Janus: Toward Preventing Counterfeits in Supply Chains Utilizing a Multi-Quorum Blockchain

Vika Crossland[1]*, Connor Dellwo[2]*, Golam Bashar[3], and Gaby G. Dagher[3]
[1] Computer Science, Central Washington University, United States
[2] Computer Science, Washington State University, United States
[3] Computer Science, Boise State University, United States

March 2023

Abstract

The modern pharmaceutical supply chain lacks transparency and traceability, resulting in alarming rates of counterfeit products entering the market. These illegitimate products cause harm to end users and wreak havoc on the supply chain itself, costing billions of dollars in profit loss. In this paper, in response to the Drug Supply Chain Security Act (DSCSA), we introduce Janus, a novel pharmaceutical track-and-trace system that utilizes blockchain and cloning-resistant hologram tags to prevent counterfeits from entering the pharmaceutical supply chain. We designed a multi-quorum consensus protocol that achieves load balancing across the network. We perform a security analysis to show robustness against various threats and attacks. The implementation of Janus proves that the system is fair, scalable, and resilient.

Keywords— Blockchain Pharmaceutical Supply Chain Consensus Protocol

1 Introduction

A supply chain is a network of linked stakeholders that process a product and pass it either up or down the chain [17]. In the pharmaceutical industry, prescription drugs are manufactured and ultimately passed down to an end user, typically a hospital or a patient. Major stakeholders in the pharmaceutical supply chain include suppliers, manufacturers, warehouses, distributors, pharmacies, and end users.

In 2020, the Institute for Supply Management (ISM) conducted research to survey global supply chains on the impact of COVID-19. By the end of March 2020, 95% of organizations in the survey reported that they had already experienced disruptions as

*These authors contributed equally.

a result of the pandemic, or were expecting to Ref. [1]. This shows how modern supply chains have been weakened. More specifically, the current pharmaceutical supply chain (PSC) is suffering from a lack of traceability, security, and transparency. These faults ultimately contribute to the presence of illegitimate products in the market. An illegitimate product can be any of the following: (1) a counterfeit product, (2) an adulterated product, (3) a product that is part of a fraudulent transaction, or (4) a product otherwise deemed a hazard to users that is not fit to be dispensed [9]. Illegitimacy in the market in the form of counterfeits is arguably one of the most impactful issues that the PSC is facing. The World Health Organization (WHO) estimates that the presence of counterfeit products in the pharmaceutical market can range anywhere from less than 1% in developed countries to over 10% in some developing countries [21]. These illegitimate products affect stakeholders throughout the chain. The industry suffers a net loss from production due to these unofficial drugs entering the market. More urgently, counterfeit products can end up seriously harming or causing death to end users.

Beginning in November 2023, the Food and Drug Administration (FDA) will require PSC stakeholders (except for end users) to comply with more stringent guidelines regarding the traceability of pharmaceuticals, which were recently established by the Drug Supply Chain Security Act (DSCSA) [10]. The goal of the DSCSA, which takes effect in the United States, is to create an electronic track-and-trace system for products in the PSC. In 2023, when the legislation is in full effect, stakeholders will be required to transmit all supply chain communications electronically and track their products at the individual package level [9]. Having an electronic system to track individual products throughout the PSC can significantly reduce the number of counterfeits in the market. The emerging applications of blockchain technology could be utilized to form an electronic, immutable, and decentralized system that provides traceability, security, and transparency through blockchain's inherent nature.

While blockchain can be used to form this immutable electronic system, the challenge of verification of physical products with digital data arises. It also poses the challenge of ensuring end-to-end visibility. Current stakeholders in the PSC typically have their own local databases that store supply chain data which others in the PSC cannot access. By eliminating blind spots in the current system, end-to-end visibility can increase stakeholders' trust in the system and can also lead to any errors in the chain getting caught earlier on. Furthermore, blockchain systems maintain a ledger to provide sufficient tracking information that all involved stakeholders can access, resulting in better coordination between the parties.

Researchers have already proposed blockchain-based solutions to modernize the PSC [2][7]. Alzahrani and Bulusu [2] designed a system in which blocks are proposed when stakeholders in the chain initiate actions within the PSC (e.g., a warehouse sending out a shipment). For a block to be approved and added to its blockchain, a lead validator node must randomly select mining nodes from the network to validate it. Each package in the chain should have a near-field communication (NFC) tag, which holds product details, a read-counter, and a tag ID. Tags are read by receiving parties (e.g., a warehouse getting a shipment from a manufacturer) and checked to ensure that the product data and number of reads on the tag are correct. While NFC tags may be a beneficial aspect to connect the physical data of the PSC to its virtual blockchain, it is worth mentioning the security risks that they may pose. For example, NFC tags require a relatively close scanning distance, but they can still be easily scanned by almost anyone, and the data stored on them can be read and potentially stolen. Furthermore, data on NFC tags can be overwritten. This could pose great

threats to the PSC. Dwivedi et al. [7] also proposed the use of lead validator and regular validator nodes. However, in their system, the lead validator is responsible for the validation of transactions as well as the proposal of a block. Having a single leader in this position (that is solely responsible for transaction validation) is a step towards centralization and requires more trust to rely on that node fully.

Problem Statement. Given a set of stakeholders in the PSC, the objective of this paper is to design a trustless and scalable system for the PSC that: (1) achieves end-to-end visibility to prevent counterfeit drugs from entering the market and efficiently identify issues in the PSC process, (2) employs a decentralized decision-making protocol which eliminates the need for the stakeholders to trust each other while increasing their trust in the process, and (3) uses a quorum-based consensus protocol to ensure scalability.

Our system, called Janus [1], utilizes a cloning-resistant hologram tagging system that helps stakeholders trace products through the chain to confirm authenticity. It exploits the immutable nature of blockchain to increase transparency, security, and traceability while being fair, random, and scalable. While Janus could be applied in other fields, we have targeted it at the pharmaceutical industry because of these traits, as well as the fact that it complies with the DSCSA, which will be fully enforced in November 2023 [10]. Our design ensures a tight link between the sequential steps in the physical supply chain process and the virtual blockchain, which is beneficial to complex markets such as the PSC. While our system can be applied to different types of supply chains with the same purpose of preventing counterfeits, we focus on the pharmaceutical supply chain as an example to showcase the protocol.

1.1 Contributions

Our contributions in this paper are as follows:

1. We propose a novel blockchain-based pharmaceutical track-and-trace system, named Janus, that prevents counterfeits from entering the PSC and ensures secure delivery between stakeholders.
2. Our design prevents any stakeholder in the system from introducing counterfeit products into the pharmaceutical market. We achieve this by utilizing nested hologram tags that identify where individual items are in the chain, providing end-to-end transparency of products in the system.
3. To maintain the security of the system, we introduce an equitable multi-quorum consensus protocol that achieves load-balancing among stakeholders of different types while maintaining fairness among stakeholders of the same type.
4. We implemented our system, including the multi-quorum consensus protocol. The results showed that Janus is fair among stakeholders concerning mining contribution, and it is scalable with respect to a linear increase of nodes and transactions in the network.

