Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 190 (2021) 471–478

Procedia Computer Science

www.elsevier.com/locate/procedia

2020 Annual International Conference on Brain-Inspired Cognitive Architectures for Artificial Intelligence: Eleventh Annual Meeting of the BICA Society

Privacy methods and zero-knowledge poof for corporate blockchain

Anatoly Konkin*, Sergey Zapechnikov

Institute of Cyber Intelligence Systems, National Research Nuclear University (Moscow Engineering Physics Institute), Kashirskoye shosse 31, Moscow, 115409, Russia

Abstract

Nowadays distributed ledger technology or blockchain is widely used in the corporate sector for various industries. Although implementation issues (coding practice, lack of capabilities, etc.) are not among the major barriers for the technology adaption, there are still some informational security challenges to adjust and scale blockchain networks for corporate usage. One of them is to provide functionality for private transactions stored in a blockchain. Some methods including mix networks, ring signatures, and off-chain protocols were applied to meet the privacy requirements. However, these methods have some limitations associated with the key blockchain characteristics such as decentralized storing system and immutability verification of private data. This article examines zero-knowledge proof (ZKP) methods for corporate blockchain networks. The article provides the review of existing methods for private transactions, discovers the implementation of ZKP methods, also performance and scalability issues are discussed.

Keywords: blockchain; private transactions; off-chain messaging; mix networks; ring signatures; zero-knowledge proofs; non-interactive zero-knowledge proofs.

1. Introduction

Blockchain provides an approach for data storing by using broadcast transactions in a way to replicate data on the nodes of blockchain network participants. Originally built as an infrastructure for Bitcoin cryptocurrency [1], blockchain applications have gone far beyond cryptocurrencies and digital assets. Today the following industries are expected to be disrupted by a new technology according to PwC research [2]: accounting and financial services, supply

* Corresponding author. Tel.: +7-985-333-3018.
E-mail address: aykonkin@gmail.com

1877-0509
10.1016/j.procs.2021.06.055

chain management, energy trading and utilities, Internet of thing (IoT) and manufacturing.

The idea behind blockchain is to allow processing monetary operations without the need for a trusted third party. Blockchain network with nodes of independent participants constructs robust infrastructure aligned with properties of distributed storage, immutable data, traceability of ownership and functionality of smart contracts. The evolution of blockchain platforms overcomes the issues of business uncertainties and technological restrictions (mainly performance issues). At the same time, one of the major barriers to rolling out blockchain for corporate needs is to fulfill the requirements for security and limitations for potential threats of personal data disclosures while the data is replicated among all blockchain nodes [3].

Modern blockchain platforms provide a range of tools to adjust broadcast transactions and enhance privacy. However, these methods for private transactions affect the core blockchain features as the following:

- Elimination of the need for intermediaries or trusted third parties (TTP).
- Traceability of transactions and data stored in blockchain [4].

The article is arranged with the following sections. In section 2 there is an overview of the methods for private transactions in blockchain from the perspective of identity and transaction data privacy issues. Next in section 3 we discover zero-knowledge proofs (ZKP) methods and ZKP adoption for blockchain. Section 4 examines a new adjusted approach to implement ZK-SNARK (zero-knowledge succinct non-interactive argument of knowledge) method for the corporate blockchain. Section 5 concludes the study, and also some performance issues are discussed.

2. Privacy ensuring methods for blockchain

2.1. Types of privacy issues in blockchain.

A typical transaction data structure in blockchain provides fields with addresses of a sender and a receiver, and some data (or payload) that is recorded on blockchain nodes (see [5] for Ethereum transaction details). Most privacy issues are not applicable for public networks, because public blockchain networks such as Bitcoin and Ethereum have anonymous accounts without any need for additional KYC-procedures (“know your customer”). To illustrate privacy ensuring methods for corporate blockchain networks, two types of issues are discussed: identity privacy and transaction privacy.

2.2. Identity privacy issues.

Identity privacy implies the issues of disclosing addresses of a sender and a receiver. Public blockchain networks with anonymous accounts are free to use diverse pseudo-random addresses for one authentic user to obfuscate the actual sender and receiver [6]. In corporate blockchain networks there are two most common methods to obfuscate sender and receiver credentials in a blockchain: mix networks and ring signatures.

