9. *Kanter I., Kinzel W., and Kanter E.* Secure exchange of information by synchronization of neural networks // Europhys. Lett. 2002. No. 57. P. 141–147.
10. *Klimov A., Mityagin A., and Shamir A.* Analysis of neural cryptography // LNCS. 2002. V. 2502. P. 288–298.
11. *Coutinho M., De Oliveira A. R., Borges F., et al.* Learning perfectly secure cryptography to protect communications with adversarial neural cryptography // Sensors. 2018. No. 18. Article 1306. https://pubmed.ncbi.nlm.nih.gov/29695066/
12. *Abadi M. and Andersen D. G.* Learning to protect communications with adversarial neural cryptography // arXiv:1610.06918. 2016.
13. *Xie P., Bilenko M., Finley T., et al.* Crypto-nets: Neural networks over encrypted data // arXiv:1412.6181. 2014.
14. *Hecht-Nielsen R.* Kolmogorov's mapping neural network existence theorem // IEEE First Annual Int. Conf. on Neural Networks, San Diego, 1987. V. 3. P. 11–13.
15. *Dathathri R., Saarikivi O., Chen H., et al.* CHET: an optimizing compiler for fully-homomorphic neural-network inferencing // Proc. PLDI 2019. N.Y.: ACM, 2019. P. 142–156.
16. *Елисеев В. Л.* Искусственные нейронные сети как механизм обфускации вычислений // Прикладная дискретная математика. Приложение. 2019. № 12. С. 165–169.
17. *Фергюсон Н., Шнайер Б.* Практическая криптография. М.: Диалектика, 2005.

УДК 004.75 DOI 10.17223/2226308X/13/26

МЕТОД СОКРЫТИЯ ПРИВАТНЫХ ДАННЫХ ДЛЯ БЛОКЧЕЙН-СИСТЕМЫ ПРОВЕДЕНИЯ ТЕНДЕРОВ[1]

Д. О. Кондырев

Предложен новый метод, позволяющий решить проблему приватности информации в открытых блокчейн-системах с использованием криптографического протокола доказательства с нулевым разглашением zk-SNARK. Метод реализован в виде криптографической схемы на основе библиотеки libsnark и интегрирован в модифицированный Ethereum C++ клиент.

Ключевые слова: *тендеры, распределённые системы, блокчейн, доказательство с нулевым разглашением, zk-SNARK, платформа Ethereum.*

На сегодняшний день большинство конкурсных закупок и электронных торгов проводятся через специализированные информационные системы. В таких системах участники должны быть уверены в том, что никто не имеет возможности нарушить правила проведения тендера или получить доступ к конфиденциальной информации. Решить проблему доверия при проведении тендеров позволяет блокчейн. Однако при использовании этой технологии все данные сохраняются в открытом виде и доступны всем участникам. В случае с тендерами открытость информации нарушает тайну заявок, которая должна быть сохранена до окончания этапа запроса предложений.

Ранее была разработана блокчейн-система для проведения тендеров с шифрованием заявок [1]. Однако такой подход не позволяет проверить корректность зашифрованной заявки в момент её подачи. Ещё одним недостатком является то, что все участники могут наблюдать факт подачи заявки пользователем.

[1]Работа выполнена при поддержке Математического центра в Академгородке (г. Новосибирск), соглашение с Министерством науки и высшего образования Российской Федерации № 075-15-2019-1613, и Лаборатории криптографии JetBrains Research.

В данной работе предложена и реализована система тендеров, которая удовлетворяет критериям безопасности, открытости и конфиденциальности. Вопрос доверия решён с помощью технологии блокчейн, а сокрытие приватной информации — с помощью криптографического протокола неинтерактивного доказательства знания с нулевым разглашением zk-SNARK [2]. Система основана на платформе Ethereum. Вся ключевая информация о тендерах сохраняется в блокчейне, а проверка правил и отслеживание выполнения условий участниками реализованы в виде кода смарт-контрактов.

Для реализации алгоритма сокрытия информации о заявках в Ethereum C++ клиент добавлен отдельный модуль *tenderzkp*. Он построен на базе протокола zk-SNARK с предобработкой для NP-полного языка системы ограничений ранга 1. Протокол использует эллиптическую кривую Баррето — Наерига. Реализация криптографической схемы предоставлена библиотекой libsnark [3].

В модуле *tenderzkp* реализованы функции создания и верификации доказательства о корректности заявки. Доказательство строится на основе ограничений на приватные и открытые входные данные заявки, выраженных с помощью базовых схем библиотеки libsnark.

Для работы с добавленной криптографической схемой в Ethereum C++ клиент созданы новые предкомпилированные контракты с адресами 0x00...09 и 0x00...0a и разработана Solidity-библиотека, которая инкапсулирует низкоуровневое взаимодействие с предкомпилированными контрактами и предоставляет интерфейс для работы с ними в виде Solidity-функций. Чтобы добавить возможность вызывать методы разработанной криптографической схемы из сторонних приложений, расширен JSON-RPC API Ethereum клиента.

Предложенный метод может быть использован не только для тендеров, но и в других системах, где есть необходимость скрывать часть информации в открытой блокчейн-сети. Он расширяет область применения технологии блокчейн в промышленных программных комплексах.

ЛИТЕРАТУРА

1. *Hardwick F. S., Akram R. N., and Markantonakis K.* Fair and transparent blockchain based tendering framework — A step towards open governance // IEEE Intern. Conf. TrustCom/BigDataSE, New York, USA, 2018. P. 1342–1347.
2. *Ben-Sasson E., Chiesa A., Genkin D., et al.* SNARKs for C: Verifying program executions succinctly and in zero knowledge // CRYPTO'2013. LNCS. 2013. V. 8043. P. 90–108.
3. `https://github.com/scipr-lab/libsnark` — libsnark: a C++ library for zkSNARK proofs.

UDC 004.056 DOI 10.17223/2226308X/13/27

VALIDATION-FREE OFFCHAIN TRANSACTIONS WITH UNLINKABLE DOUBLE SPEND DETECTION

S. N. Kyazhin, K. A. Klimenko

The so-called layer-two protocols are a class of blockchain scaling solutions. They allow to minimize onchain traffic, and therefore make state transitions (payments, for example) faster and more suitable for everyday use, while still preventing double spend attacks. Unfortunately, these solutions also have some downsides and tradeoffs (channel capacity, route availability, operator availability, etc.). In this work we study the possibility of simplifying and improving existing protocols for offchain transactions and describe a scheme that, without transaction validation, allows to detect a double