Proceedings of the 2019 Winter Simulation Conference
N. Mustafee, K.-H.G. Bae, S. Lazarova-Molnar, M. Rabe, C. Szabo, P. Haas, and Y.-J. Son, eds.

SIMULATION-BASED BLOCKCHAIN DESIGN TO SECURE BIOPHARMACEUTICAL SUPPLY CHAIN

Wei Xie
Bo Wang
Zehao Ye

Mechanical and Industrial Engineering
Northeastern University
360 Huntington Avenue
Boston, MA 02115, USA

Wencen Wu

Computer Engineering Department
San Jose State University
1 Washington Sq
San Jose, CA 95192, USA

Jie You
Qi Zhou

QuarkChain Inc.
55E 3rd Ave
San Mateo, CA 94401, USA

ABSTRACT

Bio-drugs grow rapidly and become one of the key drivers of personalized medicine and advancement of life sciences. Driven by the unique challenges in biopharmaceutical supply chain management and also built on two-layer QuarkChain, we introduce a blockchain enabled interoperability framework and it has the reputation based Proof-of-Authority (PoA) smart contract. Given the real-time monitoring data streams of distributed systems, blockchain can improve the transparency and integrity of delivery processes. We introduce stochastic simulation to guide the blockchain design so that we can protect drug products from theft, temperature diversion, and counterfeiting, while improving the supply chain reliability, efficiency, and responsiveness. The preliminary empirical study demonstrates that our approach has promising performance.

1 INTRODUCTION

The biopharmaceutical industry is growing rapidly and becoming one of key drivers of personalized medicine for the treatment of many sever illnesses, including cancer cells and adult blindness. The number of biomolecules increases threefold in the last decade. They account for over 40 percent of new launched pharma products (Otto, Santagostino, and Schrader 2014) and this percentage is expected to continuously increase. Biopharmaceutical industry also grows in double digits annually in both sales and profits. However, the drug safety and shortage become the main concerns of Food and Drug Administration (FDA). A majority of drug shortage is due to the lengthy lead time and quality issues. *In this paper, we focus on simulation-based blockchain development for complex global biopharmaceutical supply chain to improve drug safety, as well as delivery process reliability, responsiveness and integrity.* Compared to classical supply chain, biopharma supply chain has key challenges as follows.

- *Complexity*: The biomanufacturing becomes more and more globalization. Roughly 80% of active pharmaceutical ingredients (API) and 40% of finished drug products are imported into the U.S. from overseas. Manufacturers in China and India are the key sources. Thus, the number of transactions of API and bio-drugs from manufacturers to patients increase dramatically. In addition, new drugs (e.g., advanced cell and gene therapies) tend to become more and more personalized. For example, the CAR

T-Cell therapy, KymriahTM (Novartis), approved in 2018 by the US FDA (FDA 2017), requires that each therapy to be manufactured in each individual patients own cells, on demand. For personalized bio-drugs, supply chain needs to be integrated with some tracking mechanism that can maintain detailed chain of identity and chain of custody.

- *Cold chain:* Since bio-drugs are based on living organisms, they are vulnerable to Protein Post-Translational Modifications (PTM) and degradation. For example, the CAR-T-Cell therapy manufactured from a patient's own immune cells needs to be kept frozen in order for the cells to remain viable. In the pharma industry, there is 95 percent of global cold-chain costs linked to biopharma products (Otto, Santagostino, and Schrader 2014). Cold-chain, required for the storage, handling, and transportation of many bio-drugs, are very complex, and there are risks of temperature deviations during delivery. New law requires building an electronic, interoperable system to identify and trace bio-drugs as they are distributed in the U.S., which enhances FDAs ability to help protect patients from exposure to drugs that may be counterfeit, stolen, contaminated, or otherwise harmful; see (FDA 2013).
- *Long lead time, high marginal value and vulnerable to counterfeiting:* Biopharmaceuticals are expensive to manufacture and the lead time for production process is lengthy, e.g., 15–20 weeks (Otto, Santagostino, and Schrader 2014). Bio-drugs tend to have the short expected product life cycle (i.e., 1.5–3 years) with high marginal value (i.e., the sale prices for one gram of bio-drug substance reach to \$500 to \$2,000). How to protect the products from theft, counterfeiting and diversion becomes critically important.

Blockchain technology exhibits various strengths (Babich and Hilary 2019), including (1) visibility; (2) resilience; and (3) integrity and automation. Through developing appropriate blockchain for global biopharmaceutical supply chain, we can overcome the challenges above. First, through combining with smart sensors tracking the delivery process, we can record whom, when, where, and how a particular drug was stored and handed during the shipment from manufacturer to patient. Second, instead of relying on a centralized trust system, blockchain network is decentralized and it can automatically verify and execute transactions. With appropriate design of smart contracts, blockchain could hedge against various sources of attacks (e.g., counterfeiting, theft and deviation). Third, through real-time information sharing, blockchain network can fully integrate participants and support the interoperation to secure the drug delivery and ensure fast reactions to any issues.

Blockchain development for supply chain management is still in its infancy. Tian (2016) proposed a supply chain tractability system based on blockchain technology, which could increase food security level. Hasan and Salah (2018) proposed a blockchain-based solution and general framework for the proof of delivery for physical items involving single and multiple transporters. Alzahrani and Bulusu (2018) proposed a new anti-counterfeiting supply chain using new field communication and blockchain. It considers the decentralized supply chain that exploits the block chain technology (block-supply chain), and a new consensus protocol that deals with the problem of selecting validators. This design guarantees authenticity, integrity and transparency.

As far as we know, there is no existing literature paper introducing blockchain network to facilitate complex global biopharmaceutical supply chain risk management. Built on two-layer commercial blockchain (called QuarkChain, see $https://github.com/QuarkChain/pyquarkchain/wiki$), we introduce a blockchain enabled interoperability framework for biopharma supply chain management, which accounts for the unique challenges mentioned above. With more and more personalized bio-drug discovery and the expansion of globalization, the number of transactions will increase dramatically. In addition, the sensors that real-time monitor the drug delivery lead to a large amount of data records. *Thus, we explore the two-layer blockchain, propose smart contracts and introduce new blockchain platform for global biopharma supply chain, which can provide reliable and efficient bio-drug delivery to hedge against the theft, counterfeiting and deviation risk.*

Two-layer blockchain utilizes the state partition and parallel computing mechanism to effectively solve the scalability issue. Unlike the classical blockchain composed of single chain that is in charge of all the transactions, two-layer blockchain includes: (1) one root chain layer securing the blockchain network; and (2) one extensible sharding layer consisted multiple shard chains processing transactions. To deal with increasing supply chain complexity, we divide all transactions occurring in global biopharma supply chain into different shard chains, which could be based on geographical locations. Thus, the detailed transaction information is saved and verified locally by shard chains in parallel. The verification process is based on the smart contract with reputation based Proof-of-Authority (PoA), which is proposed to hedge against cyberattacks, including counterfeiting on either drug source information and monitoring sensor data. Then, each verified transaction is hashed, uploaded and further confirmed by root chain before broadcasting it to the whole blockchain network. For each transaction, we record time, location, responsible personnel, and sensor monitoring data, which can facilitate reputation learning, interoperation and fast response to any issue occurring in the supply chain. We further introduce a simulation model and algorithm to guide the development of blockchain enabled interoperability platform for biopharma supply chain risk management. The empirical study indicates that the proposed framework can improve: (1) the detection of malicious modification cyberattacks, drug counterfeiting and temperature deviation; and (2) the blockchain efficiency.