Mix networks algorithm includes intermediaries or trusted third parties (TTP) that assembles a group of transactions, obfuscate or mix the addresses of transactions parties and after that sends to target addresses [7]. As a result, the other blockchain participants do not have details to interpret relationships between senders and target receivers (Fig. 1):

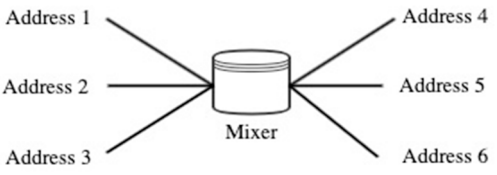

Fig. 1. Mix service

Such algorithms are easy to implement and compatible with various blockchain protocols by adjusting TTP or applying cloud storage [8]. However, TTP becomes the most crucial point of vulnerability for all the blockchain nodes. Therefore, mix networks are applicable only in corporate solutions with intermediaries as a central point that satisfies complex requirements for its infrastructure and governance model.

To overcome these limitations ring signatures methods are applied. These methods provide the functionality to frame a group of addresses as a ring. Using this ring a sender generates an electronic signature by utilizing addresses of ring participants in sequential order as follows (see [9]).

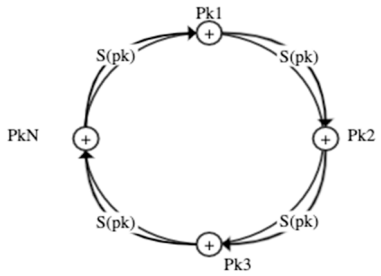

Fig. 2. Ring signatures

Fig. 2 depicts the public keys of ring participants and the process of computing a group's electronic signature. Although ring signature methods provide a strong mechanism to solve identity privacy issues, it leads to performance limitations due to the complex process to compute electronic signatures. What is more, an attacker might use simple search methods to discover the exact sender if the number of ring participants is relatively small.

2.3. Transaction privacy issues.

Transaction privacy issues refer to the requirements for confidentiality of data or some content recorded in a transaction. Most corporate blockchain networks set "off-chain" protocols with additional services for private data that is not replicated among blockchain nodes [10]. Thus, an additional database for private data aside from a blockchain node has to be installed (Fig. 3).

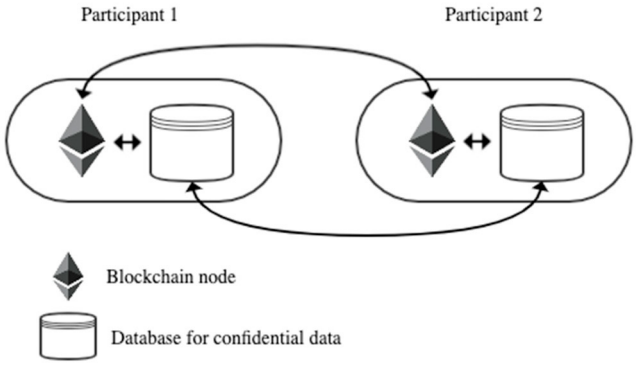

Fig. 3. Off-chain protocols

While blockchain protocol coexists with additional protocol to synchronize private data, one loses the traceability of transactions and data in a blockchain. Also, whereas the programming logic of additional protocol is isolated from algorithms of smart contracts in blockchain, some issues of binding might arise and lead to a complicated debugging process.

Nowadays ZKP (zero-knowledge proof) protocols are considered as the most promising tools to meet privacy

issues for corporate blockchain networks (Table 1).

Table 1. Privacy methods for corporate blockchain

Methods	Advantages	Disadvantages
Mix networks	• Easy to implement. • Compatible for various blockchain protocols	• Include intermediaries or trusted third parties (TTP) • Absence of transability of transactions.
Ring signatures	• Strong private mechanism.	• Absence of transability of transactions. • Performance issues.
Off-chain protocols	• Strong private mechanism. • Applicable for corporate blockchain networks with strong governance model. • High prevalence in corporate blockchains.	• Absence of transability of transactions.
ZKP (zero-knowledge proof)	• Strong private mechanism. • All the key features of blockchain are available.	• Possible performance issues.

3. Zero-knowledge proofs methods for blockchain

3.1. Zero-knowledge proofs properties.

Zero-knowledge proofs (ZKP) are a set of cryptographic protocols that allow participants to prove the statement without revealing any additional information concerning this statement [11]. As it was shown above, ZKP methods fulfill the requirements for privacy and maintain the key features of blockchain: the absence of TTP and traceability of data. ZKP are characterized by the following properties [12]:

- Completeness: an efficient method to verify if the statement is correct.
- Soundness: negligible probability to confirm if the statement is incorrect.
- Zero-Knowledge: blockchain participants except for the data owner do not have any additional information about private data.

