

Blockchain based Counterfeit Medicine Authentication System

Dr. Rajesh Kapoor¹, Tanishk Y. Gupta², Kushal S. Amin³, Kaustubh S. Ardekar⁴

Faculty, Department of Information Technology¹

Students, Department of Information Technology^{2,3,4}

KC College of Engineering, Thane, India

Abstract: *The quality and safety of medications are crucial to public health and well-being. Responding to the critical need for medication information provenance and anti-counterfeiting, this study proposes blockchain based solutions for medication information storage, inquiry and anti-counterfeiting along the medicinal supply chain. Leveraging the features of decentralized, tamper proof, traceability and maintenance of blockchain technology, the proposed methodology can assure the transparency and openness of medicinal supply chains. An access control policy model based on smart contracts is designed to prevent medication information from being altered or disclosed at nodes of blockchain. In addition to smart contracts, Practical byzantine fault tolerance (PBFT) is used. The proposed solution eliminates the need for centralized institutions and third-party organizations to provide a full record of medication circulation process. The result is, our method can render high level of security and privacy that is crucial to integrity of a medication information management system.*

Keywords: Medication anti-counterfeiting, traceability, blockchain, PBFT consensus, supply chain

I. INTRODUCTION

Counterfeit medicine authentication is essential for patients' health and business operations. Counterfeiting of several products creates many issues for various manufacturing sectors and causes serious threats to medicine. This is very damaging to public health and also creates profit loss to the pharmaceuticals company. To trace counterfeit drugs already several techniques have been used in the medicine supply chain. Authors, proposed the usage of barcode or RFID code on medicine for verifying its legitimacy. Same as, a Data-Matrix tracking process has been proposed in [4], where every medicine has a Data-Matrix where contains Id of Product, Id of Manufacturer ID, unique ID of the package, the authentication code and optional metadata. The central verification register (CVR) is also mentioned. Most of the authors use RFID to their works on the medicine supply chain. But implementation of RFID is costly according to medicine price. In this paper we gift a prototype of blockchain system for medicine traceability and mandate that rebuilds the full-provider architecture, ensuring authenticity and privacy of traceability data, and meantime achieves a ultimately stable blockchain data storage. Pseudocode explains the practical workflow of the medicine supply-chain has also been given. This paper is arranged as follows. Blockchain based medicine traceability related works are presented in Section II, Design framework of our prototype is explained from three aspects from four aspects, Medicine Supply Chain Data Storage in blockchain, Detecting counterfeit medicine, and Methodology for the prototype work in Sections III. Then, Section IV explains the implementation and evaluation of the prototype. Finally, the paper is concluded in Section V.

II. MOTIVATION

The counterfeiting of medicines causes a severe threat to society. The counterfeit medicines make a dangerous impression on the health of the people and also cause revenue loss to the legitimate medicine manufacturing establishments. The faulty deliver chain machine is likewise the cause for counterfeit tablets within the pharmaceutical industry. Thus far various anti-counterfeiting techniques have been offered, but most of the existing systems are not good. Blockchain technology is one of the best alternatives in a series where we need data privacy and

data access at the same time. Thus we are attempting to assure the calibre of the drug, the refuge of the transaction, and the surety of the data by using blockchain technology.