Therefore, the main contributions of this paper are summarized as follows. First, built on two-layer blockchain structure in Quarkchain, we introduce the blockchain enabled interoperability framework accounting for the unique challenges in the biopharamaceutical supply chain risk management to hedge the cyberattacks and drug counterfeits. Second, we propose the reputation based Proof-of-Authority as preliminary smart contract design. Third, we introduce a simulation model and algorithm to guide the framework development for biopharma supply chain risk management.

This paper is organized as follows. In Section 2, we present the basic mechanism of blockchain. Then, built on QuarkChain's two-layer design, we introduce a reliable and efficient blockchain platform for biopharma supply chain risk management in Section 3. A simulation model and algorithm is developed to guide the blockchain design. We conduct the empirical study in Section 4 and conclude this paper in Section 5.

2 INTRODUCTION OF BLOCKCHAIN MECHANISM

In this section, we introduce the blockchain mechanism. *Since the biopharmaceutical industry is highly regulated in order to protect the public health, we consider the permissioned network design with smart contract (SC).* A blockchain is a distributed database and also a global hedger which records all transactions in the network as a timestamp chain of blocks. Figure 1(a) shows the structure of blockchain design. Each block contains three parts: header, transaction data body and validation. In header, "Time" reflects when the transactions happen and "Height" specifies the number of blocks in the chain. "Nonce" is a number added to a hashed block and it is used to encipher the block. A block could be made of validation records and several transactions which are saved in merkle root after hashed. Each *i*-th block, denoted by B_i, is identified by its cryptographic hash,

$$H_i \equiv \mathrm{Hash}(B_i).$$

Hash is a specific algorithm that can transfer letters and numbers into a sequence of string called hash code, or hash. Each block references to the hash of the block that comes before it, which establishes a chain of the blocks, called *blockchain*. Blocks could be added if new valid transaction records need to be written in the global ledger.

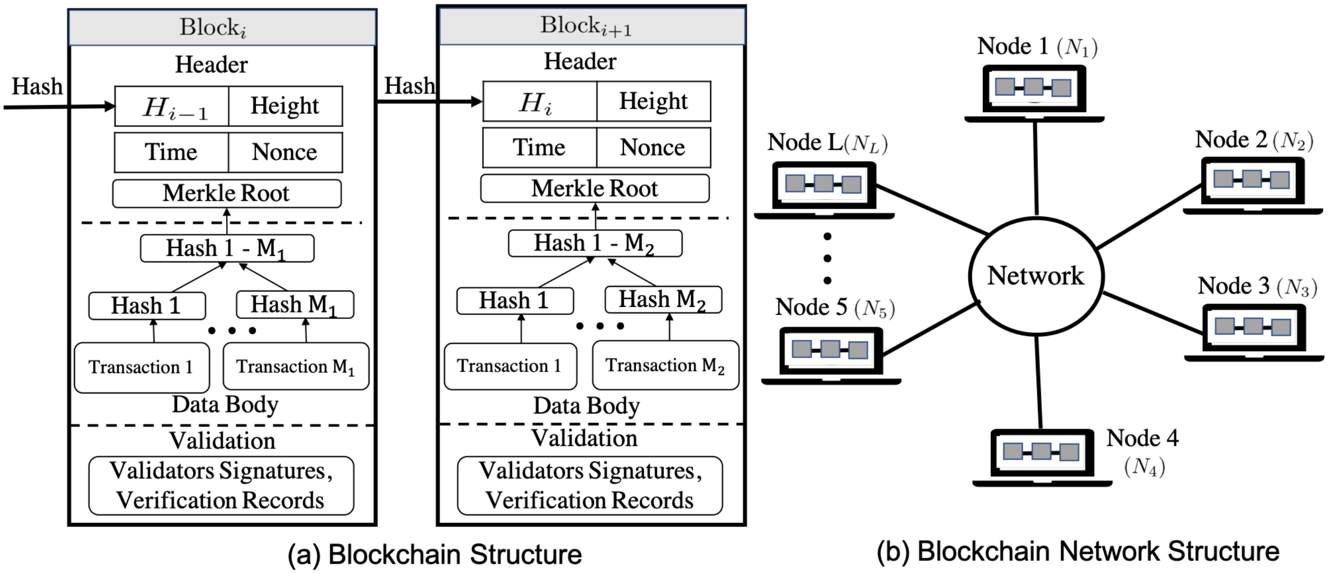


Figure 1: The structure of blockchain and blockchain network.

Any participant with access to this ordered, back-linked list of blocks can get the world view of transaction data that have been exchanged on the network (Christidis and Devetsikiotis 2016). In the real applications, each block could include multiple transactions ordered based on certain priority, such as gas fee and reputation score. To simplify the illustration, suppose every block only records one transaction. Then, each i-th block could be formulated as a triple, denoted by $B_i(h_p, T_x, v)$, where h_p is a point to the previous block in chain, T_x represents the transaction recorded in the i-th block, and v is the validation information, e.g., the validators signatures and verification records; see Figure 1(a). The validation is based on certain rule that every transaction is required to follow, e.g., smart contract. Given the incoming transaction T_x and also the current state or all previous transactions which could be accessed through h_p, the validation process returns the verified message and then a block is added to blockchain.

Thus, blockchain can be formulated as a list, denoted by $C[\cdot]$, which includes several blocks (Garay, Kiayias, and Leonardos 2015). Typically, $C[-1]$ refers to the last element/block in the blockchain list, e.g., $C[-1] = B_{-1}(h_p, T_x, v)$, and $C[i:j]$ refers to a sub-array including block i to block j. *There are some important properties from blockchain: consistency and tractability.* Consistency means that transactions are verified consistently and then we append blocks to the chain. Tractability means if information in block $C[x]$ is changed, each block in sub-array $C[x,-1]$ is also automatically changed. Thus, it is easy to trace back and find out which block had been changed.

The blockchain C with the record of all transactions is replicated and shared among the participants of a network (called *blockchain network*) with structure shown in Figure 1(b). Suppose that each i-th node, denoted by $\mathscr{N}_i$, represents a participant, denoted by N_i, with a single computer. All nodes are equally involved in maintaining a blockchain, but different nodes can have different roles for running the blockchain. In the permissioned blockchain network, suppose all the participants are identifiable. In this paper, we consider a static setting with a fixed set of nodes. Let $\mathbf{N} = (N_1, N_2, \dots, N_L)$ denote all participants, where L is the number of participants and nodes in the network. Since the blockchain is replicated among the nodes, the network can be formulated as

$$\mathscr{N} = \{\mathscr{N}_1(C,\mathrm{SC}),\ \mathscr{N}_2(C,\mathrm{SC}), \dots, \mathscr{N}_L(C,\mathrm{SC})\}$$

where $\mathscr{N}_\ell(C,\mathrm{SC})$ for $\ell = 1,2,\dots,L$ represents Node ℓ with blockchain copy C and smart contract (SC) as a piece of code residing on this blockchain.

Participants interact with the blockchain through a pair of their own private and public keys. They use their private keys to sign their own transactions which are verified on the blockchain network via their public keys (Christidis and Devetsikiotis 2016). The private key can be used to create a digital signature for displaying the sender's authenticity of transaction T_x, $\mathit{signature} = \mathit{hash}(\mathit{hash}(\mathit{private\_key}), \mathit{hash}(T_x))$. The public key is transformed from the private key by a irreversible hash function, $\mathit{public\_key} = \mathit{hash}(\mathit{private\_key})$. Thus, given $\mathit{public\_key}$ and T_x, the receiver or other nodes can verify the signature, $\mathit{hash}(\mathit{public\_key}, \mathit{hash}(T_x)) \overset{?}{=} \mathit{signature}$.

To facilitate the automatic interactions and help the network reach *consensus* or a common global view of the world state, each blockchain network needs to establish rules that each transaction should conform to (Christidis and Devetsikiotis 2016). This can be achieved by smart contract which can be viewed as a digitized traditional contract. It is a piece of code residing on a blockchain and the blockchain network assigns unique addresses to the contract. Therefore, the smart contract residing on replicated and shared ledger allows the automatic verification for new transaction and further facilitate data-driven interactions between mutually distrustful counterparties.

A smart contract (SC) has the structure shown in Figure 2; see the description in Bahga and Madisetti (2016). It includes a set of executable functions $V(\cdot)$ and state variables of blockchain network (i.e., the world state of data that have been recorded in blockchain), denoted by S. Any participant can trigger the functions $V(\cdot)$ in the contract by sending a new transaction T_x to the contract for the verification, and the verification result is also based on the current state S. Then, the verified transaction information is broadcast to each node in the blockchain network as message,

$$(\mathit{Message}, S_{\mathrm{new}}) = \mathrm{SC}(T_x; V(\cdot), S). \tag{1}$$

Basically, following certain logic, SC first selects a verification panel, denoted by VP. Given the transaction T_x and the current state accessed through h_p, the verification function $V(\cdot)$ returns the validation records v,

$$v \equiv ((Y_i, \mathrm{Signature}_i)_{i \in \mathrm{VP}}, z) = V(h_p, T_x; \mathrm{VP}). \tag{2}$$

where $(Y_i, \mathrm{Signature}_i)$ denotes the accept/reject decision and signature from validator i in VP, and z is the final decision based on some form of "majority" vote. Thus, the broadcast message in Equation (1) includes the transaction and verification results, Message $= (T_x, v)$. A new block containing this message is generated and it is appended to the chain C. Smart contract triggers the events to update the blockchain network state which becomes the world view for the next transaction, $S = S_{\text{new}}$. If the nodes do not verify the suggested transaction, the proposed block is discarded. Notice that once triggered by an incoming transaction T_x, the smart contract code executes independently and automatically on each node in the blockchain network. *To reach consensus on its execution result, a smart contract is "deterministic" (Christidis and Devetsikiotis 2016) or consistent across different nodes in the network.*

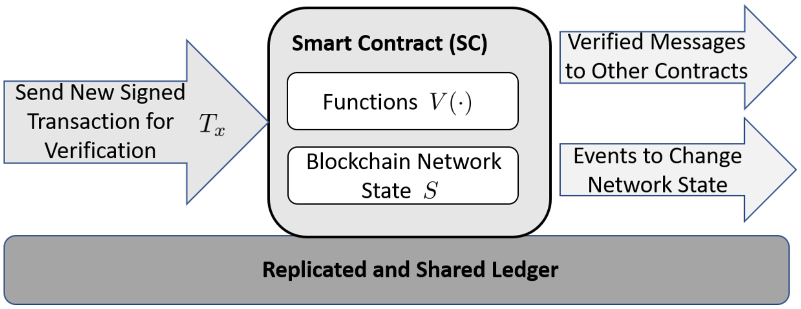

Send New Signed Transaction for Verification
T_x
Smart Contract (SC)
Functions $V(\cdot)$
Blockchain Network State S
Verified Messages to Other Contracts
Events to Change Network State
Replicated and Shared Ledger

Figure 2: Smart contract structure.

3 BLOCKCHAIN DEVELOPMENT FOR BIOPHARMA SUPPLY CHAIN RISK MANAGEMENT

Driven by the key challenges presented in Section 1, we introduce a permissioned blockchain network for complex global biopharma supply chain to secure the delivery process and improve the drug safety in Section 3.1. Then, built on two-layer QuarkChain, we present a blockchain platform in Section 3.2, which could improve transaction processing throughput and deal with the increasing complexity of biopharma supply chain. We further provide the simulation algorithm procedure in Section 3.3, which could be used to guide the blockchain platform development.

3.1 Blockchain Design for Global Biopharma Supply Chain

For the highly regulated biopharmaceutical supply chain, we study a permissioned blockchain network. In this paper, we consider the static setting with fixed participants including manufacturers, transporters and patients.

- Bio-drug Manufacturer ($\mathscr{M}$). A manufacturer produces the product and initializes the transportation. It creates the first transaction for a delivery.
- Transporter ($\mathscr{T}$). A transporter delivers the item from the previous participant, e.g., the previous transporter or the manufacturer, to the next participant, e.g., the next transporter or the patient. Transporters keep updating the status of the product by submitting transactions to the network.
- Patient ($\mathscr{P}$). A patient purchases the bio-drug product from the manufacturer, and creates the last transaction to confirm receiving the ordered product.

Thus, all participants in the network can be divided into three disjoint sets: $\mathbf{N} = \mathbf{N}_m \cup \mathbf{N}_t \cup \mathbf{N}_p$, where $\mathbf{N}_m, \mathbf{N}_t$ and $\mathbf{N}_p$ represent the sets of nodes from manufacturers, transporters and patients.

The bio-drug order arrival and delivery stochastic processes occurring in biopharma supply chain are the driving forces for the dynamic evolution of blockchain. Each bio-drug product has a unique product ID (PID) generated by one of manufacturers in $\mathbf{N}_m$. Suppose the random sample ω has one-to-one mapping with PID. Let $t_0(\omega)$ be the order arrival time. Suppose the order arrival immediately triggers the product release and the selection of participants involved in the delivery process, denoted by $\mathbf{N}_D(\omega) = (\mathscr{M}, \mathscr{T}, \mathscr{P})$, where $\mathscr{M}$ and $\mathscr{P}$ represent a manufacturer and a patient from sets $\mathbf{N}_m$ and $\mathbf{N}_p$, and $\mathscr{T}$ is a subset of transporters from $\mathbf{N}_t$. Let $D(\omega)$ be the delivery sample path. The transportation time for each shipment is random.

The types of transactions in the delivery process include initialization, transportation and final receiving. Each delivery typically has one transaction in the initialization and final receiving stages respectively, and it has multiple transactions in transportation stage. Each transaction includes the transaction data, sender and receiver's signatures,

$$T_x = (\text{TransactionData}, \text{SenderSignature}, \text{ReceiverSignature}). \tag{3}$$

In the initialization stage, the manufacturer provides the data records, e.g., PID, the product expire time, the storage condition requirement, and the production quality. In the transportation and receiving stages, the transaction data include the real-time sensor data, including time, location and storage condition (i.e., temperature). This information can help us track the shipment and response to any potential problem quickly.

We consider data modification cyberattacks which could happen during transaction data generation and after the transactions are included in blocks. During the transaction generation, the cyberattack risk is induced by the transaction data that have been tampered by the person handling the product. To ensure that the blockchain contains valid and correct transactions, we propose a Proof-of-Authority (PoA) smart contract which can automatically execute the verification to reduce the impact of the cyberattacks. *This smart contract is designed based on the reputation-based voting mechanism.*

In this PoA smart contract SC_{PoA}, a voting panel, denoted by $\text{VP}(\omega, \omega^c_{\mathscr{N}})$, is randomly selected from $\mathbf{N}_D(\omega)$ to validate any transaction $T_x(\omega)$. This design is based on two considerations. First, the participants in $\mathbf{N}_D(\omega)$ are responsible for any potential drug quality and delivery delay related issues. Second, since *the manufacturing and storage "process" determines the quality of bio-drugs*, this could facilitate the further research on developing the big data analysis for the reputation learning by utilizing the bio-drug quality test samples randomly collected from biopharmaceutical supply chain. The number of validators, denoted by $m = |\text{VP}(\omega, \omega^c_{\mathscr{N}})|$, influences the blockchain network security. A common random number, denoted by $\omega^c_{\mathscr{N}}$, is used on all nodes in the network $\mathscr{N} = (\mathscr{N}_1, \mathscr{N}_2, \ldots, \mathscr{N}_L)$ to make sure that the same voting panel is selected when different nodes execute the smart contract following Equation (1), which can ensure the consensus. The verification function in Equation (2) becomes

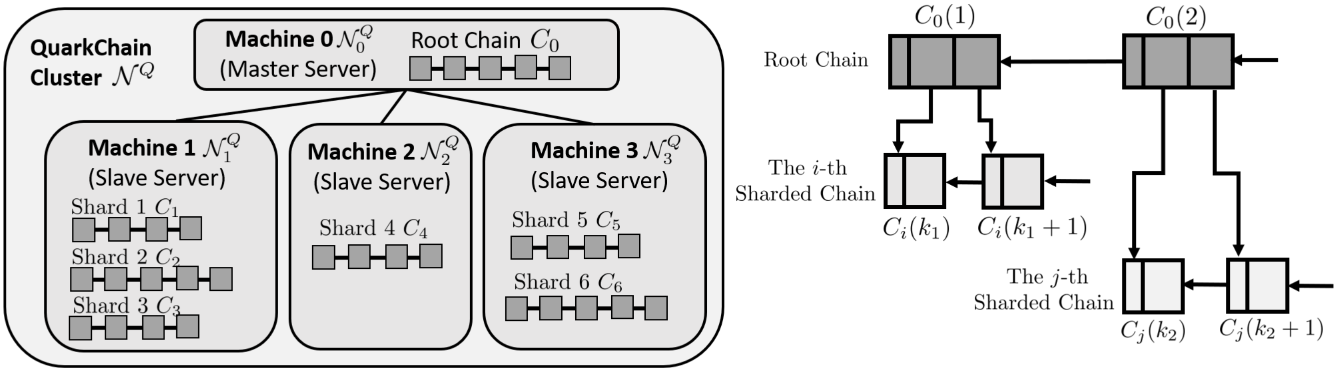
$$v = ((Y_i, \text{Signature}_i)_{i \in \text{VP}(\omega, \omega^c_{\mathscr{N}})}, z) = V(h_p, T_x(\omega); \text{VP}(\omega, \omega^c_{\mathscr{N}})) \tag{4}$$

where $Y_i \in \{0, 1\}$ represents the reject/accept vote from the i-th validator in $\text{VP}(\omega, \omega^c_{\mathscr{N}})$ and the final decision z is based on the majority vote. Thus, triggered by the arrival of transaction $T_x(\omega)$, the smart contract will return the validation results v, including validators signatures and their voting records. *Since all the interactions occur via signed messages and validations in Equations (3) and (4), participants can get a cryptographically verifiable trace of the biopharma supply chain operations.* For simplification, we suppose that each participant has a fixed reputation score here. In the future research, this score will be learned through analyzing transaction, voting and bio-drug quality testing data that could be randomly collected from the delivery process.

3.2 Two-Layer BlockChain Platform

The increasing complexity of global biopharma supply chain requires a blockchain platform with high transaction processing throughput. *However, due to the decentralized nature of a blockchain network, scalability has been a challenging problem faced by most existing solutions because all the nodes in the blockchain network need to reach consensus on including any new transaction.* In the centralized world, sharding is one of the most widely used technologies to solve the scalability problem, for example, BigTable, Cassandra, etc. The key idea of *sharding* is the state partition: divide the global state into a collection of sub-states, so that the transactions can be processed in different shards in parallel.

An innovative sharded blockchain protocol, called QuarkChain, has been introduced by Zhou (2018b). QuarkChain has a two-layer architecture: one layer is called sharding layer, which is composed of a number of shard chains, $C_1, C_2, \ldots, C_R$, processing transactions simultaneously, where R is the total number of shard chains. The sharding layer is extensible, meaning that R can be increased to improve the network throughput. The other layer is the root chain layer, denoted by C_0, which ensures the overall security of the network and serves as the coordinator for cross-shard transactions among shard chains. In QuarkChain network, the network state S (the full transaction history) is partitioned into subsets of state $S_1, S_2, \ldots, S_R$, where $\cup_{r=1}^R S_r = S$. The r-th subset S_r is recorded by shard chain C_r. Figure 3 illustrates the two-layer design, in which a cluster is the equivalence of a "full node" defined in Ethereum that keeps the full transaction history of the blockchain network. A QuarkChain cluster consists of a collection of machines/CPUs, one of which runs the root chain, and others run different shard chains. Each block in a sharded blockchain has two hash pointers: one links to the previous sharded block and the other pointer links to a root block; see Figure 3(b). We define the machines in a QuarkChain cluster as $\mathscr{N}_i^Q$ for $i = 1, \ldots, m$, where m is the number of machines in a QuarkChain cluster, which can be different in different clusters. Thanks to the sharding technology, one machine $\mathcal{N}_i^Q$ only runs a subset of the shard chains, thus, only processes transactions on the corresponding shard chains. In this way, a much larger volume of transactions can be processed in parallel by different shard chains compared to the number of transactions processed by a single blockchain like Ethereum. Therefore, a much higher throughput can be achieved. For example, even though Bitcoin only processes 6 to 7 transactions per second and Ethereum currently processes 15 transactions per second, QuarkChain testnet has achieved more than $10,000$ transactions per second (Zhou 2018a).



(a) QuarkChain Cluster

(b) Root Chain and Sharded Chain Connection

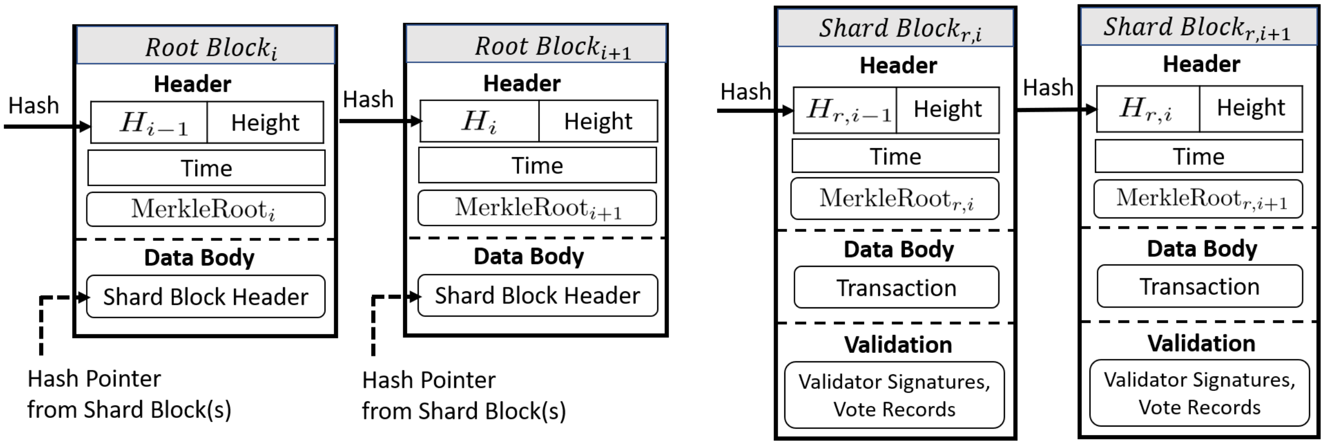
Figure 3: QuarkChain Cluster (from quarkchain wiki).

We build the two-layer blockchain platform for bio-pharmaceutical supply chain based on QuarkChain. Each participant could utilize a cluster with many machines running different shard chains. One essential question in the design is how to partition the state of the network. Usually, in-shard transactions are processed by shard chains, and cross-shard transactions require the involvement of root chain, which increases the time to reach consensus (Zhou 2018b). In the global biopharma supply chain, we partition the system state based on geographical positions of the transactions with the assumption that local deliveries (i.e., within a country) contribute to the majority of deliveries. In other words, transactions happen within one country will be processed by one shard. For simplification, we assume each delivery is included in one shard here. That means all transactions in each delivery $D(\omega)$ are processed in a certain shard chain, say C_r. Suppose each shard chain has its own PoA-based smart contract following the design in Section 3.1.

To ensure the bio-drug quality, each shipment is closely monitored by real-time sensors, which could lead to large volume of transaction data. *To hedge against the modification attacks, we propose a root-chain-first PoA which has a hierarchical verification structure.* Basically, both the root chain and shard chains run PoA with different set of authorities. The selection of local authorities and the PoA-based smart contract SC_r^{PoA} on shard chain C_r can follow the idea proposed in Section 3.1. Global authorities can include reliable trusted parties (e.g., FDA) who are responsible for the safety of public health. We denote the authority set for root chain as $\mathbf{N}_A$ and the smart contract as SC_0^{PoA}. A transaction is first verified in a shard chain and is included in a shard block based on the PoA-based smart contract. The shard block containing the transaction is finalized only after it is confirmed by the root chain. Confirmation refers to the process that the header of the shard block is first checked by an authority of the root chain. If verified, the authority then produces and broadcasts a root block that contains the header. The structures of root chain and shard chain are illustrated in Figure 4, where $\mathrm{MerkleRoot}_{r,i}$ is the hash of Data Body and Validation in the r-th shard chain and $\mathrm{MerkleRoot}_i$ is the hash of Data Body in the root chain for any block i. Compared to shard blocks that verify all the details of a transaction, each root block only checks the block headers of shard blocks, thus, is able to process a large amount of shard blocks efficiently. The state sharding technology and root-chain-first consensus enable the parallel processing of transactions and achieve resilience to data modification attack.

3.3 Algorithm Development and Simulation Procedure

In this section, we provide the simulation modeling and algorithm for two-layer blockchain platform that could facilitate the development of reliable and efficient Biopharma supply chain. Suppose all the participants can be divided into R different shards, including Manufacturer nodes $\mathbf{N}_m^{(r)}$, transporter nodes $\mathbf{N}_t^{(r)}$, and patient nodes



(a) Root Chain Structure

(b) The r-th Shard Chain Structure

Figure 4: The root and shard chains structure.

$\mathbf{N}_p^{(r)}$, with $r = 1,\ldots,R$. *Suppose almost all transactions are processed within shards and the impact of processing cross-shard transaction is negligible.* A fixed global authority panel $\mathbf{N}_A$ works for root chain confirmation. To mimic the data modification risk, suppose there exists a certain proportion p_0 of participants who could perform dishonestly. Suppose there is a underlying "reputation score" for each participant from 0 to 1 measuring the honest level. A bad participant with score level $(1-u)$ has probability u to modify the transaction it involves. Any selected good validator will reject the modified transaction with probability u in verification process, while other bad nodes always accept the transactions. Suppose that all bad nodes work in collusion. For simplification, suppose that we have a fixed set of bad reputation participants, denoted by $\mathbf{N}_B$ and $|\mathbf{N}_B|/|\mathbf{N}| = p_0$.

3.3.1 Simulation Modeling Development

Let F_A denote the distribution of bio-drug order inter-arrival time. For each order ω_k with $k = 1,2,\ldots,K$, we first specify the participants involved in the delivery process $\mathbf{N}_D(\omega_k)$, including one manufacturer $\mathscr{M}(\omega_k)$, one patient node $\mathscr{P}(\omega_k)$ and J_k transporters $\mathscr{T}_j(\omega_k)$ with $j = 1,\ldots,J_k$. Suppose the delivery happens in region $r(\omega_k)$ and all transactions in this delivery are processed in shard chain $C_{r(\omega_k)}$. Denote the order arrival time as $t_0(\omega_k)$. Once receiving the order, the manufacturer $\mathscr{M}(\omega_k)$ immediately releases the product to the first transporter $\mathscr{T}_1(\omega_k)$. They create the first transaction $T_{x,1}(\omega_k)$ with their signatures, and then send it to smart contract on $C_{r(\omega)}$ waiting for verification. If one of $\mathscr{M}(\omega_k)$ and $\mathscr{T}_1(\omega_k)$ belongs to $\mathbf{N}_B$, the data is modified with probability u.

Once receiving any transaction $T_{x,j}(\omega_k)$ with $j = 1,\ldots,J_k$, the PoA-based smart contract on shard $r(\omega_k)$, denoted by $\mathrm{SC}^{PoA}_{r(\omega_k)}$, randomly selects a voting panel from all nodes involved in this delivery, $\mathrm{VP}_j(\omega_k,\omega^c_{\mathscr{N}}) \subset \mathbf{N}_D(\omega_k)$. Suppose $\mathrm{VP}_j(\omega_k,\omega^c_{\mathscr{N}}) = \{\mathscr{N}_{j,1}(\omega_k),\ldots,\mathscr{N}_{j,m}(\omega_k)\}$, where the size of voting panel m is determined by design. For each voting, if transaction $T_{x,j}(\omega_k)$ only involves good participants, all nodes in voting panel will vote "Accept." If transaction $T_{x,j}(\omega_k)$ involves any bad node, the good validator will vote "Reject" with probability u and the bad validators will vote "Accept". We record detailed voting result $v_j(\omega_k) = ((Y_{j,\ell}(\omega_k), \text{Signature}_\ell)_{\ell\in\mathrm{VP}(\omega,\omega^c_{\mathscr{N}})}, z_j(\omega_k))$, and the final decision to accept or reject this transaction is based on majority voting,

$$z_j(\omega_k) = \text{round}\left(\frac{1}{m}\sum_{\ell=1}^{m} Y_{j,\ell}(\omega_k)\right). \tag{5}$$

Each validator can only process one transaction at a time. Let F_v denote the distribution of each verification processing time. The processing priority could be based on gas fee. For simplification, we consider the first-come-first-serve (FCFS) queue here. *Thus, the verification for each transaction is based on the outputs from selected validators (nodes) and we model the PoA based verification process as in a queueing network Q_r including nodes in the shard chain C_r.* Thus, the verification time $t_{v,j,\ell}(\omega_k)$ includes both waiting and processing times, which depends on the utilization of each node or validator. Since the VP decision is based on the decisions from all m

selected validators, the total verification time for transaction $T_{x,j}$ is,

$$t_{v,j}(\omega_k) = \max_{\ell=1,\dots,m} t_{v,j,\ell}(\omega_k). \tag{6}$$

If the final decision $z_j(\omega_k)$ obtained by Equation (5) is "Accept", one node in voting panel is randomly selected to generate a shard block $B_i^{(r)}(h_p^{(r)}, T_{x,j}(\omega_k), v_j(\omega_k))$ including transaction and detailed voting records, append it to the shard chain $C_{r(\omega_k)}$. For simplification, we assume the block generation and propagation time are included in random verification delay $t_{v,j}$ because it tends to dominate the whole verification time. Otherwise, if $z_j(\omega_k)$ is "Reject", we stop this delivery ω_k and record the corresponding outcome as "Not Finished", $o_k = NF$.

Then, the shard block header $B_i^{(r)}.Header$ is sent to the PoA-based smart contract SC_0^{POA} on root chain for confirmation. One node is randomly selected from $\mathbf{N}_A$ to check the transaction hash, generate the the root-block $B^{(0)}(h_p^{(0)}, B_i^{(r)}.Header)$, append it to the root chain C_0 and broadcast the newly generated block to the blockchain network to reach consensus. We also model the root-chain confirmation process by a FCFS queue network Q_0 including $\mathbf{N}_A$ authority nodes. Suppose the confirmation processing time for each transaction follows the distribution F_{RC}. Denote the overall confirmation time as $t_{RC,j}$, including waiting and processing times.

After the transaction $T_{x,j}(\omega_k)$ is confirmed, the transporter $\mathscr{T}_j(\omega_k)$ for $j = 1,\dots,J_k$ will ship the product to the next stop, and collect the sensor data of storage conditions along the way. We assume a homogeneous random delay for each shipment time $t_{d,j}(\omega_k) \sim F_d$. Then, $\mathscr{T}_j(\omega_k)$ will send the product to the next transporter $\mathscr{T}_{j+1}(\omega_k)$ or the patient $\mathscr{P}(\omega_k)$ if it is the last transporter, and generate the transaction $T_{x,j+1}(\omega_k)$ including sensor data. The transaction $T_{x,j+1}(\omega_k)$ will be signed and wait for verification and confirmation, which follows the same procedure described above. After the last transaction $T_{x,J_k+1}(\omega_k)$ is verified and confirmed, the delivery $D(\omega_k)$ is finished and we record the cycle time of this delivery $t_c(\omega_k) = t - t_0(\omega_k)$, where t is the current system time. If there is any transaction with modified data for this finished order k, the outcome $o_k = FC$ as "Finished Counterfeit" drug; otherwise, $o_k = FA$ as "Finished Authentic" drug. The detailed implementation can be found in Algorithm 1.

3.3.2 Biopharma Supply Chain Performance Measures of Interest

For the biopharma supply chain system with blockchain platform, we are interested in both safety and efficiency. Here, we consider three system performance measures: (1) expected cycle time for each order $t_c = \mathrm{E}[t_c(\omega)]$; (2) expected percentage of counterfeited drugs reaching to patients $q_c = \lim_{K\to\infty} \mathrm{E}[K_{FC}/K_F]$; and (3) expected percentage of filled (i.e. finished) orders $q_f = \lim_{K\to\infty} \mathrm{E}[K_F/K]$, where $K_{FC} = \sum_{k=1}^{K} \mathbb{I}(o_k = FC)$ is the count of "Finished Counterfeit" drugs and $K_F = \sum_{k=1}^{K} \mathbb{I}(o_k = FC/FA)$ is the count of all "Finished" drugs, $\mathbb{I}(\cdot)$ denotes the indicator function.

Suppose we run W replications of simulation. At each w-th replication with $w = 1,\dots,W$, we collect the simulation outputs $t_c^{(w)}(\omega_k)$, $o_k^{(w)}$ for $k = 1,\dots,K$, we can compute corresponding $K_{FC}^{(w)}$ and $K_F^{(w)}$, and the three measures can be estimated by,

$$\hat{t}_c^{(w)} = \frac{1}{K_F}\sum_{k=1}^{K} t_c^{(w)}(\omega_k)\mathbb{I}(o_k = FC/FA); \;\; \hat{q}_c^{(w)} = K_{FC}^{(w)}/K_F^{(w)}; \;\; \hat{q}_f^{(w)} = K_F^{(w)}/K. \tag{7}$$

We further control the simulation estimation error by taking average over W replications,

$$\hat{t}_c = \frac{1}{W}\sum_{w=1}^{W} \hat{t}_c^{(w)}; \;\; \hat{q}_c = \frac{1}{W}\sum_{w=1}^{W} \hat{q}_c^{(w)}; \;\; \hat{q}_f = \frac{1}{W}\sum_{w=1}^{W} \hat{q}_f^{(w)}. \tag{8}$$

The estimated performance measures can provide insights about the system safety (i.e. $\hat{q}_c$), and system efficiency and scalability (i.e. $\hat{t}_c$ and $\hat{q}_f$).

4 EMPIRICAL STUDY ON THE PERFORMANCE OF BLOCKCHAIN PLATFORM DESIGN

Based on the simulation framework described in Section 3.3, we perform the simulation experiments to study the performance of proposed blockchain design for biopharma supply chain, in terms of both efficiency and security. Set the total number of nodes to be 1000 with $|\mathbf{N}_m| = 100$, $|\mathbf{N}_t| = 800$, $|\mathbf{N}_p| = 100$, $|\mathbf{N}_A| = 100$, and evenly allocate them to all shards. The delivery orders are evenly assigned to all shards. Suppose the number of shipments is

Algorithm 1: Two Layer Blockchain Platform for Biopharma Supply Chain Risk Management

```
Input: Node sets $\mathbf{N}_A$, $\mathbf{N}_B$, $\mathbf{N}_m^{(r)}$, $\mathbf{N}_t^{(r)}$, $\mathbf{N}_p^{(r)}$ with $r = 1,\dots,R$; inpuinteroperability t models $F_A$, $F_v$, $F_{RC}$,
    and $F_d$; verification panel size $m$.
Output: $\hat{t}_c$, $\hat{q}_c$, and $\hat{q}_f$.
Function Verify($\mathbf{N}_D(\omega_k)$, $T_{x,j}(\omega_k)$, $m$):
    (A1) Once receiving $T_{x,j}(\omega_k)$, the smart contract $\mathrm{SC}^{PoA}_{r(\omega_k)}$ on shard $r(\omega_k)$ randomly selects $m$ nodes
      from $\mathbf{N}_D(\omega_k)$ as voting panel $\mathrm{VP}(\omega_k, \omega^c_{\mathscr{N}}) \subset \mathbf{N}_D(\omega_k)$;
    for Each node $\mathscr{N}_{j,\ell}(\omega_k) \in VP(\omega_k, \omega^c_{\mathscr{N}})$ do
        (A2) $\mathrm{SC}^{PoA}_{r(\omega_k)}$ sends $T_{x,j}(\omega_k)$ to the validator $\mathscr{N}_{j,\ell}(\omega_k)$ and wait for the verification;
        (A3) After the verification is finished, record the time $t_{v,j,\ell}(\omega_k) \sim F_v$;
        if $\mathscr{N}_{j,\ell}(\omega_k) \in \mathbf{N}_B$ then
            $Y_{j,\ell}(\omega_k) = 1$, record in $v_j(\omega_k)$;
        else if $T_{x,j}(\omega_k).Sender \in \mathbf{N}_B$ or $T_{x,j}(\omega_k).Receiver \in \mathbf{N}_B$ then
            $Y_{j,\ell}(\omega_k) = \begin{cases} 0, & with\ probability\ (1-u) \\ 1, & with\ probability\ u \end{cases}$ , record in $v_j(\omega_k)$;
        else
            $Y_{j,\ell}(\omega_k) = 1$, record in $v_j(\omega_k)$;
    (A4) Record the decision $z_j(\omega_k)$ by applying Equation (5). Compute the overall verification time
      $t_{v,j}(\omega_k)$ by applying Equation (6). Set the time $t = t + t_{v,j}(\omega_k)$;
    if $z_j(\omega_k) == 0$ then
        (A5) Transaction $T_{x,j}(\omega_k)$ not verified. Stop this delivery $\omega_k$ and set $t_c(\omega_k) = \infty$, $o_k = NF$;
        return False
    else
        (A6) Randomly select one node $\mathscr{N}_{j,\ell}(\omega_k)$ from voting panel to generate a shard-block
          $B_i^{(r)}(h_p^{(r)}, T_{x,j}(\omega_k), v_j(\omega_k))$ on shard-chain $C_{r(\omega_k)}$;
        (A7) Send shard-block header $B_i^{(r)}.Header$ to the smart contract on root chain $\mathrm{SC}^{PoA}_0$. Randomly
          select one node $N_A(\omega_k)$ from global authorities panel $\mathbf{N}_A$ for confirmation;
        (A8) $N_A(\omega_k)$ verifies $B_i^{(r)}.Header$ and generates the root-block $B_{i'}^{(0)}(h_p^{(0)}, B_i^{(r)}.Header)$ on $C_0$.
          Update the blockchain network state $S$. Record the confirmation time $t_{RC}(\omega_k) \sim F_{RC}$;
for Each Delivery $\omega_k$ do
    (1) Based on $F_A$, generate the order arrival time $t = t_0(\omega_k)$. Specify the set $\mathbf{N}_D(\omega_k)$. The manufacturer
      $\mathscr{M}(\omega_k)$ creates the bio-drug data and releases the drug product to the first transporter $\mathscr{T}_1(\omega_k)$;
    (2) $\mathscr{M}(\omega_k)$ and $\mathscr{T}_1(\omega_k)$ generate the first transaction $T_{x,1}(\omega_k)$, trigger the smart contract $\mathrm{SC}^{PoA}_{r(\omega_k)}$ for
      verification, and call Verify($\mathbf{N}_D(\omega_k)$, $T_{x,j}(\omega_k)$, $m$);
    while $j \leq J_k + 1$ && Verify($\mathbf{N}_D(\omega_k)$, $T_{x,j}(\omega_k)$, $m$) $! = False$ do
        if $j \leq J_k$ then
            (3) Ship the product to next stop with the shipment time $t_{d,j}(\omega_k) \sim F_d$. Transporter $\mathscr{T}_j(\omega_k)$
              collects the sensor data along the shipment. Update the time $t = t + t_{d,j}(\omega_k)$;
            (4) Transporter $\mathscr{T}_j(\omega_k)$ sends the product to the next transporter $\mathscr{T}_{j+1}(\omega_k)$ or the patient
              $\mathscr{P}(\omega_k)$. $\mathscr{T}_j(\omega_k)$ and $\mathscr{T}_{j+1}(\omega_k)$ together generate new transaction $T_{x,j+1}(\omega_k)$. Trigger the
              smart contracts $\mathrm{SC}^{PoA}_{r(\omega_k)}$ and call Verify($\mathbf{N}_D(\omega_k)$, $T_{x,j+1}(\omega_k)$, $m$);
        else
            (5) End this delivery $k$, set $t_c(\omega_k) = t - t_0(\omega_k)$, record finished status $o_k$;
(6) Driven by the drug-order interarrival distribution $F_A$, the new arrivals are put into the corresponding
  shard queues. Run simulations with runlength $K$ by following the procedure and compute $\hat{t}_c$, $\hat{q}_c$, and $\hat{q}_f$
  as in Equation (8). Repeat it for $W$ replications.
```

uniformly distributed between 9 to 19, so that the number of participants involved in each delivery is uniformly distributed between 10 to 20. We set the percentage of bad nodes $p_0 = 2.4\%$ with reputation score $(1-u) = 0.2$ Here, the selection of p_0, u and the expected number of transactions in each delivery can lead to the percentage of counterfeit drugs close to 30% recorded in World Health Organization (WHO) (2006). Assume the inter-arrivals of orders, verification, and confirmation times of each node follow the exponential distributions, i.e., $F_A = \exp(\mu_A)$, $F_v = \exp(\mu_v)$ and $F_{RC} = \exp(\mu_{RC})$, where $\mu_A = 10$, $\mu_v = 9$ and $\mu_{RC} = 0.1$ are the mean levels. We assume each shipment time follows gamma distribution, $F_d = \Gamma(3.0, 1.0)$.

We first show the advantage of the two layer blockchain design over the traditional single chain. We compare the single chain with a two-layer chain with 2 shards and 10 shards under fixed $m = 5$, and we run simulation experiments with run-length $K = 1000$ transactions, after 200 warm-up, and $W = 100$ replication. We consider the expected transaction processing throughput, $\mathrm{Th} = \mathrm{E}\left[\sum_{k,j} \mathbb{I}(T_{x,j}(\omega_k).\mathrm{Time} \in [t, t+1])\right]$, which can be estimated through $\widehat{\mathrm{Th}} = \sum_{k,j} \mathbb{I}(T_{x,j}(\omega_k).\mathrm{Time} \in [t_{start}, t_{end}])/(t_{end} - t_{start})$ where $[t_{start}, t_{end}]$ is the simulation time. Notice that $T_{x,j}(\omega_k)$.Time is the time when transaction $T_{x,j}(\omega_k)$ finishes the verification and confirmation, and it is added into the blockchain network; see Step (A8) in Algorithm 1. *Based on the simulation results, the estimated average throughput for single chain, two-layer chains with 2 and 10 shards are* 2.920 ± 0.001, 5.317 ± 0.015*, and* 24.949 ± 0.124. Since two-layer blockchain processes transactions in parallel, it can provide higher throughput and the advantage becomes more significant as the number of shards increasing.

When it comes to safety, we consider the two-layer blockchain with 2 shards and voting panel size $m = 1, 5$. We compare its performance with the cases, including (1) without blockchain and (2) two-layer blockchain with the perfect information where good validators can identify any modified transaction after verification. In terms of safety level, $\hat{q}_c$, $\hat{q}_f$ are reported, and we record the false reject rate that is the percentage of authentic drugs not passing verification, $q_{fr} = \lim_{K\to\infty} \mathrm{E}[K_{FR}/(K - K_F)]$, where $K_{FR} = \sum_{k=1}^{K} \mathbb{I}[(\omega_k \text{ not modified }) \;\&\; (o_k = NF)]$ is the count of false rejected deliveries. We can obtain estimate $\hat{q}_{fr}$ similarly as $\hat{q}_c$ and $\hat{q}_f$. We run simulations at each setting with run-length $K = 1000$ orders, after 200 warm-up, and $W = 100$ replication, and record the results in Table 1. Compared with supply chain without blockchain which has around 30% counterfeit drugs delivered to patients, the percentage of counterfeit drugs reaching to patients decreases dramatically after incorporating the proposed blockchain. As m increases, the drug safety level increases at the expense of longer verification time. With uncertain information, the false reject rate also slightly increases since we simply assume voting based on the expected reputation. In reality, the additional information should be collected through more validations.

Table 1: Simulation results of different blockchain designs.

	m	Throughput	Verification Time	Counterfeit	Finish Rate	False Reject
without blockchain	—	—	—	30.45±0.16%	100±0%	—
partial information	1	12.940±0.028	58.685±0.097	0.20±0.02%	68.85±0.15%	8.05±0.10%
	5	5.317±0.015	148.010±0.239	0.06±0.01%	69.24±0.13%	8.07±0.09%
perfect information	1	12.946±0.030	59.343±0.097	0±0%	68.30±0.14%	0±0%

5 Conclusions

Built on two-layer blockchain structure in QuarkChain, we introduce a blockchain framework to facilitate the biopharma supply chain interoperation and risk management to hedge against drug counterfeit, false information and malicious modification cyberattacks. The state of blockchain network is partitioned based on the geographical positions of the transactions. Multiple shard chains coordinated by root chain can process the transactions in parallel, which can significantly increase the blockchain processing throughput and efficiency. Further, driven the critical challenges in biopharma supply chain, we introduce the preliminary design of root-chain-first and reputation-based PoA consensus protocol to improve the bio-drug safety. A stochastic simulation approach is developed to study the effectiveness of the proposed blockchain enabled interoperability framework. The empirical results indicate that our approach has promising performance to hedge against the cyberattacks and improve the drug safety and the transaction processing efficiency.

ACKNOWLEDGMENTS

The authors acknowledge helpful discussion with Jared Auclair and Peter Baker. They are experts in regulation and drug quality. Jared Auclair is the director of Biopharmaceutical Analysis Training Lab and ICH (International Council for Harmonisation). Peter Baker has over ten years experience as FDA investigator.

REFERENCES

Alzahrani, N., and N. Bulusu. 2018. "Block-supply Chain: A New Anti-counterfeiting Supply Chain Using NFC and Blockchain". In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*. June 15th, Munich, Germany, 30–35.

Babich, V., and G. Hilary. 2019. "Distributed Ledgers and Operations: What Operations Management Researchers Should Know About Blockchain Technology". *Manufacturing & Service Operations Management*.

Bahga, A., and V. K. Madisetti. 2016. "Blockchain Platform for Industrial Internet of Things". *Journal of Software Engineering and Applications* 9(10):533–546.

Christidis, K., and M. Devetsikiotis. 2016. "Blockchains and Smart Contracts for the Internet of Things". *IEEE Access* 4:2292–2303.

FDA 2013. "Title II of DQSA, Drug Supply Chain Security Act (DSCSA)". https://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa, accessed 23rd June 2019.

FDA 2017. "FDA Approval Brings First Gene Therapy to the United States". https://www.fda.gov/news-events/press-announcements/fda-approves-novel-gene-therapy-treat-patients-rare-form-inherited-vision-loss, accessed 23rd June 2019.

Garay, J., A. Kiayias, and N. Leonardos. 2015. "The Bitcoin Backbone Protocol: Analysis and Applications". In *Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques*. April 26th-30th, Sofia, Bulgaria, 281–310.

Hasan, H. R., and K. Salah. 2018. "Blockchain-based Proof of Delivery of Physical Assets with Single and Multiple Transporters". *IEEE Access* 6:46781–46793.

Otto, R., A. Santagostino, and U. Schrader. 2014. "From Science to Operations: Questions, Choices, and Strategies for Success in Biopharma". Technical report, McKinsey & Company, Boston, Massachusetts.

Tian, F. 2016. "An Agri-food Supply Chain Traceability System for China based on RFID & Blockchain Technology". In *Proceedings of 13th International Conference on Service Systems and Service Management*. June 24th-26th, Kunming, China, 1–6.

World Health Organization (WHO) 2006. "Counterfeit Medicines: An Update on Estimates". https://www.who.int/medicines/services/counterfeit/impact/TheNewEstimatesCounterfeit.pdf, accessed 23rd June 2019.

Qi Zhou 2018a. "QuarkChain: A High-Capacity Peer-to-Peer Transactional System". https://github.com/QuarkChain/pyquarkchain, accessed 23rd June 2019.

Qi Zhou 2018b. "QuarkChain Explained, Part 4: Sharding in QuarkChain: Consensus". https://medium.com/quarkchain-official/quarkchain-explained-part-4-sharding-in-quarkchain-consensus-8032704319bd, accessed 23rd June 2019.

AUTHOR BIOGRAPHIES

WEI XIE is an assistant professor in the Department of Mechanical and Industrial Engineering at Northeastern University. She received her M.S. and Ph.D. in Industrial Engineering and Management Sciences at Northwestern University. Her research interests are in computer simulation, data analytics, and stochastic optimization for cyber-physical system risk management. Her email address is w.xie@northeastern.edu.

WENCEN WU is an Assistant Professor of the Computer Engineering Department of San Jose State University. She obtained her Ph.D from the Georgia Institute of Technology. Her research interests include autonomous multi-robot systems, cyber-physical systems, and distributed parameter systems. Her email address is wencen.wu@sjsu.edu.

BO WANG is a Ph.D. candidate of the Department of Mechanical and Industrial Engineering at Northeastern University. His research interests are data analytics, input modeling and uncertainty quantification in stochastic simulation. His email address is wang.bo2@husky.neu.edu.

JIE YOU is a software engineer of QuarkChain Inc.. He obtained his Ph.D in Computer System and Engineering from Rensselaer Polytechnic Institute. His research interests include autonomous multi-robot systems, cyber-physical systems, distributed parameter systems, and blockchain technology. His email address is jyouyj@gmail.com.

ZEHAO YE is a master student of the Department of Mechanical and Industrial Engineering at Northeastern University. His research interests are blockchain and stochastic simulation. His email address is ye.ze@husky.neu.edu.

QI ZHOU is the Founder and CEO of QuarkChain Inc., a blockchain company providing flexible, scalable, and user-oriented blockchain solutions. He received his Ph.D from the Georgia Institute of Technology. He was a former software engineer at Google, Facebook, and DSSD, a unicore acquired by EMC and has extensive experience in high-performance and distributed systems. His email address is qizhou@quarkchain.org.