**Cryptographic Solutions for Supply Chain Security**

|  |
| --- |
| Dumpa Venkata Sai Jagadeesh, Karthik Ullas, Kavitha C.R.\* |
| *Department of Computer Science and Engineering*  *Amrita School of Computing, Bengaluru* |
| *Amrita Vishwa Vidyapeetham, INDIA* |
| *\*Corresponding Author: cr\_kavitha@blr.amrita.edu* |

***Abstract* – In today’s worldwide economy, securing the supply chain is essential to ensure the integrity, authenticity, and traceability of goods. This project addresses the various challenges associated with supply chain security through the usage of cryptographic solutions. Some of the major issues are product counterfeiting, unauthorized tampering, and the need for transparency while tracing. We propose an extensive system that applies cryptographic algorithms and cutting-edge technologies to overcome these challenges. Counterfeit products and unauthorized tampering are significant threats to the integrity of the supply chain. Ensuring the products are legitimate and that there was no mishandling and they can be easily traced are crucial for trust and reliability in the supply chain. Algorithms: Hash Functions, and Rivest-Shamir-Adleman(RSA) have been used. Technologies: Blockchain, distributed ledger technologies (DLT), Machine Learning (ML), IoT and RFID have been used in our project.**

I. INTRODUCTION

Ensuring supply chain security is crucial in today's world of managing complex supply chains, especially when dealing with external risks. Enter blockchain technology – a sophisticated database system that makes sharing information in a business network more secure and transparent. This transparency is vital due to the challenges faced by modern supply chains.

In the realm of information transparency, various concerns arise, demanding a careful approach to tackle complexities. Challenges like verifying product authenticity, preventing unauthorized changes, and ensuring clear traceability cast shadows on the smooth operation of today's supply chains. This is where a cryptographic framework comes into play. It's a smart solution that not only addresses these challenges but also strengthens the overall security of the supply chain.

This introduction aims to explore the collaboration between supply chain security and blockchain technology. As the exploration unfolds, the goal is to uncover the layers that make up today's world of supply chain management. The upcoming sections will delve into the background, the reasons behind choosing blockchain, and the specifics of creating and using a cryptographic framework. Through this detailed examination, the aim is to provide valuable insights into enhancing supply chain security in the constantly evolving landscape of modern business practices.

II. LITERATURE SURVEY

Alex et al. [1] have implemented Public Key Cryptography with the WIPR encryption scheme and addressed Privacy Threats in RFID by preventing the interception of UII information, and tracking of tags. Sungyong et al. [2] have tried to use Blockchain technology when paired with key escrow encryption systems to significantly improve the integrity and availability of supply chain data, provide non-repudiation, and deal with denial of service attacks and collusion threats. Mustufa et al. [3] have used a Novel Integration methodology to secure information sharing in supply change management via blockchain technology. Vikas et al. [4] have implemented advanced technologies like blockchain, machine learning, and Physically Unclonable Functions into supply chain processes could significantly improve supply chain security. Mary et al. [5] have concluded that the use of DLTs has the potential to significantly improve security and trust in supply chains due to their inherent features like immutability, consensus protocols, and provenance.

III. METHODOLOGY

We have used Public Key cryptography to find cryptographic solutions for the supply chain. In Public Key Cryptography we’re using the Rivest-Shamir-Adleman (RSA) algorithm which is an asymmetric algorithm that uses two different keys for encryption and decryption. We have initialized the blockchain node with the miners public key and then created a transaction t1 and the recipient is receiving the address and a transaction value of 0.5. The transaction is signed by the sender using the private key to verify the authenticity. This is how the process works, If it’s a genesis block then set the previous hash to ‘\_’ and set the block number to zero, else if it’s not a genesis block then set the previous block hash to the hash of the last block in the blockchain and increment the blockchain, and increment the block number based on the previous block. After that, we need to send all the pending transactions to the current block which has Time Stamp, Block Number, and Previous Block Hash. Now we need to validate using the proof of work function, to ensure that the block hashes correctly. We need to add a reward transaction at the end of the block for successfully mining the block. After the proof of work is successful, we need to add the newly mined block to the existing blockchain that includes confirmed transactions, and the links between blocks are maintained. We’re repeating the same process for another transaction t2, updating the balances, and validating the blockchain. To prove that our algorithm is correct, we’re trying to make two more transactions t3 and t4, wherein t3 we’re doing the intentional signature modification, and t4 we’re trying to modify the recipient key intentionally.

