IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⋇ Impact Factor 7.39 ⋇ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11771

Authentication of Products and Counterfeit Elimination Using Blockchain

Megha M.N[1], Prof. B. P Sowmya[2]

PG Scholar, Dept. of MCA, PES College of Engineering, Mandya, Karnataka, India[1]

Assistant Professor, Dept. of MCA, PES College of Engineering, Mandya, Karnataka, India[2]

Abstract: Interest in blockchain technologies has grown over the past few years. Even while the use case involving financial transactions has received the greatest attention, it could have an impact on other industries. Transparency is increased through blockchain, and the need for reliable middlemen is diminished. This essay examines the viability of using blockchain technology to spot fake goods. This essay covers the various anti-counterfeiting tactics, blockchain technologies, and the traits that make blockchain such an attractive application case. Three different designs have been created, and we are still working to refine an existing system concept. It is known that reducing counterfeits won't be possible by employing simply technological means. Having tamper-proof packaging, a dependable alarm system, raising awareness, and battling counterfeiters legally are important elements. These elements, when paired with blockchain technology, can result in a thorough and effective counterfeiting reduction approach. Some phrases that are similar include blockchain, encryption, and authentication.

INTRODUCTION

Even though there are many fakes all around us, it may not seem like a distant concept. It is estimated that counterfeiting costs the US economy over $600 billion yearly and impacts a variety of goods, including clothing, electronics, software, and retail goods. In fact, the International Chamber of Commerce projects that by 2022, the negative effects of piracy and counterfeiting will cost the world economy US$4.2 trillion and jeopardise 5.4 million actual jobs. In the pharmaceuticals sector, where it now responsible for roughly 1 million fatalities annually in a $75 billion industry, estimates indicate that the market for fake drugs is expanding twice as quickly as that for actual treatments. Due to this, the worldwide illicit drug trade is up to 25 times more profitable than the market for bogus drugs. Every transaction is built on the principle of trust. Sending money, exchanging commodities, or doing both becomes difficult when there is no confidence between the parties. It becomes even more challenging when banks and other stakeholders are involved in several transactions. A transaction frequently involves more than one third party. In addition to the banks of the sender and the recipient, international money transfers also require the services of other intermediary organisations, such as clearing houses. The parties to the transaction must have faith in all parties involved, not just one another. By doing away with these middlemen, procedures can become more transparent, more efficient, and quicker. The success of Bitcoin has demonstrated that it is possible to do away with these middlemen.

LITERATURE SURVEY

1. Protocols for public key cryptosystems

New cryptographic protocols which take full advantage of the unique properties of public key cryptosystems are now evolving. Several protocols for public key distribution and for digital signatures are briefly compared with each other and with the conventional alternative.

2. Ethereum: A secure decentralised generalized transaction ledger

The blockchain paradigm when coupled with cryptographically-secured transactions has demonstrated its utility through a number of projects, with Bitcoin being one of the most notable ones. Each such project can be seen as a simple application on a decentralised, but singleton, compute resource. We can call this paradigm a transactional singleton machine with shared-state. Ethereum implements this paradigm in a generalised manner. Furthermore it provides a plurality of such resources, each with a distinct state and operating code but able to interact through a message-passing framework with others. We discuss its design, implementation issues, the opportunities it provides and the future hurdles we envisage

3. Practical byzantine fault tolerance and proactive recovery

Our growing reliance on online services accessible on the Internet demands highly available systems that provide correct service without interruptions. Software bugs, operator mistakes, and malicious attacks are a major cause of service interruptions and they can cause arbitrary behavior, that is, Byzantine faults. This article describes a new replication algorithm, BFT, that can be used to build highly available systems that tolerate Byzantine faults. BFT can be used in

DOI: 10.17148/IJARCCE.2022.11771

practice to implement real services: it performs well, it is safe in asynchronous environments such as the Internet, it incorporates mechanisms to defend against Byzantine-faulty clients, and it recovers replicas proactively. The recovery mechanism allows the algorithm to tolerate any number of faults over the lifetime of the system provided fewer than 1/3 of the replicas become faulty within a small window of vulnerability. BFT has been implemented as a generic program library with a simple interface. We used the library to implement the first Byzantine-fault-tolerant NFS file system, BFS. The BFT library and BFS perform well because the library incorporates several important optimizations, the most important of which is the use of symmetric cryptography to authenticate messages. The performance results show that BFS performs 2% faster to 24% slower than production implementations of the NFS protocol that are not replicated. This supports our claim that the BFT library can be used to build practical systems that tolerate Byzantine faults.

