A Case Study on Authentication of Product Using Blockchain: Authentication of Product & Counterfeits Elimination Using Blockchain

N. Shilpa[1], T. Nikhil[2], T. Deekshith Raj[3], P. Saketh Reddy[4], S.Raja Sehkar Reddy[5]

[1]Assistant professor, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

[2,3,4,5] IV[th]Btech Student, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

ABSTRACT

Blockchain technologies have gained interest over the last years. While the most explored use case is financial transactions, it has the capability to agitate other markets. Blockchain remove the need for trusted intermediaries, can facilitate faster transactions and add more transparency. This paper explores the possibility to deflate counterfeit using blockchain technology. This paper provides an overview of different solutions in the anti-counterfeit area, different blockchain technologies and what characteristics make blockchain especially interesting for the use case. We have developed three different concepts and the expansion of an existing system concept, is pursued further. It is shown, that reducing counterfeits cannot be achieved by using technological means only. Increasing awareness, fighting counterfeiters on a legal level, a good alert system, and having tamper-proof packaging are all important aspects. These factors combined with blockchain technology can lead to an efficient and comprehensive approach to reduce counterfeiting

INTRODUCTION

Although it may seem like a far-off idea, we are surrounded by a lot of counterfeits. From fashion and retail products to software, digital media, electronics, piracy, and intellectual property, reports put the cost of counterfeiting somewhere around $600bn a year in the US alone. In fact, the International Chamber of Commerce predicts that the ―negative impacts of counterfeiting and piracy are projected to drain US$4.2 trillion from the global economy and put 5.4 million legitimate jobs at risk by 2022. In Pharmaceuticals, the counterfeit medicine market is now responsible for around 1 million deaths per year, in an industry estimated to be worth $75bn annually. In fact, the counterfeit medicine industry is estimated to be growing at twice the rate of legitimate pharmaceuticals, making it up to 25 times more lucrative than the global narcotics trade. Trust is a central element in all transactions. No matter if sending money or exchanging goods, it becomes difficult if

there is no trust between the entities involved. It becomes even more difficult, as with many transactions, third parties are involved, such as banks. Often, not only one third-party is involved in a transaction, but multiple. An international money transfer does not only include the bank of the sender, the bank of the receiver, but also multiple intermediary entities such as clearing houses. The entities involved in the transaction do not only have to trust each other, but also the third parties. Removing these third parties can decrease transaction cost, facilitate faster transactions and add more transparency. Bitcoin has successfully shown that removing such third-parties is possible. The cryptocurrency permits direct sending coins to a transaction partner, without the need to use banks and clearing houses. The assets are directly transferred from one account to another. There are no intermediaries and thereby no need to trust third parties. In addition, the question if a transaction is valid is not answered by an institution, but by algorithms used. Therefore, it completely removes the need to trust any third party. The technology behind Bitcoin, the blockchain, can however not only be used for financial transactions and crypto currencies in general. The technology has potential to ―redefine the digital economy‖ [10], because it allows immutable transactions, which can be checked at all times from everyone. This is because the information is publicly available and distributed globally. It is ―chronologically updated and cryptographically sealed‖ [11]. The full range of applicable use cases for this technology has to be seen, but tracking ownership and history of a product is surely one of them [12]. This paper explores the possibility to reduce counterfeit using blockchain technology.

Authentication ,the act of establishing or conforming something as genuine. Authentication is of utmost importance because the use of counterfeit medicines can be harmful to the health and wellbeing of the patients. Their use may result in treatment failure or even death. Authentication is generally done through the overt or covert features upon the product

―We now have more fakes than real drugs in the market.‖ ― Christophe Zimmermann, the anti-counterfeiting and piracy coordinator of the World Customs Organization [6]. Current anti-counterfeiting supply chains rely on a centralized authority to combat counterfeit products. This architecture results in issues such as single point processing, storage, and failure. Blockchain technology has emerged to provide a promising solution for such issues. In this paper, we propose the block-supply chain, a new decentralized

supply chain that detects counterfeiting attacks using blockchain and Near Field Communication (NFC) technologies. Block-supply chain replaces the centralized supply chain design and utilizes a new proposed consensus protocol that is, unlike existing protocols, fully decentralized and balances between efficiency and security. Our simulations show that the proposed protocol offers remarkable performance with a satisfactory level of security compared to the state-of-the-art consensus protocol Tender mint.