[1] We decided to name our system after the Roman myth of Janus: God of beginnings and ends [28]. Janus was portrayed as having two faces: one facing forward and one facing back. We believe this to be an appropriate link to our research, as blockchain is an immutable ledger that allows users to build forward but also look back at previous blocks/transactions. Janus utilizes this backtracking ability to provide a means of tracing a product back to a stakeholder. This aids in determining the authenticity of a product.

1.2 Limitations

While end users, such as patients, are certainly stakeholders in the PSC, our model does not include them in the network. The network is designed to be private-permissioned, meaning only authorized nodes can join and view the blockchain and network activity. This means that end users would not have the ability to personally track their product's origin, limiting transparency at the patient level. Instead, our system relies on complete trust between the end user and their pharmacy.

While Janus prevents stakeholders from acting dishonestly and claiming they never received a shipment when they actually did, there is always the potential for honest mistakes, such as losing packages in delivery. This is a limitation of Janus, as it does not have steps in place to detect or resolve these types of errors.

2 Related Work

Many researchers have been studying numerous applications of blockchain since Satoshi Nakamoto introduced the first implementation of blockchain in his famous Bitcoin white paper [19]. Due to its immutable nature, the technology has proved promising for different industries, including supply chains. In addition, it can be exploited to benefit systems in a number of ways, such as boosting transparency between stakeholders, building a decentralized system, and creating a traceable ledger.

To conduct our research, we followed the snowballing method. We first searched for closely-related works (blockchain in PSC), and discovered additional references based on the related works and citations of those papers. The same approach was followed to find moderately-related and loosely-related works. In Table 1, we compare our proposed system to some of these closely-related works.

2.1 Blockchain in Pharmaceutical Supply Chain

Researchers have been working on developing ways to use blockchain to improve the PSC [2][7][11][26]. Dwivedi et al. [7] described how blockchain can be implemented in the traditional PSC system to share information securely. Their proposed design used both local and global blockchains for storing transactions between stakeholders in the network. Local blockchains store transactions between stakeholders of the same type, while global blockchains store transactions between the different types of stakeholders. In order to establish consensus, transactions are generated and sent to a validation leader to be checked. If the transaction is accepted as valid, the validation leader proposes a new block for the remaining validators to vote on. Alzahrani and Bulusu [2] also utilized a validation leader. However, instead of having both global and local blockchains, they proposed creating a blockchain for each individual product. Products are tracked and traced on the blockchain via NFC tags. Both systems outlined in Refs. [2][7] came short of achieving true decentralization. Due to the single-leader-based consensus protocol, their system is vulnerable, as a malicious leader can decide the conclusive order of transactions [14]. Additionally, a single leader can act as a single point of truth and thus a single point of failure. While both Refs. [2][7] came short in their virtual processes, it is important to note that issues in the pharmaceutical blockchain can occur in the physical aspect as well. To date, the blockchain community has not reached a consensus on which method of labeling products should be preferred to connect the physical product with the digital data on the blockchain. The architectures designed in Refs. [11][26] utilized quick response (QR) codes as the

medium to protect counterfeit products from entering the supply chain. In addition to counterfeit prevention, the QR codes in Ref. [26] were used to track temperature control throughout the PSC, further acknowledging the importance of using blockchain in pharmaceutical tracking.

2.2 Blockchain in Non-Pharmaceutical Supply Chains

Recently, non-pharmaceutical fields have also started to focus on blockchain as a potential improvement to their supply chain systems. Food and agriculture safety is one sector that is gaining attention in commercial and academic projects. As of now, most of the solutions are centralized and not free from fraud and tampering. Hence, research has begun to propose different blockchain-based traceability schemes in agri-food supply chain systems.

Non-pharmaceutical supply chains utilize quick response (QR) codes [6] and radio frequency identification (RFID) tags [18][25] to track products in the food supply chain. According to Refs. [12][29], these tags are vulnerable to various attacks, especially cloning and modification attacks. Additionally, RFID tags are vulnerable to privacy attacks as shown by Ref. [8]. Depending on the frequency band used, these tags can be read from distances ranging from 1 m to 100 m [29]. RFID tags and QR codes are cost-efficient but utilize simple technology that can be compromised in a matter of seconds. This can pose a huge threat to large supply chain systems including the PSC, as it can aid malicious parties in introducing counterfeit products into the chain.

Kamilaris et al. [13] reviewed some of the proposals in existence that use blockchain in the agri-food sector. Their research concluded that the technology is a valid approach to creating a more transparent food supply chain due to blockchain security and reliability. In Ref. [24], a system utilizing the Interplanetary File Storage System (IPFS) to store transactional data from the agri-food supply chain while storing the hashes of that data in the Ethereum blockchain is proposed. Only authorized users are allowed to participate in the network, which implements a reputation-based system in order to establish additional trust between participants. Their architecture suffers from some shortcomings. Currently, the system lacks a means for returning items or providing refunds. Also, the reputation system has no protection in place to prevent fake or biased reviews.

2.3 Blockchain in the Pharmaceutical Industry

Blockchain can benefit the pharmaceutical industry as it offers three important features: privacy, transparency, and traceability. Therefore, many researchers have already designed various blockchain frameworks to utilize these properties. Schöner et al. [23] proposed the use of blockchain to keep a transparent ledger of activity for the pharmaceutical research and development process. Transparency on the chain would allow investors access to all previous stages of the research process. Similarly, Leal et al. [15] designed a system in which pharmaceutical products were tracked throughout the manufacturing stage. This can aid in the detection and tracking of counterfeit products from pharmaceutical manufacturers.

Table 1: Comparative evaluation of main features in closely-related works

Approach	Consensus		Fairness		Secure Against Malicious Leader(s)
	Single Leader	Multi-Leader	Local	Global	
Alzahrani & Bulusu [2]	✓	✗	✗	✓	✓
Dwivedi et al. [7]	✓	✗	✓	✓	✗
Mondal et al. [18]	✓	✗	✗	✓	✓
Sidorov et al. [25]	✓	✗	✗	✗	✗
Our Protocol: Janus	✗	✓	✓	✓	✓

3 Preliminaries

3.1 Holographic Encryption

In the anti-counterfeiting PSC, there exist two types of package authentication: physical and digital. Physical package authentication can be accomplished via holography. Modern holograms present advantageous track-and-trace features that can help generate unique IDs in the form of encrypted serial numbers. The unique ID can be linked to packaging via a unique code, allowing the verifier to explore the record of an individual product and identify when and to whom that item was shipped. The ID can then be tied to another ID (e.g., pallet ID or container ID). This linking creates a parent-child relationship between the individual package and any containers or pallets in which the item is placed. This system allows the package to be tracked throughout the numerous layers of the PSC, from the manufacturer through distribution to the pharmacy.