3.2. ZKP principles for blockchain.

Zero-knowledge proofs are divided into interactive and non-interactive protocols. The first group implies interactive process when both prover and verifier are online during several rounds of messaging and apply the following algorithm:

1. Prover sends to a verifier send certain message known as a commitment.
2. Verifier responds with the string known as a challenge.
3. Prover sends a message with ZK-prove computed using the commitment (step 1) and the challenge (step 2).
4. Steps 1-3 continue before verifier accepts the commitment.

The Figure 4 shows an interactive process for zero-knowledge proofs protocols.

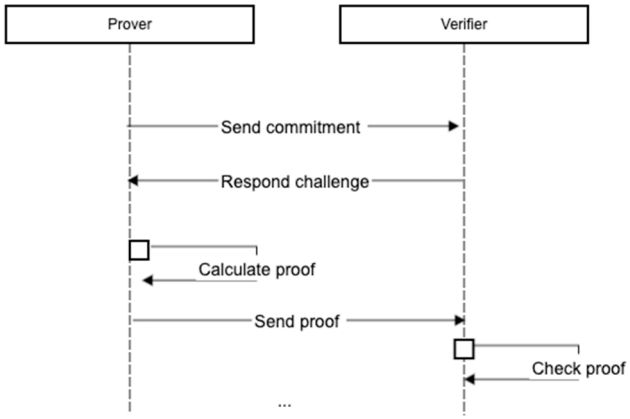

Fig. 4. Zero-knowledge proofs interactive protocols

While the interactive process involves several rounds of communication, it reduces blockchain network performance and also imposes supplementary requirements to be online for both a prover and a verifier during the process. Hence non-interactive zero-knowledge proofs (NIZK) protocols were adjusted for blockchain. The scheme for NIZK protocols is as follows:

1. Prover generates a random number and calculates a number of challenges emulating several rounds of communication.
2. Prover sends generated proof based on a number of challenges emulated on step 1.
3. Verifier check the proof and responds if proof is correct.

The Figure 5 represents the process of NIZP protocols:

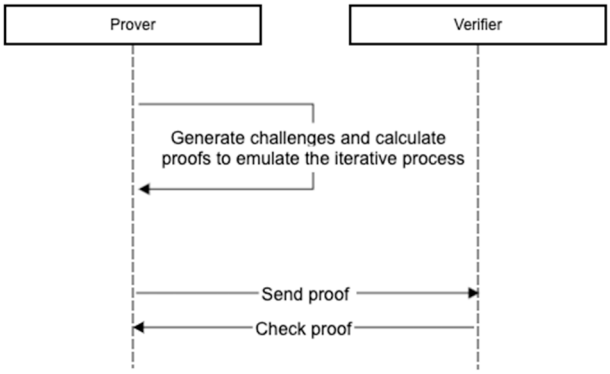

Fig. 5. Zero-knowledge proofs non-interactive protocols (NIZK)

NIZK protocols are more capable of applying in blockchain due to the absence of rounds of messaging. NIZK scheme is defined by the algorithms: Setup, Prove, and Verify (see [13]):

1. Setup (λ) is an initiation algorithm to set parameters that is responsible for security of NIZK scheme C, where input parameter λ defines the security level for blockchain.
2. Prove (x, w) is a function to generate proof applying a number of challenges, input parameter w represents secret information concerning this statement (witness), and parameter x serves to generate a proof π.
3. Verify (x, π) is a function that receives an input parameter π and outputs Boolean value b, which is equal to 1 if

verifier accepts the proof and 0 otherwise.

Components of the NIZK scheme are depicted in the Figure 6.

