An Application of Blockchain to Secure the Conventional Product Authentication Management System

Md. Azizul Hakim Sowrov[1], Md Asaduzzaman[1], Ifthekharul Islam[1], Md Mushfiqur Rahman[1] and Rashed Mazumder[2]

[1]Bangladesh University of Professionals, Mirpur-12, Dhaka, Bangladesh
[2]Institute of Information Technology, Jahangirnagar University, Dhaka-1342, Bangladesh
rakhu345@yahoo.com

Abstract. Products counterfeit is a multi-billion dollars market, and the growth of this field is high. There have been many technological enhancements like Radio Frequency Identification (RFID) and Encrypted Quick Response (EQR) code. These technologies have been used to track down those products in the supply chain downstream and identify products for authenticity. Under these circumstances, all existing solutions must rely on a central database for operating. The matter of this subject points out the drawback of single point of failure. As a result, these systems are more prone to cyber-attacks. In some cases, supply chain insiders play as a bad actor of the system too. To prevent this, tracing concrete proof of provenance of transactions is needed. In addition, business operations require contract and consensus. These can be solved using blockchain technology. As business requires privacy and cannot rely on public network. Thus, the solution of this need requires to be built enterprise blockchain environment.

Keywords: Blockchain, Hyperledger Fabric.

1 Introduction

Product counterfeit is world-wide problem. Over the years, many national and international brands have been suffering in this problem. Every year many nation and international brands like luxury product loses billions of dollars due to counterfeit syndicates. Usually, companies generate a loss of more than 12 billion us dollars per year due to product counterfeit [1]. Over the year, many technological solutions have been introduced to tackle this problem. In addition, many systems have been built to tackle the issue of security attacks on the product authentication system. However, many data breaches, improper handling of data, and leakage of users' private data are common still now [2, 3]. As a solution, one of the prominent tools can be blockchain. Implementation of blockchain in the system can handle the private data in such a way that can resist any alternation, modification, and changes [8, 9, 10].

1.1 Motivation

Protecting the data in the system is a major concern now a day. There have been lots of ransomware threats and data breaches are happening repeatedly. The existing system relying on central database lack of

a) Immutability from single point of failure
b) Lack of concrete proof of origin of data alteration
c) Immutable record of transaction log
d) Consensus based transaction among relevant parties
e) Lack of proper user identity management using certificates from certificate authority

Because of these problems, the product authentication systems are more prone to cyber-attacks.

1.2 Background

Blockchain technology drawn attention in the field of academic and researchers through the contribution of Satoshi's electronic cash (p-to-p) where blockchain has been introduced 2008 [4]. In blockchain network, one of the

major technologies is distributed ledger. In DLT based system, multiple peers are connected through network and data is distributed in such way that every peer has own copy of ledger, and it is kept consistent among all nodes [5]. This helps system to overcome single point of failure of a centralized system. Digital signature is a scheme to provide data integrity, authenticity and it has a feature called non-repudiation. When an author signs a digital data or document, the author cannot deny the association with the data. This technique is used in many domains like online banking, digital identity management, medical records, and government services. It provides data authentication, integrity and non-repudiation using asymmetric encryption [6]. This is very helpful proving that which transaction or alteration of data is done by which party in the system. Certificate Authority (CA) is the trusted third party that provides digital certificate and verify those certificates in Public Key Infrastructure (PKI) [7]. Certificate authority prevents user from misrepresenting ownership of public key of someone. CA signs public key, entity information with CA's private key and provides a certificate. Using this certificate ownership of a public key can be linked to an entity or user. The Hyperledger Fabric blockchain ledger provides data integrity, data immutability and temper proof history of data alteration. Each block contains several transaction log data, meta data about the block, block header, hash of own block and previous block [8]. In product authentication system to achieve temper-proofness of data such ledger is very crucial. Any modification can destroy the cryptographic link of blocks which makes the alteration impossible. Blocks can be appended only, and to append a block transaction must go through several validation layers and consensus mechanism in the system. Karl Wust, et al. analyzed blockchain and its types. They showed a relation between enterprise and business need and how private blockchain is well suited for enterprises [9]. In this experimental proposal, we implemented the concept of Hyperledger Fabric (HLF) which is a type of private blockchain [10].

