраза [3].

В технологии блокчейн ЭЦП используются для подписи транзакций, аутентифицируя отправителя и обеспечения контроля целостности транзакции. ЭЦП является одним из наиболее важных криптографических примитивов, благодаря которому блокчейн может быть верифицирован. Наиболее широко используются схемы подписи на основе эллиптических кривых, в частности широко используется алгоритм ЭЦП на эллиптических кривых ECDSA [4]. ECDSA, состоит из трех различных алгоритмов:

- алгоритм генерации ключей;
- алгоритм выработки подписи;
- алгоритма проверка подписи

В блокчейне Биткоина и Ethereum используется эллиптическая кривая известная как кривая Коблица SECP-256k1, которая определена в [5]. В технологии блокчейн также применяются следующие виды подписи:

- мультиподпись;
- слепая подпись;
- подпись на кольце;
- пороговая подпись.

Доказа́тельство с нулевы́м разглаше́нием (информа́ции) в криптографии (англ. Zero-knowledge proof) — интерактивный криптографический протокол, позволяющий одной из взаимодействующих сторон («The verifier» — проверяющей) убедиться в достоверности какого-либо утверждения (обычно математического), не имея при этом никакой другой информации от второй стороны («The prover» — доказывающей). Причём последнее условие является необходимым, так как обычно доказать, что сторона обладает определёнными сведениями в большинстве случаев тривиально, если она имеет право просто раскрыть информацию. Вся сложность состоит в том, чтобы доказать, что у одной из сторон есть информация, не раскрывая её содержание. Доказательства с нулевым разглашением могут быть использованы для обеспечения конфиденциальности данных транзакций в блокчейне. Некоторые блокчейны сети, такие как Zerocoin [6] или Zerocash [7] используют доказательства с нулевым разглашением для того, чтобы транзакции были не отслеживаемыми и их нельзя было соотнести с определенным адресом.

В криптографии протокол конфиденциального вычисления (также безопасное, защищенное или тайное многостороннее вычисление, англ. secure multi-party computation) — криптографический протокол, позволяющий нескольким участникам произвести вычисление, зависящее от тайных входных данных каждого из них, таким образом, чтобы ни один участник не смог получить никакой информации о чужих тайных входных данных. Данный протокол использует блокчейн платформе Enigma [8], в блокчейн Hawki [9] для достижения высокого уровня безопасности, а также позволяет выполнять кроссчейн переводы.

В криптографии проверяемая случайная функция (VRF) — это псевдослучайная функция с открытым ключом, которая обеспечивает доказательства того, что ее выходные данные были вычислены корректно. Владелец секретного ключа может вычислить значение функции, а также соответствующее доказательство для любого входного значения. Используя доказательство и связанный с ним открытый ключ (или ключ проверки), можно проверить, что это значение действительно было рассчитано кор-

ректно, однако эта информация не может быть использована для поиска секретного ключа [10].

Проверяемая случайная функция используется в блокчейнах, основанных на модели консенсуса Proof of Stake [11] для выбора узлов, которые будут публиковать следующий блок и членов комитета по голосованию.

В работе [12] сформулированы следующие исследовательские задачи.

Задача 1. [12] Разработать криптографический протокол, в котором не анонимные пользователи могут публиковать транзакции, которые не могут быть связаны с их сетевыми адресами или другими транзакциями.

Задача 2. [12] Разработать криптографический протокол, в котором не анонимные пользователи могут получать подробную информацию о конкретных транзакциях, не раскрывая, для других участников информацию о том, какие транзакции они ищут.

Задача 3. [12] Разработать эффективные и масштабируемые криптографические протоколы для анонимной публикации в блокчейнах сетях с доступом, требующим разрешения, на основе асинхронных византийскоустойчивых алгоритмов консенсуса для согласования транзакций и процесса смешивания пользовательских данных.

В работе [13] сформулированы следующие исследовательские задачи.

Задача 4. [13] Разработать децентрализованный протокол авторизации для блокчейн сетей с доступом, требующим разрешения, который обеспечит контроль доступа для пользователей.

Задача 5. [13] Разработать модель консенсуса, устойчивой к появлению ветвления в блокчейне.

Задача 6. [13] Разработать устойчивую к кражам блокчейн систему, позволяющую возвращать украденные активы.

Задача 7. [13] Разработать блокчейн систему на основе постквантовой криптографии.

Заключение

Всестороннее исследование базовых криптографических методов защиты информации в технологии блокчейна необходимо для глубокого понимания безопасности и конфиденциальности систем, основанных на технологии блокчейн. В данной работе представлен обзор криптографических методов защиты информации, используемых в технологии блок-

чейн, а также указаны перспективные направления криптографических исследований в области технологии блокчейн.

Библиографические ссылки

1. Paulavi£ius R., Grigaitis S., Igumenov A., and Filatovas E. A decade of blockchain: Review of the current status, challenges, and future directions // Informatica, vol. 30, no. 4, p. 729–748, Jan. 2019.
2. Bodkhe U., Tanwar S., Parekh K., Khanpara P., Tyagi S., Kumar N., and Alazab M. Blockchain for industry 4.0: A comprehensive review // IEEE Access, vol. 8, p. 79764–79800, 2020.
3. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of applied cryptography // CRC Press, 1997.
4. ANSI. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), National Bureau of Standards. ANSI X9.62. 2005. URL: https://standards. globalspec.com/std/1955141/ANSIX9.62.
5. SECG. Recommended Elliptic Curve Domain Parameters. SEC 2 Version 2.0. 2010. URL: https://www.secg.org/sec2-v2.pdf.
6. Miers I., Garman C., Green M., and Rubin A.D. ‘‘Zerocoin: Anonymous distributed e-cash from bitcoin,’’ in Proc. IEEE Symp. Secur. Privacy, May 2013, p. 397–411.
7. Sasson E.B., Chiesa A., Garman C., Green M., Miers I., Tromer E., and Virza M. Zerocash: Decentralized anonymous payments from bitcoin, in Proc. IEEE Symp. Secur. Privacy, May 2014, pp. 459–474.
8. Zyskind G., Nathan O., and Pentland A. Enigma: Decentralized computation platform with guaranteed privacy, 2015, arXiv:1506.03471. [Online]. URL: https://arxiv.org/abs/1506.03471
9. Kosba A., Miller A., Shi E., Wen Z., and Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in Proc. IEEE Symp. Secur. Privacy (SP), May 2016, p. 839–858.
10. Goldberg, Sharon; Vcelak, Jan; Papadopoulos, Dimitrios; Reyzin, Leonid Verifiable Random Functions (VRFs).
11. Blockchain Technology Overview, NIST Technical Series, NISTIR 8202. URL: https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf .
12. Henry R., Herzberg A., and Kate A. Blockchain access privacy: Challenges and directions // IEEE Security Privacy, vol. 16, no. 4, p. 38–45, Jul./Aug. 2018.
13. Raikwar M., Gligoroski D., and Kralevska K. SoK of Used Cryptography in Blockchain // IEEE Access, vol. 7, p. 148550-148575, 2019, doi: 10.1109/ACCESS.2019.2946983.