Simulation and Analysis of Blockchain Operations Model with RSA Algorithm in CrypTool2

Hana Stefanović

Comtrade Information Technology School of Applied Studies
Belgrade, Serbia
hana.stefanovic@its.edu.rs
[0000-0003-0890-4410]

Ana Savić

School of Electrical and Computer Engineering
Academy of Technical and Art Applied Studies
Belgrade, Serbia
ana.savic@viser.edu.rs
[0000-0002-8099-1136]

Goran Bjelobaba

University of Belgrade, Faculty of organizational sciences
Department for e-business
Belgrade, Serbia
gbjelobaba@gmail.com
[0000-0003-3684-3248]

Nikola Popović

Alfa BK University
Faculty of Mathematics and Computer Science
Belgrade, Serbia
nikolap6901@gmail.com
[0000-0002-5038-0086]

Abstract—In this paper the simulation model of blockchain operations is created and tested through a few transactions among the participants. The participants are able to send and receive coins or to mine blocks to earn coins, while all transactions are stored in the blocks' data, including the address of sender and the address of the receiver. The address is a hash value of a public key for asymmetric cryptography. The RSA (Rivest-Shamir-Adleman) asymmetric algorithm is used, including public key and private key. The model is created in CrypTool2 software, including three blocks and smaller numbers for generating the RSA public and private key pairs than in real blockchain transactions, in order to minimize the simulation time. Some attacks are also simulated, and those transactions are not accepted because of invalid signature, since the attacker does not have someone's private key.

Keywords - blockchain technology, CrypTool2, valid and invalid transactions, RSA algorithm

I. INTRODUCTION

Blockchain is a contemporary technology composed of various elements that work together to create a network that ensures trust between users. It is a decentralized and distributed database that allows for the verification of transactions and cannot be altered or deleted [1]. The network is made up of blocks, chains, and nodes, and is based on distributed general ledger technology. The use of cryptographic techniques ensures data encryption and record integrity, making it a secure approach to data storage [2].

Authors utilize CrypTool2, a software tool specifically designed for cryptographic and security-related simulations and analysis [3]. CrypTool2 offers a user-friendly interface that enables the creation and testing of various cryptographic algorithms, including the RSA (Rivest-Shamir-Adleman) asymmetric algorithm employed in our simulation model. The software provides functionality for generating RSA public and private key pairs, as well as simulating blockchain-based transactions and attacks. By utilizing CrypTool2, we can effectively model and evaluate the behavior of our blockchain-based simulation in a controlled environment [4].

Each block in the network is a list of transactions that are recorded chronologically and stored on various computers connected through a peer-to-peer protocol. Nodes in the network continuously verify the authenticity of records, and the function of mining is used to validate these transactions. Once a transaction has been validated, it cannot be altered or deleted [5].

The process of selecting a valid block of transactions is known as proof-of-work, which protects the network from misuse. Once a block has been validated, it is propagated to other nodes in the network and connected with other transactions in the new block, forming a chain of blocks or a blockchain. The hash, which is a fingerprint of data, connects each block together and cannot be decrypted, making it a secure approach to data storage [6]. The blockchain is comprised of three layers, namely the protocol layer, the network layer, and the application or business layer. Each layer contributes distinct elements to the blockchain with the purpose of advancing its development [7]. The utilization of blockchain technology across various domains offers several advantages due to its key features such as decentralization, immutability, transparency, and security [8].

A. Decentralization

The flexibility of blockchain is attributed to its decentralized nature where there is no central entity controlling the process. Multiple and distributed nodes ensure the network cannot be easily attacked or destroyed. However, some doubt has been raised regarding decentralization, especially in large-scale mining activities as highlighted in research studies [9].

B. Immutability/Resistance to abuse

Blockchain is characterized by its resistance to change or deletion of transaction records, making it difficult to modify records unnoticed. The use of public-private keys or cryptographic signatures ensures integrity and authentication, thus reducing the possibility of fraud [10].

C. Transparency

The use of a book available to all users or a predefined set of users provides transparency. In public or open blockchains, all participants have equal rights to access and update the book according to existing consensus mechanisms, making transactions transparent and visible. However, transparent data in public systems can become an issue when confidential information is accidentally made publicly available or needs to be modified due to errors or inaccuracies [11].