III. LITREATURE SURVEY

Nowadays, some technical and practical works which are already proposed in the medicine supply chain to detect substandard drugs with blockchain, but there are some general discussions. Such as, Mettler et al. [5] specially proposed the opportunity to save you counterfeit medicinal drug within side the drug enterprise the usage of blockchain. Kurki [6] discussed the advantages and instructions for utilizing blockchain within the drug supply chain. Bocek et al. [4] had developed a prototype of Ethereum smart contract-based drug supply chain traceability system [7], without explaining the specific design of the workflow. The methods discussed by Shaik included the use of providing product with public and private keys as QR code, the app used to scan the QR should have cryptographic functionality to decrypt the QR code. The manufacturer is also supposed to run server to accept request and match the buyers name, and items code. The scanning app need to have cryptographic capability to decrypt ciphertext of the object code encoded withinside the QR code [9]. Benattia and Baudry et.al explains traceability-CPS based architecture for supply chain management consists of several layers that interact to form a traceability-CPS. Also, the proposed structure lets in deliver chain tracking and information analytic to beautify product. Safety and quality. The proposed algorithm consist on computing the most frequent item sets in the product transaction database. This item sets are then used as genuine product trajectories and can serve in detecting abnormal product behaviour. In this blockchain technology for information sharing is proposed. Is this the information is in the control of the owner so third party interference is difficult. Users are always aware of the data that is being collected about them and how it is used. The blockchain block contains sender, amount, receiver, transaction id, product id and metadata [6]. Ethereum is a open-source Blockchain. Ethereum is a technology that's home to digital money, global payments and applications. The procedure is straightforward as to get into the portal, select out a pockets that helps you to connect with Ethereum and control your funds, Get the ETH, use programs powered, powered by Ethereum, start building [11]. The limitations in the existing systems are that brands used QR codes on products to prove the validity of the product. But the QR code can be copied and used to label counterfeit products [9]. In the RFID primarily based totally device that low-Cost RFID tags may be used for car identity of products, however because of cloning of RFID tags, this technique isn't suitable [14].

IV. PROPOSED METHOD

Counterfeit has unfolded international and has big outcomes on organizations, manufacturers, and consumers. It affects the influence of the organization and the wellbeing of the consumers. India is not excluded. The proposed machine is aimed toward client products, and it facilitates song he goods via way of means of preserving the product and the deliver chain integrity via way of means of the usage of Blockchain. This offers the clients the strength to music the records of the whole product from producer to client the use of blockchain and QR code.

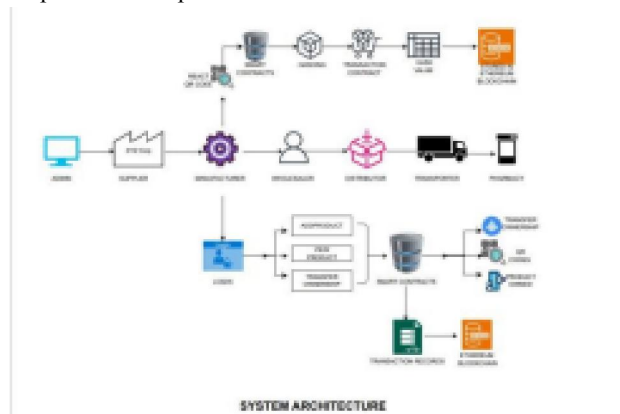


Fig 1 System Architecture

A. System Model.

The proposed system will be a decentralized application (DApp) which will be implemented using the Ethereum Network as the main blockchain for keeping all the records and managing the transactions regarding the products of the companies listed on DApp.

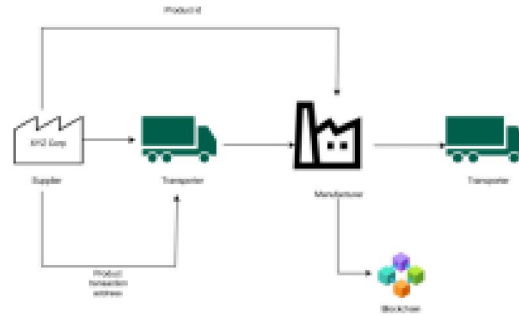
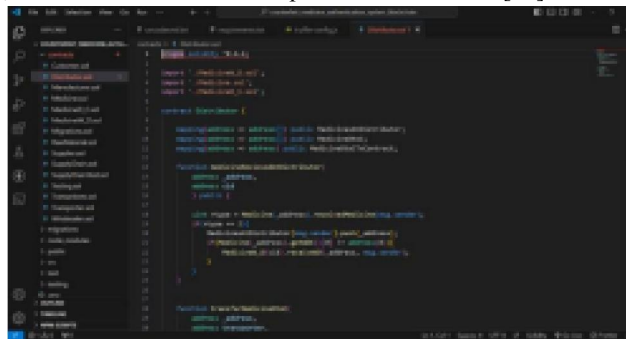


Fig 2 Flow of Transaction

Ethereum:

Ethereum It is a decentralized blockchain which uses a proof-of-work consensus mechanism. Proof-of-work is adding block to the blockchain by solving the mathematical expressions. Solving the puzzle “proves” that nodes have done the “work” by using computational resources. It confirms that the block is added and recorded in the blockchain. This process is known as mining. Mining is typically brute force trial and error, but successfully adding a block is rewarded in Ethereum (ETH) [1][9]. Smart contract Smart contracts are programs that are stored inside Blocks. Smart contracts replace the involvement of third-party members. These are basically protocols that execute when the conditions are satisfied. They never change, that means no one can tamper with the contract [15].



```

    pragma solidity ^0.8.0;

    contract Distributor {
        address[] public distributors;
        address[] public products;

        constructor(address[] memory _distributors, address[] memory _products) {
            distributors = _distributors;
            products = _products;
        }

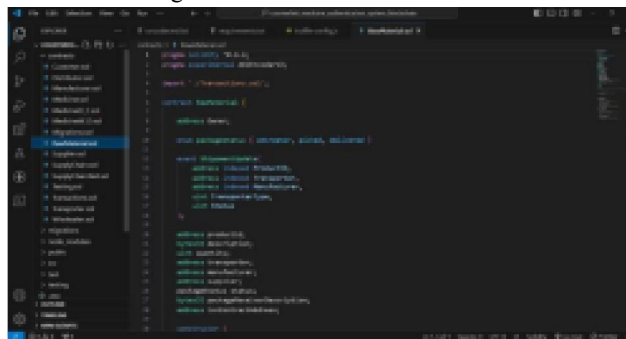
        function addDistributor(address _distributor) public {
            distributors.push(_distributor);
        }

        function addProduct(address _product) public {
            products.push(_product);
        }

        function isDistributor(address _distributor) public view returns (bool) {
            for (uint i = 0; i < distributors.length; i++) {
                if (distributors[i] == _distributor) return true;
            }
            return false;
        }

        function isProduct(address _product) public view returns (bool) {
            for (uint i = 0; i < products.length; i++) {
                if (products[i] == _product) return true;
            }
            return false;
        }
    }
  
```

Fig. 3 Distributor Smart Contract



```

    pragma solidity ^0.8.0;

    contract RawMaterial {
        address[] public rawMaterials;

        constructor(address[] memory _rawMaterials) {
            rawMaterials = _rawMaterials;
        }

        function addRawMaterial(address _rawMaterial) public {
            rawMaterials.push(_rawMaterial);
        }

        function isRawMaterial(address _rawMaterial) public view returns (bool) {
            for (uint i = 0; i < rawMaterials.length; i++) {
                if (rawMaterials[i] == _rawMaterial) return true;
            }
            return false;
        }
    }
  
```

Fig. 4 Raw Material Smart Contract

V. IMPLEMENTATION

Smart contract

Smart contracts are programs that are stored inside Blocks. Smart contracts replace the involvement of third-party members. These are basically protocols that execute when the conditions are satisfied. They never change, that means no one can tamper with the contract [9]. To design a framework CFDD (Counterfeit Drug Detection) using Blockchain technology which is capable of tracing drugs throughout the pharmaceutical supply chain in order to combat the issues of fake medicines.

- Reduced falsification associated losses- CFDD can hold clean music and hint file of whole pills adventure from producer to patient. Therefore, detection of counterfeit pills could grow to be smooth withinside the deliver chain.
- The use of blockchain withinside the pharmaceutical deliver chain can permit specific places of drug treatments to be identified. It is viable to ship or carry out the batch reminders correctly and speedy whilst keeping improved affected person fitness safety.
- The improved traceability helps the optimization of products go with the drift and a green gadget of inventory management. Blockchain generation is especially able to preserving song of the drug records at some stage in the pharmaceutical deliver

chain. Important aspects that make Blockchain data secure and safe are that the blocks are timestamped and immutable making tampering of information impossible. Organizations can have either a private blockchain or a public. The organizations will share a distributed ledger between the parties involved in the manufacture and distribution of the drug on these blockchains. Moreover, in those blockchains best restricted get admission to is supplied which relies upon at the facts sharing agreement most of the parties. With Blockchain we will hold whole song of the medication starting from producers to stop consumers. Every time the drug travels from one entity to another, the statistics is saved at the block deliver chain. This makes the traceability of drugs an easy task and thus helps in combating counterfeits from the industry