1.3 Objectives

The core target of this experimental proposal is securing the data in product authentication systems using the blockchain technology as a tool. In this product authentication use case, the security triad is considered. Along with that, importance was given on non-repudiation of data modification. The objectives are as follow:

a) To ensure no single point of failure in the system
b) To provide traceability of transaction ensuring proof-of-origin of alterations
c) To ensure immutability of data log of asset values
d) To prevent supply chain insider from foul play using endorsement policy-based consensus mechanism for all transactions

2 Proposed System

2.1 System Structure

The proposed proposal is built on three major components. The external client application, smart contract, and the HLF network. Client is external application that is used to interact with the blockchain network. This client application contains wallet, smart contract, and API to establish connection to the network. This client application physically holds smart contract where channel holds smart contract logically [11]. The wallet contains identity of organizations and its users in X.509 format which is issued by certificate authority [12]. The crypto material is essential to validate user identity in the network. Membership Service Provider (MSP) manages users' identity in the network. It performs identity validation, signature generation and verification [13]. There are many parties such as manufacturer, distributor, and retailers each have their own client application. Under this circumstance, they can interact under blockchain network. These smart contracts are signed by other relevant parties that are part of operational contract. The network will not allow execution of smart contract if one party modifies the smart contract that is not signed by other relevant parties. Hence, no modification of smart contract in one party's end can modify asset values in the network without prior permission of relevant parties. The network consists of immutable blockchain ledger, peer nodes representing distributor, manufacturer, and retailer. Some other peers are endorsing peer which endorses transactions as defined in endorsement policy. Ordering peer validates the signatures in each transaction, it checks if the version of asset is current version to prevent double spending of asset. The blockchain

ledger consists of asset change log that is immutable. In addition, the ledger of world state stores the current version of the asset only.

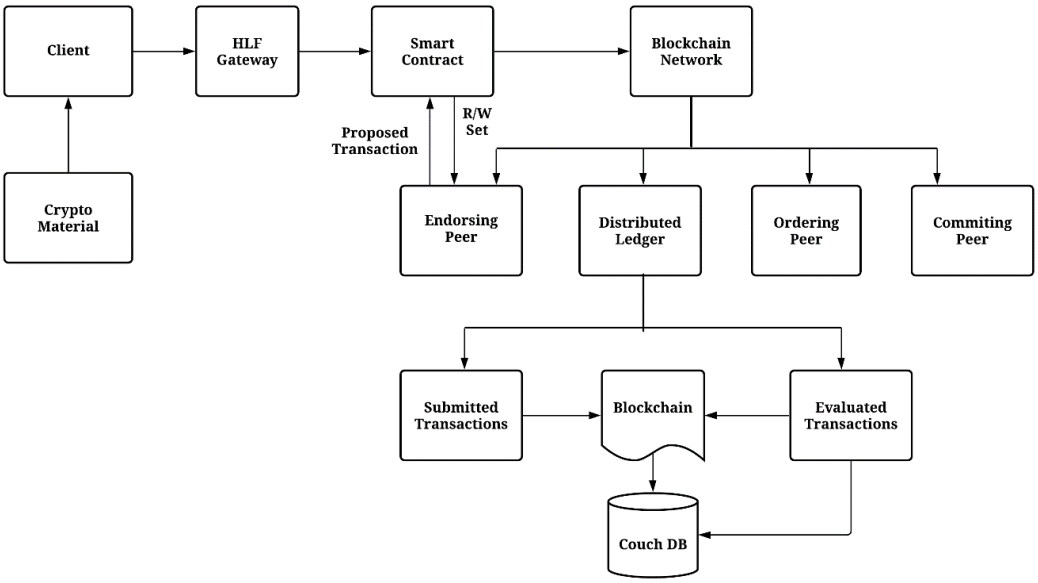

Fig. 1. Overview of the System Using HLF [11]