D. Security

Blockchain provides a high level of security due to the anonymity of transactions. Any transaction or digital event taking place in a blockchain network must be agreed upon by the consensus of the majority of users participating in the process, ensuring verification and security [9].

II. BLOCKCHAIN SIMULATION MODEL

A blockchain simulation model is a computer-based model that simulates the behavior of a blockchain network. It allows users to understand and test the functionality of a blockchain network without the need for actual implementation [12], [13]. A simulation model consists of different elements of a blockchain network, including nodes, transactions, and consensus algorithms. By adjusting these elements, users can simulate various scenarios and observe the network's behavior in response to different inputs [14].

There are different types of simulation models, such as agent-based models and discrete event simulation models. These models can be used to simulate different types of blockchain networks, such as public and private blockchains [15]. Simulation models can be used for various purposes, such as testing the performance and scalability of a blockchain network, evaluating the effectiveness of consensus algorithms, and analyzing the impact of different network parameters on the overall network behavior [4].

Blockchain simulation models provide a valuable tool for understanding and optimizing blockchain networks, helping to reduce the costs and risks associated with implementing new blockchain solutions [11].

The simulation model with three blocks (block ID 0, block ID 1 and block ID 2) and two participants, Ana and Goran, is presented in Fig. 1.

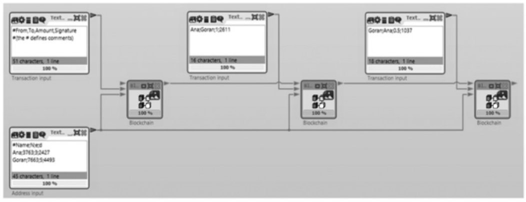

Fig. 1. The simulation model of blockchain operations with 3 blocks and 2 participants

A blockchain simulation model is a computer-based model that enables users to simulate the behavior of a blockchain network without actual implementation [16]. It serves as a valuable tool for understanding and optimizing blockchain networks, allowing users to test different scenarios and observe network behavior [9]. The simulation model presented in this study consists of three blocks (Block ID 0, Block ID 1, and Block ID 2) and involves three participants, Ana, Hana and Goran. The participants engage in transactions and maintain balances within each block. The transactions and balances within these blocks are illustrated in Figs 2-7. Figs 2-7 provide a detailed representation of the transactions and balances in each block. Fig. 2 displays the transactions that occurred within Block ID 0, including sender and receiver addresses and the amount of coins transferred. Fig. 3 showcases the balance of coins held by Ana and Goran within Block ID 0. Fig. 4 illustrates the transactions within Block ID 1. Fig. 5 presents the balance of Ana and Goran after the transactions within Block ID 1. Fig. 6 represents the transactions within Block ID 2. Fig. 7 shows the final balance of Ana and Goran after the transactions within Block ID 2. These figures provide a visual and informative overview of the simulation model, giving insights into the specific transactions made by participants and the corresponding changes in their balances as the blockchain progresses. The simulation model, along with the detailed depiction of transactions and balances, facilitates the evaluation of blockchain network performance, consensus algorithms, and the impact of various parameters on network behavior. It serves to reduce costs and risks associated with the implementation of new blockchain solutions.

The transactions and balance in each block are given in Figs 2-7.

