Advances in Science, Technology and Engineering Systems Journal
Vol. 7, No. 3, 106-115 (2022)
www.astesj.com
Special Issue on Innovation in Computing, Engineering Science & Technology

ASTES Journal
ISSN: 2415-6698

Secured Multi-Layer Blockchain Framework for IoT Aggregate Verification

Ming Fong Sie, Jingze Wu, Seth Austin Harding, Chien-Lung Lin, San-Tai Wang, Shih-wei Liao[*]

Department of Computer Science and Information Engineering, National Taiwan University, Taipei, 106, Taiwan

ARTICLE INFO

Article history:
Received: 27 March, 2022
Accepted: 25 May, 2022
Online: 04 June, 2022

Keywords:
IoT
Blockchain
ID-based Signature
Aggregate Verification
Digital Provenance
Supply Chain Management

ABSTRACT

Technologies designed for digital provenance, especially the Internet of Things (IoT) and blockchain, may allow for security, transparency, and traceability in the global supply chain. However, upstream nodes in the supply chain that work for large-scale production suppliers are not considered. In addition, most IoT blockchain systems adopt an ID-based signature scheme that may affect the efficiency of IoT devices. We propose using aggregate verification to improve the security and efficiency of ID-based verification, reduce network traffic on the blockchain, and transfer computing overhead to aggregator nodes. This paper implements a multi-layer blockchain for Agriculture 4.0 supply chain management that has higher efficiency, effectiveness, and security in comparison to conventional blockchains. We design a Multi-Layer Aggregate Verification (MLAV) solution to improve supply chain management with IoT Blockchain for Agriculture 4.0 through the following methods. First, we use a multi-layer IoT blockchain system to reduce Ethereum gas fee. Second, we design an ID-based Aggregate Verification scheme, thereby eliminating the certificate management cost in the traditional Public Key Infrastructure (PKI) and reducing bandwidth and computation time requirements. Third, we implement a three-layer blockchain infrastructure. In Layer 1, IoT devices sense and upload data to the system's database; in Layer 2, smart contracts execute aggregate ID-based signature verification from IoT devices and upload the transactions to the private blockchain; in Layer 3, a batch converts the layer 2 data and uploads its Merkle root to Ethereum, thereby reducing the required gas fee.

1 Introduction

This paper is an extension of a work originally presented in BRAINS 2021 [1] that uses a multi-layer architecture designed to facilitate smallholders in joining an agricultural blockchain infrastructure. We use aggregate verification to solve the efficiency bottleneck of ID-based signature verification. We also lay out the framework for distributed supply chain management for access control with smart contracts to allow the smallholder to gain access to loans.

With the ushering in of Agriculture 4.0, in recent years there has been widespread adoption of technologies such as the Internet of Things, big data, artificial intelligence, cloud computing, and remote sensing [2]. Agriculture 4.0, also known as digital farming or smart farming, has been brought about by combining telematics and data management with known precision agriculture concepts. These changes have improved the accuracy and practicality of farming operations [3].

However, regarding data management, food safety, and quality monitoring of the agricultural supply chain, Agriculture 4.0 still has significant shortcomings. Particularly in the COVID-19 pandemic, it is essential to prevent cross-contamination and food pathogen outbreaks. The agricultural supply chain should have data transparency, and there should exist a high level of traceability from source to consumer. The World Government Summit in 2018 pointed out that Agriculture 4.0 will need to focus on both the demand side and the value chain (supply) side of the food equation to use technology to meet the real needs of the consumer and to re-engineer the value chain [4]. The tamper-proof property and transparency of blockchain technology allow it to meet these requirements effectively. IoT Blockchain is highly suited for ensuring traceability and consistency of information generated by IoT devices.

Large companies have already begun to adopt distributed supply chain management systems with blockchain technology. In 2017, Walmart established the Walmart Food Safety Center in Beijing and invested US$25 million to use IBM's blockchain solutions to build a global food safety system [5] already tracking 1,500 items on the supply chain blockchain in 2021. Proof of Concept (PoC) and blockchain pilot projects have been established in the United

[*] Corresponding Author: Shih-wei Liao, Email: liao@csie.ntu.edu.tw

https://dx.doi.org/10.25046/aj070312

States and China for two products: mango slices and fresh-cut pork products [6]. The cost of supply chain management systems is very high, and there are restrictions on their scalability; therefore, IoT blockchain systems are only suited for large companies. We believe that the benefits brought about by IoT Blockchain should serve not only high-level large-scale food and agricultural suppliers but also grassroots farmers and food producers in providing customized platforms and advice. Blockchain is becoming ever-more democratized and is decentralized in nature; it is therefore highly suited to providing equal opportunity for traditionally disadvantaged entities.

Therefore, the contributions of this paper can be outlined as follows. An Agricultural Supply Chain Finance operational procedure is created with smart contracts that define the rules and functions of three types of nodes: farmer, distribution channel, and financial institution. A corresponding IoT blockchain system is then designed and implemented to record valuable data on both production activity and order history of farmers. There are two types of IoT devices in this system: farming sensors and mobile phones. The farming sensor is a custom-designed piece of hardware that is used in an agricultural setting; for mobile phones, a custom-designed Android app is developed that connects to our IoT blockchain system. Batch verification is leveraged by our IoT Blockchain system to increase ID-based signature verification.

The remainder of this paper is structured as follows: In Section II, we summarize related works. In Section III, we discuss the benefits of using our multi-layer blockchain. Section IV defines and details the aggregate verification algorithm we use. In Section V we describe the blockchain management framework and system architecture. In Section VI, we propose the implementation and evaluation. In Section VII, we have our conclusion.

2 Related Works

2.1 Distributed Ledger Technology

Distributed ledger technology (DLT) is a shared transaction ledger technology that can store, distribute, and exchange certifications publicly or privately between peer entities. In the context of the blockchain, a distributed ledger records transactions between participants and nodes. This data can be duplicated and synchronized across decentralized peer-to-peer networks with consensus algorithms. DLT may then facilitate the flow of information between nodes and help to resolve inefficiencies relating to information asymmetry[7] [8].

Blockchain technology is a specific type of DLT that was developed in 2008 for the implementation of the cryptocurrency Bitcoin [9]. In the Bitcoin network, by leveraging the Proof of Work (PoW) consensus mechanism, blocks are added to a linearly growing, chronologically ordered blockchain. Each block contains the timestamp, transaction data, and hash value of the previous block.

2.2 Ethereum Layer 2 and Smart Contract

Our platform uses the Ethereum blockchain, an open-source, public blockchain structured around a decentralized Ethereum Virtual Machine (EVM) that may process smart contracts [10]. Data agreements are reached via the Proof of Work consensus algorithm. Ethereum 2.0 is expected to switch to the Proof of Stake (PoS) consensus algorithm, which may significantly reduce computational resources wasted during mining and prevent attacks from application-specific integrated circuits (ASIC) [11]. In addition, Ethereum layer-2 technologies such as Arbitrum could collect transactions off-chain and batch it on-chain, scaling up transaction speed, improving privacy, and holding EVM compatibility by using Arbitrum Virtual Machine (AVM), all while still benefiting from layer-1 security [12].

The concept of smart contracts was first proposed in [13]. Its original idea was centered around a ”computerized transaction protocol that executes the terms of a contract.” Developers began integrating this innovative concept into the blockchain environment. The idea of a smart contract has become ”executable code that runs on top of the blockchain to facilitate, execute, and enforce an agreement between untrusted parties without the involvement of a trusted third party” [14].

2.3 IoT Blockchain in Agriculture 4.0

IoT Blockchain is a new technology that integrates the Internet of Things with blockchain technology. It features the following advantages [15] in Agriculture 4.0:

- Transparency for participating companies [16]: New levels of transparency and visibility are essential for improving product traceability and ensuring product authenticity and legality [17, 18].
- Food safety and quality monitoring [19]: A real-time food tracking system built on blockchain technology provides an information platform that enables all supply chain members to access all information, thereby providing openness, neutrality, and reliability for the food supply chain[20].
- Promoting the digitization and disintermediation of the supply chain: Blockchain reduces verification and transaction costs by eliminating intermediaries [21]. By replacing trade financing (banks acting as financial intermediaries) with a blockchain platform, processing time may be reduced from between 7 and 10 days to between 1 and 4 hours [22].
- Improving data security of information sharing: Centralized databases may be prone to data loss or have data that is difficult to retrieve [23]. All data in the blockchain is immutable because the order of transactions is stored in chronological blocks and broadcast to all nodes [24]. The stored data is tamper-proof because updating and deleting of transactions is determined by the consensus mechanism[25, 26].
- Agricultural Finance: Blockchain technology can implement fast, real-time payments for agricultural financial services that increase cash flow and working capital while reducing transaction costs and risks [27].

Ethereum is the first Turing-complete blockchain framework that enables smart contract integration [10]; given enough time and memory as well as the necessary instructions, smart contracts can solve any computational problem no matter the complexity. There are numerous advantages of smart contracts on the blockchain over traditional contracts.

- The content of the contract is open-source, transparent, and tamper-proof. The immutable smart contract code is guaranteed to execute, which reduces the occurrence of fraud.
- Higher efficiency: using a programming language, there are almost no misunderstandings or disputes, and consensus may easily be reached.
- No third-party arbitration is required. The system automatically executes according to the smart contract, thereby reducing time and verification costs.

2.4 IoT Blockchain

Massive amounts of data are generated from IoT devices and stored in the cloud. It is also an emerging security concern. Blockchain-based IoT systems might solve this security problem in distributed infrastructure [28]. The user could integrate with PKI to access data from IoT devices and interact with blockchain miner nodes to keep track of every transaction on chain [29]. In [30], the author introduce multi-layered network architecture by defining the IoT device layer, router layer, cloud compute layer, offers an authentication framework, and reducing IoT network burden also improves transaction throughput and security.

2.5 Supply Chain Finance

This research focuses on the agricultural supply chain, which is highly competitive. Large-scale downstream enterprises hold an advantageous position. They place heavy requirements on upstream suppliers for purchases, prices, and payment conditions, causing massive pressure on upstream suppliers. Most of these upstream suppliers are small-scale enterprises or farmers; it is difficult for suppliers to obtain loans from financial institutions, resulting in limited funding for upstream entities. A new set of modes has been developed to solve this problem: Agricultural Supply Chain Finance. Agricultural Supply Chain Finance is a proposed framework for financial support for upstream suppliers that promotes the establishment of long-term strategic, synergistic relationships between upstream suppliers and major distributors and improves the competitiveness of the entire agricultural supply chain.

The lack of mutual trust in the agricultural supply chain stems from one primary source: agricultural production suppliers rarely keep financial records. Since most agricultural operations are tax-exempt, farmers neither pay taxes nor report taxes. Therefore, most farms in Taiwan do not have records of either production or sales. As a result, when applying for loans from financial institutions, it is difficult for these agricultural production suppliers to provide sufficient financial data; coupling this with the lack of sufficient existing credit information, financial institutions are often unwilling to lend to these suppliers.

2.6 Aggregate Verification

Aggregate verification is a computationally efficient method for verifying a large number of digital signatures quickly. It is more computationally efficient than individual verification of each signature. With large quantities of data rapidly generated by a variable number of IoT devices, we adopt an aggregate verification method that may be used even in cases of high traffic in the network.

Among the most important considerations in implementing blockchain technology is the measurement of time between uploading data and attaining immutability (confirmation time). For systems with a large number of nodes frequently generating new data, aggregate verification may be implemented to efficiently verify many signatures simultaneously in one action [31]. One such example of this form of implementation may be in IoT devices which require periodic firmware and software updates. In this case, aggregate verification may be implemented for future-proofing the devices by evolving to internet threats, fixing functionality by releasing firmware updates [32]. Upon release of updated firmware, a group of distributed IoT devices may have an update securely and remotely installed automatically rather than being individually, manually installed by the owner of each device.

In the case of immediate verification of items uploaded to the blockchain, some blockchains may choose to require fewer block confirmations for signature verification, thereby compromising security [33]. Therefore, in addition to the aggregate verification case described above, a new aggregate verification application has been proposed in [31] in which a system may need to verify a smaller number of signatures with high efficiency and minimized confirmation time. For example, an IP camera surveillance system may have cameras with a framerate of 15 FPS, with each device generating approximately 1.25 million images in one day. Digital signatures may be used to quickly verify large amounts of pictures and uploaded to the blockchain in large clusters.

3 Benefits of Multi-Layer Blockchain

This section describes the advantages of using our multi-layer blockchain on the system level and on the framework level.

3.1 Multi-Layer Blockchain System

With the application of blockchain technology in the supply chain, corporations and large upstream manufacturers simplify collecting information and production-related data for all transactions in the supply chain (e.g. IBM's global food safety system), assisting institutions in strengthening risk management and control. However, the disadvantaged small upstream producers do not benefit from blockchain technology. Low-income smallholders who operate without a working contract are among the highest upstream entities in the agricultural supply chain; they and the information related to their production activities are essentially nonexistent or anonymous on the supply chain. As participants in the supply chain, they have limited or no access to the information in the blockchain system.

Following our previous work [1], we create a platform to facilitate these small upstream entities in joining the blockchain system; the overview of our platform is shown in Fig. 1. We propose the Certificateless verification process on a client node based on aggregate verification, identity-based cryptography, and zero-knowledge cryptography, which resolves the critical escrow problem and secures the proof. The Key Generation Center (KGC) constructs only the partial private key of the IoT device. The IoT device generates the entire private key by choosing a piece of secret information and combining it with the partial private key constructed by the KGC. The system parameters published by KGC compute the corresponding public key of the IoT device, and the IoT's secret information is chosen by itself. In addition to our multi-layer platform, we also develop an Android app. The outermost layer of our platform is the Database layer which allows app users to record and read production-related data. The Database layer also provides storage for IoT-generated data for large manufacturers. In order to ensure the tamper-proof property and connectivity of all product information, the Smallholder Node and the Aggregator Node upload information to the Quorum chain in the form of a hash. As Quorum is a permissioned blockchain and lacks information transparency, the data is then uploaded to Ethereum for public access [34]. In order to reduce the gas fee and increase the blockchain recording rate in Ethereum, we convert the data for each product unit into Merkle tree format and only upload the Merkle root on Ethereum. The detailed technical process description may be found in Section V.

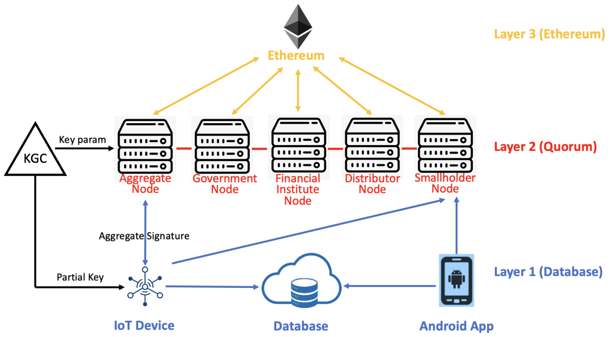

Figure 1: Multi-layer Platform: Blockchain View

3.2 Supply Chain Management Framework Based On Smart Contracts

When operating blockchain-based supply chains, the blockchain system must define a set of rules to determine the roles, responsibilities and read-write permissions of participants, which involves maintaining a distributed, authenticated, and synchronized ledger of transactions [35, 36]. Traceable transactions with roles could ensure the stability of the supply chain system [36].

Our supply chain framework is designed to benefit smallholders equally; a blockchain system with smart contracts clearly defines the different rules, responsibilities, and relations of the three types of nodes: Upstream Producer, Financial Institution, and Distribution Channel. The detailed operation process description may be found in ”Operation Procedure” in Section V.

With the multi-layer blockchain framework, small upstream entities may upload to the blockchain and access their production activity records, contracts, and transaction records while also solving the largest hurdle: financing. In the past, due to factors such as low fixed assets, low equivalent collateral, and no access to personal financial information, it has proven difficult for smallholders to gain the trust of financial institutions or to obtain any form of funding channel. Through the application of IoT Blockchain, the upstream producer's production activity data and historical order information may be provided to third-party entities for evaluation. This ultimately provides a means by which they may gain trust and become eligible for loans from financial institutions.

Blockchain is increasingly being viewed as a viable solution for alleviating the complexity of global supply chains [20, 37]. The solutions we provide may also be applied to international trade and global supply chains. Addressing the eight technical and non-technical challenges summarized by the OECD [38], our implementation framework and blockchain system may realize the goal of both Inclusion of Informal Actors and Governance.

4 Verification Process

This section presents the details of our verification process on a client node (farmer node or aggregator node) based on aggregate verification, identity-based cryptography, and zero-knowledge cryptography. The aggregator node scheme includes system setup and registration phases, data uploading procedure, aggregate verification, and performance simulation.

4.1 Aggregator Node

Smallholders only need to upload a few pictures and messages to the chain; there is no real-time requirement, and they do not need to consider its writing efficiency or computational cost. Smallholders may register as a client node and perform write/read operations to the blockchain through our Android app.

For large suppliers (such as central kitchen) nodes, one node may have hundreds of IoT devices operating simultaneously, with huge amounts and multiple types of complex data simultaneously uploading to the chain; special consideration must be made for throughput, security, and the tamper-proof property.

Therefore, we design an aggregator node; IoT devices are not directly connected to the blockchain but send messages and signatures to an aggregator node which is a relay device that holds powerful computing resources for the network. After executing aggregate verification, the aggregator node then uploads the data to the chain. The advantages of using an aggregator node include:

- Reducing computational cost: IoT devices have limited computing resources, and many devices that use batteries have power restrictions. Therefore, we place energy-consuming operations (uploading procedure) on the aggregator node after centralizing the signature and message to ensure durability in IoT device operations.

- Meet real-time requirements: The message may be quickly uploaded to the chain after aggregate verification, avoiding the possibility of human tampering.

4.2 System Setup and Registration

When an IoT device or a client node (aggregator or farmer) first enters the system, the System Setup and Registration processes are executed. According to the aforementioned multi-layer architecture, data uploading to the chain takes place on Layer 2: Quorum. A Quorum chain is a consortium blockchain; its implementation includes an identity-based signature scheme (IBS). A short public identifier such as an IoT device's MAC address may be used as a verification key. The following system parameters are defined in a tuple: (q, P, G1, G2, e) [39]. The notations and parameters throughout this paper are listed in Table 1.

Table 1: Notation and Parameters

Notation	Description
RID	Real Identity of the device
q	Prime order
P	Generator of G1
G1	Additive group of q
G2	Multiplicative group with same order as G1
e	G1 x G1 → G2, a bilinear mapping
h()	One-way hash function like SHA3-256
H1()	MapToPoint hash function $H1 : \{0, 1\}^* \rightarrow G_1$
⊕	Exclusive or
DM	IoT device
MT	Model type
Chk	Checksum generated by SHA3-256
BT_seed	BitTorrent seed of the data

Next, the IBS selects two randomly generated numbers c_1 and c_2 as a pair of secret master keys and generates their corresponding public keys PK_{MAC1} and PK_{MAC2} as follows:

$$\begin{aligned} c1, c2 &\in Z_q^* \\ PK_{MAC1} &= c1 \times P \\ PK_{MAC2} &= c2 \times P \end{aligned} \tag{1}$$

The following hash functions are formed [40]:

$$\begin{aligned} h &: \{0, 1\}^* \rightarrow \{0, 1\}^f \\ H1 &: \{0, 1\}^* \rightarrow G_1 \end{aligned} \tag{2}$$

The system publishes <q, P, G1, G2, e, h, H1, PK$_{MAC1}$, PK$_{MAC2}$>.

Upon entry of an IoT device or a client node, our platform must also execute a key generation procedure. The Hardware Security Module (HSM) stores system parameters c_1, c_2 and generates the pseudo-identity and its corresponding public and private keys for the client node by executing the following three procedures.

- Identity Authentication: Each device must first input <RID, fp, or pw> where RID refers to the real ID of the farmer, fp refers to fingerprint, and pw refers to password. This step is necessary for activating the device's HSM.

- Sub-Identity Calculation: HSM selects $t \in Z_q^*$ and computes the first sub-identity $SID1 = tP \in G1$ as well as the second sub-identity $SID2 = RID \oplus H1(t \times c1 \times PK_{MAC2})$.

- Key Calculation: To finish the procedure, HSM calculates the corresponding private key $PrK1 = c1 \times SID1$, $PrK2 = c2 \times H1(SID1 \oplus SID2)$. After Identity Authentication, Sub-Identity Calculation, and Key Calculation procedures have been executed, HSM outputs <ID = (SID1, SID2), PrK = (PrK1, PrK2)>.

After Identity Authentication, Sub-Identity Calculation, and Key Calculation procedures have been executed, HSM outputs <ID = (SID1, SID2), PrK = (PrK1, PrK2)>.

4.3 Data Uploading Procedure

IoT device D uses off-chain programs to download device information DM from BT_seed, and computes DM's checksum. IoT device D uploads new data to an aggregator node according to the following procedure.

- D prepares device DM and retrieves model type MT

- DM collects data, recording TimeStamp and checksum Chk generated by h(DM).

- D stores data into a peer-to-peer file sharing system such as BitTorrent or IPFS while also acquiring the BT_seed of DM.

- D provides a signature as follows:

$$\begin{aligned} v &\leftarrow h(ID \,||\, MT \,||\, TimeStamp) \\ w &\leftarrow h(ID \,||\, Chk \,||\, BT\_seed) \\ \sigma_D &= (v \times PrK1) + (w \times PrK2) \end{aligned} \tag{3}$$

Finally, D sends <ID, MT, TimeStamp, Chk, BT_seed, σ_D > to the aggregator node. The aggregator node then performs aggregate verification. The smart contract checks the validity of the aggregator's signature; if correct, the smart contract records (MT, TimeStamp, Chk, BT_seed) onto the blockchain.

4.4 Aggregate Verification

In our implementation of aggregate verification, we apply a new signature verification method that allows for superior efficiency and zero-knowledge proof. The algorithm for verifying the signature is proposed in Algorithm 1. An aggregator node receives a new transaction sent from D in the following format: <ID, MT, TimeStamp, Chk, BT_seed, σ_D >, and the aggregator node can then verify the signature σ_D with the following equation [32]: $e(\sigma_D, P) \overset{?}{=} e(v \cdot SID1, PK_{MAC1}) \cdot e(w \cdot H1(SID1 \oplus SID2), PK_{MAC2})$, where e is the bilinear mapping function [40] as in Table 1. The verification procedure is shown below:

$$\begin{aligned} & e(\sigma_D, P) \\ &= e(v \cdot PrK_1 + w \cdot PrK_2, P) \\ &= e(v \cdot PrK_1, P) \cdot e(w \cdot PrK_2, P) \\ &= e(v \cdot c_1 \cdot SID_1, P) \cdot e(w \cdot c_2 \cdot H_1(SID_1 \oplus SID_2), P) \\ &= e(v \cdot SID_1, c_1 \cdot P) \cdot e(w \cdot H_1(SID_1 \oplus SID_2), c_2 \cdot P) \\ &= e(v \cdot SID_1, PK_{MAC1}) \cdot e(w \cdot H_1(SID_1 \oplus SID_2), PK_{MAC2}) \end{aligned} \tag{4}$$

```
Algorithm 1: Verify the signature D
Data: <ID, MT, TimeStamp, Chk, BT_seed, $\sigma_D$ >
Result: $true$ or $false$
if $e(\sigma_D, P) ==$
  $e(v \cdot SID1, PK_{MAC1}) \cdot e(w \cdot H1(SID1 \oplus SID2), PK_{MAC2})$
  then
    if Chk of DM is correct then
        upload hash of BT_seed on the blockchain;
        return $true$;
    else
        return $false$;
else
    return $false$;
```

In the case that an aggregator node receives a large quantity of new data in a short time period, the aggregator node must verify multiple or numerous signatures. Under these circumstances, aggregate verification is applied as shown below. Let us suppose that n distinct transactions must be verified. Each transaction is denoted as < MT^n, TimeStamp^n, Chk^n, BT_seed^n, σ_D^n > . The aggregator node can perform aggregate verification on all signatures with the following calculation: $e(\sum_{i=1}^{n} \sigma^i, P) \overset{?}{=} e(\sum_{i=1}^{n} v_i \cdot SID_1^i, PK_{MAC1}) \cdot e(\sum_{i=1}^{n} w_i \cdot H1(SID_1^i \oplus SIDi_2^i), PK_{MAC2})$. The verification procedure is shown below:

$$
\begin{aligned}
& e(\sum_{i=1}^{n} \sigma^i, P) \\
&= e(\sum_{i=1}^{n} (v^i \cdot PrK_1^i + w^i \cdot PrK_2^i), P) \\
&= e(\sum_{i=1}^{n} (v^i \cdot Prk_1^i, P) \cdot e(\sum_{i=1}^{n} (w^i \cdot PrK_2^i), P) \\
&= e(\sum_{i=1}^{n} (v^i \cdot c_1 \cdot SID_1^i, P) \cdot e(\sum_{i=1}^{n} w^i \cdot c_2 \cdot H_1(SID_1^i \oplus SID_2^i), P)) \\
&= e(\sum_{i=1}^{n} v^i \cdot SID_1^i, c_1 \cdot P) \cdot e(\sum_{i=1}^{n} w^i \cdot H_1(SID_1^i \oplus SID_2^i), c_2 \cdot P) \\
&= e(\sum_{i=1}^{n} v^i \cdot SID_1^i, PK_{MAC1}) \cdot e(\sum_{i=1}^{n} w^i \cdot H_1(SID_1^i \oplus SID_2^i), PK_{MAC2})
\end{aligned}
\tag{5}
$$

4.5 Performance Simulation

We evaluate the performance of aggregate verification and other cases presented [41]. Cases 1-5 consist of two types of operations: the first is response from a verification node to a requesting node (R1). The second is the response from a response node to a requesting node (R2). R1 is then divided into two sub-cases (Case 1 and Case 2), while R2 is similarly separated into Case 3, Case 4, and Case 5. Each case depends on the type of response node which receives the version-check request message sent from the requesting node. Their proposed blockchain scheme has five different operation cases:

- Case 1: an IoT device sends a request to a verification node that has the newest data to verify whether its data is the newest.
- Case 2: an IoT device sends a request to a verification node that has the newest data to confirm its data is old and then downloads the newest data.
- Case 3: an IoT device first asks its neighbor IoT device to verify the data version and then verifies whether it has the newest data.
- Case 4: an IoT device first asks its neighbor IoT device to verify whether the data has a newer version and sends a download request to a verification node if it does not have the newest data.
- Case 5: an IoT device broadcasts a join verification message to a blockchain network to ask other nodes to join the verification process to check whether the data version of a device is equal to that of its neighbor node.

We define the cost of cryptographic operations required for each verification procedure. The parameters in Table 1 let S be the time of scalar multiplication in G1, P the time of bilinear pairing operation, and the time of MapToPoint hash operation is H. The pairing operation is the most time-consuming of those operations. We only consider these operations, which determine the speed of signature verification, omitting all other procedures such as one-way hash and point addition.

We use parameter size selection for the elliptic curve cryptography scheme [42] to ensure a security level of the 1024-bit RSA algorithm as a benchmark. G is an additive cyclic group of order q (160-bit prime number) on the elliptic curve, and P is the generator of G. The processing time of Tate pairing on an MNT curve with an 80-bit security level, 160-bit q, and embedding degree k=6 running on an Intel i7 3.07 GHz machine in experiment [43]. Table 2 shows the symbol and execution time in milliseconds.

Table 2: Symbols and Execution Time

Symbol	Description	Execution Time
P	Bilinear pairing operation	3.25
S	Scalar multiplication	0.41
H	MapToPoint hash operation	0.13

Table 3: The Comparison of Operations

Case	Operations
Case1	$2S + 1P$
Case2	$2S + 1P$
Case3	$5S + 3P$
Case4	$5S + 3P$
Case5	$6H + 3S + 2P$
Our scheme	$2H + 3S$

Our computational cost-performance comparison and overhead are shown in Fig. 2. In our scheme, there are five components (RID, q, P, G1, and e) that are passed into the smart contract for updating the data. Next, we explain the update message calculation of Case 1 to Case 5 based on [41], which requires more operations than in Case 1; Case 2 includes two decryption operations and one verification operation. The time in Case 3 and Case 4 to process n messages in five decryption and three verification processes. In Case 5, the data is considered verified if the original verification is confirmed by other nodes; this is done via a six-block confirmation with PoW consensus. The request nodes need to receive six verification messages from other blockchain nodes to confirm the integrity of the data. As a result, the total computational cost is three decryption operations, two verification operations, and six ECDSA verifications.

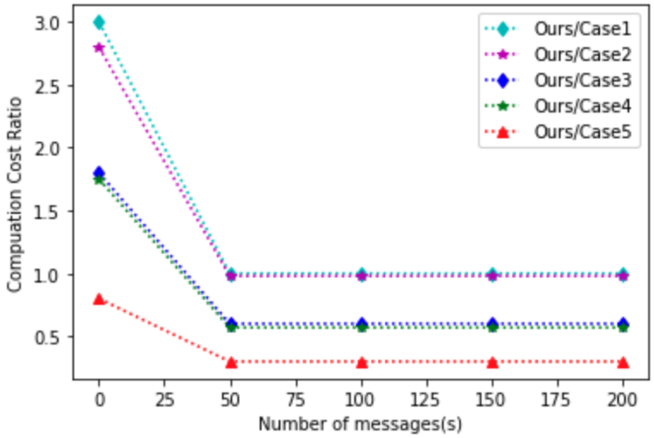

Figure 2: Computation Ratio

5 Management Framework and System Architecture

This section will focus on our blockchain management framework operation procedure and the details of our system architecture. Traditional paper contracts are replaced with smart contracts in the practical process of smallholder agricultural supply chain finance. We digitize the loan application and the information that may prove an upstream producer can reimburse the lender (operational plans, historical transaction records, agricultural production status, current delivery schedule, etc.) and upload this information to the blockchain system. We describe the relationship of the three layers that compose the system architecture.

5.1 Objects and Nodes

There are three main roles: 1. Smallholder (loan applicant) 2. Agricultural financial institution (lending institution) 3. Distribution channel (supermarket or hypermarket)

There are two separate procedures for signing the transaction contract and for the payment verification by the distribution channel: I. The buyer (distribution channel) and the seller (smallholder) sign a smart contract and upload it to Ethereum. II. Smallholders supply to large distributors. After the distribution channels confirm acceptance, they upload the acceptance records to the blockchain. The distribution channel regularly settles the sales volume and pays the smallholders, and at the same time, the sales volume data and payment information are uploaded to the blockchain. An order is not complete until the final payment has been processed.

5.2 Operation Procedure

The operation structure is shown in Fig. 3. The distribution channel (DC) first signs a contract with the smallholder through a smart contract and uploads it to the blockchain after a certain number of parties confirm its correctness. The smallholder must provide other information to financial institutions that may prove their ability to repay the loan, such as business plan books, historical transaction records, and agricultural production conditions to the agricultural financial institution (AFI). After the AFI confirms eligibility and approves the loan, the smallholder begins production. If the DC has paid the deposit, the deposit is then transferred to the smallholder's account in the AFI.

While the smallholder grows crops, production status is regularly uploaded to the blockchain through IoT devices for inspection by AFI and DC. For example, at the i'th production checkpoint, the IoT device uploads photos of the production progress to the blockchain via aggregate verification. Therefore, AFI can make phase i payment to the smallholder based on the production progress ledger. If the photos of the production status do not meet the mark and the smallholder cannot complete production on time, the AFI will recover the funds.

After the smallholder has completed production, they will upload the supply orders to the system when they deliver the produce to the DC. After the DC accepts the produce, the supply orders are uploaded to the blockchain to complete the acceptance of produce. Finally, the AFI makes the final payment to the smallholder, deducting interest and handling fees of the loan according to the previous production progress account book, and settles the remaining receivables.

On our agricultural supply chain blockchain financing platform, all kinds of transaction contracts, supply documents, and production activities are recorded in the blockchain system to allow for agricultural production and sales activities to be transparent and immutable. Relevant information from farmers stored in the blockchain system also proves their repayment ability, providing them with credentials for loans.

5.3 System Architecture

Fig. 4 shows the architecture of the blockchain system for the proposed financing platform. We choose Ethereum as our blockchain system because smart contract functionality is built-in. As shown in the user group located at the bottom of Fig. 4, the IoT device uploads new photos over a set interval. The original data is stored in the database while the following hash value is uploaded to the blockchain: <ID, CT, TimeStamp, Chk, BT_seed, σF >. Other data such as transaction contracts, supply records, and sales records are uploaded to the blockchain in smart contracts. After applying for permission, distribution channels may confirm contract information through the Inspection API. Agricultural financial institutions and agricultural loan reviewing entities may also view the field of agricultural product production materials and inspection documents.

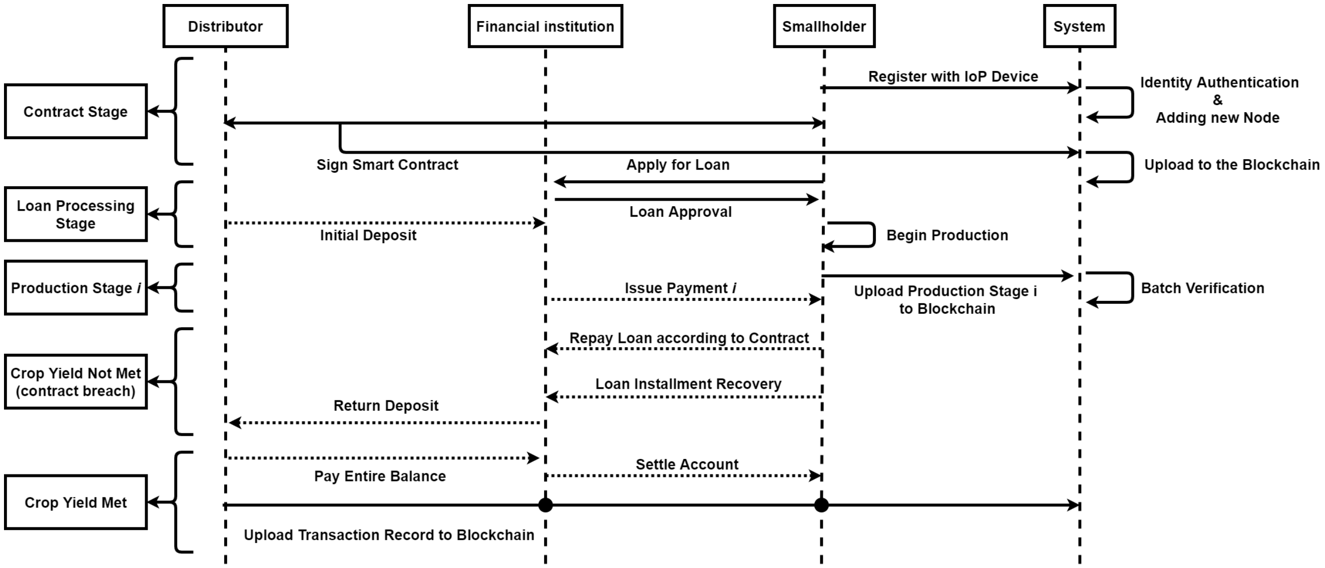

Figure 3: Operation Procedure

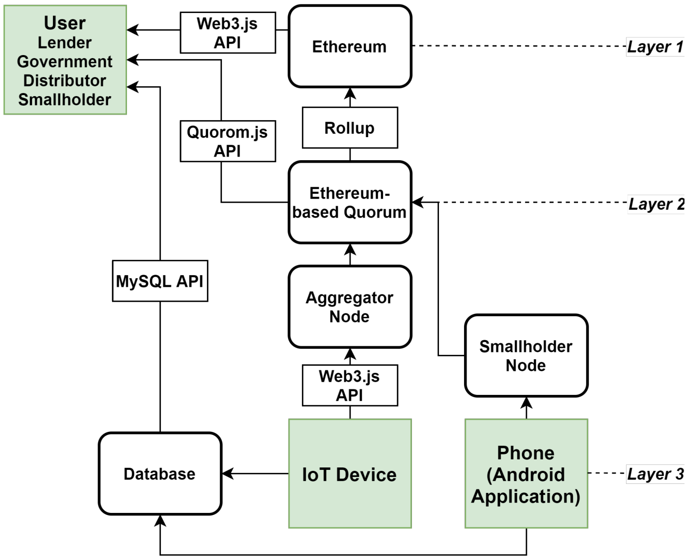

Figure 4: System Architecture

6 Implementation

Layer 2 is built on Quorum (version 2.7.0) with a modified version of the RAFT consensus mechanism [44]. It was initially built on three nodes in different data centers, where each node has 2GB of memory. In addition to fast handling and verification of transactions, this blockchain system must also support frequent on-chain data and contract status queries. Therefore, according to our evaluation results, the on-chain data must be stored in an SSD with at least 5000 read and write IOPS to handle more than 1,000 transactions and queries per second.

In the current situation, each node requires about 10 GB of disk space; it may also be stored in RAM when there is a backup power supply, but the cost is higher. Regarding the parameter settings of the blockchain, to avoid frequent retransmission of transactions between nodes, we set both global slots and global queue block numbers to 76798.

The need for a cheap and easy-to-manufacture device to monitor crops from a close range has arisen from a lack of availability of sensors suited for camera monitoring that have environmental resistance. Most smart farming IoT sensors do not employ the use of cameras. We create a new smart farming IoT device with a simple but robust design that may allow for crop monitoring using a mini-spherical camera: Hi3516CV300 with auto-zoom lens (3x optical zoom) *PTZ 355 degrees left and right, 90 degrees up and down. The camera is mounted to the top of a 1m x 1m x 1m transparent plastic box that crops can grow in.

Our IoT devices include (1) Wireless temperature and humidity sensing devices: measure temperatures ranging from -50C to 120C, and Humidity measurements ranging from 0 percent to 100 percent.; (2) 2.4GHz wireless sensing control device; (3) Weighing transducer: the force or mass is converted into a measurable electrical signal, and the detected weight data is uploaded to the cloud platform through the communication device; (4) Carbon monoxide temperature and humidity sensor (with routing function): Carbon dioxide sensing range: 400 10,000ppm; (5) The above-mentioned camera mount.

The number of transactions per month is shown in Fig. 5. In the case of high transaction volume in the future, it is necessary to adjust the data ratio of each layer of the LevelDB database and use batch parallel reading to increase the access efficiency of the SSD. In addition, to accelerate smart contracts, we also need to rewrite and compile Quorum to use evmos.

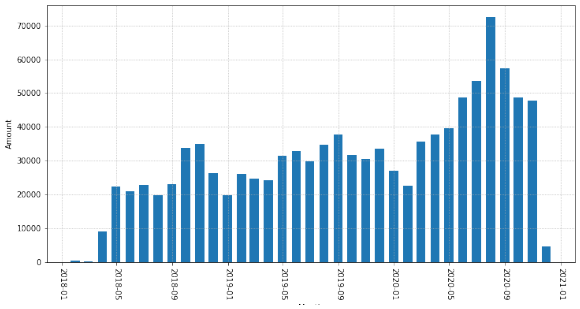

Figure 5: 2018/01 - 2020/12 Number of Transactions

7 Conclusion

In this paper, we propose secured MLAV for an IoT Blockchain architecture. We implement a high-efficiency and high-security agriculture 4.0 framework to allow for smallholders to join the agricultural supply chain blockchain. First, we create the Agricultural Supply Chain Finance operational structure and corresponding smart contracts which define the rules and stipulate the responsibilities and read and write permissions of the three types of nodes in the network (farmers, distribution channels, and financial institutions); second, we design an IoT blockchain system and an IoT camera sensor that allows for upstream producers' production activity data and historical order information to be uploaded to the blockchain. This data will provide guarantees to help them gain trust and qualify for loans from financial institutions; third, through aggregate verification technology, we successfully allow for multiple IoT devices to upload large amounts of data to the blockchain system in a short time. To guarantee security, smallholders can join the blockchain network with high efficiency, high transaction speed, and ID-based signature verification. Through the application of IoT Blockchain, the upstream producer's production activity data and historical order information may be provided to third party entities for evaluation. This ultimately provides a means by which they may gain trust and become eligible for loans from financial institutions.

7.1 Future Work

This paper provides a framework for securely and efficiently generating and storing data on a novel IoT blockchain system in an agricultural supply chain setting. Future work on this research may detail different application scenarios of our IoT blockchain framework in both agricultural and non-agricultural settings. The supply chain considerations, the corresponding smart contracts, and the Operation Procedure in Fig. 3 would need to be changed to fit the application scenario accordingly; however, the IoT blockchain infrastructure and batch verification algorithm may require little to no altering. In addition, future work could focus further on blockchain oracle implementations that allow for guided decisions based on automatic data analysis. An example application scenario in an agricultural setting could be in using our IoT sensor for monitoring of insects on crops. This may hold valuable implications in defining a crop's organic status because in many regions, in order to attain organic status, it must be ensured that insecticides were not used. The number of insects and the type of insects on crops may indicate whether insecticides were used, and therefore confirm the organic status of the crop.

Conflict of Interest The authors declare no conflict of interest.

Acknowledgment Ming-Fong Sie, Jingze Wu, and Seth Austin Harding contributed equally to this paper.

References

[1] J. Wu, M.-F. Sie, S. A. Harding, C.-L. Lin, S.-T. Wang, S.-w. Liao, "Multi-Layer Aggregate Verification for IoT Blockchain," in 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 43–44, IEEE, 2021, doi:10.1109/BRAINS52497.2021.9569817.

[2] Z. Zhai, J. F. Martínez, V. Beltran, N. L. Martínez, "Decision support systems for agriculture 4.0: Survey and challenges," Computers and Electronics in Agriculture, **170**, 105256, 2020, doi:10.1016/j.compag.2020.105256.

[3] V. Saiz-Rubio, F. Rovira-Más, "From smart farming towards agriculture 5.0: a review on crop data management," Agronomy, **10**(2), 207, 2020, doi:10.3390/agronomy10020207.

[4] M. De Clercq, A. Vats, A. Biel, "Agriculture 4.0: The future of farming technology," Proceedings of the World Government Summit, Dubai, UAE, 11–13, 2018.

[5] R. Kamath, "Food traceability on blockchain: Walmart's pork and mango pilots with IBM," The Journal of the British Blockchain Association, **1**(1), 3712, 2018.

[6] H. Haswell, M. Storgaard, "Maersk and IBM unveil first industry-wide cross-border supply chain solution on blockchain," IBM, http://www-03. ibm. com/press/us/en/pressrelease/51712. wss, 2017.

[7] J. Nurgazina, U. Pakdeetrakulwong, T. Moser, G. Reiner, "Distributed ledger technology applications in food supply chains: a review of challenges and future research directions," Sustainability, **13**(8), 4206, 2021, doi:10.3390/su13084206.

[8] A. Ellebrecht, "Chain of Custody and Transparency in Global Supply Chains," in Sustainable Global Value Chains, 227–237, Springer, 2019, doi:10.1007/978-3-319-14877-9_13.

[9] S. Nakamoto, A. Bitcoin, "A peer-to-peer electronic cash system," Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 2008.

[10] G. Wood, et al., "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, **151**(2014), 1–32, 2014.

[11] V. Buterin, "Ethereum: Platform Review," Opportunities and Challenges for Private and Consortium Blockchains, 2016.

[12] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, E. W. Felten, "Arbitrum: Scalable, private smart contracts," in 27th USENIX Security Symposium (USENIX Security 18), 1353–1370, 2018.

[13] N. Szabo, "Formalizing and securing relationships on public networks," First Monday, **2**(9), 1997.

[14] M. Alharby, A. Van Moorsel, "Blockchain-based smart contracts: A systematic mapping study," arXiv preprint arXiv:1710.06372, 2017.

[15] Y. Wang, J. H. Han, P. Beynon-Davies, "Understanding blockchain technology for future supply chains: a systematic literature review and research agenda," Supply Chain Management: An International Journal, 2019.

[16] S. Mansfield-Devine, "Beyond Bitcoin: using blockchain technology to provide assurance in the commercial world," Computer Fraud & Security, **2017**(5), 14–18, 2017, doi:10.1016/S1361-3723(17)30042-8.

[17] X. Lin, S.-C. Chang, T.-H. Chou, S.-C. Chen, A. Ruangkanjanases, “Consumers’ intention to adopt blockchain food traceability technology towards organic food products,” International Journal of Environmental Research and Public Health, **18**(3), 912, 2021, doi:10.3390/ijerph18030912.

[18] F. Casino, V. Kanakaris, T. K. Dasaklis, S. Moschuris, S. Stachtiaris, M. Pagoni, N. P. Rachaniotis, “Blockchain-based food supply chain traceability: a case study in the dairy sector,” International Journal of Production Research, **59**(19), 5758–5770, 2021, doi:10.1080/00207543.2020.1789238.

[19] J. Xu, S. Guo, D. Xie, Y. Yan, “Blockchain: A new safeguard for agri-foods,” Artificial Intelligence in Agriculture, **4**, 153–161, 2020, doi:10.1016/j.aiia.2020.08.002.

[20] A. Park, H. Li, “The effect of blockchain technology on supply chain sustainability performances,” Sustainability, **13**(4), 1726, 2021, doi:10.3390/su13041726.

[21] H. Chen, Z. Chen, Y. Cheng, X. Deng, W. Huang, J. Li, H. Ling, M. Zhang, “Poster: An Efficient Permissioned Blockchain with Provable Reputation Mechanism,” in 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS), 1134–1135, IEEE, 2021, doi:10.1109/ICDCS51616.2021.00123.

[22] Y. Guo, C. Liang, “Blockchain application and outlook in the banking industry,” Financial Innovation, **2**(1), 24, 2016, doi:10.1186/s40854-016-0034-9.

[23] R. Kumar, R. Tripathi, N. Marchang, G. Srivastava, T. R. Gadekallu, N. N. Xiong, “A secured distributed detection system based on IPFS and blockchain for industrial image and video data security,” Journal of Parallel and Distributed Computing, **152**, 128–143, 2021, doi:10.1016/j.jpdc.2021.02.022.

[24] A. S. Rajawat, R. Rawat, K. Barhanpurkar, R. N. Shaw, A. Ghosh, “Blockchain-based model for expanding IoT device data security,” in Advances in Applications of Data-Driven Computing, 61–71, Springer, 2021, doi:10.1007/978-981-33-6919-1_5.

[25] J. Lian, S. Wang, Y. Xie, “Tdrb: An efficient tamper-proof detection middleware for relational database based on blockchain technology,” IEEE Access, **9**, 66707–66722, 2021, doi:10.1109/ACCESS.2021.3076235.

[26] X. Fu, H. Wang, P. Shi, “A survey of Blockchain consensus algorithms: mechanism, design and applications,” Science China Information Sciences, **64**(2), 1–15, 2021, doi:10.1007/s11432-019-2790-1.

[27] M. Tripoli, J. Schmidhuber, “Emerging Opportunities for the Application of Blockchain in the Agri-food Industry,” FAO and ICTSD: Rome and Geneva. Licence: CC BY-NC-SA, **3**, 2018.

[28] N. Kshetri, “Can blockchain strengthen the internet of things?” IT professional, **19**(4), 68–72, 2017, doi:10.1109/MITP.2017.3051335.

[29] A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), 618–623, IEEE, 2017, doi:10.1109/PERCOMW.2017.7917634.

[30] S. Varshney, P. Vats, S. Choudhary, D. Singh, “A Blockchain-based Framework for IoT based Secure Identity Management,” in 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), volume 2, 227–234, IEEE, 2022, doi:10.1109/ICIPTM54933.2022.9753887.

[31] K. Hakuta, Y. Katoh, H. Sato, T. Takagi, “Batch verification suitable for efficiently verifying a limited number of signatures,” in International Conference on Information Security and Cryptology, 425–440, Springer, 2012, doi:10.1007/978-3-642-37682-5_30.

[32] J.-W. Hu, L.-Y. Yeh, S.-W. Liao, C.-S. Yang, “Autonomous and malware-proof blockchain-based firmware update platform with efficient batch verification for Internet of Things devices,” Computers & Security, **86**, 238–252, 2019, doi:10.1016/j.cose.2019.06.008.

[33] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, B. Ford, “Enhancing bitcoin security and performance with strong consistency via collective signing,” in 25th {usenix} security symposium ({usenix} security 16), 279–296, 2016.

[34] J. Polge, J. Robert, Y. Le Traon, “Permissioned blockchain frameworks in the industry: A comparison,” Ict Express, **7**(2), 229–233, 2021, doi:10.1016/j.icte.2020.09.002.

[35] A. Shwetha, C. Prabodh, “A Comprehensive Review of Blockchain Based Solutions in Food Supply Chain Management,” in 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), 519–525, IEEE, 2021, doi:10.1109/ICCMC51019.2021.9418305.

[36] Q. Song, Y. Chen, Y. Zhong, K. Lan, S. Fong, R. Tang, “A supply-chain system framework based on internet of things using blockchain technology,” ACM Transactions on Internet Technology (TOIT), **21**(1), 1–24, 2021, doi:10.1145/3409798.

[37] J. Liu, H. Zhang, L. Zhen, “Blockchain technology in maritime supply chains: applications, architecture and challenges,” International Journal of Production Research, 1–17, 2021, doi:10.1080/00207543.2021.1930239.

[38] J. Tholen, D. de Vries, A. Daluz, C.-C. Antonovici, W. V. Brug, R. Abelson, D. Lovell, “Is there a role for blockchain in responsible supply chains?” in OECD Global Blockchain Policy Forum, 2019.

[39] J. Kurose, K. Ross, “Computer Networking: A Top Down Approach, 2012,” .

[40] D. Hankerson, A. J. Menezes, S. Vanstone, Guide to elliptic curve cryptography, Springer Science & Business Media, 2006.

[41] B. Lee, J.-H. Lee, “Blockchain-based secure firmware update for embedded devices in an Internet of Things environment,” The Journal of Supercomputing, **73**(3), 1152–1167, 2017, doi:10.1007/s11227-016-1870-0.

[42] E. Barker, A. Roginsky, et al., “Transitions: Recommendation for transitioning the use of cryptographic algorithms and key lengths,” NIST Special Publication, **800**, 131A, 2011.

[43] N.-W. Lo, J.-L. Tsai, “An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings,” IEEE Transactions on Intelligent Transportation Systems, **17**(5), 1319–1328, 2015, doi:10.1109/TITS.2015.2502322.

[44] D. Ongaro, J. Ousterhout, “In search of an understandable consensus algorithm,” in 2014 USENIX Annual Technical Conference (Usenix ATC 14), 305–319, 2014.