IV. RESULTS

Using these cryptographic techniques, we have mined transaction t1 successfully, with a transaction value of 0.5 as shown in figure 1 and transaction 2 with a transaction value of 1.0 as shown in figure 2. After transaction 2, the balance was updated the blockchain node had a balance of 3.0, and the receiving address had a balance of 1.0. In transaction t3, when we tried to modify the signature, it showed that the signature was invalid as shown in figure 3 and the verification failed. In transaction t4, we had made intentional recipient key modifications, and it yet again showed that the verification failed as shown in figure 4.

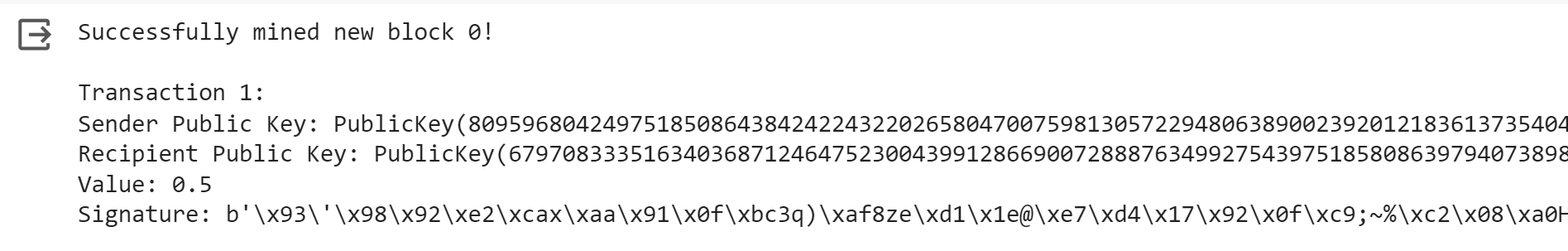


Figure 1: Transaction t1 Public Key, Private Key, Signature

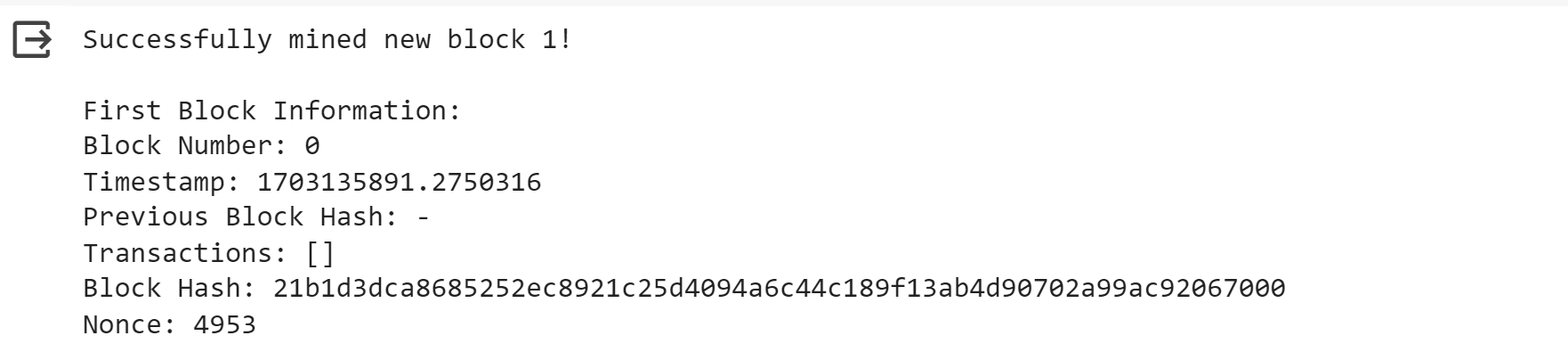


Figure 2: Transaction t1 information

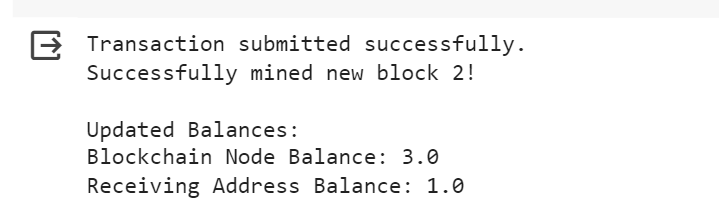


Figure 3: Transaction t2

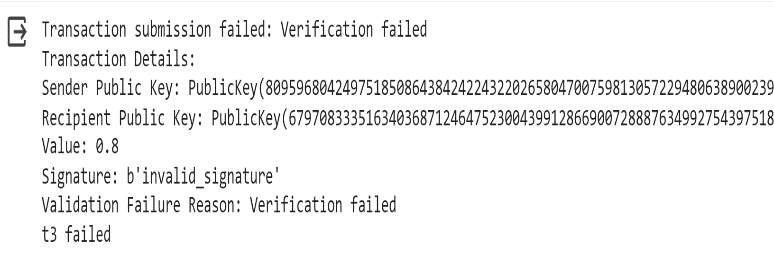


Figure 4: Transaction t3

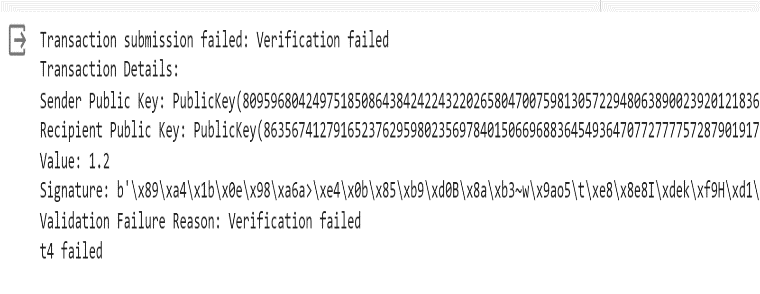


Figure 5: Transaction t4

V. CONCLUSION

The achievement of successfully implementing hash functions and the RSA algorithm within our Supply Chain solutions represents a significant advancement in our technological framework. By seamlessly integrating digital signatures, we've fortified our ability to establish and validate the authenticity of critical information. Furthermore, the incorporation of hash functions has provided a robust mechanism to meticulously verify the integrity of data, ensuring a comprehensive and secure foundation for our supply chain operations. This strategic amalgamation of cryptographic techniques serves as a testament to our commitment to elevating the security and reliability of our supply chain ecosystem.

VI. REFERENCES

[1] A. Arbit, Y. Oren and A. Wool, "A Secure Supply-Chain RFID System that Respects Your Privacy," in IEEE Pervasive Computing, vol. 13, no. 2, pp. 52-60, Apr.-June. 2014, doi: 10.1109/MPRV.2014.22.

[2] S. Cha, S. Baek and S. Kim, "Blockchain Based Sensitive Data Management by Using Key Escrow Encryption System From the Perspective of Supply Chain," in IEEE Access, vol. 8, pp. 154269-154280, 2020, doi: 10.1109/ACCESS.2020.3017871.

[3]Abidi MH,  Alkhalefah H, Umer U, Mohammed MK. Blockchain-based secure information sharing for supply chain management: Optimization assisted data sanitization process. *Int J Intell Syst*. 2021; 36: 260-290. , doi: 10.1002/int.22299

[4] V. Hassija, V. Chamola, V. Gupta, S. Jain and N. Guizani, "A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6222-6246, 15 April15, 2021, doi: 10.1109/JIOT.2020.3025775.

[5] M. Asante, G. Epiphaniou, C. Maple, H. Al-Khateeb, M. Bottarelli and K. Z. Ghafoor, "Distributed Ledger Technologies in Supply Chain Security Management: A Comprehensive Survey," in IEEE Transactions on Engineering Management, vol. 70, no. 2, pp. 713-739, Feb. 2023, doi: 10.1109/TEM.2021.3053655.