Sādhanā (2022)47:208
https://doi.org/10.1007/s12046-022-01984-2

© Indian Academy of Sciences

Blockchain-based anonymous anti-counterfeit supply chain framework

N ANITA*, M VIJAYALAKSHMI and S MERCY SHALINIE

Department of Computer Science and Engineering, Thiagarajar College of Engineering, Madurai,
Tamil Nadu 625015, India
e-mail: anita.anjalinatarajan@gmail.com; mviji@tce.edu; shalinie@tce.edu

MS received 5 August 2021; revised 29 June 2022; accepted 29 August 2022

Abstract. For the last decade, businesses and industries have been facing difficulties in tracking their products. During the supply chain process, the attackers add their counterfeit products into the market along with legitimate products. With the increase in the number of counterfeits entering the open market, it is hard to discover the source of the counterfeit product. Most of the existing anti-counterfeit solutions are centralized. However, current solutions lack in anti-counterfeiting, decentralization, auditing, transparency, traceability, and tag cloning. To mitigate these issues, we proposed a Blockchain-based Anonymous Anti-Counterfeit (BA2C) supply chain framework that exploits Radio Frequency Identification (RFID) and blockchain technologies. The proposed model streamlined all the transactions through Ethereum, a blockchain-based platform with the support of Proof of Authority (PoA) consensus. Furthermore, the confidentiality of transactions is gained by incorporating zk-SNARKS on the Ethereum blockchain. In this work, the proposed model was tested in terms of transaction cost, latency, and throughput. Further, it was compared with the existing system and was found to perform better transactions in the supply chain management in terms of lower cost and higher scalability. This work concluded that the proposed model was more appropriate to evaluate the critical issues of the supply chain.

Keywords. Anonymous; blockchain; counterfeit; Ethereum; supply chain; zero-knowledge proof.

1. Introduction

Billions of products are produced every day globally, through complex supply chains that extend to all parts of the world. The supply chain consisting of individual manufacturers, suppliers, warehouses, and end-users is incredibly complicated [1]. When something goes wrong along a supply chain, it will take more time and energy to know where and how a shipment was going wrong. False labeling of products, fake or unsuited, components, and materials used for manufacturing products, and misuse of another trademark are just a few examples of how fake goods and theft of intellectual property hurt consumers and businesses [2]. Brand owners and intellectual property lose billions of dollars in income each year to counterfeits who sell fake products, often at the same price as the brand. Most of the imported counterfeit goods come from China, which causes difficulty in identifying the original goods [3]. The global amount of piracy and counterfeiting is expected to hit almost $2.3 trillion by 2022 [4]. When fake products enter the market, there is a risk to public safety, and the people lose confidence in brands they trust. Brands have promptly increased spending on the anti-counterfeit manufacturing process to address this growing problem, as well as identify the attackers who are dangerous and smart.

A recent report from ABI Research shows that the demand for blockchain will drive the technology's revenue to $10.6 billion by 2023 [5]. Counterfeit items are found in almost any online location. The Internet is a perfect platform for counterfeiters because, while disguising the essence of their goods, they can also hide in plain sight [6]. The boom in counterfeiting has triggered a dramatic increase in the number of anti-counterfeit and product authentication technologies such as a hologram, and security printing, and security label [7]. It is therefore important to develop and deploy effective product mitigation strategies that ensure a trustworthy and secure supply chain. Anti-counterfeiting is the only way to discourage fake goods from entering the legitimate supply chain [8]. The Supply chain system processes a large amount of data and thereby brings more complexities to the architecture of the network. Such an evaluation of the supply chain structure has brought several critical issues linked to the problem of counterfeit such as traceability, reliability, availability, and accountability [9]. Traditional supply chains are centralized and depend on trading from a third party. The centralized supply chain creates several challenges, huge processing

*For correspondence

Published online: 18 October 2022

burdens, substantial storage, authentication of their records, and a single point of failure [10].

Blockchain technology overcomes the existing pitfalls with its enormous features, which include decentralization, security, traceability, reliability, and immutability [11]. Based on a peer-to-peer (P2P) topology, blockchain is a distributed ledger technology (DLT) that allows data to be stored on thousands of servers worldwide, enabling everyone on the network to see in near real-time the entries of others. A blockchain distributed system is used to collect, store, and manage product information of each product throughout its life cycle. Blockchain with unique product information provides a secure and shared exchange record for each product [12]. As a product moves through its life cycle, a variety of participants such as producers, manufacturers, suppliers, distributors, retailers, and end-users, possess it. Each of these actors plays a vital role in this system by logging into the blockchain network about product information of the key and its current status. While blockchain provides strong security, it has loopholes because each transaction added to the block enforces publicly accessible blockchain-related addresses [13]. However, blockchain-based anti-counterfeiting solutions for the supply chain are not yet available [14].

Hence, we propose a generic Blockchain-based Anonymous Anti-Counterfeit framework for supply chain management. The proposed BA2C work allows all nodes throughout the system to participate rather than a small set of nodes. Further, we propose an approach for detecting a cloned RFID tag is explained in detail in section IV. The Electronic Product Code (EPC) global Network is an industry-standard for RFID-enabled supply chain networks to increase the identification of products within the supply chain [15]. The benefit of the generic framework is the prevention of counterfeit products, cloned tags, and improves scalability. The main contributions of this work are as follows:

- A blockchain-based framework designed for counterfeit product traceability in the supply chain to ensure product authentication and tag cloning.
- This study conceptualizes, implement, and test smart contract algorithms that govern and ensure proper interactions among stakeholders in supply chain. Anyone may easily prove the organization's legitimate source and serve as evidence for the customer's purchase of items using smart contract information.
- This study uses Zero-Knowledge Succinct Non Interactive Argument of Knowledge (zk-SNARK) to ensure the privacy of supply chain participants.
- Proposed BA2C model using PoA consensus achieve better latency and throughput than traditional consensus such as Proof of Work (PoW), Proof of Stake (PoS).
- Finally, analyze efficiency of BA2C model with existing systems. Retailers may utilize this anti-counterfeit model to demonstrate if they supply real things and no longer have to deal with counterfeits.

The rest of the paper is structured as follows. We present the literature survey in section 2. Section 3 describes the background and motivation of our work by discussing various exemplary use case scenarios. Section 4 explains the system framework and system requirement. In section 5, we present algorithmic explanation. Implementation details of the proposed BA2C work are presented in section 6. Evaluation and results are discussed in section 7. Finally, the conclusions are provided in section 8.

2. Literature survey

The use of blockchain and smart contracts for supply chain management that are under research is explored in this section.

A lightweight RFID ownership transfer protocol against the de-synchronization attack which is added to a tag's original owner works well in a centralized system [16]. A product ownership management system (POMS) for RFID products has been proposed for anti-counterfeit strategy in post supply chain management systems [17]. In POMS, customers can reject the purchase of the counterfeit product, even with a genuine EPC. A block-supply chain has been proposed to detect counterfeit attacks such as modification, cloning, and reapplication attack using blockchain, and Near Field Communication (NFC) [18]. The authors developed an efficient and scalable consensus protocol to solve the validate selection. As a result, the block-supply chain has been able to track and trace products. The consensus latency of the proposed system is lower than tender mint consensus, and restricted to counterfeit attacks. Blockchain framework for Proof Delivery of physical assets has been proposed to ensure traceability, accountability, Integrity with single and multiple transporters [19]. A blockchain framework has been introduced to allow traceability of devices, which uses confirmation-based transfer of ownership [20]. In this work, confirmation of the receiver of transaction is needed after the sender has sent the transaction ownership. This helps to report the missing product during transportation, human error or delay in distribution automatically. In the proposed DL-tag solution a public ledger acts, as an intermediary proof of existence for significant events that occur on the supply chain, and also ensures that only the data hashes based on actual product-related data transactions are stored in the ledger [21].