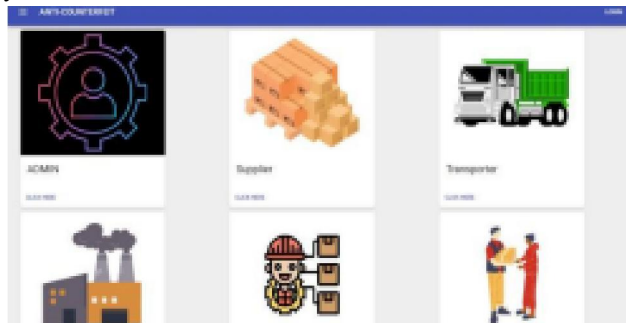


Fig. 5 Interface

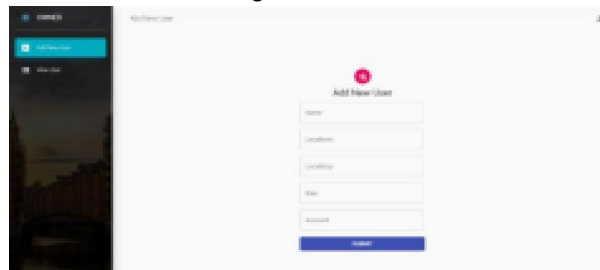


Fig 6 Admin can add users and assign roles to them

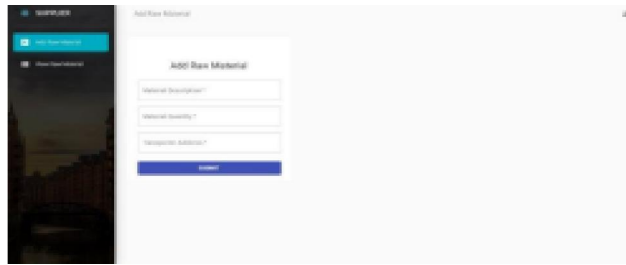


Fig 7 Supplier



Fig 8 Product Details

After creating medicines, the QR code of the hash value will be generated.

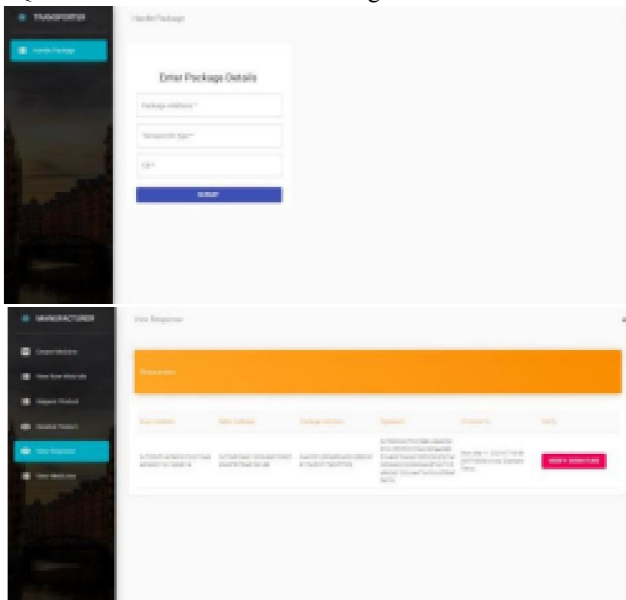


Fig 9 Digital Signature

The manufacturer can create new medicines as well as will request and receive the products. The manufacturer will use digital signature using raw material id and manufacturer address.

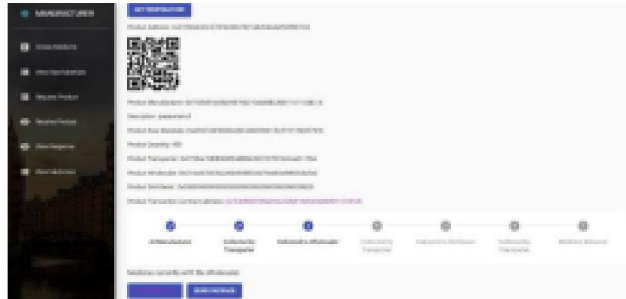


Fig 10 Medicine Details

The unique hash value will be generated for medicine and QR code will be generated.