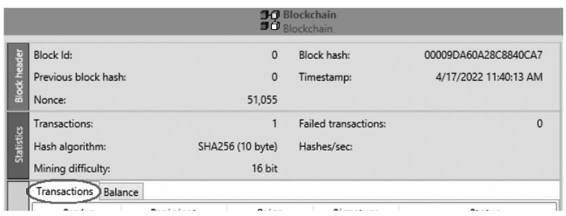

Fig. 2. Block ID 0 transactions

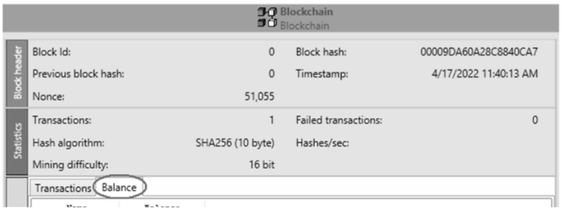

Fig. 3. Block ID 0 balance

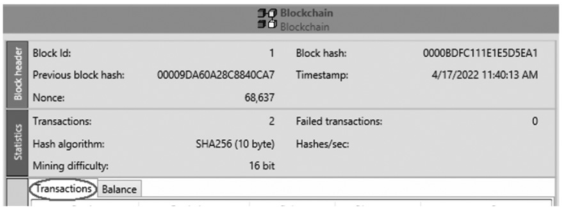

Fig. 4. Block ID 1 transactions

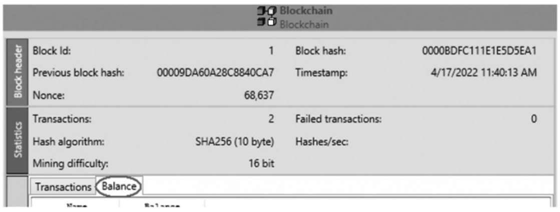

Fig. 5. Block ID 1 balance

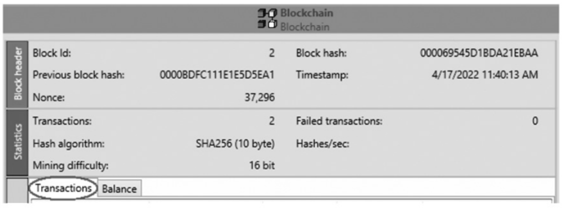

Fig. 6. Block ID 2 transactions

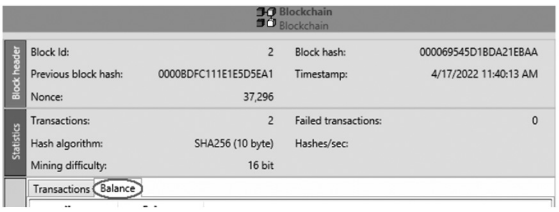

Fig. 7. Block ID 2 balance

After adding the text output block after block ID 2, in order to analyze all transactions in JSON (JavaScript Object Notation) file, the model given in Fig. 8. is created, while the JSON format data is presented in Fig. 9.

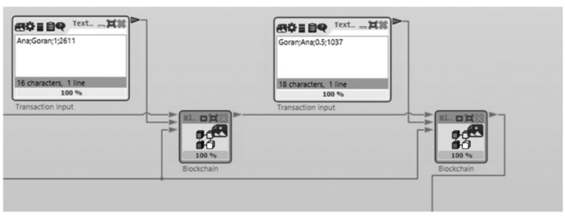

Fig. 8. Adding the Text Output block in order to analyze transactions in JSON format

Fig. 9. Transaction data in JSON format

III. ADDING A NEW PARTICIPANT

The new participant's (Hana) address is generated, using the RSA key generator, as it is presented in Fig.10.

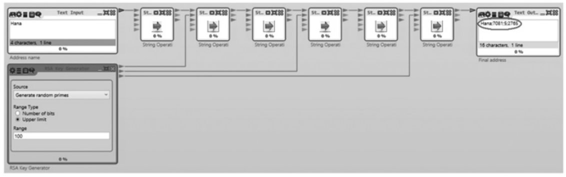

Fig. 10. Creating the new participant's address

The model with new participant added is presented in Fig.11.

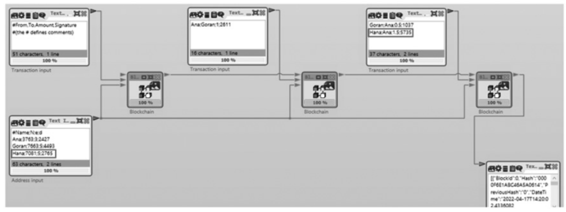

Fig. 11. The simulation model with new participant (Hana) and her transactions

The transactions after adding the new participant are presented in Fig.12-Fig.14.