Tsang [27] presented single-random-phase holographic encryption. The proposed method is motivated by the double-random-phase encryption technique. Basically, the work simplifies the architectures of the encryption and the decryption techniques by adopting a single-random-phase mask as the encryption key. The encryption method is divided into three stages. First, the input image needs to be encrypted and pasted onto a random position in a larger global image. The remaining areas of this image are then filled with unsystematically generated content. As such, the generated image as a whole is significantly distinct from the source image, while the visual quality of the source image is preserved. Second, a digital Fresnel hologram is developed from the latest image and transformed into a phase-only hologram based on bi-directional error diffusion. In the last stage, a static random phase mask is counted to the phase-only hologram as the private encryption key. In the decryption process, the transnational image together with the original image it contained can be rebuilt from the phase-only hologram, but only if it is overlaid with the correct decryption key. Here, the input image is altered in a random fashion and transformed into a phase-only hologram. Random phase noise is further associated with a phase-only hologram as the encryption key. As the converted image is unrecognized even to the actor who encrypts the image, it is hard to deduce the relationship between the source image and the hologram through various forms of plain text attacks.

By utilizing holographic encryption on the physical products in the PSC and linking its data to the blockchain, we can provide a digital traceability scheme for tracking from source to end consumers. This type of tagging system is resistant to various at-

tacks including cloning and modification attacks, making it a secure choice for the PSC [16]. Peng et al. [22] introduced a process for encrypting holographic information utilizing the expanded Diffie-Hellman (EDH) algorithm. By utilizing this structure of holographic encryption on physical products and storing the hashes in the blockchain, Janus can provide a digital traceability scheme for tracking from source to end consumers.

3.2 Blockchain Network Types

To ensure a safe and trusted blockchain network, there are varying levels of privacy that can be applied to the network. Commonly-used privacy levels are public, public-permissioned, and private. In a public blockchain network, transaction visibility is public and open to anyone. The most well-known implementation of a public blockchain is the Bitcoin ledger [19]. We define public-permissioned blockchains to be where the ledger is available to view by anyone, but participation requires authorization. On the contrary, private blockchains preserve the most amount of privacy as they cannot be viewed or contributed to without proper credentials. Private blockchains are more applicable for sensitive systems such as health care or banking, where patient and customer data are valuable and confidential [3].

3.3 Drug Supply Chain Security Act (DSCSA)

In 2013, Congress enacted the Drug Quality and Security Act, which introduced the Drug Supply Chain Security Act (DSCSA). Its goal is to negate illegitimate products from the PSC [10]. Stakeholders in the chain must follow guidelines that will increase the security of the system. These guidelines include electronic submission of transactions, annual proof of licensure of warehouses and third-party logistics providers, and specific labeling rules [10]. In November 2023, the DSCSA will be in full effect and stakeholders will be required to comply with its rules and regulations. In compliance with the DSCSA, our system includes package-level labeling that allows for a more strict track-and-trace system. Blockchain would be an ideal solution for the PSC to seamlessly follow DSCSA guidelines as it creates an immutable ledger of electronically submitted transactions, further providing a secure track-and-trace system.

4 Solution Overview

Janus provides a decentralized way to authenticate products in the PSC while preventing counterfeits from entering the market. To connect the physical aspects of the supply chain to the virtual data of the blockchain, Janus utilizes hologram tags that hold critical information about the package that the tag occupies. This information can be used down the supply chain to identify a product and verify its legitimacy. After a physical inspection, the receiver is responsible for generating a transaction that notifies the network that the shipment has arrived. All transactions in the network are assigned to their appropriate quorums, as explained in Section 5.3. These quorums are responsible for validating transactions and adding them to a proposed block. Once transactions have been validated, a separate quorum votes on the validity of the proposed block, thus determining whether or not the block should be added to the blockchain.

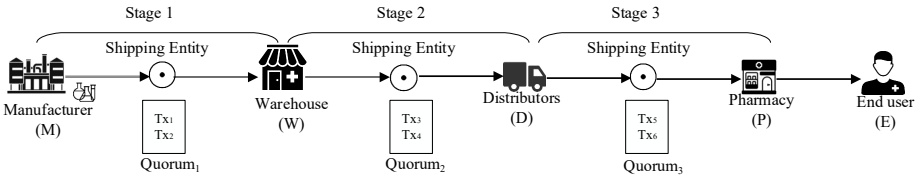

Figure 1: High-level overview of the system flow in which products move from stage to stage until they reach the end user.

Our system uses a membership service authority (MSA) to ensure the integrity of the members in the network. The MSA is not a single entity in our design, thus not a single point of trust. We suggest that the MSA instead consist of all members in the network. The MSA certifies a potential network node's public key by creating a transaction that active members in the network can verify. Once the new entity is approved and has an eligible key, it can contribute to the network as an authorized member.

Table 2 contains key notations that will be used throughout the paper.

Symbol	Definition
PSC	Pharmaceutical Supply Chain
M	Manufacturer
W	Warehouse
D	Distributor
P	Pharmacy
E	Shipping Entity
TID	Tag ID
PID	Product ID
S	Source Stakeholder
F	Destination Stakeholder
T_x	Transaction
t_1	Outermost Hologram Tag
p	Package
T'_x	Set of Proposed Transactions
$\mathcal{Q}$	Quorum
q	Number of Nodes
B_Q	Block Quorum

Table 2: Table of notations.

5 Proposed Solution: Janus Protocol

Our proposed architecture establishes a trading and transmission mechanism to allow secure exchange between authorized entities in the PSC. The proposed model reflects a layered architecture that is categorized into two layers: physical and virtual.

The physical layer manages the cooperation between entities for physical products. These communications include the exchange of goods along with proof of an auditable delivery (i.e., signed transactions). To track and trace the products, each package has a hologram tag. Tags are generated and placed by manufacturers on each product. Once a product is created and ready to ship out, a tag is generated, holding the following information: tag ID (TID), product ID (PID), the product's National Drug Code (NDC), serial number, lot number, expiration date, and a list of descendent tags nested inside the tagged container. By having the descendant tag information in the parent tag, stakeholders can see which packages to expect inside a shipment. This nested system also allows stakeholders at any step in the chain to trace their product back to an authorized manufacturer, proving authenticity.

When a delivery arrives at its destination, the first phase is for the receiver to do a physical check on the shipment: (1) check the box for any obvious physical tampering, (2) check that the hologram tag has not been tampered with (i.e., the tag has been reapplied or ripped, indicating that the box has been opened or tampered with), and (3) scan the tag to ensure that the contents of its shipment are correct (check previous transaction's details, specifically PID and TID).

After receiving a shipment, the destination stakeholder initiates a transaction signifying that the shipment has been received. Transactions are aspects of the virtual layer, providing the essential connection between the physical data of the PSC and the virtual data on the blockchain.