2.2 System Module

The system modules are wallet module, gateway module, peer module, and chaincode module. The peer module consists of organization peer, MSP, ordered. The **wallet** module responsible

a) To store crypto material like public key, private key, certificate from CA
b) To provide crypto materials to MSP for identity validation, signature generation and verification

The **gateway** module is responsible

a) To define the connection profiles
b) To use connection profile to discover and connect to other peers including CA

The **peer** module is responsible

a) To perform validation steps
b) To generate signature and verify
c) To validate identities

The **chaincode** module is responsible

a) To define the transaction
b) To Invoke transaction to manage asset data
c) To perform create, read, update, and delete operation on asset
d) To change ownership of asset only if a peer owns the asset

2.3 Procedure

This the general procedure for modules including manufacturer, distributor, retailer, and customer. Users of the system are manufacturer, distributor, retailer, and customers. The procedure starts with client application validating

user identity in the network. They can only execute the smart contract after validation of their identity. In the network all the enrolled members identity is managed by Membership Service Provider (MSP). MSP ensures all the provided crypto materials are valid. Once connection is established the user can propose a transaction. The endorsing peer checks endorsement policy, according to the policy, the endorsing peer notify other peers to sign the transaction. In case of manufacturer changing ownership of product or batch of product, it would require both manufacturer and distributor sign the proposed transaction. Then a read/write set would return to the user with proposed transaction and signed transaction.

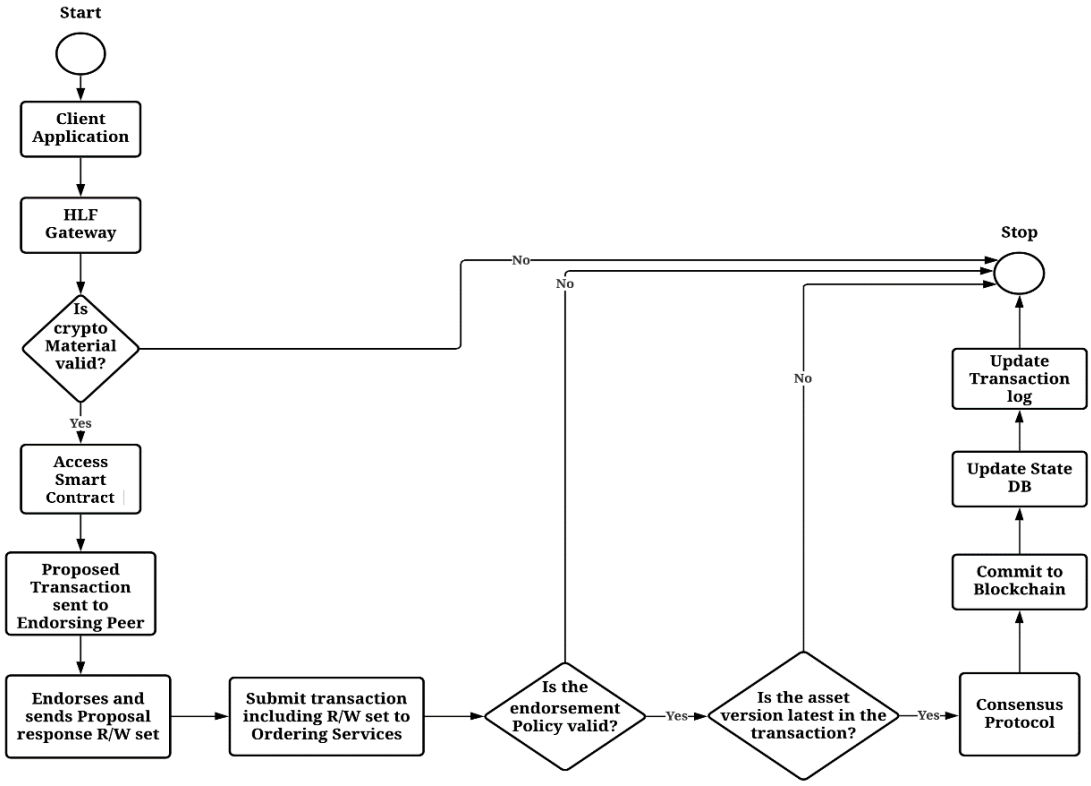

Fig. 2. Activity Diagram of the Chaincode [1]