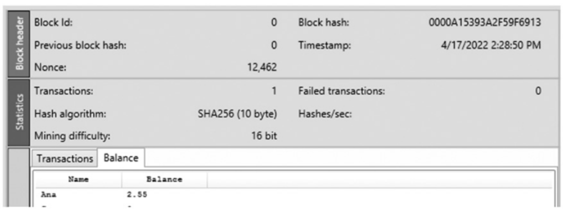

Fig. 12. Block ID 0 balance after adding the new participant

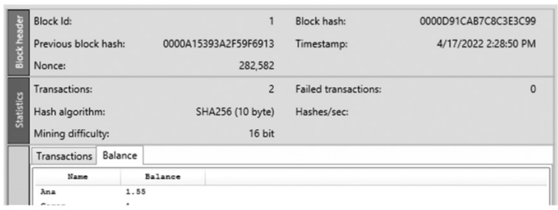

Fig. 13. Block ID 1 balance after adding the new participant

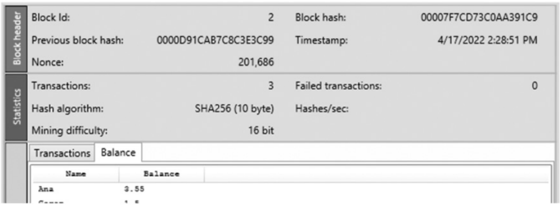

Fig. 14. Block ID 2 balance after adding the new participant

IV. SIMULATION MODEL OF BLOCKCHAIN ATTACK

When Hana attempts to attack Ana in order to earn extra coins, some errors and warnings are generated, indicating that the transaction is not valid. This is because Hana does not possess Ana's signature, as depicted in Fig.15 and Fig.16. By using the general names of the participants (Hana and Ana) consistently throughout the sentence, it maintains coherence and clarity in describing the situation where one participant (Hana) tries to attack another participant (Ana) in the simulation.

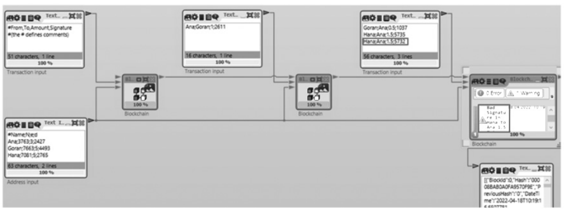

Fig. 15. The simulation model of blockchain attack (Hana wants to get some coins from Ana)

The transaction is not valid, since Hana does not have Ana's private key and cannot sign the transaction (the "Bad signature" and "Failed transactions" messages are generated), as it is presented in Fig.16. Also, the balance is not changed, and Hana does not earn any coins from Ana. It is shown that the balance is not changed.

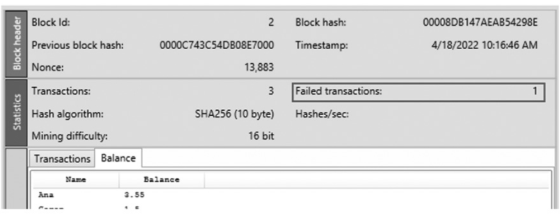

Fig. 16. The illustration of failed transaction

V. CONCLUSION

In this paper, the authors have presented a simulation model of blockchain operations that can be used to test various transactions between users. This model has been implemented using CrypTool2 software, and it includes three blocks with smaller numbers for generating RSA public and private key pairs than in real blockchain transactions, in order to minimize the simulation time.

The simulation model enables the participants to send and receive coins or mine blocks to earn coins, with all transactions being stored in the blocks' data, including the address of the sender and receiver. The address is a hash value of a public key for asymmetric cryptography, and the RSA (Rivest-Shamir-Adleman) asymmetric algorithm is used, including public key and private key.

The authors have also simulated some attacks on the blockchain, where these transactions were not accepted due to invalid signatures. In this way, the model can identify and prevent potential threats to the blockchain.

Overall, the simulation model presented in this paper provides a useful tool for testing and analyzing blockchain transactions. The simulation demonstrates both successful and unsuccessful financial transactions and illustrates the potential for using blockchain technology in various applications [10], [17].

The simulation model presented in the paper could be used as a basis for further development of blockchain-based systems and applications. It could be utilized in the testing and validation of new blockchain models, as well as in the education and training of professionals in the field of blockchain technology. Furthermore, the simulation model could be used in the development and testing of decentralized applications, such as cryptocurrencies, smart contracts, and supply chain management systems. Overall, the simulation model presented in the paper has the potential to contribute to the advancement and practical application of blockchain technology in various domains.