Algorithm 1 provides a step-by-step procedure of the processes that occur during each stage in the supply chain. In Fig. 1, there are three primary stages: one from Manufacturer (M) to Warehouse (W), one from W to Distributor (D), and one from D to Pharmacy (P). In steps 1-9, the source stakeholder S fulfills an order made by the destination stakeholder $\mathcal{D}$. If S is a manufacturer, they are responsible for creating and placing all hologram tags that belong in the shipment and generating a transaction verifying that the order has been fulfilled. Otherwise, S just creates the transaction. Either way, the transaction gets broadcast to the whole network $\mathcal{N}$ for its appropriate quorum to validate. If the transaction is valid, it is added to a proposed block. Otherwise, it is rejected. In steps 10-15, S hands off the shipment to shipping entity E for delivery to $\mathcal{D}$. A copy of the first transaction made in step 4 is created and signed by E, signifying the successful pickup of the delivery. This signed transaction is broadcast to $\mathcal{N}$ and its appropriate quorum validates it. Just as in steps 8-9, it is added to a proposed block if deemed valid and simply rejected if determined invalid. In steps 16-27, E makes the delivery to $\mathcal{D}$ and $\mathcal{D}$ must perform a physical check to ensure that there has been no obvious tampering. If the inspection passes, $\mathcal{D}$ scans the hologram tag on the shipment, crosschecks the data, and generates a signed transaction $\sigma_{T_x,\mathcal{D}}$ notifying that the shipment has been received successfully by $\mathcal{D}$. This transaction is validated by its appropriate quorum and added to a proposed block if valid.

5.1 Transactions

The blockchain will be made up of different types of transactions, primarily:

— **Source Transactions.** A transaction T_x is a source transaction if it is generated and signed by a source stakeholder S in a stage ($\sigma_{T_x,S}$). □

— **Shipping Transactions.** A transaction T_x is a shipping transaction signifying that a shipment has been sent out if it is a source transaction signed by a shipping entity E in a stage ($\sigma_{T_x,E}$). □

Algorithm 1 Source-to-Destination Stage Delivery Process

Input: source stakeholder S, destination stakeholder $\mathcal{D}$, shipping entity E, transaction T_x, outermost hologram tag t_1, and the physical shipment/package itself p.
Output: $\sigma_{T_x,\mathcal{D}}$.

$\mathcal{D}$ places order to S for product
if S is a manufacturer:
    S generates t for each product and package in the order:
    $t \leftarrow$ {tag ID, product ID, national drug code, serial number, lot number, expiration date, metadata}
S generates signed transaction $\sigma_{T_x,S} = Sig_s(T_x)$ indicating that the order from $\mathcal{D}$ has been fulfilled
$T_x \leftarrow$ {source ID, destination ID, product data, data of t_1}
$\sigma_{T_x,S}$ is broadcast to $\mathcal{N}$
Quorum validates $\sigma_{T_x,S}$
if $\sigma_{T_x,S}$ is valid:
    $\sigma_{T_x,S}$ is added to proposed block and S proceeds to Step 10
S gives shipment to E for delivery to $\mathcal{D}$
E generates signed transaction $\sigma_{T_x,E} = Sig_E(\sigma_{T_x,S})$ to notify that p is in the delivery stage to $\mathcal{D}$
$\sigma_{T_x,E}$ is broadcast to $\mathcal{N}$
Quorum validates $\sigma_{T_x,E}$
if $\sigma_{T_x,E}$ is valid:
    $\sigma_{T_x,E}$ is added to proposed block and E proceeds to Step 16
E arrives at the facility of $\mathcal{D}$ with p
$\mathcal{D}$ must perform a physical check to ensure that p has not been obviously tampered with
if p is noticeably tampered with:
    break
else:
    $\mathcal{D}$ continues to Step 22
$\mathcal{D}$ scans t_1 and generates signed transaction $\sigma_{T_x,\mathcal{D}} = Sig_{\mathcal{D}}(\sigma_{T_x,E})$ signifying that p has been received by $\mathcal{D}$
return $\sigma_{T_x,\mathcal{D}}$ to $\mathcal{N}$
Quorum validates $\sigma_{T_x,\mathcal{D}}$
if $\sigma_{T_x,\mathcal{D}}$ is valid:
    $\sigma_{T_x,\mathcal{D}}$ is added to block and $\mathcal{D}$ proceeds to Step 33
Repeat Step 1 through Step 27 until product has reached the pharmacy level

— **Destination Transactions.** A transaction T_x is a destination transaction signifying that a delivery has been made to its destination if it is a shipping transaction signed by a destination stakeholder $\mathcal{D}$ in a stage ($\sigma_{T_x,\mathcal{D}}$). □

All transactions consist of the source (S), destination ($\mathcal{D}$), tag information of the outer tag (T_{i}), and the signature of the stakeholder initiating the transaction. If a transaction is generated but has no destination, the responsibility of validation will fall on the quorum of the highest order. For example, if W generates a transaction that is not about a product shipping out and therefore has no destination, validation will be done by Quorum 3, as defined in Section 5.3.

A transaction or proposed block must receive 2/3 valid votes from its quorum to be deemed valid.

5.2 Validation

Validation differs between transactions and blocks. To verify transactions generated as a product enters the chain, responsible quorums must check that S and $\mathcal{D}$ are both authorized addresses in the system, as well as check that the signature on the transaction comes from an authorized entity in the network. To verify transactions indicating that E is transporting a delivery, the S and $\mathcal{D}$ must match those on the previous transaction, and the signature of E must be an authorized member of the network. For transactions indicating an order has been delivered to its destination, quorums must check that the new signature matches the destination of the original transaction and belongs to an authorized entity on the network. Members must also crosscheck the *TID* and the *PID* with the original transaction/order to ensure that the data match.

Blocks are validated differently than transactions. Block quorum B_Q is responsible for computing the hash of the previous block in the chain and comparing it to the hash in the proposed block's header. If the hashes match and all quorum member signatures in the signature section are from authorized nodes, the block is considered valid.

5.3 Quorums

Our system takes advantage of the use of multiple quorums in order to achieve fairness, randomness, and scalability. In our system, there should be *N-1* quorum types, where N represents the number of stakeholder types in the network. Since we consider M, W, D, P, and E as primary stakeholders contributing to the network, four types of quorums would be formed. In reference to this model, we consider the following quorums:

Quorum 1: a quorum that consists of M, W, and E nodes

Quorum 2: a quorum that consists of W, D, and E nodes

Quorum 3: a quorum that consists of D, P, and E nodes

Quorum 4: a special block quorum B_Q that can consist of any stakeholder type in the network

Quorums are assigned to mine on their respective transactions. For example, Quorum 1 described above would be assigned to mine transactions that take place between M, W, and E. By having stakeholders mine on transactions of their own type, our system achieves local and global fairness. We define local fairness as the fairness among stakeholders of the same type and global fairness as the fairness across the network amongst stakeholders of different types. For further explanation and implementation of local and global fairness, see Section 7.2.

As mentioned earlier, Quorum 4 is unique, as it can consist of any stakeholder type in the network. This quorum, unlike others that validate transactions, is responsible solely for block validation.

All quorum members are selected randomly via our random-selection algorithm, which utilizes the hash of the previous block. This algorithm ensures local fairness between stakeholders in the same quorum pools. Entities that generate transactions will be responsible for running the random-selection algorithm. Because the algorithm relies on the hash of the previous block, all quorum members calculated will be the same even if multiple entities run it simultaneously.