The manufacturer can then send the transaction to the ordering peer. This peer will check if the asset version is latest. It will ensure that asset version is not changed in between a transaction being processed and being committed to ledger. After validating the transaction and verifying all the signatures, the orderer node will notify all the peer to update the transaction log in the blockchain ledger and updating the ownership change in the world state.

3 Implementation

In this work, we implemented a proof-of-concept to simulate the process. Our prime focus is to keep on securing product data and building smart contract a.k.a. chaincode to communicate with Hyperledger Blockchain network to perform the validations and evaluate the transaction as defined. Log of both valid and invalid transaction is recorded in the blockchain ledger [14]. Each transaction which is alteration of product asset goes through several layer of validation process. Transaction contains signature of the invoker and others involved in the transaction. Hence, no one can refuse attempt of invalid transaction, or valid transaction. Any alteration can be traced back [6].

3.1 The Wallet

In each client application the wallet contains crypto materials like key pairs and certificate from certificate authority. This is very crucial to prove identity of each client in the network. Certificates are in X.509 form. Key of each user is used to not only access the system but also to sign each transaction they are involved in. MSP performs identity validation based on those crypto materials to give access to user in the system. Moreover, this wallet is required for invoking smart contract aka chaincode.

3.2 Gateway

Gateway is the bridge between client application and the blockchain network. Gateway contains the connection profile. The connection profile defines all the peer connections, their certificate authorities URL. This connection profile is used to discover the peer and validating their certificate prior to commit any transactions.

3.3 Transactions

All the products are assets in the network. Transactions refers to state change or query of those assets. Transactions are proposed at first by invoking the chaincode. User identity, authorization to invoking transaction, chaincode validity is checked prior to this. Once this transaction with txID: 7da9671e is proposed, then the endorsing peer signs, and the transactions will be broadcasted to all the relevant peers.

```
[1/16/2022 12:34:07 AM] [INFO] quizzical_dewdney|[        org1peer] 2022-01-15 18:34:07.956 UTC [chaincode.externalbuilder.
node] waitForExit -> INFO 1c5 2022-01-15T18:34:07.956Z info [c-api:lib/handler.js]
[mychannel-7da9671e] Calling chaincode Invoke() succeeded. Sending COMPLETED message back to peer   command=run
[1/16/2022 12:34:07 AM] [INFO] quizzical_dewdney|[        org1peer] 2022-01-15 18:34:07.956 UTC [endorser] callChaincode
-> INFO 1c6 finished chaincode: smart-contract duration: 43ms channel=mychannel txID=7da9671e
[1/16/2022 12:34:07 AM] [INFO] quizzical_dewdney|[        org1peer] 2022-01-15 18:34:07.956 UTC [comm.grpc.server] 1 ->
INFO 1c7 unary call completed grpc.service=protos.Endorser grpc.method=ProcessProposal grpc.peer_address=127.0.0.1:33388
grpc.code=OK grpc.call_duration=44.6671ms
[1/16/2022 12:34:07 AM] [INFO] quizzical_dewdney|[         orderer] 2022-01-15 18:34:07.968 UTC [comm.grpc.server] 1 ->
INFO 00d streaming call completed grpc.service=orderer.AtomicBroadcast grpc.method=Broadcast grpc.peer_address=127.0.0.
1:38866 grpc.code=OK grpc.call_duration=5.2825ms
[1/16/2022 12:34:08 AM] [INFO] quizzical_dewdney|[        org1peer] 2022-01-15 18:34:08.085 UTC [gossip.privdata]
StoreBlock -> INFO 1c8 Received block [17] from buffer channel=mychannel
[1/16/2022 12:34:08 AM] [INFO] quizzical_dewdney|[        org1peer] 2022-01-15 18:34:08.086 UTC [committer.txvalidator]
Validate -> INFO 1c9 [mychannel] Validated block [17] in 0ms
[1/16/2022 12:34:08 AM] [INFO] quizzical_dewdney|[        org1peer] 2022-01-15 18:34:08.141 UTC [kvledger] CommitLegacy ->
INFO 1ca [mychannel] Committed block [17] with 1 transaction(s) in 55ms (state_validation=3ms
block_and_pvtdata_commit=11ms state_commit=32ms) commitHash=
[921f74a73fa18fa321949a0bbb6c0718fdca0dc6e62fbb48a2e14d258d74d33d]
```