A generic framework without proper exploration on the intermediaries would exploit the Ethereum and smart contracts to track, trace, and perform business transactions [22]. All the transactions are recorded and stored in an immutable ledger with a decentralized file system, to provide high level of transparency and traceability in the supply chain. An Anonymous Reputation-based System (ARS) is proposed by exploiting a ring signature with the zero-knowledge proof for retail marketing in Industrial Internet of Things (IIoT) [23]. With the help of ARS, the system preserves the consumer identity and confidential information that can be integrated with proof of stake (PoS) efficiently. The output was evaluated for an on/off-chain using simulation. A blockchain-based product traceability scheme has been implemented, in which product records are held in a distributed ledger, where the product transfer and monitoring takes place with the help of smart contracts [24]. The traceability framework was created for the e-commerce supply chain using a blockchain-based model with features such as distributed consensus structure, block framework, and data management. A hierarchical deterministic wallet, used to manage keys at different levels was also used in the framework. The product traceability tag is designed to efficiently verify the source, information, and ownership of a tag [25]. This work was not designed for use in large companies and product tracking. Quality traceability system architecture for steel products were implemented to address the quality and safety problems from raw material with the help of blockchain-based IIoT [26].

Consequently, the analysis avoids incomplete information and poor accountability within the traditional information system. A blockchain-based solution for Agri-food supply chain has been proposed in [27]. They have provided detailed information regarding trading, traceability, delivery, and reputation. They have also analyzed the smart contract with an overview of security and vulnerability. A tracking system of ICs is designed for supply chain management using smart contract and Physically Unclonable functions (PUF), that aims at mitigating the counterfeit problem [28]. A stable, blockchain-based secure platform for the provision of IoT data provenance using Proof-of-Concept (PoC) to meet non-functional requirements has been suggested and failed to provide solution for privacy and scalability [29]. Traditional supply chain challenges include, single point of failure, increased cost, complexity, reduced quality of service, traceability, and the impact of falsified product. However, the current solutions cannot achieve accurate traceability, lack of counterfeit goods, scalability, and registration of identities, the user privacy, and data storage. Since the invention of blockchain, various decentralized storage systems have been used to store data. Table 1 provides a relative comparison of the state-of-the-art blockchain solutions to product transactions in supply chain. The proposed work is based on the literature of the previous research, combined with the pros and cons of the scheme. The proposed work is based on a decentralized anti-counterfeit framework using blockchain. The solution addresses the problems in the existing supply chain and eventually achieves anti-counterfeit product, key recovery, user privacy, scalability, and traceability. In previous work [25] the focus was mainly on the cost and gas consumption for the blockchain-based supply chain systems. Only a few researchers recorded performance measurements configured network for Ethereum in a private environment. None of the findings include PoA consensus and zk-SNARK integration on Ethereum. PoA could be better suited than PoW and PoS for private blockchains in supply chain management. Moreover, it uses Anonymous Distribution to store private information on the blockchain. The gas cost for a secret transaction is less than 1$, and the transaction creation takes less than 10 seconds on a normal computer.

3. Background

3.1 *UPort*

Each Uport identity comprises of two smart contract templates designed by Uport: controller and proxy. Ethereum creates a controller instantiation which consists of a reference to the newly created public key. The proxy consists of a reference to the newly created private key, and proxy functions invoked by controller contracts. A restriction is defined in the controller and enforced by EVM. A user can create multiple Uport identities that are unlinkable**.** User attributes such as their name, address, or date of birth are stored as JSON objects on the decentralized platform Interplanetary File System (IPFS). They upload it to IPFS to store the attributes of users on their identity and receive a resulting hash pointing to the content on the IPFS network. IPFS is a distributed file system that works well with blockchain. The Uport tool in blockchain technology does not push product ownership identity in centralized services to individuals and identity in control of themselves. This challenges hackers to hack identity.

3.2 *Ethereum*

The user initially generates a public and private key pair of device to create an identity on the platform. The public key acts as the local identifier of the user and also a currency-holding Ethereum Address (EA). The private key is used to sign transactions from this address and to prove ownership of the public key. The data stored on IPFS replicated automatically depends on the user behavior data that will replicate once a user accessed it. Although the data stored

Table 1. State-of-the-art blockchain-based approaches to supply chain product transactions.

References(s)	Year	Purpose	Critical issues									Pros	Cons
			1	2	3	4	5	6	7	8	9		
[17]	2017	Product ownership management system against counterfeit products	Y	Y	Y	N	Y	N	N	N	Y	Low cost for the transaction (<$1 U.S), privacy, avoid impersonation	Incentive mechanism, Anonymity, security in Ethereum
[18]	2018	Block supply chain against counterfeit attacks.	Y	N	Y	N	Y	N	N	N	N	Detect modification, cloning, reapplication attack	Malicious validator, Privacy
[19]	2019	Blockchain-based steel IoT traceability system	Y	Y	N	N	N	Y	N	N	N	Traceability, Privacy, high product quality	Scalability, vulnerable to counterfeit attacks
[20]	2019	A novel architecture for traceability of electronic devices	Y	Y	Y	N	Y	Y	N	Y	Y	Detect counterfeit ICs, avoid cloning	Privacy, Reliability
[21]	2019	Distributed ledger tags for product provenance	N	N	Y	N	Y	Y	N	Y	Y	Product authenticity, low-cost transaction	Product sustainability
[22]	2019	Blockchain framework to trace & track workflow for Agricultural supply chain	Y	Y	N	N	N	Y	N	N	N	Provide high Integrity, security, reliability	Scalability, Privacy, Proof of delivery
[23]	2019	Anonymous reputation system for preserving consumer confidential information	Y	N	N	N	N	Y	Y	Y	N	Privacy guaranteed, Anonymity, confidentiality, unlinkability	System efficiency, scalability
[24]	2019	DApp for product traceability system	Y	Y	N	N	Y	Y	N	N	N	Resist to man-in-the-middle attack	Authentication, Access control
[25]	2020	A framework for e-commerce supply chain	N	N	Y	N	Y	Y	N	N	Y	Efficiency, traceability.	Anonymity, Scalability.
[26]	2020	Product traceability system architecture for steel product	Y	N	N	N	N	Y	N	N	N	High Transparency, traceability, 51% attack	Solution for counterfeit product, End to end delay
[27]	2020	End to End blockchain-based solution for Agri-food supply chain	Y	Y	N	N	Y	Y	N	N	Y	Accountability, auditability, autonomy	Malicious detection, Scalability
[28]	2020	Anti-BIUFF approach for counterfeit mitigation in Integrated Circuit	Y	Y	Y	N	Y	N	N	N	N	Efficiency, Anti-counterfeit	Scalability, Anonymity
[29]	2020	Blockchain-based secure framework for data provenance in IoT	Y	Y	N	N	Y	N	N	N	N	Integrity, Availability, data provenance	Privacy, scalability, counterfeit product detection
Proposed system	–	Privacy preserving blockchain based solution for counterfeit product	Y	Y	Y	Y	Y	Y	Y	Y	Y	Privacy, Tag authentication, low cost, restrict to MITM, impersonation attack	–

1. Traceability, 2. Smart contract, 3. Anti-counterfeit product, 4. Key recovery, 5. Tag used, 6. Privacy, 7. Anonymity, 8. Confidentiality, 9. Scalability.

in an off-chain system lacks the basic properties of a blockchain is more cost-effective, works better, and is more robust than data stored in the smart contract.