2. LITERATURE SURVEY

Anti-counterfeiting solutions should protect organizations from financial and reputation losses, and, especially in the case of pharmaceutical products, customer safety. argues that good anti-counterfeiting techniques should generally be simple to apply, but difficult to imitate and have four main features: They should be difficult to duplicate, it should be possible to identify them without special equipment, it should be difficult to re-use them, and it should be visible if they were tampered with. From a product perspective, there are three general technologies to reduce counterfeits

Overt (Visible) Features expected to assist the users to confirm the genuineness of a pack. Such features will be significantly visible, and complex or expensive to reproduce. This includes holograms, colour shifting inks, security threads, water marks etc. The advantage of overt technologies is that they can be checked by the end consumer.

Covert (Hidden) Features the rationale of a covert feature is to aid the brand owner to recognize a counterfeit product. The general public will not be aware of its presence nor will have the resources to confirm it. This includes UV, bi-fluorescent and pen-reactive ink, as well as digital watermarks and hidden printed messages. Covert technologies help to identify counterfeits in the supply-chain and are especially efficient combined with overt technologies.

Track and trace include Radio Frequency Identification (RFID) tags, Electronic Product Codes (EPCs) and barcodes. Track and trace technologies allow for simpler tracing of products, thereby enabling the reduction of counterfeits, as the history of a product is available. The tag or barcode is included by the manufacturer. Distributors scan the identification, enabling them to check the authenticity of the product and update the status. Finally, retailers can also scan the product, to check the history and authenticity of the product. This approach does not only tackle the counterfeit problem, but also enables track and trace through the whole product lifecycle.

2.1 Features of the project

Supply chain tracking:

The product's journey through the supply chain is tracked by updating the blockchain with information like the manufacturer, date of production, and location of production.

Consumer verification:

Consumers can verify the authenticity of a product by scanning its barcode or serial number and checking it against the blockchain record.

Anti-counterfeiting measures:

Products can be designed with unique physical features, such as holograms or watermarks, that are difficult to reproduce. Additionally, the barcode and other product information can be encrypted and secured using advanced cryptographic techniques.

Data analytics:

The data collected from the blockchain can be used to identify patterns and anomalies in the supply chain that may indicate the presence of counterfeit products.

Integration with existing systems:

The blockchain-based system can be integrated with existing supply chain management systems to streamline the authentication process.

Security and privacy:

The system should be designed with strong security and privacy measures to protect against data breaches and unauthorized access.

These are just a few potential features of a blockchain-based product authentication and counterfeits elimination system. The actual features of the system will depend on the specific requirements and goals of the project.

2.2 Technologies required for implementation

2.2.1. Bitcoin: A Peer-to-Peer Electronic Cash System

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed,

but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and re-join the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust-based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes

2.2.2. Hyperledger Blockchain Performance Metrics

This is the first white paper from the Hyperledger Performance and Scale Working Group. The purpose of this document is to define the basic terms and key metrics that should be used to evaluate the performance of a blockchain and then

communicate the results. This paper also serves as a platform-agnostic resource for technical blockchain developers and managers interested in using industry-standard nomenclature.

While we appreciate that there may be discrete definitions for the terms "blockchain" and "Distributed Ledger Technology (DLT)," for the purposes of this paper we will treat both terms synonymously and use the term "blockchain" throughout.

This document provides some guidance on selecting and evaluating workloads. We expect that refinements to these definitions and new blockchain-specific metrics will warrant future revisions of this document.

In future documents, the Working Group plans to discuss workloads in greater detail and to offer additional guidance on standard procedures and emerging best practices for evaluating blockchain performance. To provide your feedback and stay informed about subsequent versions of this paper, please join us in the Performance and Scale Working Group.

2.2.3. 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.

2.2.4. 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.

2.2.5. 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 behaviour, 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 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.

2.2.6. 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.

2.2.7. 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 developer preview of the Hyperledger Fabric (called “v0.5-developer-preview”) has been released in June 2016.

3. METHODOLOGY

In this paper author is using Blockchain technology to authenticate supply chain products as this product may be supplied from multiple third-party distributors and this distributor can make clone/fake/counterfeits of this product BAR CODE and then manufacture fake products and add this counterfeit label to fake product and this fake product can cause huge loss of financial and lives if fake medicine manufacture.

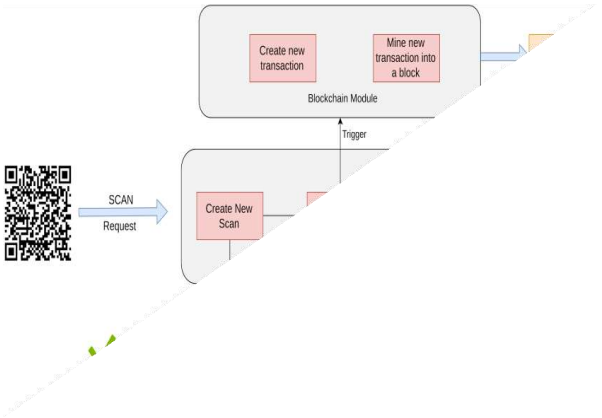
Not only supply chain any other online transaction require third party to complete transaction and peoples has to trust on third parties to complete their transaction and sometime this third parties can make fraud transaction or misuse user data.