Fig. 3. Successful Execution of Valid Transaction

In addition, these endorse the transaction according to endorsement policy. Endorsement policy defines the signature of required parties for the transactions. Once the signature is done, the ordering peer validates all the signatures, it checks if during this process asset version changes. After that, it prepares the blocks and broadcast it to all the relevant parties to commit it in the chain.

In case of attempt to submit invalid transaction, the transaction would fail to convince other peer to agree on the transaction and will result in endorsement failure. Thus, it cannot change the asset state. Those invalid transaction logs are recorded in the immutable blockchain ledger. In case of regulatory bodies want to inspect those further.

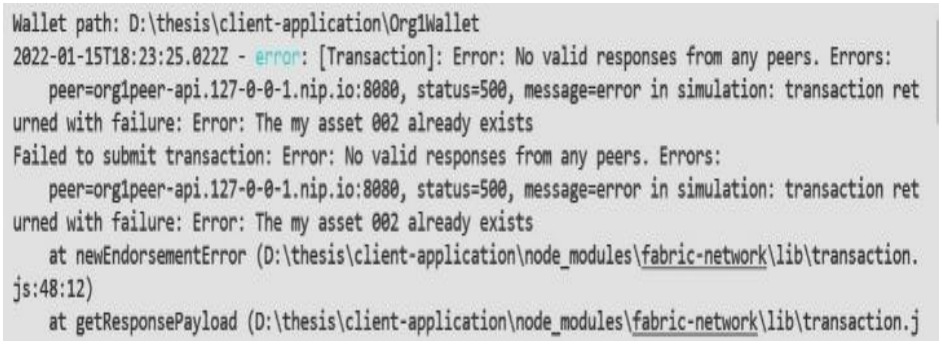

Fig. 4. Peers Rejecting Invalid Transaction Attempt

4 Security Analysis

In this system several layers of security are implied. It is highly infeasible for the attackers to attack the system. Usually, blockchain implementation can eliminate the problem of single point of failure where the system uses distributed ledger. Even the data in the world state of the system which uses CouchDB as database can be restored from the transaction log [14]. The transaction log in the blockchain is immutable and can't be modified once written. Security of the data in the world state is discussed in the following:

All the assets in the world state are encrypted with AES encryption scheme. Eavesdropper won't be able to read the message in the system. All the communication is on a secure communication channel that is protected by Transport Layer Security. Membership Service Provider ensures that only authorized entity can access the system. To access the system MSP validates users' identity. Users' identity will be only valid if it comes from trusted Certificate Authority. The relevant parties for all the transactions are defined in Endorsement Policy. A transaction is required to be signed by relevant parties before it can be committed to block and change asset value in the world state. Consensus mechanism relies on this Endorsement Policy. Besides the chaincode cannot be edited or updated by single organization without agreement of other relevant peers as per channel configuration.

Thus, the data is protected from unauthorized access, injection, modification, or deletion. Even if data is altered in one peer by unauthorized party, the other peer won't agree as each peer have their own version of ledger to cross check the validity of transactions.