REFERENCES

[1] G. Bjelobaba, M. Paunovic, A. Savic, H. Stefanovic, J. Doganjic, and Z. M. Bogavac, "Blockchain Technologies and Digitalization in Function of Student Work Evaluation," Sustain., vol. 14, no. 9, pp. 1–22, 2022, doi: 10.3390/su14095333.

[2] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," Proc. 13th EuroSys Conf. EuroSys 2018, vol. 2018-Janua, 2018, doi: 10.1145/3190508.3190538.

[3] H. Stefanovic, A. Savic, R. Veselinovic, and G. Bjelobaba, "An application of visual cryptography scheme with digital watermarking in sharing secret information from car number plate digital images," 2021. [Online]. Available: www.ijeijournal.com.

[4] J. Menez, P. van Oorschot, and S. . Vanstone, Handbook of Applied Cryptography, 5th ed. CRC press Series on Discrete Mathematics and Its Applications, 2001.

[5] H. Hyvärinen, M. Risius, and G. Friis, "A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services," Bus. Inf. Syst. Eng., vol. 59, no. 6, pp. 441–456, 2017, doi: 10.1007/s12599-017-0502-4.

[6] Andreas M, "Mastering Bitcoin: Unlocking Digital Cryptocurrencies," 2014, [Online]. Available: https://sci-hub.do/https://books.google.com/books?hl=zh-CN&lr=&id=IXmrBQAAQBAJ&oi=fnd&pg=PR4&dq=Antonopoulos,+Andreas+M.+2014&ots=9C9UrwGrNX&sig=3l49cnJsCUpJcR51eJK10_OaH-E.

[7] C. Farchi, B. Touzi, F. Farchi, and A. Mousrij, "Sustainable per-

formance assessment: A systematic literature review," J. Sustain. Dev. Transp. Logist., vol. 6, no. 2, pp. 124–142, 2021, doi: 10.14254/jsdtl.2021.6-2.8.

[8] G. Danezis and S. Meiklejohn, "Centrally Banked Cryptocurrencies," May 2017, doi: 10.14722/ndss.2016.23187.

[9] P. Velmurugadass, S. Dhanasekaran, S. Shasi Anand, and V. Vasudevan, "Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm," in Materials Today: Proceedings, 2020, vol. 37, no. Part 2, pp. 2653–2659, doi: 10.1016/j.matpr.2020.08.519.

[10] H. Yi, "Securing e-voting based on blockchain in P2P network," Eurasip J. Wirel. Commun. Netw., vol. 2019, no. 1, Dec. 2019, doi: 10.1186/s13638-019-1473-6.

[11] M. Finck, "Blockchains and Data Protection in the European Union," Eur. Data Prot. Law Rev., vol. 4, no. 1, pp. 17–35, Mar. 2018, doi: 10.21552/edpl/2018/1/6.

[12] A. W. Dent and C. J. Mitchell, User's guide to cryptography and standards. Boston: Artech House, 2005.

[13] H. Stefanovic, A. Savic, R. Veselinovic, and G. Bjelobaba, "An application of visual cryptography scheme with digital watermarking in sharing secret information from car number plate digital images," in International Journal of Engineering Inventions–IJEI, 2021, vol. 10, no. 2, pp. 1–11, [Online]. Available: www.ijeijournal.com.

[14] M. Rauchs et al., "Distributed Ledger Technology Systems: A Conceptual Framework," SSRN Electron. J., no. August, 2018, doi: 10.2139/ssrn.3230013.

[15] A. E. Gencer, S. Basu, I. Eyal, R. van Renesse, and E. G. Sirer, "Decentralization in Bitcoin and Ethereum Networks," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10957 LNCS, pp. 439–457, 2018, doi: 10.1007/978-3-662-58387-6_24.

[16] D. Lizcano, J. A. Lara, B. White, and S. Aljawarneh, "Blockchain-based approach to create a model of trust in open and ubiquitous higher education," J. Comput. High. Educ., vol. 32, no. 1, pp. 109–134, Apr. 2020, doi: 10.1007/s12528-019-09209-y.

[17] D. Shah, D. Patel, J. Adesara, P. Hingu, and M. Shah, "Integrating machine learning and blockchain to develop a system to veto the forgeries and provide efficient results in education sector," Vis. Comput. Ind. Biomed. Art, vol. 4, no. 1, Dec. 2021, doi: 10.1186/s42492-021-00084-y.