4. Making byzantine fault tolerant systems tolerate byzantine faults

This paper argues for a new approach to building Byzantine fault tolerant replication systems. We observe that although recently developed BFT state machine replication protocols are quite fast, they don’t tolerate Byzantine faults very well: a single faulty client or server is capable of rendering PBFT, Q/U, HQ, and Zyzzyva virtually unusable. In this paper, we (1) demonstrate that existing protocols are dangerously fragile, (2) define a set of principles for constructing BFT services that remain useful even when Byzantine faults occur, and (3) apply these principles to construct a new protocol, Aardvark. Aardvark can achieve peak performance within 40% of that of the best existing protocol in our tests and provide a significant fraction of that performance when up to f servers and any number of clients are faulty. We observe useful throughputs between 11706 and 38667 requests per second for a broad range of injected faults.

5. Architecture of the hyperledger blockchain fabric

A blockchain is best understood in the model of state-machine replication [8], where a service maintains some state and clients invoke operations that transform the state and generate outputs. A blockchain emulates a “trusted” computing service through a distributed protocol, run by nodes connected over the Internet. The service represents or creates an asset, in which all nodes have some stake. The nodes share the common goal of running the service but do not necessarily trust each other for more. In a “permissionless” blockchain such as the one underlying the Bitcoin cryptocurrency, anyone can operate a node and participate through spending CPU cycles and demonstrating a “proof-of-work.” On the other hand, blockchains in the “permissioned” model control who participates in validation and in the protocol; these nodes typically have established identities and form a consortium. A report of Swanson compares the two models

The Hyperledger Project (www.hyperledger.org) is a collaborative effort to create an enterprise-grade, open-source distributed ledger framework and code base. It aims to advance blockchain technology by identifying and realizing a cross-industry open standard platform for distributed ledgers, which can transform the way business transactions are conducted globally. Established as a project of the Linux Foundation in early 2016, the Hyperledger Project currently has more than 50 members.

Hyperledger Fabric (github.com/hyperledger/fabric) is an implementation of a distributed ledger platform for running smart contracts, leveraging familiar and proven technologies, with a modular architecture allowing pluggable implementations of various functions. It is one of multiple projects currently in incubation under the Hyperledger Project. A developerpreview of the Hyperledger Fabric (called “v0.5-developer-preview”) has been released in June 2016 (github.com/hyperledger/fabric/wiki/Fabric-Releases).

PREVIOUS STUDY

The original product (BAR CODE) may be purchased through a variety of third-party distributors, who may also make knockoffs of the original product with the original label still attached. In the event that fraudulent drugs are developed, both major monetary loss and human lives may be lost. Any online transaction involving a third party, not merely supply chains, must be carried out with the customer's trust. Regrettably, occasionally, third parties engage in fraud or abuse user data.