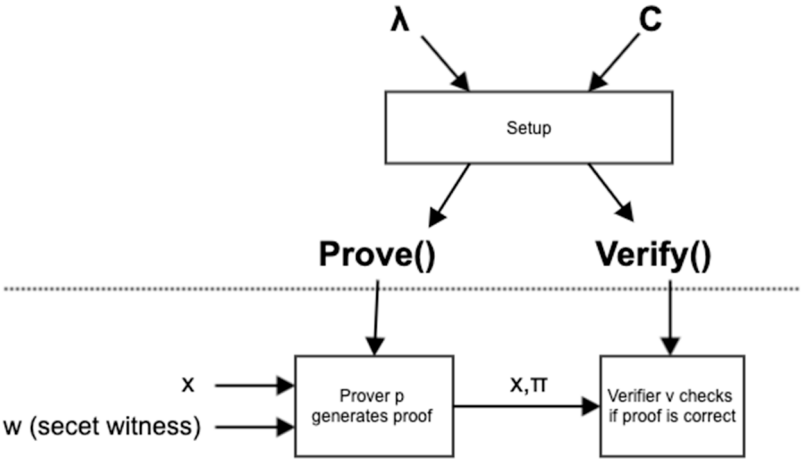

Fig. 6. NIZK scheme

The following major criteria to measure the performance of NIZK protocols might be applied:

- Algorithmic complexity to generate proof (or time to generate proof).
- Algorithmic complexity to check if a proof is correct (or time to check proof).
- Communication complexity (proof size in bits).
- Size of transactions (average per transaction).
- Trusted setup (yes/no).

The last criteria define if generated proofs rely on initial parameters (i.e., if initial parameters are compromised, the whole NIZK protocols is also compromised) [13].

4. NIZK protocol for corporate blockchain

In this section we consider some aspects of NIZK protocols implementation for corporate blockchain using platform Masterchain [14]. Masterchain is Ethereum-based platform built with certified GOST crypto algorithms (a set of standards maintained by the Euro-Asian Council for Standardization). Use cases in Masterchain adjust PKI (public key infrastructure) and digital signature methods for authentication. However, this approach causes some limitations for privacy and performance. NIZK protocol for Masterchain is subject to the following requirements and restrictions in corporate blockchain network:

- Privacy requirements for anonymity of authentication.
- Restrictions for requests to PKI including certification authority (CA).
- Volume of operations in blockchain exceeds the resources of PKI.

The basic use case for applying NIZK protocol for Masterchain is the proof of ownership for digital financial assets (DFAs) stored in a blockchain. The use case includes the following roles:

- Seller (prover) to register new DFAs in blockchain.
- Operator to accept the registration of DFAs.

- Buyer (verifier) to purchase DFAs.

Due to the legal obligations and commercial requirements, trading transactions with DFAs between Seller and Buyer have to be private without revealing information about ownership of DFAs.

The Figure 7 depicts a new approach to applying NIZK protocol for DFAs using secret salt to prove ownership:

1. Seller (prover) register DFAs in a blockchain.
2. Operator DFAs generate and respond with IDs for registered DFAs.
3. Seller (prover) generates secret salt and HMAC (hash-based message authentication code) for DFAs and its IDs.
4. Seller (prover) records IDs and HMAC in a blockchain.
5. Seller (prover) applies secret salt to generate proof for a Buyer (verifier) with NIZK protocol.

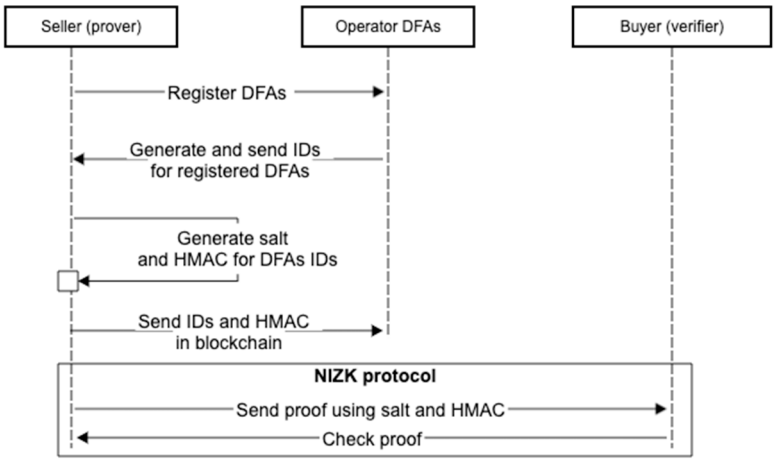

Fig. 7. NIZK scheme for corporate blockchain

This new approach matches legal requirements to register DFAs with KYC procedures and not to reveal private data concerning trading transactions and ownership of DFAs. Business requirements for the implementation of NIZK protocol for Masterchain have the following ranges and parameters:

- Time to generate proof – low, in hours.
- Time to check proof – high, in seconds.
- Proof size – low, in kilobits.
- Size of transactions – low, in megabits.
- Trusted setup - no.