Fig 11 Transporter The Transporter will handle the package.

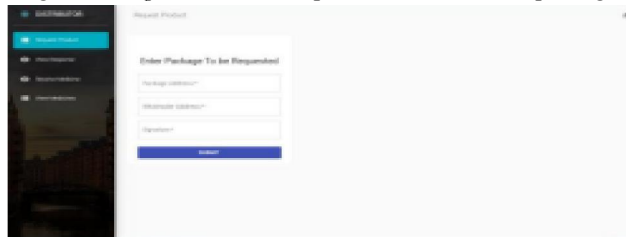


Fig 12 Manufacturer

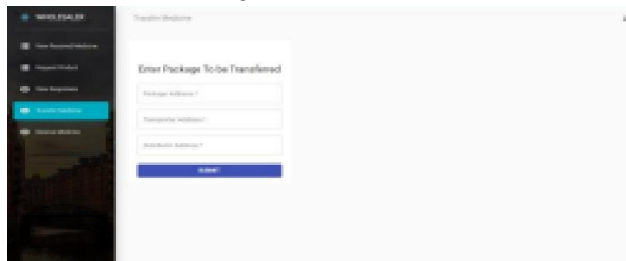


Fig 13 Wholesaler

Wholesaler can receive and transfer the medicine to distributor through transporter, received from manufacturer. Distributor will receive and view the medicine sent by wholesaler through transporter. The Distributor will send the medicine to the pharmacy or the end user or patients.

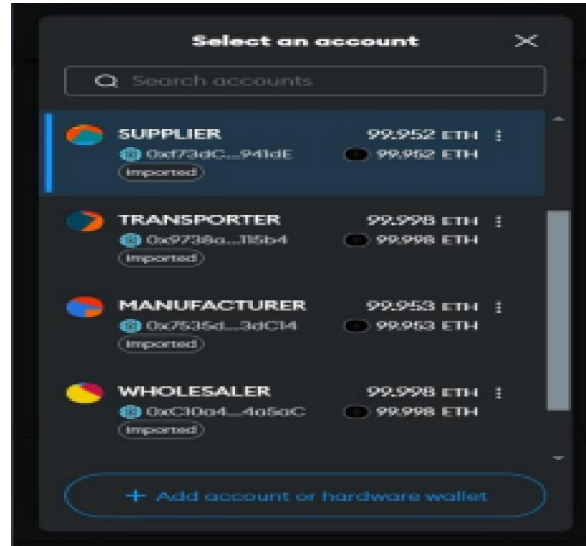


Fig 14 MetaMask Wallet

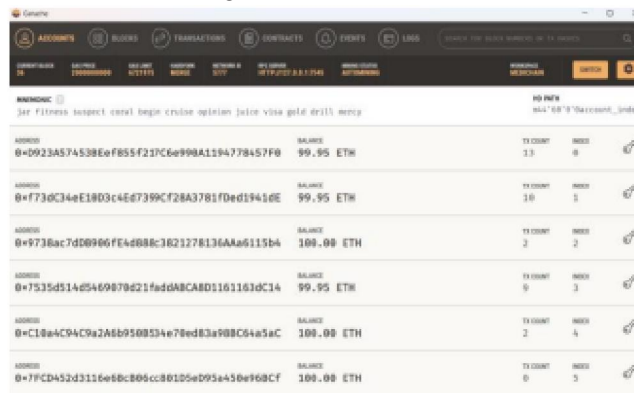


Fig 15 Ganache

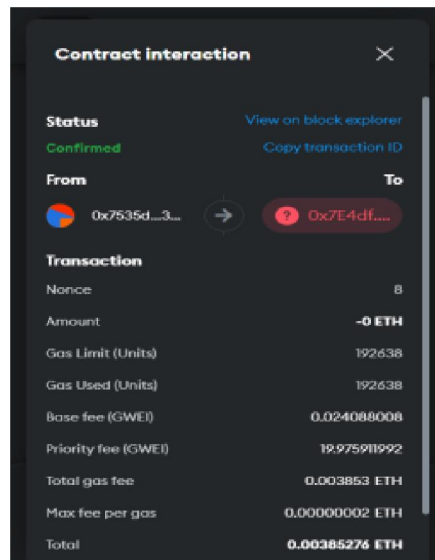


Fig 16 Transaction interaction

The two main issues which will be overlooked by CFDD are: firstly, pharmaceutical companies will be able to track their products throughout the supply chain, building an airtight circuit prohibiting the entry of counterfeit drugs. Secondly, stakeholders specifically labs will be able to take posterior action by detecting the exact location of their drugs.

VI. CONCLUSION

The proposed framework can provide both manufacturer's authenticity as well as drug security. The current methodologies for combating counterfeit drugs works on third-party trust and thus lacks in terms of security for the drug safety. In comparison to these current methodologies, the proposed framework is based on Blockchain and is hence highly secure and capable of dealing with the fake drugs menace.

REFERENCES

- [1] Constantine Xipolitopoulos, Maria Nefeli Nikiforos, Maria Malakopoulou, and Adamantia Pateli. Success factors for crowd funding campaigns with machine learning techniques. 09 2020.J. Breckling, Ed., *The Analysis of Directional Time Series: Applications to Wind Speed and Direction*, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.
- [2] Firmansyah Ashari. Smart contract and blockchain for crowdfunding platform. *International Journal of Advanced Trends in Computer Science and Engineering*, 9:3036–3041, 06 2020.M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in *Proc. ECOC'00*, 2000, paper 11.3.4, p. 109.
- [3] 5. Huixin Wu and Feng Wang. A survey of noninteractive zero knowledge proof system and its applications. *The Scientific World Journal*, 2014, 2014. (2002) The IEEE website. [Online]. Available: <http://www.ieee.org/>
- [4] SHA 256. Available: <https://github.com/feross/simple-sha256> Paik, Michael, Ashlesh Sharma, Arthur Meacham, Giulio Quarta, Philip Smith, John Trahanas, Brian Levine, Mary Ann Hopkins, Barbara Rapchak, and Lakshminarayanan Subramanian. "The case for Smart Track." In *Information and Communication Technologies and Development (ICTD)*, 2009 International Conference on, pp. 458-467. IEEE, 2009.*FLEXChip Signal Processor (MC68175/D)*, Motorola, 1996.
- [5] "Sylim P, Liu F, Marcelo A, Fontelo P. Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention. *JMIR Res Protoc*. 2018;7(9):e10163. Published 2018 Sep 13. doi:10.2196/10163..
- [6] Shen, M., Tang, X., Zhu, L., Du, X., &Guizani, M. (2019). Privacy Preserving Support Vector Machine Training over Blockchain-Based Encrypted IoT Data in Smart Cities. *IEEE Internet of Things Journal*, 1–1. doi:10.1109/jiot.2019.2901840
- [7] K. Toyoda, P. T. Mathiopoulos, I. Sasase and T. Ohtsuki, "A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain," in *IEEE Access*, vol. 5, pp. 17465-17477, 2017, doi: 10.1109/ACCESS.2017.2720760.*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.
- [8] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," in *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366-1385, 1 July 2018, doi: 10.1109/TKDE.2017.2781227.
- [9] Pahlavan K., Li X., Ylianttila M., Chana R., Latva-aho M. (2000) An Overview of Wireless Indoor Geolocation Techniques and Systems. In: Omidyar C.G. (eds) *Mobile and Wireless Communications Networks*. MWCN 2000. Lecture Notes in Computer Science, vol 1818. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45494-2_1
- [10] S. Maria Celestin Vigila and K. Muneeswaran, "Elliptic curve based key generation for symmetric encryption," 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies, Thuckafay, 2011, pp. 824-829, doi: 10.1109/ICSCCN.2011.6024664. [11] qrious. Available: <https://github.com/neocotic/qrious>

[12] H. H. Cheung and S. H. Choi, "Implementation issues in RFID-based anti-counterfeiting systems," *Comput. Ind.*, vol. 62, no. 7, pp. 708–718, 2011. [13] SHA 256. Available: <https://github.com/feross/simple-sha256>