5 Compare with Existing System

The existing system lacks immunity to single point of failure. Determining the proof-of-origin of transaction is a complicated process in the existing system. Where in blockchain technology supported system, each transaction is signed the author of a statement cannot deny the association with the transaction. The ledger which contains historical value of each transaction and asset changes is hash linked, it is temper proof. Both digital signature and immutable record provides a concrete proof of origin of each data changes. In case of attempt to invalid transaction the invoker of the transaction can be easily traced as the ledger keep record of invalid attempts too. Inspecting the ledger from transaction metadata the signature of invoker can be found. In case of one peer failing or being under cyber or physical attack. The peer will fail to convince the other peers on committing the transaction for the distributed nature. This distributed feature is not found in existing conventional system. Besides, the participants identity is certified by CA eliminates the impersonating of ownership of someone else's public key. All these methods make the system better and more secure than existing systems.

6 Conclusion

Product authentication and securing the data in the system is much broader area as it appeared. In this work we analyzed how existing product authentication can be made better with implementing blockchain technology specifically using private blockchain to satisfy enterprise needs [9, 10]. We focused on securing the data in the network in such way that all the alterations can be trace backed to the invoker. We build a prototype using Hyperledger fabric blockchain framework [10] to run an experiment on some data and performed few transactions on those to simulate the process. We found that, private blockchain can provide more secured solution also can provide interface for handling transaction as businesses handles transaction in real life. With endorsement policy, chaincode based contracts. The digital version of an asset comes with the double spending problem which can be solved with keeping assets historical log in temper proof ledger and keeping it consistent among all the distributed peers [14]. Apart from it, all the transactions going through several layer of validation [15] make it highly infeasible for the attackers to attack the system. In addition, it is very useful to prevent the data breaches and other security attacks.

References

1. Maria Pinto da Cunha Brandão, A., Gadekar, M.: The counterfeit market and the luxury goods. Fashion Industry - An Itinerary Between Feelings and Technology (2020).
2. Team,B.F.,Company,M.K.&: The year ahead: Shoring up fashion's cyber defenses, https://www.businessoffashion.com/articles/technology/the-state-of-fashion-2022-bof-mckinsey-cyber-security-retail-ecommerce/, last accessed 17/12/2021
3. Cluley, G., Graham Cluley, 1.3 million online fashion shoppers exposed after data breach at UK ecommerce provider, https://grahamcluley.com/online-fashion-shoppers-exposed-ecommerce-breach/.
4. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260(2008).
5. Liu, X., Farahani, B., Firouzi, F.: Distributed Ledger Technology. Intelligent Internet of Things. pp. 393–431 (2020).
6. Kaur, R., Kaur, A.: Digital signature. 2012 International Conference on Computing Sciences. pp. 295–301 (2012).
7. Yangtao, Y., Quan, L., Fen, L.: A design of certificate authority based on elliptic curve cryptography. 2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science. pp. 454–457 (2010).
8. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S.W., Yellick, J.: Hyperledger fabric: a distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference. pp. 1–15 (2018).
9. Wust, K., Gervais, A.: Do you need a blockchain? 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). pp. 45–54 (2018).
10. A blockchain platform for the enterprise, https://hyperledger-fabric.readthedocs.io/en/release-2.2/, last accessed 07/01/2022
11. Blockchain Network, https://hyperledger-fabric.readthedocs.io/en/release-2.2/network/network.html, last accessed 08/01/2022
12. Wallet, https://hyperledger-fabric.readthedocs.io/en/release-2.2/developapps/wallet.html, last accessed 14/01/2022
13. Membership Service Provider (MSP), https://hyperledger-fabric.readthedocs.io/en/release-2.2/membership/membership.html, last accessed 01/02/2022
14. Ledger, https://hyperledger-fabric.readthedocs.io/en/release-2.2/ledger/ledger.html, last accessed 07/03/2022
15. Transaction Flow, https://hyperledger-fabric.readthedocs.io/en/release-2.2/txflow.html, last accessed 08/03/2022