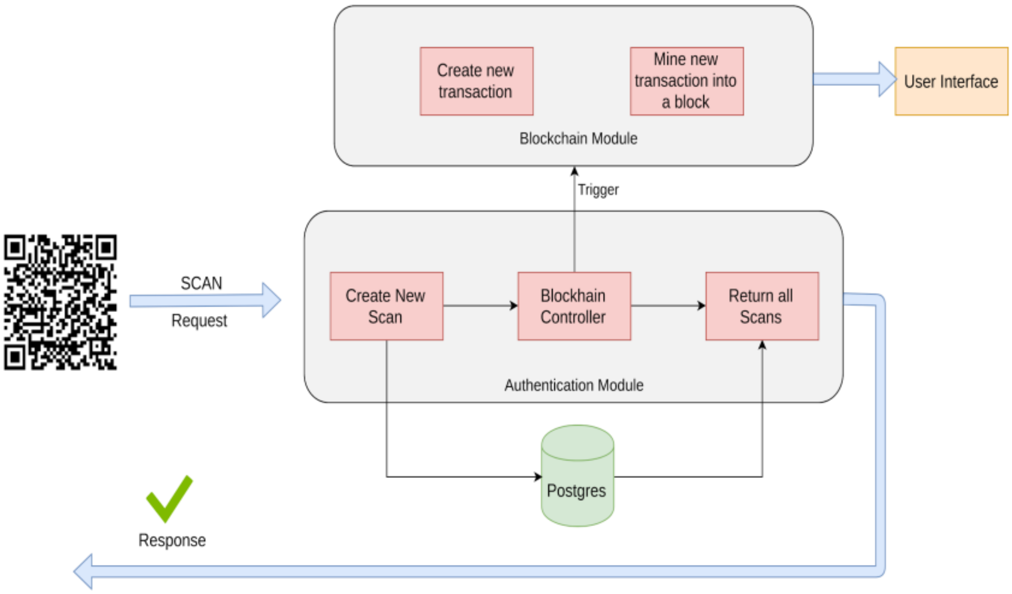
METHODOLOGY

With the use of blockchain technology, there is no longer a need for a third party, and verification may be completed solely by computer algorithm. We are converting all product information and barcodes into digital signatures to avoid fraudulent counterfeit. Because the blockchain platform allows for tamper-proof data storage, these digital signatures will be kept on a server there. If data on the blockchain server is unintentionally changed, verification will fail at the following block storage and the user may be alerted about the change.

1) Save Product with Blockchain Entry: In this module user will enter product details and then upload product bar code image and then digital signature will be generated on uploaded barcode and then this transaction details will be store in Blockchain. Before storing transaction Blockchain will verify all old transaction and upon successful verification new transaction block will be store

DOI: 10.17148/IJARCCE.2022.11771

2) Retrieve Product Data: Using this module user can search existing product details by entering product id
3) Authenticate Scan: Here in this module we don’t have any scanner so we are uploading original or fake bar code images and then Blockchain will verify digital signature of uploaded bar code with already store bar codes and if match found then Blockchain will extract all details and display to user else authentication will be failed.



CONCLUSION

This method allows the buyer to monitor the product's journey from the manufacturer to the client and provides assurance that the scans were real. The producer can verify the legitimacy of the journey by tracking the movement of their products. The arrangement is easy to use and costs little to maintain. Manufacturers can use RFID or NFC tokens in place of QR codes to further strengthen their system.

BIBLIOGRAPHY

[1] Satoshi Nakamoto, ―Bitcoin: A Peer-to-Peer Electronic Cash System‖, 2008
[2] Hyperledger, ―Hyperledger Blockchain Performance Metrics‖, V1.01, October 2018
[3] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.
[4] Armin Ronacher, ―Flask Docs‖, http://flask.pocoo.org/docs/‖
[5] G. Wood, __Ethereum: A secure decentralised generalized transaction ledger,‘‘ Tech. Rep., 2014.
[6] OECD (2016), Illicit Trade: Converging Criminal Networks, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, https://doi.org/10.1787/9789264251847-en.
[7] M. Castro and B. Liskov, __Practical byzantine fault tolerance and proactive recovery,‘‘ ACM Trans. Comput. Syst., vol. 20, no. 4, pp. 398–461, Nov. 2002.
[8] Clement, E. Wong, L. Alvisi, M. Dahlin, and M. Marchetti, __Making byzantine fault tolerant systems tolerate byzantine faults,‘‘ in Proc. 6th USENIX Symp. Netw. Syst. Design Implement., 2009, pp. 153–168.
[9] Cachin, __Architecture of the hyperledger blockchain fabric,‘‘ Tech. Rep., Jul. 2016..
[10] S. Underwood, ―Blockchain Beyond Bitcoin‖, in Communications of the ACM, vol. 59, no. 11, p. 15-17, 2016.