Quorum member selection is outlined in Algorithm 2. To create a quorum $\mathcal{Q}$, we first take the hash of the previous block. Our random-selection algorithm is performed using the number of nodes in the network n, the list of eligible miners in each quorum selection pool $\mathcal{G}$ where $\mathcal{G} = [g_1, g_2, ..., g_k]$, and the block header of the previous block in the chain $\mathcal{H}_r$. The algorithm randomly selects $\ln(\mathcal{G})$ nodes to join a quorum. A quorum must consist of two or more members. Single-member quorums are not permitted.

Algorithm 2 Quorum Members Selection

Input: list of eligible miners $\mathcal{G}$, number of nodes in the network n, seed s_1, and block header $\mathcal{H}_r$ of the previous block

1: $\mathcal{Q} \leftarrow \{\}$
2: $s_1 \leftarrow h(\mathcal{H}_r)$
3: $\mathcal{Q} \leftarrow$ `randomSelect(`n`, `$\mathcal{G}$`, `s_1`)`
4: return $\mathcal{Q}$

5.4 Block Architecture and Validation

Each block in the chain will consist of a header, a body, and a signature section. The block's header will contain the hash of the previous block as well as the timestamp of the current block's creation. The body will hold all of the valid transactions of the current block. Below the body, the signature section will hold the signatures of the quorum members who validated the transactions.

Block quorum B_Q must check that the block has proper structure, as well as compute the hash of the previous block and use it to run the selection algorithm. They can then check to ensure that all quorum members responsible for validating the transactions in the proposed block are authorized and participating honestly. In order for a block to be added to the blockchain, a minimum of 2/3 valid votes are required from B_Q.

6 Consensus Protocol

Blockchain requires a consensus protocol — a technique for establishing a single version of the records of transactions approved by the majority of participants. As our proposed design relies on a permissioned blockchain where all nodes are known, a malicious participant would be discovered if it exercised to alter the chain in an unacceptable way. Therefore, public consensus protocols such as Proof of Work (PoW) [19], Proof of Stake (PoS) [4], and Delegated Proof of Stake (DPoS) [30] are not perfect solutions. Some popular consensus protocols for private blockchain systems are Practical Byzantine Fault Tolerance (PBFT), Tendermint, and Hyperledger Fabric.

Many researchers and blockchain developers have started to focus on creating fair, scalable, and efficient consensus protocols that fit different use cases. For example, Alzahrani and Bulusu [2] designed a protocol based on Tendermint to be used in the PSC. It relies on random-selection for validator nodes, promoting fairness and some degree of decentralization. While their protocol does have lead-validator nodes, they are responsible only for randomly-selecting $\log(n)$ validator nodes and broadcasting proposed blocks. Validators must go through two rounds of voting to reach consensus: prevoting and precommitting. At each round, responses from 2/3 of the $\log(n)$ validators must be received. After the pre-committing round, responses are counted, and the final decision to reject or append the block to the blockchain is made.

In Ref. [7], a lead validator node was also proposed in the consensus protocol. However, in their design, the leader was responsible for proposing blocks as well as broadcasting them to the regular validators. These validators then check the validity of the block proposed by their leader, responding with a 0 to signify an invalid vote or a 1 to signify a valid vote. Whichever response receives more than half the votes determines if a block is added or rejected. Thus, for a lead validator to push a block to the chain, it must receive over 50% valid votes.

Our proposed consensus protocol relies on votes from authorized quorum members and does not use leader nodes. Instead, different quorums for each transaction type as well as a quorum designated for block validation vote to reach consensus on decisions regarding the blockchain. This provides a decentralized and trustless system.

6.1 Reaching Consensus

To reach consensus, our design requires all members of a quorum to place a vote of valid or invalid. The final decision is based on all responses received. A minimum of 2/3 valid votes are required for approval of any decision regarding the blockchain. For quorums consisting of two members, both members must reach consensus. If they cannot agree, the transaction will be thrown out.

Algorithm 3 gives a step-by-step overview of how blocks are created and validated. In steps 1-3, quorum members view and share transactions that appear in their mempools. Quorum member Q_i requests the transactions from all other members' mempools, with all other members being Q_j. By requesting each other's transactions, they can ensure everyone has the same view. In steps 4-5, quorum members create a draft block including all valid transactions from mempools of all members. Transactions missing in the draft block are also then requested from others, as per steps 6-7. Once all transactions have been received, Q_i follows steps 8-10 builds a fully drafted block, and hashes it to create a signed hash of the drafted block. It is then broadcast to the quorum and requests the signed hashes of drafted blocks created by the remaining members in the network to complete steps 11-12. If the 2/3 threshold is met approving the hash of the draft block, members append their signatures and forward it to the block quorum responsible for validation. If this block then achieves at least 2/3 of signatures from the block quorum, it is added to the main chain as per step 19.

7 Experimental Evaluation

The following subsections describe and observe the results of the experiments we performed to test the fairness and scalability of our system, as well as the likelihood of

Algorithm 3 Building and Mining a Block $\mathcal{B}_n$

Input: A set of transactions T'_x with authorized signatures that have not yet been added to the chain, a quorum $\mathcal{Q}$ of q nodes, and a threshold of δ where δ is 2/3, and a time limit t_{limit}.
Output: If successful, a valid block is generated. Otherwise, it will return null.

Initialization. Members of $\mathcal{Q}$ take all headers of transactions TH that exist in their mempool.
`broadcast`$(Q_i, \mathcal{Q}, \mathcal{TH}_i)$
`request`$(Q_i, \mathcal{Q}, \mathcal{TH}_j)$
Q_i verifies $\mathcal{TH}_j$. If any Q_j produces a falsified $\mathcal{TH}_j$, that transaction is rejected.
Q_i creates a draft block $\mathcal{DB}$ that contains all valid transactions from their mempool and all Q_j mempools
$\mathcal{DB} \leftarrow \bigcup_{i \leftarrow 1}^{q} \mathcal{TH}_{ij}$
for all transactions $T'_x \in \mathcal{DB} - \mathcal{TH}_i$ **do**
    `request`$(Q_i, \mathcal{Q}, T'_x)$
end for
Q_i builds a drafted block $\mathcal{DRB}$
$\mathcal{H}_n \leftarrow$ `block_hash`$(\mathcal{DRB}_i)$
Q_i generates $\mathcal{H}_{nQ_i}$ by appending its signature onto $\mathcal{H}_n$
`broadcast`$(Q_i, \mathcal{Q}, \mathcal{H}_{nQ_i})$
`request`$(Q_i, \mathcal{Q}, \mathcal{H}_{nQ_j})$
if $\mathcal{H}_n$ achieves δ:
All members of $\mathcal{Q}$ append their signatures onto DRB and forward it to the block quorum $\mathcal{BQ}$.
else:
    Repeat Step 2 through Step 12.
    if $t_{\text{elapsed}} < t_{\text{limit}}$
        break
`broadcast`$(\mathcal{Q}, \mathcal{BQ}, \mathcal{H}_{nQ_i})$
if $\mathcal{H}_{nQ_i}$ achieves majority of the signatures from $\mathcal{BQ}$:
It will be added to the main chain
else:
Null

a malicious quorum forming. We have also provided the results of the communication cost evaluation of our system. To perform our tests, we created a multi-threaded program, where each thread is assumed to be a node. These experiments are purely statistical and are hardware agnostic.

