UDC 004.056.53

A.V. Ilienko, Ph.D., S.S. Ilyenko, Ph.D., L.P. Halata Ph.D.
(National Aviation University, Ukraine)

Implementing a certificate verification method using the blockchain approach

Material presents a blockchain-based method for verifying digital certificates, addressing the challenges of incorrect verification. By utilizing decentralized technology, the proposed solution enhances security and integrity in data protection. Smart contracts automate the verification process, ensuring transparency and efficiency of digital certificate management in networks.

Introduction

The daily exchange of information between users and web pages requires increased security measures, and HTTPS has become one of the main standards for building and organizing secure connections. Additionally, HSTS, Certificate pinning, and HTTP Public Key Pinning are popular methods that help prevent unnoticed certificate substitution by comparing them to a trusted template in the browser's secure storage. However, the problem of using digital certificates for authentication remains relevant, as not all websites use digital certificates, and if they do, their verification is not always correct or complete. The CVE-2019-13050 attack on SKS and GnuPG key servers in 2019 highlighted the issue of incorrect verification of digital certificates.To address this problem, the study proposes a certificate verification method using the blockchain approach, which involves multiple certificate checks. The blockchain approach is a unique technology that enables decentralized storage of information for all transaction data. It was first used in the financial sector to create cryptocurrencies like Bitcoin. Recently, blockchain technology has been expanding its applications by integrating mechanisms that allow decentralized transactions to take place. These mechanisms, known as "smart contracts," operate based on predefined rules, such as specific requirements for quality, price, and quantity, and enable automatic matching of potential buyers and sellers based on distributed ledgers. Blockchain technology allows for direct transactions between equal participants in a peer-to-peer network. Transactions on this network assume that any participant can conduct a transaction with any other participant without the need for a third-party intermediary. In a multi-layered transaction model, which typically involves centralized storage of transaction data, data management is usually centralized. In a traditional model based on blockchain technology, transactions are conducted directly between suppliers and consumers.

All transaction data is stored in a distributed chain of data blocks (B). The relevant information is stored in the same format on the computers of all participants.Transactions are primarily conducted based on "smart contracts," which are rules established individually (e.g., specific requirements for quality, price, quantity, etc.).The transaction model is generally automated and decentralized, requiring no involvement of intermediaries.

Working principle of the proposed solution for transferring digital certificates using blockchain. As mentioned in the first part of this work, digital certifi-

cates are one of the most widely used auxiliary tools for securing data in open networks. However, the main drawback of this technology is the absolute trust in the certificate issuers. In this work, I propose a new approach to organizing a Public Key Infrastructure (PKI), which will help eliminate existing issues and utilizes blockchain technology. The main components of blockchain include ledgers (registration books) that allow tracking of the owner of an asset at a specific point in time. A ledger is a sequential list of transaction groups with a timestamp, from a technical perspective. A centralized database (DB) is required for the registration of transactions. Management and changes are typically carried out in separate units that operate within their own needs and then integrate into the central system, passing the data. Each node stores and processes its portion of the DB and executes its own portion of the code. In the case of an error on one node, access to the central block is denied. Blockchain networks have different rules. Systems that operate on software based on this approach have these rules built in. Thus, how will a decentralized PKI infrastructure work in practice? Let's consider the description of the technology itself. Imagine a certain owner who possesses a large number of public keys, where each key represents a specific transaction stored in the registry. How can we understand that all these keys belong to this owner? To solve this problem, a zero transaction is created, which contains information about the owner and their assets (from which a commission is deducted for placing the transaction in the registry). The zero transaction acts as a kind of anchor to which subsequent transactions with data about public keys will be attached. Each such transaction contains a specialized data structure, or notification. A notification is a structured set of data that includes functional fields and contains information about the owner's public keys, the persistence of which is guaranteed by the placement in one of the associated registry entries. The next logical question is how the zero transaction is formed. The zero transaction, like subsequent transactions, consists of six data fields. The formation of the zero transaction involves the use of a key pair, which appears when the user registers their wallet, from which a commission is deducted for placing the zero transaction and - later - notifications in the registry. The digital signature of the public key is formed through consecutive applications of hash functions SHA256 and RIPEMD160. Here, RIPEMD160 is responsible for compact representation of data, whose size does not exceed 160 bits. This is important - as the registry is not a cheap database. The public key itself is entered into the fifth field. In the first field, data are stored that establish a link with the previous transaction. In the zero transaction, this field is empty, which distinguishes it from subsequent transactions. The second field contains data for checking the consistency of transactions. The contents of these fields are formed using iterative hashing, as demonstrated in the example of linking the second and third transactions. To implement the proposed approach, several key steps need to be taken: Establish a decentralized PKI infrastructure: This involves setting up a network of nodes that can verify and validate digital certificates using the blockchain approach. Implement smart contracts: These contracts will be responsible for ensuring the integrity and authenticity of the digital certificates by enforcing the predefined rules and conditions. Integrate the blockchain network with existing certificate verification systems: This will enable seamless integration with existing systems and allow for the verification of digital certificates using the blockchain approach. The proposed solution for digital certificate verification was implemented using the Ethereum blockchain platform. The digital certificates were issued by a trusted third-party authority and were signed with the authority's private key. The

public key of the authority was stored in the blockchain, enabling any node in the network to verify the authenticity of the digital certificate.The distributed ledger was implemented using the Ethereum blockchain, and the consensus algorithm used was Practical Byzantine Fault Tolerance (PBFT). The smart contracts were implemented using the Solidity programming language and were deployed on the Ethereum blockchain.The verification process was automated using the smart contracts. The smart contracts defined the rules and procedures for verifying the digital certificates, ensuring that the verification process is secure, transparent, and efficient. The practical implementation of the proposed solution was conducted using the Ethereum blockchain platform. The digital certificates were issued by a trusted third-party authority and were signed with the authority's private key. The public key of the authority was stored in the blockchain, enabling any node in the network to verify the authenticity of the digital certificate.The distributed ledger was implemented using the Ethereum blockchain, and the consensus algorithm used was Practical Byzantine Fault Tolerance (PBFT). The smart contracts were implemented using the Solidity programming language and were deployed on the Ethereum blockchain.The verification process was automated using the smart contracts. The smart contracts defined the rules and procedures for verifying the digital certificates, ensuring that the verification process is secure, transparent, and efficient.Conclusion: The proposed blockchain-based solution for digital certificate verification provides a decentralized, secure, and efficient method for verifying digital certificates. The use of blockchain technology ensures the integrity and security of the data, while the consensus algorithm ensures the consistency and reliability of the data. The smart contracts automate the verification process, ensuring that the verification process is secure, transparent, and efficient.The practical implementation of the proposed solution using the Ethereum blockchain platform demonstrates the feasibility and effectiveness of the proposed approach. The proposed solution has the potential to revolutionize the way digital certificates are verified, providing a more secure, efficient, and transparent method for digital certificate verification

Conclusions

The proposed approach to implementing a certificate verification method using the blockchain approach offers a secure and decentralized solution to the problem of incorrect verification of digital certificates. By leveraging the principles of blockchain technology, this approach ensures the integrity and authenticity of digital certificates, providing a more secure and reliable method for protecting data in open networks.

References

1. Panda, S. K., Jena, A. K., Swain, S. K., & Satapathy, S. C. (Eds.). (2021). Blockchain technology: applications and challenges.
2. Mougayar, W. (2016). The business blockchain: promise, practice, and application of the next Internet technology. John Wiley & Sons.
3. Fan, P., Liu, Y., Zhu, J., Fan, X., & Wen, L. (2019). Identity Management Security Authentication Based on Blockchain Technologies. Int. J. Netw. Secur., 21(6), 912-917.