In practice, there is no strong need for a trusted setup because of the operator role who may provide initial parameters for blockchain.

Experiments were adjusted using zk-SNARK algorithms and ZoKrates framework. We see directions for further research in the field of comparing the exact values for NIZK scheme in DFAs using also Bulletproofs and zk-STARK algorithms.

5. Conclusion

The article addresses the issues of privacy in a blockchain. Two types of issues were outlined: identity privacy and transaction privacy. The authors compare methods for privacy issues. First, mix networks that are easy to implement,

but require intermediaries (trusted third parties) for all blockchain transactions. Second, ring signatures that are the strong mechanisms for private, but too demanding for performance. Third, off-chain protocols that are the most commonly used in corporate blockchain but diminish some intrinsic key features of blockchain as traceability.

Zero-knowledge proof protocols are supposed to eliminate drawbacks in the methods above and establish robust procedures for privacy and security. The article introduces NIZK (non-interactive zero-knowledge proof) protocols as most appropriate for corporate blockchain.

Next a new approach to applying the NIZK scheme for the corporate blockchain use case for trading DFAs (digital financial assets) was proposed and implemented for the Masterchain platform. Although obtained results of performance match target business requirements for DFAs, further research to enhance the performance needs to be adjusted.

Acknowledgement

This work was supported by the Ministry of Science and Higher Education of the Russian Federation (state assignment project No. 0723-2020-0036).

References

[1] Q.Feng, D.He, S.Zeadally, K.Khan, “A survey on privacy protection in blockchain system”, Journal of Network and Computer Applications, vol. 126, pp.45-58, 2019.

[2] S.Davies, S.Likens, “PwC's Global Blockchain Survey”, 2018, Accessed on: Nov.23,2020. [Online] Available: https://www.pwc.com/gx/en/industries/technology/blockchain/blockchain-in-business.html.

[3] Deloitte, “Deloitte's 2020 Global Blockchain Survey”, 2020. [Online] Available: https://www2.deloitte.com/us/en/insights/topics/understanding-blockchain-potential/global-blockchain-survey.html

[4] Z.Guan, Z.Wan, Y.Yang, Y.Zhou, B.Huang, “BlockMaze: An Efficient Privacy-Preserving Account-Model Blockchain Based on zk-SNARKs”, IEEE Transactions on Dependable and Secure Computing, doi: 10.1109/TDSC.2020.3025129, Sep.2020.

[5] G.Wood, “Ethereum: a secure decentralised generalised transaction ledger Eip-150 revision”, 2014. [Online] Available: https://gavwood.com/paper.pdf

[6] Z.Guan, Z.Wan, Y.Yang, Y.Zhou, B.Huang, “BlockMaze: An Efficient Privacy-Preserving Account-Model Blockchain Based on zk-SNARKs”, IEEE Transactions on Dependable and Secure Computing, doi: 10.1109/TDSC.2020.3025129, Sep.2020.

[7] D.Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”, Communications of the ACM, vol.24, no.2, pp. 84-88, 2018.

[8] I. Sukhodolskiy, S. Zapechnikov, A Blockchain-Based Access Control System for Cloud Storage, 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018.

[9] B. Wang, J.Sun, Y.He, D.Pang, L.Ningxiao, “Large-scale Election Based On Blockchain”, Procedia Computer Science, vol.129, pp. 234-237, 2018.

[10] S.Tai, “On or Off the Blockchain? Insights on Off-Chaining Computation and Data”, European Conference on Service-Oriented and Cloud Computing, 2017.

[11] C. Reitwiebner, “zkSNARKs in a Nutshell” , 2016. [Online] Available: http://chriseth.github.io/notes/articles/zksnarks/zksnarks.pdf

[12] H.Mayer, “zk-SNARK explained: Basic Principles”, 2016. doi: 10.13140/RG.2.2.20887.68007, [Online] Available: https://blog.coinfabrik.com/zk-snarks-explained-basic-principles/

[13] E.Morais,T.Koens,C.Wijk, A.Koren, “A Survey on Zero Knowledge Range Proofs and Applications”, 2018. [Online] Available: https://arxiv.org/pdf/1907.06381.pdf

[14] Association Fintech, “Masterchain whitepaper”, 2017. [Online] Available: https://fintechru.org/directions/raspredelennyy-reestr/