7.1 Setup and Environment

All of our experiments were performed using a Windows 64-bit machine running Windows 10 Pro. The machine has an Intel i7-4810MQ CPU and 16 GB of RAM. Our tests were written in C++ and compiled and executed in Windows Visual Studio. Because C++ cannot natively accommodate numbers as large as the standard 256-bit hash, we use the first 1/4 of the previous block hash to compute the quorum members. The full source code can be accessed here [2].

[2]https://github.com/JANUSBLOCK/Janus.git

7.2 Fairness

In this experiment, we assess the fairness of our algorithm on two scales: local and global. Local fairness refers to the balance of work among stakeholders of the same type, while global fairness refers to the load-balancing achieved across the system as a whole.

To test the fairness of our system, we assume there are four primary stakeholder types, each represented by 20 nodes on the x-axis, while the y-axis represents the number of times a node was selected. Three quorums are generated in each iteration. We ran the test 5,000 times to simulate the generation of 5,000 blocks in the network, for a total of 15,000 quorums.

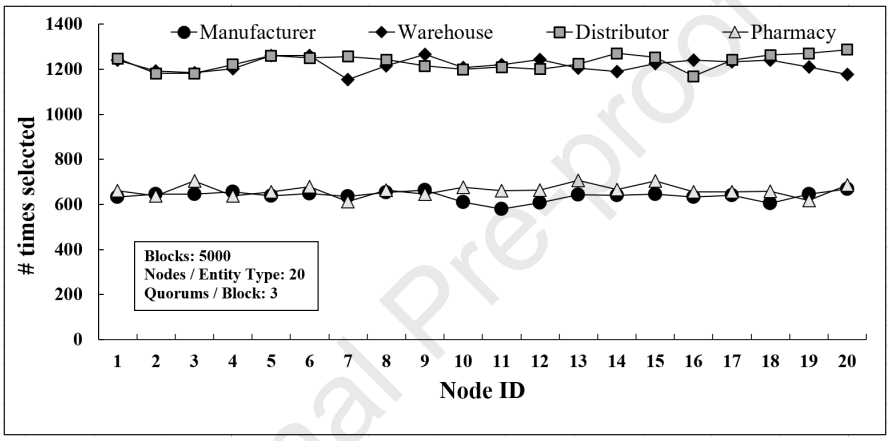

Figure 2: Local and global fairness.

Fig. 2 illustrates the results of the fairness experiment. To better observe local and global fairness, we consider two types of stakeholders: linking and outer. Linking stakeholders are those that operate between two other stakeholders in the PSC (i.e., warehouses and distributors). Outer stakeholders are those that operate on either end of the PSC (i.e., manufacturers and pharmacies). We observe that each stakeholder has a linear projection regardless of their type, where nodes were selected roughly the same number of times throughout the 5,000 trials. This indicates that we achieve local fairness. Looking at the graph as a whole, we can also see that our system achieves global fairness because certain stakeholders are selected for quorums more frequently than others. Linking stakeholders are involved in double the transactions, justifying why they are selected roughly 1,200 times versus 600 as outer stakeholders. Thus, our algorithm accomplishes the task of being globally fair among stakeholders across the network.

7.3 Scalability

Scalability is crucial for an efficient system, especially the size of the PSC. To assess the scalability of our design, we consider a linear increase in the number of nodes and transactions in the network.

To test the scalability of Janus, we track the runtime in seconds (y-axis) that it takes for quorums in networks with different numbers of nodes (x-axis) to synchronize

their transaction information and build a draft block when there are a large number of transactions. We ran this test 100 times, each iteration recording responses for networks with 1,000 to 5,000 nodes sharing 2,000 to 8,000 transactions.

Fig. 3 graphs the results of our scalability experiment. We observe a slight increase in runtime as the number of nodes progresses from 1,000 to 3,000 for all numbers of transactions. This increase is a result of the increase in quorum size. After our system reached 3,000 nodes, it began to level off. This is because the quorum size for the subsequent networks is the same. Our graph shows a gradual increase in runtime that is consistently proportional between network size (number of nodes) and number of transactions. The overhead of the protocol should increase at a reasonable rate (e.g., linearly) as the number of nodes and transactions increases [5]. Thus, our system is proven to be scalable.

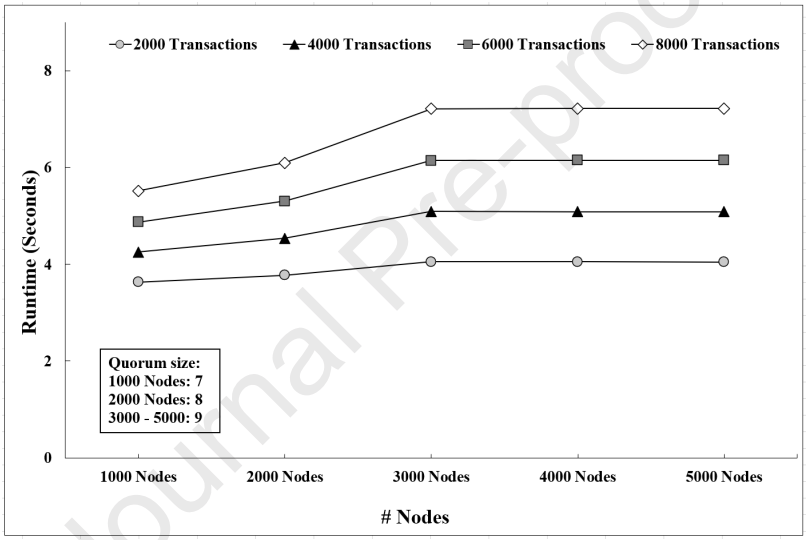

Figure 3: Scalability as nodes/transactions increase.

7.4 Resiliency Against Malicious Quorums

To prove the security of our algorithm, we performed an experiment to test resiliency against malicious quorums. To assess the resiliency, we consider that a percentage of nodes in the network are malicious to determine the frequency in which malicious quorums are formed. We define a malicious quorum as one in which at least 2/3 of the members are malicious.

To test resiliency against malicious quorums, we consider an increasing percentage of malicious nodes in the network (x-axis) and examine how it affects the total percentage of malicious quorums formed (y-axis). This experiment was repeated 100 times, considering 10%, 15%, 20%, 25%, and 30% malicious nodes in the network.

Fig. 4 visualizes the results of our experiment. We observe that as the number of malicious nodes in the network increases, the percentage of malicious quorums increases exponentially. Based on this observation, it is fair to assume that as the

network gets larger, the probability of a malicious quorum forming (in comparison to smaller networks) significantly lessens. We observe that when the total percentage of malicious nodes in a network is between 0%-23%, has a 99% success rate of reaching a valid consensus. After the number of malicious nodes increases above 23%, the probability of a malicious quorum begins to increase exponentially. We want our network to remain 23% malicious or less to ensure that no more than 1% malicious quorums are formed. This is a reasonable expectation for a permissioned network like ours.