4. Motivation

The structure of the modern supply chain is mostly centralized, in which product authentication records are stored and managed by the central authority [30]. The trades of falsified products are higher in open market that affects the revenue and profits of business. Existing digital identity has serious challenges like a censorship problem, ethical and privacy issues, single point of failure and interoperability in data transaction. The most practical approach to data security and controlled transparency in supply chains and services, until the discovery of the blockchain, was a centralized system. The counterfeit products are to be avoided in business arena. In this regard, counterfeiters may be regulated by affixing NFC, QR, or RFID codes to products. Counterfeit drugs have a negative effect on the health and create income loss for legal pharmaceutical manufacturing companies. Several anti-counterfeiting solutions have been developed in recent years. Yet, most existing systems are insecure and vulnerable to different attacks such as impersonation and tag cloning attacks. Therefore, the authors felt that there is need of systemized algorithm to resolve the problems of counterfeit products in the supply chain.

To the best of our knowledge, this paper is the first attempt to implement a fully integrated privacy-protecting blockchain network using Uport Decentralized Identity (DID) to prevent product counterfeiting and ensure security and traceability throughout the supply chain. In the proposed BA2C model, we combine TRNG and PRNG [31] in which a 1-bit random number added to the PRNG cycle ring such that the output sequence of the Linear Feedback Shift Register (LSFR) would also be as unpredictable and irreproducible as a TRNG. Public/Private cryptography and decentralized blockchain technology offer a promising solution to the above-mentioned centralized server problem [32]. The blockchain was initially conceptualized by Satoshi Nakamoto to fix the double-spending problem inherent in digital transactions [33]. The blockchain technology will theoretically improve the problems of accountability and traceability within the supply chain of manufacturing by utilizing immutability, data tracking, distributed storage, and managed user accesses. Zero-knowledge proofs allow the authenticator to recognize the verifier that a comment is true without disclosing any information other than the comment's validity. The strong privacy guarantee of user is validated as legitimate under consensus mechanism in blockchain network by using zk-SNARK [34].

5. Proposed model

We have introduced a framework for the supply chain based on blockchain technology to the anti-counterfeit product system. In this model, the manufacturer can use this framework to store product information such as purchasing, marketing, and selling in the blockchain that is accessible to anyone using the anonymous identity. The proposed BA2C model is discussed in detail in the following section.

All product stakeholders can access the product since every product of the proposed system must be in a digital format on a blockchain. This framework is necessary for trading and updating information about the product. A smart contract of each product is created using the decentralized identity of the entities of the supply chain. The product is owned by the manufacturer, and only he has permission to enter new information into the product profile or initiate a trade with the distributor. The buyer and seller should sign the smart contract, and the details of the transaction will add to the blockchain. Blockchain network processes this data and updates the product profile to the next buyer or stakeholder. It allows the blockchain network to maintain the product ownership record.

In the proposed system, Uport decentralized identity is created for the manufacturer (M_{id}) using the mobile application with an asymmetric key pair (K_{pu}, K_{pr}). The detail of each product will be stored on an RFID tag. Each RFID tag has its unique id (T_{id}), product name, and counter. The manufacturer adds the product data to the RFID tag, which includes product name, product id, product expiry date, tag id. We consider that each supply chain entity has its EPC global Class 1 Gen 2 compatible RFID reader. The supplier EPCs allocated to each product are written into tags attached to the goods so that every person can identify the goods when they arrive.

The growing advance of RFID technology and the continuous cost reduction make the supply chain easy to trace and track the product during the transaction life cycle. Blockchain technology features such as distributed storage, immutability, rapid solution, and increased capacity can solve the problem of a data security issue, recovery process of a key, and privacy in supply chain management. The product anti-counterfeit system framework of supply chain management based on blockchain technology is shown in figure 1. The user then compiles a copy of the source code for the Smart Contract and publishes it via their Ethereum address to the blockchain.

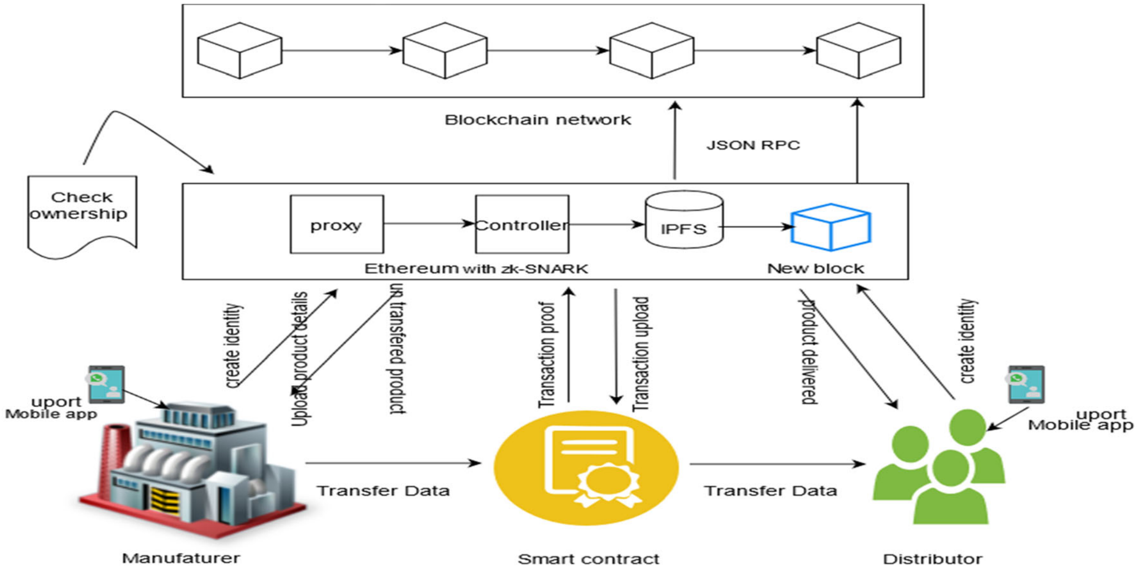


Figure 1. The proposed BA2C system framework.

Data authenticity and integrity are essential to ensure sustainable management of supply chains uses DLT, in particular the Ethereum blockchain, is a decentralized intermediary ideal for environments involving many stakeholders who do not trust each other [35]. This model requires the use of a public and less permit distributed ledger platform supporting smart contracts for the implementation of the anti-counterfeit solution. Since any node can be read from the ledger in public and permissionless blockchain, and append it to the ledger [36]. The manufacturer creates the first block known as the genesis block for the blockchain.

Table 2. List of notations.

Notation	Description
M_{uid}	Manufacturer unique identity
D_{uid}	Distributor unique identity
ka, kp	Temporary key pair
Ska, Skp	Secret encryption key pair
K_{pr}	Manufacturer public key
kp	Proving key
kv	Verification key
i	Input
K_{pu}	Manufacturer private key
T_{id}	Tag identity
K_{put}	Tag public key
K_{prt}	Tag private key
K_{pur}	Reader public key
K_{prr}	Reader private key

In PoA, miners solve a puzzle and demand rewards. Mined blocks are simply templates with header details and mine reward address. The header information is used to select a random group of validators for the block to be signed. The larger stakeholder has a greater chance of signing the new block. Once all the selected validators sign the block, it becomes the actual part of the blockchain. Finally, the manufacturer broadcasts the genesis block to all nodes in the supply chain and ships the product. In this model, the transaction process from manufacturer to distributor should be followed by the entire life cycle of the supply chain. Table 2 provides a list of notations used in the proposed work.

5.1 *Security requirements*

The proposed model satisfies the following requirements in supply chain to resist counterfeit attack are described as follows:

- To maintain confidentiality, for every participant should have a unique identity.
- Upon selling a product, the stakeholder passes ownership of the product to the consumer without delay.
- During system failure or data breach, the program will allow the product owner to recover the identity.
- Retrieval of the key can take place when the user has lost their keys. Product forgery and tag cloning is tested before each transaction.
- Each stakeholder and distributor must be able to list all the blockchain entries for a particular item of the product.

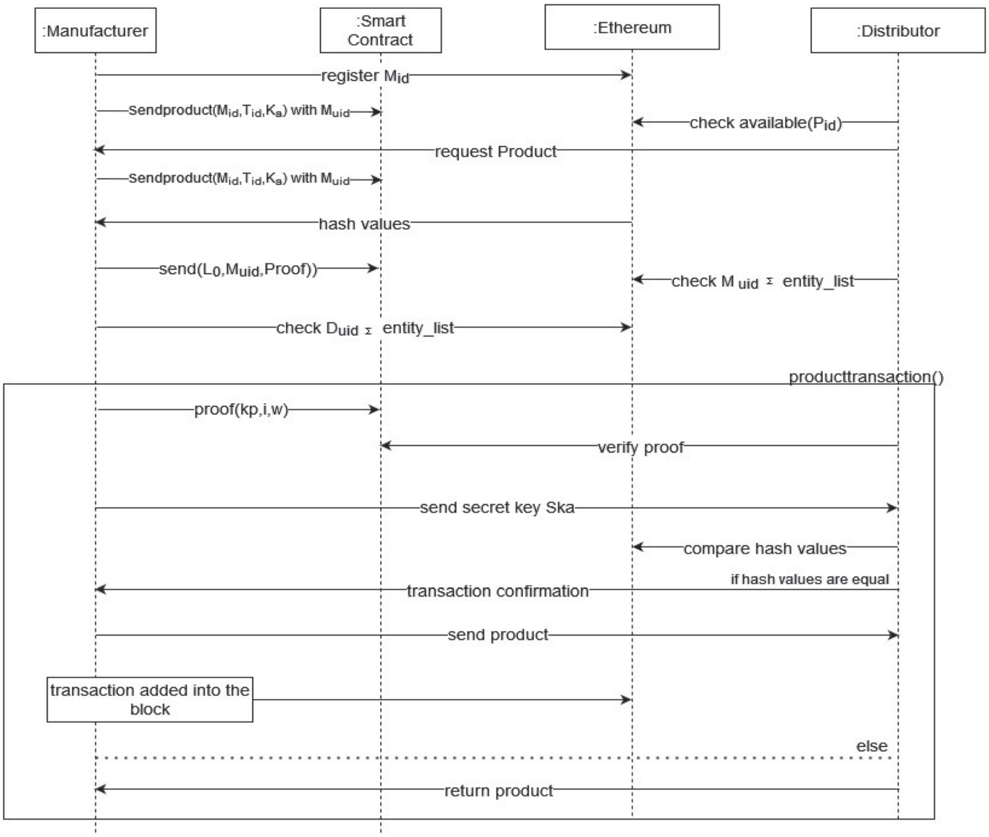


Figure 2. Manufacturer and distributor interaction in the proposed system.

5.2 *Proposed methodology*

The proposed system consists of the following phases during the process of the transaction of goods from one user to another user. The process of product authentication carried out between the manufacturer and the distributor is shown in figure 2. The following six steps are involved in the detection process of counterfeit products:

Step 1: Manufacturer generates key pair ka, kb using key generator. The manufacturer encrypts the product, using key secret key Ska derived by key derivation function (KDF). KDF used to derive secret by getting the secret information of product owner. The manufacturer calculates two hash values hash1 = H (ka) and hash2 = H (T_{id}) using SHA256 and Keccak-256 algorithms. Hash values length is at least double the length of key due to avoid collision of two hash values. The key generator generates a pair of keys, proving key and verification key (kp, kv). Proof σ is generated by using zk- SNARK [37] with public key kp, input (i) and witness as σ = Proof (kp, i, w).

Step 2: Digital signature of the hash values (hash1|| hash 2) signed by manufacturer signing key and store values into the blockchain server L_0= sign (hash1|| hash2) is obtained.

Step 3: The manufacturer sends the encrypted data L_0, σ and M_{uid} to a distributor. Under PoA consensus, Validator calculates Verf (kv, i, σ) function [37], that returns true when the proof is correct, otherwise return false. Distributor computes the hash value of encrypted data as hash3 = H (E (ka, T_{id})) and signs the hash3 (L_1=sign (hash3)). Then send the value of hash3 to the blockchain server.

Step 4: The seller confirms the originality of the product and authenticates the tag. This step definition is discussed in the section below. If the manufacturer id is a part of the $|A_u|$ list and check tag authentication, then the product will be regarded as original, else the product is falsified. The genesis block created by the manufacturer including the hash value of the transaction data (hash1, hash2, hash3, L_0, L_1) in the blockchain is authorized, and the transaction is confirmed. The distributor receives hash1 from the blockchain server.

Step 5: After the transaction confirmation the manufacturer sends key K_a to the distributor through a secure channel. The distributor confirms hash2 and decrypts the data of an encrypted product using secret encryption key. Step 6: If the product is identified as a fake, it will return to the current owner. The current owner rejects the product when the product id is not present on their |A_u| list.

Similarly, the same way of an operation is carried out by various participants namely retailer and end-user in the supply chain. An overview of the product transaction is detailed described in the following subsection.

Algorithm 1: Secret key generation for tag authentication.

```
Input: public key of tag $K_{put(i)}$, private key of reader $K_{prr}$
Output: secret key $K_{s(i)}$
Let SKE (Symmetric Key Encryption Algorithm), $K_{prt(i)}$ be private key of tag, $K_{pur}$ be public
key of reader, $T_{id}$ is tag id.
begin
    generate key pairs tag ($K_{put(i)}$),$K_{prt(i)}$) using SKE
    generate key pairs for reader using ($K_{prr}$,$K_{pur}$) using SKE
    $K_{s(i)}$=E($K_{prr}$,$K_{put(i)}$)
    $K_{put(i)}$=H($T_{id}$)
    return $K_{s(i)}$
end
```

5.3 *Tag authentication*

The public and private key pairs for both RFID tags and tag readers will be generated. These keys are created, managed in a secure environment and written on chips of both tag and reader. The key pair generation and secret key generation is explained in algorithm 1. Only the reader can compute the correct shared secret key and transfer the authentication to read the content of the tag, due to the difficulty of inverting the one-way hash function. Unauthorized readers can read only the tag id, and cannot access any private tag details. Random number R_n [34] is generated using the Truly Pseudo-Random Number Generation (TPRNG). To verify the validity of tag contents, the RFID reader will read tag identity and produce this tags public key, and use this public key to decode the encrypted code. The user may then use the tag content to generate code with a hash. The RFID reader can verify the integrity of the tag content by comparing this hash code that is decrypted.

6. Smart contracts

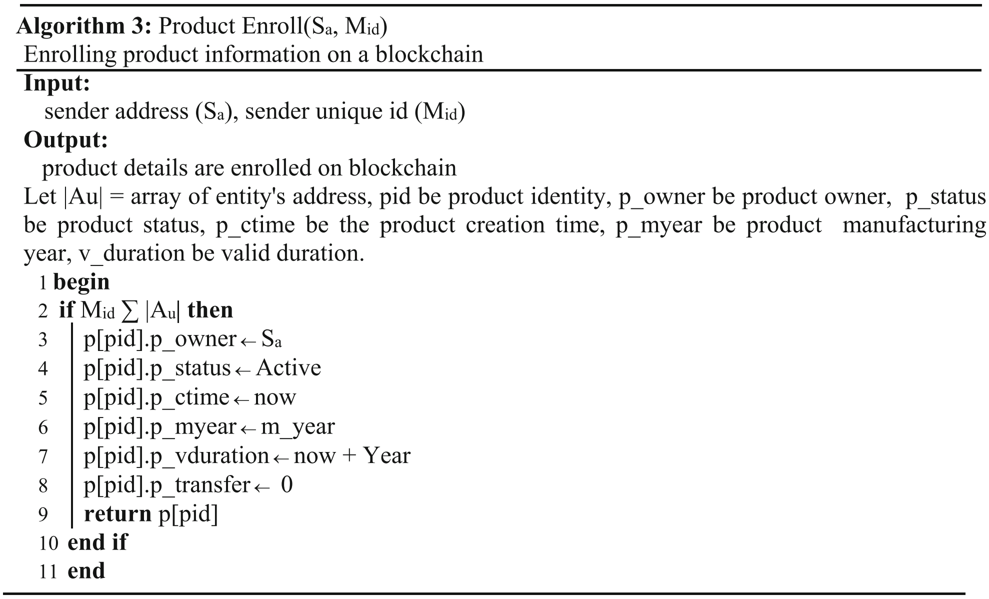
In this section, we describe the smart contract algorithms that define the working principles of proposed blockchain-based approach, and the interactions with the blockchain and platform via the proxy. These algorithms include registration, product transaction phase, product confirmation phase.

6.1 *Registration phase*

User-created DID using the mobile app with their key pairs. The entire user should register their id to IPFS. A private Ethereum network has been set up first and user data stored on a ledger that is accessible only to clients and specific service providers.

Algorithm 2: Register entity (I_d)
Register all the users' unique identity

```
Input:
    $I_d$ - unique identity of entities
Output:
    An array of entities | $A_u$|
begin
String  $I_d$
$A_u$.push( $I_d$)
for i= 0 to |$A_u$| -1 do
    msg.sender ==0 | $A_u$|;
    require($I_d$ = = |$A_u$|),'user access the service')
end for
end
```



Algorithm 3: Product Enroll(S_a, M_{id})
Enrolling product information on a blockchain

```
Input:
  sender address ($S_a$), sender unique id ($M_{id}$)
Output:
  product details are enrolled on blockchain
Let |Au| = array of entity's address, pid be product identity, p_owner be product owner, p_status be product status, p_ctime be the product creation time, p_myear be product manufacturing year, v_duration be valid duration.
begin
if $M_{id} \sum |A_u|$ then
    p[pid].p_owner $\leftarrow S_a$
    p[pid].p_status $\leftarrow$ Active
    p[pid].p_ctime $\leftarrow$ now
    p[pid].p_myear $\leftarrow$ m_year
    p[pid].p_vduration $\leftarrow$ now + Year
    p[pid].p_transfer $\leftarrow$ 0
    return p[pid]
end if
end
```

It can enable by holding an array of registered addresses in the blockchain. The modifier is activated automatically by contacting the registration contract to check whether the user is registered to gain access to the service. The proxy contact does the required task in the background on behalf of the users to make it convenient for the users. The modifier terminates the entity registration contract while the msg.sender does not belong to the $|A_u|$ list, which limits the blockchain of unwanted access.

6.2 *Product transfer phase*

Different users inside the supply chain will use the blockchain framework, so we needed a way to connect users to steps in the chain. Thus, as a transaction between two different addresses, each address representing the user, we would be able to follow that transaction through the chain when a user transferred goods to another user. After that, the product ownership moved to the added user. Pseudo code represents the product enroll function, which records the manufacturer's information when its product is stored on the blockchain. Our proposed system restricts a single administrator. In tag authentication contract, the receiver requests a product from the sender, in which tag identity is sent to the receiver. Tag id contains product details like product identification, product name, product count, expiry date, and product status. Algorithm 4 illustrates Product transfer () function, used for product transfer. The function first retrieves the product data record from the blockchain. It will not work when the current transfer message sender is not the owner of the product. The function then checks if the product is available, and the transfer function handler updates the essential product details. Before moving the product, we have to check if the recipient belongs to the $|A_u|_{list}$, and the expiry date of the product is longer than the blocktime. This pseudo code only describes the scenario where the product transferred. The manufacturer communicates with the distributor over the network.

Algorithm 4: Product transfer (S_a, pid, R_a, R_{id})

The product is transferred from the current product owner.

Input:

sender address (S_a), product id (pid), a Receiver address (R_a), Receiver unique identity (R_{id}).

Output:

boolean

Let p_transfer be transfer of product, p_status be product status, p_ntransfer be number of product transfer, $|A_u|$ - array of entities U_{id}, $|W_u|$ - address of target wallet.

```
begin
if !   proof is verified
       Reject transfer ($S_a$,pid,$R_a$,$R_{id}$)
if ! $A_u$[$R_{id}$].registered    then
       Reject transfer ($S_a$,pid,$R_a$,$R_{id}$)
end if
if ! $W_u$ [$S_a$] [$R_{id}$]  then
       Reject transfer($S_a$,pid,$R_a$,$R_{id}$)
end if
if expiry >block.timestamps && tag=!cloned    then
    p_transfer ← $R_a$
    $|S_a|$ ← p.count--
    $|R_a|$ ← p.count++
    p_ntransfer ← ntransafer++
    p_status ← shipped
    return true
   else
    p_transfer ← $S_a$
    return false
end if
end
```

The manufacturer wants to confirm the distributor is legitimate. The manufacturer interacts with the distributor through the blockchain network. The manufacturer wants to confirm the receiver is the authenticated distributor. If id belongs to the $|A_u|$ list, then the product will transfer to the receiver or else return the product to the sender. The authentication of the tag is verified, as shown in figure 3.

6.3 *Transaction conformation phase*

In this phase, given a positive transaction confirmation, the ownership of the product will be passed, and update the product trace. This function must validate the transaction validity of the creator and a product expiry date after that the product data is updated. Note that transaction status may be incomplete, progressive, and complete. Next the

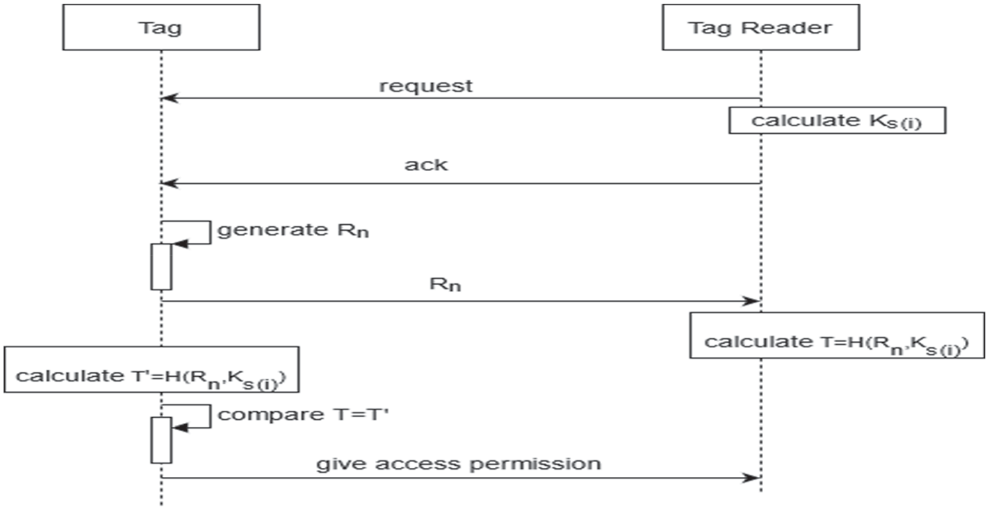


Figure 3. Tag authentication.

product ownership transfer between two users in supply chain management following completion of the transaction. The recipient's address is designated as the original owner, so the recipient behaves like the current product owner.

7. Performance evaluation

The proposed work was tested on a computer equipped with a 3.40 GHz Intel(R) Core(TM) i5-7500 CPU (4 cores) and 8 GB of RAM. We launched a private blockchain with EVM built in using Qtum, and then deployed our smart contracts to it. Here, we measure the cost of the transactions to prove the applicability of the proposed BA2C work. In blockchain, all transactions in the ledger perform both reading and writing operations.

Table 3. Cost zk-SNARK.

Operation	Gas Cost	Proof generation time (s)
Product Transfer	40471	6.24
Check identity	45726	0.64
Change Ownership	156197	3.55

7.1 *Cost*

In Ethereum cost is declared in ether, and an operation on the top of Ethereum paid in gas. Gas refers to the fee required to conduct a transaction successfully or to execute a contract on Ethereum. Then the 'gas cost' is how much gas a blockchain transaction takes to complete, and the 'gas price' is the gas unit price in ether. Consequently, the gas limit is set for each blockchain transaction to avoid running out of gas if the code contains any bugs. Therefore, the gas limit provides a safety mechanism. All the blockchain transactions can also be speeded up depending on the amount of ether spent per unit of "Gwei" gas. It is bit difficult to select the right gas price, as it needs constant network monitoring. However, providing three different categories Fast, Average, Safe Low, ETH gas station made this easier. Stakeholders can decide how much Gwei (1 Ether = 109 Gwei or 1Gwei = 0.000000001 ether), he is willing to pay per unit of gas for a specific transaction. A miner may choose to include the transactions in a block, based on the amount of Gwei offered for that transaction. In other words, many stakeholders pay more for their product transactions which would be included fast in a list of candidates. Transaction fee calculated using the formulation below.

$$T_f = G_p * G_r \tag{1}$$

In the above equation T_f, G_p, G_r represents Transaction fee, gas price, and gas required for. In the cost analysis used as a gas price of 27 Gwei was used, which is the current average price based on ETH Gas station. In our proposed system, the cost of the contract deployment is 0.94 US dollars. The cost for other functions would be less than $ 1, which means it could pay for US dollars once a product sales process is completed. Figure 4 illustrates the execution cost of a system function.

We are paying for the computation, regardless of whether the product transaction succeeds or fails. When the number of carriers increases, gas prices increase. As a consequence, the cost of a successful transaction is higher than the failed transaction. In table 3, the proof generation time for present research is 6.24 s, which is less than the previous methods, and the gas cost is less than one dollar.

7.2 *Efficiency*

7.2a *Throughput*. In this section, in terms of transaction throughput, transaction latency, we evaluated the

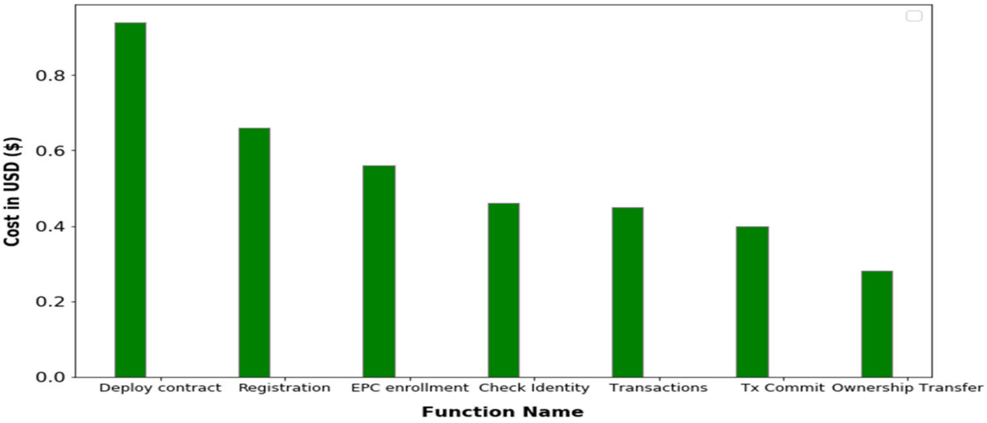


Figure 4. Cost for system function execution in USD.

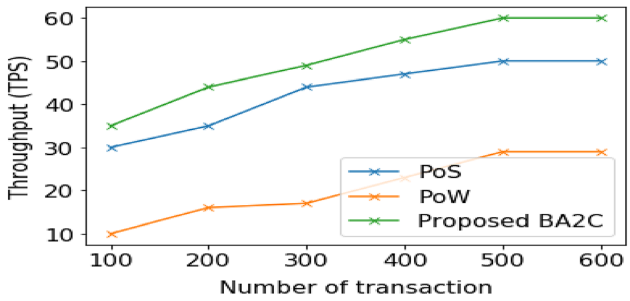


Figure 5. Comparison of transaction throughput.

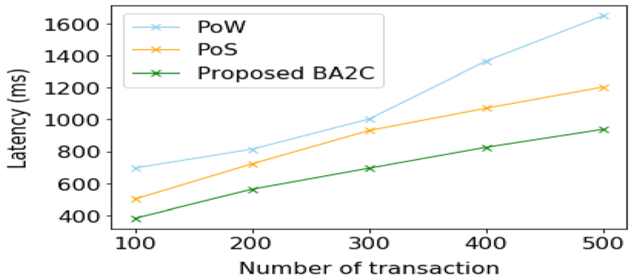


Figure 6. Comparison of transaction latency.

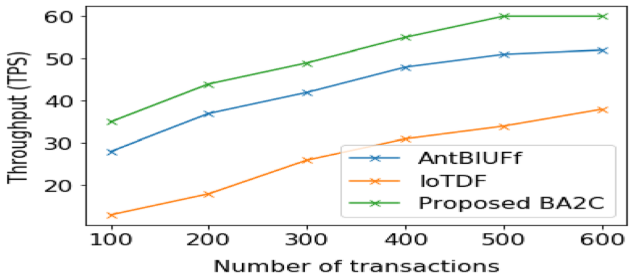


Figure 7. Throughput comparison of proposed BA2C and existing system (without counterfeit product).

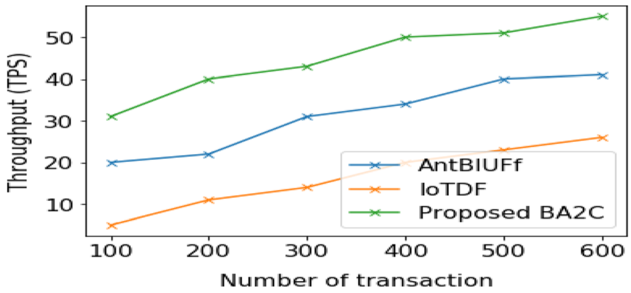


Figure 8. Throughput comparison of proposed BA2C and existing system (with counterfeit product).

performance of our system with 60 nodes. We, therefore, analyzed the efficiency of our system under the PoW, PoS, and PoA. The following formula [38] is used to determine throughput

$$T = \frac{T_{ns}}{T_{lc} - T_{fs}} \tag{2}$$

where, T represents throughput, T_{ns} represents number of successful tranasaction, T_{lc} represents transaction last confirmation time, and T_{fs} represents transaction first submission time. As shown in figure 5. The transaction throughput of our PoA- based model increases stably along with the gas price growth, and it gradually reaches the stable peak, i.e. approximately 82 TPS when the gas price is greater than 30 nodes. Concerning the PoW-based and PoS-based throughput, the maximum values of 9 TPS and 51 TPS flattened much earlier. PoA-based model performance is superior to that of the PoS and PoW-based model and is sufficiently high to satisfy the practical needs for dispute resolution.

7.2b *Transaction latency*. Latency refers to the time users have to wait before their transaction is processed. For public shared ledgers, there are a large number of nodes that need to reach a consensus to validate the transaction, and to process the transaction in such a way consensus is reached, every node needs access to the entire blockchain. A low latency device can easily send back the result of the transaction processing time and achieve a good user experience whereas, a high latency device cannot return the accuracy of the transaction in the processing time.

Product transaction latency is evaluated by an average of 100 measurements of the time spent during the product transaction submitted to the network and its exclusion and inclusion in a block. T_i is determined as the time stamp for some transaction T when transaction T was initially transmitted, T_b is the block creation timestamp including T, and latency of the transaction is determined as follows.

$$Latency = T_b - T_i \quad Where\ T_b > T_i > 0 \tag{3}$$

We repeat the experiment with 10, 20, 30, 40, 50, and 60 nodes to see how the nodes influence transaction latency. The average transaction latency remains constant, which is only approximately 32 S under PoA compared to 46 S and 40 S under PoW and PoS-based mechanism for different gas price is shown in figure 6. Overall, this experiment result demonstrates that the value of PoA transaction latency is stable and can be compared with PoW and PoS-based mechanisms. A comparison of throughput with and without counterfeit has been done between the proposed BA2C with the existing system IoT Data provenance Framework (IoTDF) [29], Anti-BlUFf [28] and the result has been depicted in figures 7 and 8 below.

The result was that the transaction throughput of BA2C seemed to be improved than existing systems in both with and without counterfeit. A comparison of efficiency with

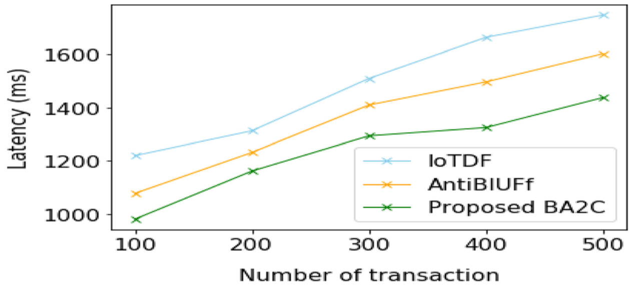


Figure 9. Latency comparison of proposed BA2C and existing systems (without counterfeit product).

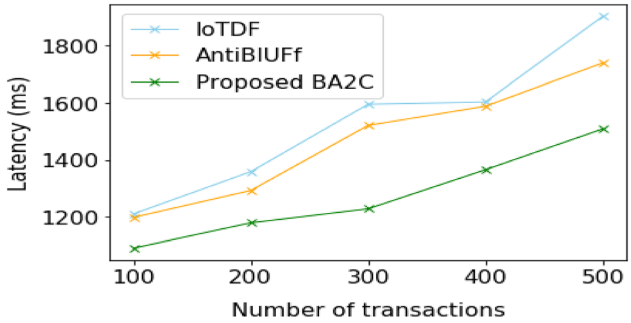


Figure 10. Latency comparison of the proposed BA2C and existing systems (with counterfeit product).

counterfeit has been done between the proposed BA2C systems with the existing system IoT Data provenance Framework (IoTDF) [29], Anti-BIUFf [28] and the result has been depicted in figures 9 and 10 below.

As a result, comparison BA2C efficiency to previous systems with throughput and significant delay over efficiency with and without attack is shown in figures 9 and 10.

8. Security analysis

The blockchain-based privacy system designed in this paper that preserves anti-counterfeit products meets the following security requirements.

1. *Immutability:* Identities and their corresponding attributes should be stored securely to avoid data leakage. Access and modification of the user data should be limited to the data business owner.
2. *Transparency:* Participants can make review transactions to alter or query the state of contracts. The proposed program transparency ensured as the transactions, and changes in the ledger state are accessible to public.
3. *Availability:* As regards ensuring availability, in this paper, smart contracts will always be deployed on the blockchain network to carry out their functions for the participating entities. It also makes the machine resources readily accessible to all users.
4. *Confidentiality:* Buyers and sellers are unknown in the supply chain network; we used the public blockchain platform Ethereum, which processes transparently. Supply chain transactions encrypted in a private Ethereum, and keys exchanged by participating in miner nodes and actors. A 20 bytes Ethereum address comes with asymmetric key pairs, which can then be used to encrypt all transactions and data.
5. *Traceability:* In the proposed BA2C system, we leverage RFID tag to track and trace product across the supply chain. RFID uses radio frequency waves for wireless and contactless transmission of data. An RFID tag ensures a manufacturer can track every single part it uses in its goods, providing visibility over every moving part in the supply chain.
6. *Anti-counterfeit product:* The sender and receiver have an identical Uport identity to be registered in the registry. During the product transaction from the sender to recipient, verify the identity of users belongs to the registry, or else the product will return to its owner.
7. *Key recovery:* The concept behind Uport is that blockchain technology will eliminate the crucial problem of holding private keys. To do so, Uport uses blockchain technology as an identity verification authority where a smart contract reflects a user's digital identity while allowing the user to revoke and restore his keys.
8. *Anonymity:* Personal Identification Information (PII) will ever exist on the blockchain network. All PII connected to the primary identifier DID of a user, which should also have limited interaction with the blockchain. A new account generated for each new DApp, the user interacts with to prevent potential knowledge of information publicly. In a zero-knowledge proof scenario, user will indeed illustrate to the network that they must have credentials through mathematical proof without revealing the user credentials itself. The benefits of privacy and security in this scenario are obvious. The mathematical proof cannot be discovered easily in zk-SNARK by the attacker.

a. *Tag cloning:* A copy of the tag is identified as being genuine. A cloning tag is possible only through the physical compromise of the RFID tag. By generating a random number using the TPRNG [17], it is possible to defend against cloning attack and provide the tag authentication.

We can safely conclude that our system is highly competitive with existing systems. All of the existing systems can complete the fundamental function, and traceability of information. However, the proposed program does have better mechanisms in terms of privacy, recovery of key and restriction from major attacks like MITM, replay attack.

The incentive mechanism is a critical consideration in implementing the proposed system. One of the key factors, while developing the process is highly motivated the chain management participants to incorporate the system.

However, this is a major task that is related to mining technique, smart contract, and environment design. We take it as a limitation that requires further analysis in future research.

9. Conclusion

In this paper, we have proposed a solution and generic BA2C framework leveraging Ethereum blockchain and smart contracts to detect counterfeit products, perform traceability without a third party, and avoid a single point of failure across supply chain management. This solution is compatible with the supply chain and is based on decentralized local databases, with RFID tags compliant with EPC-C1G2. Individuals could be uniquely identifiable in the system and could prove their ownership of the product. However, the presented aspects and details are generic enough and can be applied to provide trusted and decentralized anti-counterfeit products or medicine sales in the supply chain network. Performance evaluation results have shown the cost of original products with the proposed system is less than 1 USD. Furthermore, it employs anonymous distribution to store private information on the blockchain, allowing for non-interactive transaction generation between sender and recipient. A trustworthy set up is needed to create a proving key and a verifying key in order to deploy a zk-SNARK circuit. This process never causes a toxic waste, because each sender and receiver has an unique identity. There are so many critical issues in the supply chain network namely scalability, governance, big data storage, security, privacy issues, standards, and regulations. This research proposed a strategy for the pharmaceutical industry to overcome business challenges. Improving scalability, transparency and anti-counterfeiting have been addressed in this work via the proposed model. In the future, the authors are intended to resolve some of these crucial issues and develop solutions through the use of various incentive algorithms in the supply chain.

Acknowledgements

The authors would like to thank all reviewers and the corresponding editor for their informative comments and recommendations, which helped greatly to enhance the manuscript's content.

References

[1] Dujak D and Sajter D 2019 Blockchain applications in supply chain. In: S*MART supply network*. Springer, pp 21–46

[2] Asolo B 2018 *Blockchain soft fork & hard fork explained.* Mycryptopedia

[3] Coates R 2019 Counterfeits are still a major problem

[4] 2018 Manufacture of counterfeit products predicted to reach USD2.3 trillion, this is what businesses need to do

[5] L M& 2018 Blockchain revenues to hit $10.6 billion by 2023. https://www.mhlnews.com/technology-automation/article/22055261/blockchain-revenues-to-hit-106-billion-by-2023

[6] Kennedy J P 2020 Counterfeit Products Online. Palgrave Handb Int. Cybercrime Cyberdeviance: 1001–1024

[7] Tkachenko I, Tremeau A and Fournel T 2020 Fighting against medicine packaging counterfeits: rotogravure press vs cylinder signatures. In: 2020 *IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, pp 1–6

[8] Machado T B, Ricciardi L and Oliveira M B P P 2020 Blockchain technology for the management of food sciences researches. *Trends Food Sci. Technol.* 102: 261–270

[9] Hassija V, Chamola V, Gupta V, Jain S and Guizani N 2020 A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet Things J.*

[10] Li J, Maiti A, Springer M and Gray T 2020 Blockchain for supply chain quality management: challenges and opportunities in context of open manufacturing and industrial internet of things. *Int. J. Comput. Integr. Manuf.* 33: 1321–1355

[11] Sahoo M, Singhar SS and Sahoo SS 2020 A blockchain based model to eliminate drug counterfeiting. In: *Machine Learning and Information Processing*. Springer, pp 213–222

[12] Upadhyay A, Mukhuty S, Kumar V and Kazancoglu Y 2021 Blockchain technology and the circular economy: Implications for sustainability and social responsibility. *J. Clean Prod.* 126130

[13] Feng W, Yan Z, Yang L T and Zheng Q 2020 Anonymous Authentication on Trust in Blockchain-Based Mobile Crowdsourcing. *IEEE Internet Things J.*

[14] Ray P P, Kumar N and Dash D 2020 BLWN: Blockchain-based lightweight simplified payment verification in IoT-assisted e-healthcare. *IEEE Syst. J.*

[15] Schuster E W, Allen S J and Brock D L 2007 *Global RFID: the value of the EPCglobal network for supply chain management*. Springer Science & Business Media

[16] Xie R, Jian B and Liu D 2018 An improved ownership transfer for RFID protocol. *I. J. Netw. Secur.* 20: 149–156

[17] Toyoda K, Mathiopoulos P T, Sasase I and Ohtsuki T 2017 A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. *IEEE Access* 5: 17465–17477

[18] Alzahrani N and Bulusu N 2018 Block-supply chain: A new anti-counterfeiting supply chain using NFC and blockchain. In: *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, pp 30–35

[19] Cao B, Zhang Z, Feng D, Zhang S, Zhang L, Peng M and Li Y 2020 Performance analysis and comparison of PoW, PoS and DAG based blockchains. *Digit. Commun. Networks* 6: 480–485

[20] Cui P, Dixon J, Guin U and Dimase D 2019 A blockchain-based framework for supply chain provenance. *IEEE Access* 7: 157113–157125

[21] Benčić F M, Skočir P and Žarko I P 2019 DL-Tags: DLT and smart tags for decentralized, privacy-preserving, and verifiable supply chain management. *IEEE Access* 7: 46198–46209

[22] Salah K, Nizamuddin N, Jayaraman R and Omar M 2019 Blockchain-based soybean traceability in agricultural supply chain. *IEEE Access* 7: 73295–73305

[23] Liu D, Alahmadi A, Ni J, Lin X and Shen X 2019 Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain. *IEEE Trans. Ind. Informatics* 15: 3527–3537

[24] Wang S, Li D, Zhang Y and Chen J 2019 Smart contract-based product traceability system in the supply chain scenario. *IEEE Access* 7: 115122–115133

[25] Liu Z and Li Z 2020 A blockchain-based framework of cross-border e-commerce supply chain. *Int. J. Inf. Manag.* 52: 102059

[26] Cao Y, Jia F and Manogaran G 2019 Efficient traceability systems of steel products using blockchain-based industrial Internet of Things. *IEEE Trans. Ind. Informatics* 16: 6004–6012

[27] Shahid A, Almogren A, Javaid N, Al-Zahrani F A, Zuair M and Alam M 2020 Blockchain-based agri-food supply chain: A complete solution. *IEEE Access* 8: 69230–69243

[28] Aniello L, Halak B, Chai P, Dhall R, Mihalea M and Wilczynski A 2020 Anti-BlUFf: towards counterfeit mitigation in IC supply chains using blockchain and PUF. *Int. J. Inf. Secur.*: 1–16

[29] Sigwart M, Borkowski M, Peise M, Schulte S and Tai S 2020 A secure and extensible blockchain-based data provenance framework for the Internet of Things. *Pers. Ubiquitous Comput., pp* 1–15

[30] Williamson E A, Harrison D K and Jordan M 2004 Information systems development within supply chain management. *Int. J. Inf. Manag.* 24: 375–385

[31] Cole P and Ranasinghe D C 2008 Networked RFID systems and lightweight cryptography. London, UK Springer doi 10:973–978

[32] Research T Blockchain identity management: sparking a data security revolution. https://www.toptal.com/insights/innovation/blockchain-identity-management

[33] Nakamoto S 2019 Bitcoin: A peer-to-peer electronic cash system. Manubot

[34] Li L, Liu J and Jia P 2021 SecTEP: Enabling secure tender evaluation with sealed prices and quality evaluation in procurement bidding systems over blockchain. *Comput. Secur.* 103: 102188

[35] Buterin V 2014 A next-generation smart contract and decentralized application platform. white Pap 3(37): 2-1

[36] Bedin A R C, Capretz M and Mir S 2020 Blockchain for collaborative businesses. *Mob. Networks Appl.*, pp 1–8

[37] Mayer H 2016 zk-SNARK explained: basic principles. URL https://blog.coinfabrik.com/wp-content/uploads/2017/03/zkSNARK-explained_basic_principles.pdf

[38] Abdella J, Tari Z, Anwar A, Mahmood A and Han F 2021 An architecture and performance evaluation of blockchain-based peer-to-peer energy trading. *IEEE Trans. Smart Grid* 12: 3364–3378