To avoid this problem author using Blockchain technology which does not require any third party and verification will be done by software algorithm itself without involvement of any third party. In this to avoid forge counterfeit we are converting all products details/barcode into digital signatures and this digital signature will be stored in Blockchain server as this Blockchain server support tamper proof data storage and nobody can hack or alter its data and if by a chance if its data alter then verification get failed at next block storage and user may get intimation about data alter.

In Blockchain technology same transaction data stored at multiple servers with hash code verification and if data alter at one server, then it will be detected from other server as for same data hash code will get different. For example in Blockchain technology data will be stored at multiple servers and if malicious users alter data at one server, then its hash code will get changed in one server and other servers left unchanged and this changed hash code will be detected at verification time and future malicious user changes can be prevented.

In supply chain also all products barcode digital Blockchain signatures will be stored and if any third-party distributor makes clone of barcode, then its signature will be mismatch and counterfeit will be detected

In Blockchain each data will be stored by verifying old hash codes and if old hash codes remain unchanged then data will be considering as original and unchanged and then new transaction data will be appended to Blockchain as new block. For each new data storage all blocks hash code will be verified



4.Modules:

4.1. 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

4.2. Retrieve Product Data:

Using this module user can search existing product details by entering product id

4.3. 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.

5. TESTING, VALIDATION

5.1 INTRODUCTION

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of tests. Each test type addresses a specific testing requirement.

5.2 TESTING METHODOLOGIES

5.2.1 Unit Testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

5.2.2 Integration Testing

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

5.2.3 Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

5.2.4 System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration-oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

5.2.5 White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

5.2.6 Black Box Testing

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

5.2.7 Acceptance Testing

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

Test Results: All the test cases mentioned above passed successfully. No defects encountered

6. Conclusion

We create projects based on online transactions that involve the use of a third party to complete the transaction. People must trust third parties to complete their transactions, and third parties can sometimes commit fraud or misuse user data. To circumvent this issue, the author has chosen Blockchain technology, which does not require the involvement of a third party and allows for verification to be carried out by a software algorithm without the involvement of a third party. To avoid forging counterfeits, we are converting all product details/barcodes into digital signatures, which will be stored in a Blockchain server, which supports tamper-proof data storage and no one can hack or alter its data. If its data is altered by chance, verification will fail at the next block storage, and the user will be notified. In Blockchain technology, the same transaction data is saved on many servers with hash code verification, and if the data on one server changes, it will be noticed on the other servers since the hash code for the same data would change. In Blockchain technology, for example, data will be stored on multiple servers, and if malicious users alter data on one server, the hash code will be changed on one server while the other servers remain unchanged, and this changed hash code will be detected at verification time, preventing future malicious user changes.

7. Future Scope

Multiple techniques to reducing counterfeits were examined in this thesis. These improvements were considered, and their impact on minimising counterfeits was assessed, in order to be less reliant on external variables. Due to time constraints and the fact that several other system changes were also required, it was not possible to implement all of the suggested changes. The finalisation of these implementations for the proposed system, as well as the potential of running pilots, are among the next steps. The concept for reducing counterfeits in the humanitarian supply chain is currently being developed, as is the execution.

8. References

Satoshi Nakamoto, ―Bitcoin: A Peer-to Peer Electronic Cash System‖, 2008

Hyperledger, ―Hyperledger Blockchain Performance Metrics‖, V1.01, October 2018

R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium

on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

Armin Ronacher, ―Flask Docs‖, http://flask.pocoo.org/docs/‖

G. Wood, __Ethereum: A secure decentralised generalized transaction ledger,‘‘ Tech. Rep., 2014. Vol 13, Issue 03, MARCH/2022 ISSN NO:0377-9254 www.jespublication.com PageNo:602

OECD (2016), Illicit Trade: Converging Criminal Networks, OECD Reviews of Risk Management Policies, OECD Publishing, Paris.

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.

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.

Cachin, __Architecture of the hyperledger blockchain fabric,‘‘ Tech. Rep., Jul. 2016.

S. Underwood, ―Blockchain Beyond Bitcoin‖, in Communications of the ACM, vol. 59, no. 11, p. 15-17, 2016.