This graph represents the case in which a regular quorum is malicious, but the block quorum is honest (or vice versa). It is worth mentioning that the probability of both types of quorums being malicious is exponentially lower.

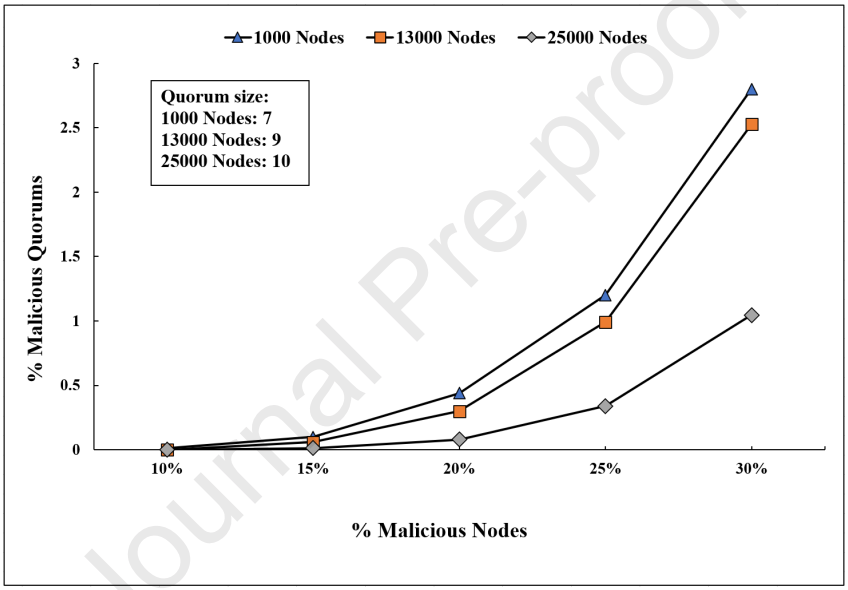

Figure 4: Potential percentage of malicious quorums forming.

7.5 Communication Cost

To evaluate the communication cost of Janus, we first examined the cost of transactions in the network. Fig. 5 visualizes the transactional cost in terms of average megabytes (MB) per quorum (y-axis) depending on the total number of transactions (x-axis). We ran this evaluation by simulating networks of 2000, 4000, and 8000 nodes transmitting 2000 to 16000 transactions. We chose these network sizes in order to establish the transaction costs at different common quorum sizes. To build a draft block that is the same for all quorum members, we assume that the probability of any given node having any given transaction is at least 65%.

We observe that more nodes in a network result in longer processing times. As anticipated, it takes longer to process the same number of transactions in larger networks, as they require communication with more nodes.

Regardless of the network size, the communication cost will increase linearly as the number of transactions increases. This contributes to the scalability of Janus, showing that it can handle as many nodes as possible without drastically affecting communication cost.

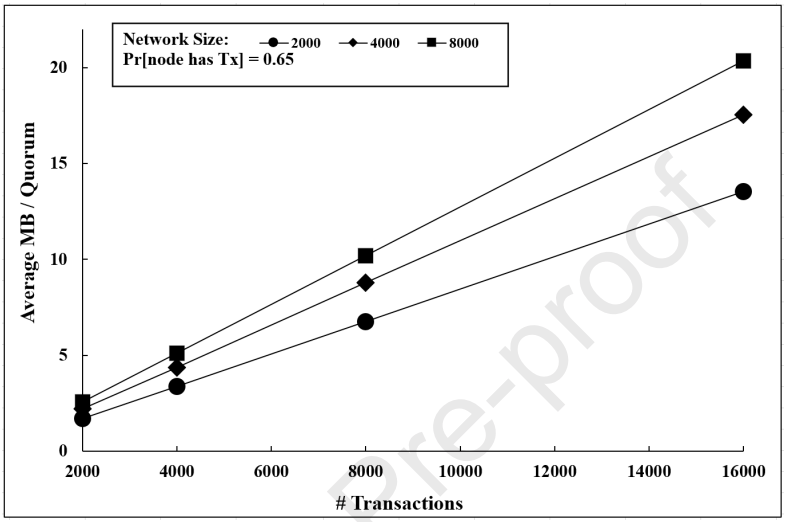

Figure 5: Communication cost as nodes/transactions increase.

8 Threats, Attacks, and Security Model

Evaluating the security of consensus protocols is challenging due to the variation of attacks encountered by blockchain systems. Threat modeling is a simple study directed by most researchers to systematically approach cyber threats and recognize potential system security concerns in advance.

We identify two threats: (1) quorum misbehaviour: a timing fault due to a miner transmitting self-contradictory blocks at the same time, and (2) denial of service: an omission weakness due to quorum members bypassing signing or announcing a transaction.

We find it important to also mention two key attacks that quorum models may be vulnerable to eclipse attacks and random manipulation attacks. Eclipse attacks can devastate a system by allowing an adversarial quorum member to attack other quorum members. Here, the malicious quorum member can monopolize all of the victim's incoming and outgoing connections, hence separating the victim from the rest of its quorum members. In this way, the adversary can modify the victim's view of the draft block. The malicious node could target multiple quorum members simultaneously.

Randomness manipulation attacks occur when a malicious quorum makes attempts to permutate the order of all transactions until it is confirmed that a malicious quorum will be formed in the future. The probability can be dramatically decreased if we choose the seed as a concatenation of the hash of the previous block and the hash of the previous-to-previous block in Algorithm 2.

Proposition 1 *If a selected quorum has malicious nodes $< \delta$ in a round, then all malicious nodes will add all the valid T_x to its block in that round.*

Proof. Assume the majority of the members are honest, then honest members will receive the valid T_x from others. Due to the majority, any invalid T_x forwarded by the malicious node will be discarded.

Let's consider the following situation: A dishonest member does not accept a block within a predefined waiting period, but all honest members send their votes to the draft block. As long as δ is satisfied, all honest peers will make the same update of their blockchain.

Proposition 2 *Assume one of the proposing quorums Q_n is faulty in a round. If the majority of other quorums remain honest, then it is impossible for them to add invalid blocks to their blockchain in the same round.*

Proof. In Janus, a draft block is appended to the main chain if and only if the block quorum accepts it. As far as the majority of this quorum remains honest, no invalid blocks can be added in case of other becomes malicious.

9 Conclusions and Future Work

We proposed a pharmaceutical-specific blockchain system that utilizes cloning-resistant hologram tags to aid in the prevention of counterfeit products from entering the pharmaceutical market. We evaluated Janus against three metrics: fairness, scalability, and resiliency. Based on our implementation and large-scale evaluation of the system, we have shown that our design maintains approximately similar workloads between all stakeholders, is scalable for large networks such as the PSC, and resilient against malicious quorums. We conclude that blockchain technology has the potential to make the supply chain management system more transparent, traceable, and resilient.

As a future work, it would be interesting to explore how to utilize blockchain to securely handle returns at any stage from a destination to a source throughout the PSC. Because returns are possible at any point in the PSC and return protocols/rules may differ between different stages, the architecture would differ from our current Janus proposal. We would need to consider how returns would be shipped back, if there is a return window, what type of transaction should be made to confirm a return from one user to another, what those transactions would consist of, and how they would get integrated into the blockchain. We would also need to ensure that return transactions would nullify the original transactions about the item that already exists on the blockchain. Another future work we would like to explore is implementing our system on an actual distributed network using Amazon web services (AWS) or similar. Additionally, it would be useful to expand the protocol to handle the exchanges between pharmacies and consumers, ensuring that no counterfeits are given out. We would also like to evaluate the quality of the interconnection between a large number of nodes on the stability of the system.

References

[1] Can blockchain rescue from supply chain disruptions due to covid-19?, Dec 2020. https://www.devdiscourse.com/article/technology/1043874-can-blockchain-rescue-from-supply-chain-disruptions-due-to-covid-19.

[2] N. Alzahrani and N. Bulusu. 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*, page 30–35. Association for Computing Machinery, 2018.

[3] G.D. Bashar, A.A. Avila, and G.G. Dagher. PoQ: A Consensus Protocol for Private Blockchains Using Intel SGX. In *International Conference on Security and Privacy in Communication Systems*, pages 141–160. Springer, 2020.

[4] G.D. Bashar, G. Hill, S. Singha, P. Marella, G.G. Dagher, and J. Xiao. Contextualizing consensus protocols in blockchain: A short survey. In *2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pages 190–195, 2019.

[5] Golam Dastoger Bashar, Joshua Holmes, and Gaby G Dagher. Accord: A scalable multileader consensus protocol for healthcare blockchain. *IEEE Transactions on Information Forensics and Security*, 17:2990–3005, 2022.

[6] B. M. A. L. Basnayake and C. Rajapakse. A blockchain-based decentralized system to ensure the transparency of organic food supply chain. In *2019 International Research Conference on Smart Computing and Systems Engineering (SCSE)*, pages 103–107, 2019.

[7] S.K. Dwivedi, R. Amin, and S. Vollala. Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism. *Journal of Information Security and Applications*, 54:102554, 2020.

[8] N. Fescioglu-Unver, S.H. Choi, D. Sheen, and S. Kumara. Rfid in production and service systems: Technology, applications and issues. *Information Systems Frontiers*, 17, 01 2014.

[9] Food and Drug Administration. Title II of the Drug Quality and Security Act, 2014. Available at `https://www.fda.gov/drugs/drug-supply-chain-security-act-dscsa/title-ii-drug-quality-and-security-act`.

[10] Food and Drug Administration. FDA In Brief: FDA provides new guidance to further enhance the security of prescription drugs in the U.S. supply chain, Jun 2021. Available at `https://www.fda.gov/news-events/press-announcements/fda-brief-fda-provides-new-guidance-further-enhance-security-prescription-drugs-us-supply-chain`.

[11] I. Haq and O. Muselemu. Blockchain Technology in Pharmaceutical Industry to Prevent Counterfeit Drugs. *International Journal of Computer Applications*, 180:8–12, 03 2018.

[12] J. Huang, X. Li, C. Xing, W. Wang, K. Hua, and S. Guo. DTD: A Novel Double-Track Approach to Clone Detection for RFID-Enabled Supply Chains. *IEEE Transactions on Emerging Topics in Computing*, 5(1):134–140, 2017.

[13] Andreas Kamilaris, Agusti Fonts, and Francesc X. Prenafeta-Bold. The rise of blockchain technology in agriculture and food supply chains. *Trends in Food Science Technology*, 91:640–652, 2019.

[14] M. Kelkar, F. Zhang, S. Goldfeder, and A. Juels. Order-Fairness for Byzantine Consensus. *IACR Cryptol. ePrint Arch.*, 2020:269, 2020.

[15] F. Leal, A.E. Chis, S. Caton, H. González–Vélez, J.M. García–Gómez, M. Durá, A. Sánchez–García, C. Sáez, A. Karageorgos, V.C. Gerogiannis, A. Xenakis,

E. Lallas, T. Ntounas, E. Vasileiou, G. Mountzouris, B. Otti, P. Pucci, R. Papini, D. Cerrai, and M. Mier. Smart Pharmaceutical Manufacturing: Ensuring End-to-End Traceability and Data Integrity in Medicine Production. *Big Data Research*, 24:100172, 2021.

[16] L. Li. Technology designed to combat fakes in the global supply chain. *Business Horizons*, 56(2):167–177, 2013.

[17] J.T. Mentzer, W. DeWitt, J.S. Keebler, S. Min, N.W. Nix, C.D. Smith, and Z.G. Zacharia. Defining Supply Chain Management. *Journal of Business logistics*, 22(2):1–25, 2001.

[18] S. Mondal, K.P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal. Blockchain Inspired RFID-Based Information Architecture for Food Supply Chain. *IEEE Internet of Things Journal*, 6(3):5803–5813, 2019.

[19] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. Available at `https://bitcoin.org/bitcoin.pdf`.

[20] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[21] World Health Organization. Counterfeit Medicines: an update on estimates 15 November 2006, 2006. Available at `https://www.who.int/medicines/services/counterfeit/impact/TheNewEstimatesCounterfeit.pdf`.

[22] Y. Peng, T. Nagase, T. Kanamoto, T. Zeniya, and S. You. A Virtual Optical Holographic Encryption System Using Expanded Diffie-Hellman Algorithm. *IEEE Access*, 9:22071–22077, 2021.

[23] M. Schöner, D. Kourouklis, P. Sandner, E. Gonzalez, and J. Förster. Blockchain Technology in the Pharmaceutical Industry. 2017.

[24] A. Shahid, A. Almogren, N. Javaid, F.A. Al-Zahrani, M. Zuair, and M. Alam. Blockchain-Based Agri-Food Supply Chain: A Complete Solution. *IEEE Access*, 8:69230–69243, 2020.

[25] M. Sidorov, M.T. Ong, R.V. Sridharan, J. Nakamura, R. Ohmura, and J.H. Khor. Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains. *IEEE Access*, 7:7273–7285, 2019.

[26] Rajani Singh, Ashutosh Dhar Dwivedi, and Gautam Srivastava. Internet of things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention. *Sensors (Basel, Switzerland)*, 20, 2020.

[27] P.W.M. Tsang. Single-random-phase holographic encryption of images. *Optics and Lasers in Engineering*, 89:22–28, 2017. 3DIM-DS 2015: Optical Image Processing in the context of 3D Imaging, Metrology, and Data Security.

[28] D.L. Wasson. Janus, Feb 2015. Available at `https://www.worldhistory.org/Janus/`.

[29] Q. Xiao, T. Gibbons, and H. Lebrun. RFID Technology, Security Vulnerabilities, and Countermeasures. In Yanfang Huo and Fu Jia, editors, *Supply Chain*, chapter 19. IntechOpen, Rijeka, 2009.

[30] F. Yang, W. Zhou, Q. Wu, R. Long, N.N. Xiong, and M. Zhou. Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access*, 7:118541–118555, 2019.

Declaration of interests

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐ The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: