# Blockchain Design for a Secure Pharmaceutical Supply Chain

Zhe Xu
*Electrical and Computer Engineering*
*UMASS Amherst*
Amherst, Massachusetts
zhexu@umass.edu

Wayne Burleson
*Electrical and Computer Engineering*
*UMASS Amherst*
Amherst, Massachusetts
burleson@umass.edu

***Abstract*— Amid the COVID-19 pandemic, the pharmaceutical supply chain faces significant challenges. While serialization regulations, such as the U.S. Drug Supply Chain Security Act (DSCSA), aim to enhance traceability, there remain challenges in fully managing and protecting the pharmaceutical supply chain. This study investigates the potential of blockchain technology as a solution, emphasizing its attributes of superior traceability, robust security, and heightened transparency. We utilize a physical-level product marking scheme to complement the traceability features of blockchain. To validate feasibility, we developed a testing platform comparing three major consortium chain solutions: Hyperledger Fabric, FISCO-BCOS, and Corda. Our research aims to offer an optimized blockchain-based pharmaceutical supply chain solution and a valuable selection guide for industry stakeholders.**

***Index terms*—Blockchain, Pharmaceutical, Security, Supply Chain, Hyperledger Fabric, Corda, FISCO-BCOS**

## I. Introduction

This section presents an overview of the common challenges in the pharmaceutical supply chain, viewed through the lens of the three core tenets of information security: Confidentiality, Integrity, and Availability (CIA).

### A. *Data Confidentiality*

Supply chain management, especially in the pharmaceutical sector, is vulnerable to man-in-the-middle (MITM) attacks, which can lead to the distribution of counterfeit drugs, theft of sensitive information, and significant disruptions in drug delivery[1]. Abdallah *et al.* emphasize the importance of data traceability within the pharmaceutical supply chain and suggest that blockchain technology offers a potential solution[2]. This technology can address traceability challenges such as complex supply chains, lack of transparency, and varying regulatory requirements, as seen in the 2018 recall of blood pressure medications due to a potentially harmful impurity[3]. Blockchain's decentralized and tamper-resistant nature ensures secure product tracking, facilitating regulatory compliance, and enhancing transparency to prevent counterfeit drug distribution, ultimately aiming for improved public health outcomes.

### B. *Data Integrity*

The pharmaceutical supply chain faces severe threats from counterfeit vaccines, especially during the COVID-19 pandemic, as highlighted by the alarming instances of counterfeit vaccine seizures[4][5]. Such infiltrations endanger public health and erode trust in health institutions. Concurrently, challenges like overproduction and lack of transparency in the supply chain exacerbate issues such as the opioid crisis in the U.S., where pill mills exploit gaps and contribute to addiction and overdose fatalities[6][7]. Both scenarios underscore the need for enhanced regulatory oversight, supply chain transparency, and collaborative efforts among stakeholders to safeguard public health.

### C. *Direct physical theft of pharmaceuticals*

Direct theft of pharmaceuticals poses a significant threat to the supply chain beyond cyberattacks. Lawrence *et al.*'s approach[9] offers a solution by using DNA or peptide markers to authenticate and trace products. This method encodes a Unique Identification (UID) into markers, ensuring product authenticity and acting as forensic evidence against theft and counterfeiting. Detection techniques, such as PCR amplification, validate these markers to prevent counterfeit products from entering the supply chain. We've adopted the UUID Version 4 standard from the IETF[8] for generating unique drug identifiers, with a vast random space ensuring minimal duplication risks. Figure 1 illustrates the encoding process of the

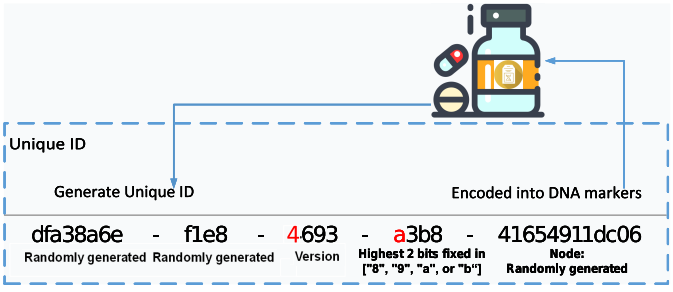


Figure 1: UUID generating[8] and DNA marking[9] process, the fixed bits in ID String is highlighted in red.

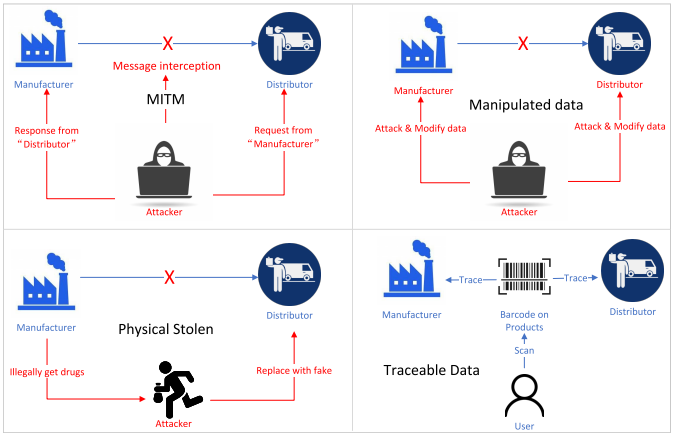


Figure 2: Examples of Challenges in The Supply Chain.

unique ID into a DNA marker, which is later utilized in a blockchain-based supply chain system.

### D. *Service Availability*

The pharmaceutical supply chain faces significant threats from cyberattacks, including ransomware and DDoS attacks[10][11]. Notably, the global logistics firm Maersk suffered a loss of $300 million due to the NotPetya ransomware in 2017[12]. DDoS attacks, in particular, can disrupt vital medication delivery, damage drug data integrity, and have substantial financial repercussions. When key components such as inventory systems and communication networks are compromised, it jeopardizes timely access to medications, erodes trust in pharmaceutical companies, and can result in substantial economic losses. Figure 2 visually illustrates various challenges in the supply chain, highlighting the diverse threats that can undermine its security.

### E. *Our Work*

In the present study, we intend to utilize the DNA marking tool, as delineated by Lawrence *et al.*[9], to generate a unique identity tag for each medication. Subsequently, this tag will serve as an anchor to monitor the drug throughout its entire lifecycle. Regarding data management, we shall develop rudimentary demonstration systems for validation, based on each of the three prevalent consortium chain solutions, and establish independent testbeds for evaluation. These assessments will encompass fundamental functionality (ensuring coverage of challenges posed by various threat models described in Section 3), performance (average response time and resource consumption), and scalability. Ultimately, we aim to derive conclusions regarding a viable solution capable of bolstering the security of the pharmaceutical supply chain.

## II. Related Work

This section presents relevant research that can provide valuable insights for this work and the key technologies we will use.

### A. *Current State of The Pharmaceutical Supply Chain*

Sarkar *et al.*[13] in their 2023 study emphasized the persistent challenge of drug traceability in the U.S., even after the introduction of the Drug Supply Chain Security Act (DSCSA) in 2018. Counterfeiters continue to exploit the system, especially during the COVID-19 pandemic, distributing contaminated drugs via illicit channels. In contrast, Europe has successfully implemented a centralized drug verification system, reducing counterfeiting risks. The U.S. urgently requires a similar centralized, blockchain-based system to ensure drug safety and combat counterfeiting effectively.

### B. *Other Blockchain-Based Solutions*

Several blockchain-based solutions have been explored to enhance the pharmaceutical supply chain. Zoughalian *et al.*[14] focused on drug authenticity using the Merkle tree and Markov chain for node credibility, integrating smart contracts for automation. Rehman *et al.*[15] proposed a method based on Ethereum, while Hardin *et al.*[16] leveraged Intel's trusted computing for data permissions and cyclic hashing. Uddin *et al.*[17] abstracted key supply chain roles. Additionally, Abir EL *et al.*[18] implemented information hiding to bolster security, and Cui *et al.*[19] encrypted data to improve blockchain performance. While these solutions offer insights into security and efficiency, they lack exploration into mainstream consortium chains and physical anti-counterfeiting measures, areas we aim to address.

### C. *Other Threats*

In another very interesting study[20], the authors proposed an attack method that uses electromagnetic interference(EMI) to influence sensor readings. It should be noted that the method described in this article mainly focuses on how to protect the security of the collected data. The security of the data generation process is not within the scope of this article.

### D. *Introduction to Blockchain*

Blockchain is a transformative technology comprising a decentralized, distributed ledger that ensures secure and transparent transactions. It bundles transactions into cryptographically linked blocks, establishing data integrity and immutability. Figure 4 demonstrates the flow of information in a blockchain-enabled supply chain, emphasizing the consensus-driven addition of new blocks. There are three main blockchain types: public (permissionless and fully decentralized), private (permissioned and centrally controlled), and consortium (partially decentralized, managed by multiple organizations). Figure 3 provides a visual representation of these categories. Given the pharmaceutical supply chain's need

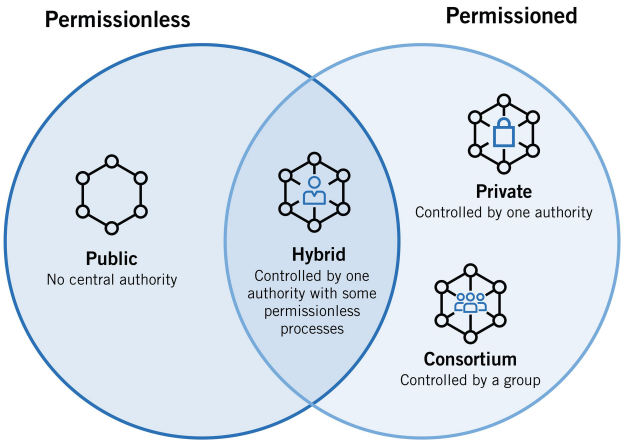


Figure 3: Blockchain Classification[21].

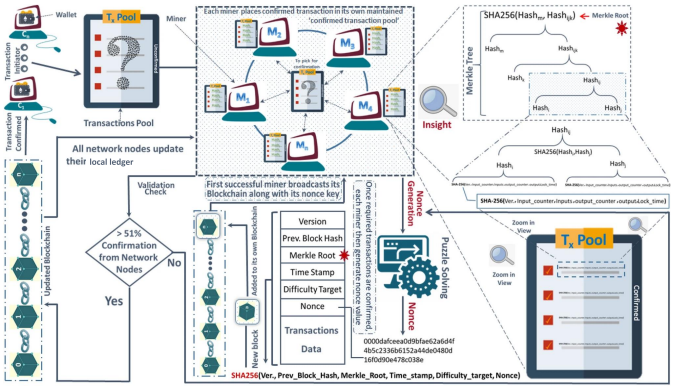


Figure 4: Blockchain Working Process[22].

for collaboration, transparency, and data control, consortium blockchains stand out as the optimal choice due to their balance of transparency and performance, ensuring stakeholders' collaboration while retaining data control.

1) *Types of Blockchains:* Consortium blockchains offer an advantageous blend of transparency, security, and scalability, making them ideal for the pharmaceutical supply chain. These blockchains, managed by a group of organizations, foster collaboration while ensuring individual data control and regulatory compliance. This hybrid approach provides the efficiency of private blockchains with the transparency of public ones. Given the pressing requirements of the pharmaceutical supply chain, including trust, data integrity, and collaboration, we conclude that consortium blockchains, as depicted in Figure 3, will be our chosen solution for supply chain management.

2) *Consensus Algorithms in Blockchain:* Consensus algorithms ensure the reliability and uniformity of data within blockchain networks. These mechanisms are primarily classified into Byzantine Fault Tolerant (BFT) and Crash Fault Tolerant (CFT) categories.

BFT algorithms handle adversarial or malicious behaviors. Notable examples include:

1. **Proof of Work (PoW)**: Used by Bitcoin, it requires miners to solve complex cryptographic puzzles to validate and append transactions to the blockchain.
2. **Proof of Stake (PoS)**: Ethereum's evolving consensus algorithm, prioritizes validators based on the quantity of cryptocurrency they hold and are willing to "stake" as collateral.
3. **Proof of Elapsed Time (PoET)**: Suited for permissioned blockchains, it relies on fair randomness, where participants await a randomly determined period before proposing a new block.
4. **Practical Byzantine Fault Tolerance (PBFT) and Tendermint**: Both BFT consensus algorithms, PBFT requires multiple communication rounds among nodes, while Tendermint merges BFT with PoS, streamlining the consensus process.

CFT algorithms, conversely, tackle non-malicious system failures. Key examples are:

1. **Raft**: A consensus algorithm designed to be straightforward to understand, often used in distributed systems for its simplicity and robustness.
2. **Paxos**: Known for its efficiency in managing multiple simultaneous operations across a distributed system.
3. **Zab (ZooKeeper Atomic Broadcast)**: Primarily employed in the synchronization of ZooKeeper servers.

In essence, while PoW has set the stage for cryptocurrencies like Bitcoin, modern algorithms such as PoS, PoET, and Tendermint provide tailored solutions, harmonizing the demands of both BFT and CFT contexts.

### *E. Introduction to Docker*

Docker, a leading virtualization technology, revolutionizes application management through containers, ensuring consistent operation across diverse environments. Its containerization promotes scalability, allowing applications to adapt to varying workloads efficiently, especially when paired with orchestration tools like Kubernetes. While Docker aids in DDoS attack mitigation by isolating applications and reducing the attack surface, its modularity facilitates quick recovery post-attack. However, as Kaur *(et al.)* (2021)[23] highlighted, containerized deployment may present vulnerabilities, which can be countered by updating and minimizing base images. Overall, Docker's capabilities in promoting scalability and security make it a vital tool in today's software landscape.

The blockchain-based system we describe will be deployed in a Docker containerized manner to enhance the availability of the system

### *F. The DNA Marker*

Lawrence *et al.*[9] introduced a method employing DNA markers, including DNA or polypeptide markers, to uniquely mark pharmaceuticals. This approach involves applying a

medium with the DNA marker directly to the pharmaceutical or incorporating it within, suitable for various forms like tablets, powders, and liquids. The DNA marker encodes specific information about the pharmaceutical, such as its manufacturer, components, and manufacturing date. The technique's strength lies in its simplicity, eliminating complex procedures, and its robustness, making reverse engineering nearly impossible. This offers a formidable defense against pharmaceutical theft, counterfeiting, and fraud.

## III. Methods

This chapter delves into the threat models linked to the pharmaceutical supply chain by introducing roles and security boundaries and analyzing threats from the CIA perspective. We aim to test the functionality and performance of prominent consortium blockchain frameworks, anticipating they offer promising technical avenues for enhancing drug quality and safety in the future.

### A. *Security Boundaries and Threat Models*

The pharmaceutical supply chain, as detailed by Uddin *et al.*[17], involves various stakeholders such as suppliers, manufacturers, distributors, and patients, with intricate processes making traceability challenging. Figure 5 depicts these stakeholders and their interrelations. Despite the complexities, the Government or Regulatory Authority(ies) sets the demand, and the Manufacturer sources materials from the Ingredient Supplier. After repackaging, distributors facilitate the drug's journey to the Patient via the Pharmacy.

Both the Government and Patients are deemed trustworthy. The government's role is to oversee the pharmaceutical supply chain, curbing potential threats, while patients, often victims of an unsound supply chain, lack incentives for illicit activities. World Bank data[24] indicates significant grey-market drug trade across income levels@2016_Top_Markets_Report_Pharmaceuticals. Our solution aims to enhance traceability, potentially addressing issues like patient-initiated drug abuse. However, challenges like collusion between

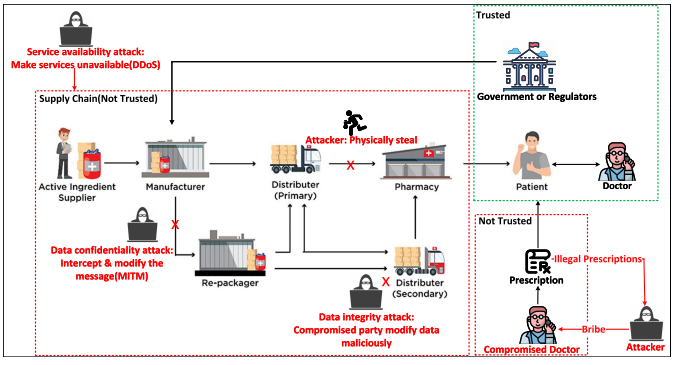


Figure 5: Supply Chain Stakeholders(modified from [17])

| Role Name | Describe | Is Trusted |
|---|---|---|
| Regulators | Post orders and audit order status | Yes |
| Manufacture | Accept orders and produce medicines, can be attacked | No |
| Distributor | Distribution of drugs, themselves and upstream and downstream are subject to attack | No |
| Pharmacy | Be classified as a "distributor" | No |
| Re-packager | Be classified as a "distributor" | No |
| Ingredient Supplier | Be classified as a "distributor" | No |
| Patient | Consumers and victims, not explicitly shown in the swim lane diagram | Yes |
| Attacker | Launch attacks on various nodes of the supply chain | No |
| Bribed Doctors | Be classified as an "attacker" | No |

Table 1: Roles Explanation

physicians and attackers persist. Hence, in our model, bribed doctors are "not trusted."

Other supply chain participants might pose risks due to non-compliance. Accordingly, we will present the key supply chain players in TableTable 1 and use UML swim lane diagrams to showcase typical attack models in subsequent sections.

### B. *Popular Consortium Blockchain Framework*

Our choice of blockchain platform is underpinned by two criteria: architectural considerations and consensus algorithms. From an architectural standpoint, FISCO-BCOS, an Ethereum-based consortium chain platform, epitomizes the "decentralization" paradigm. Hyperledger Fabric incorporates blockchain's quintessential security attributes, while Corda

by R3 mirrors traditional distributed storage solutions, albeit with enhanced data integrity and traceability. Our selection aims to encompass a spectrum of consortium blockchain frameworks rooted in varied technical architectures. On the consensus algorithm front, prevalent blockchain algorithms fall into two categories: CFT (Crash Fault Tolerance), which presupposes non-responsive failed nodes[25], and BFT (Byzantine Fault Tolerance), which accounts for potentially malicious nodes[26]. Our chosen consortium blockchain solutions endeavor to represent both of these consensus algorithm types.

Hyperledger Fabric, FISCO BCOS, and Corda by R3 are four popular blockchain platforms that have gained significant attention in recent years. Despite sharing the same underlying concept of distributed ledger technology, each platform has its unique features, design philosophies, and target applications.

1) *Hyperledger Fabric:*

Hyperledger Fabric[27] is a permissioned blockchain platform[28] that focuses on enterprise use cases. It utilizes a modular architecture that allows for flexibility and modifiability, enabling the creation of private and confidential transactions. Fabric's channel system enables multiple parties to transact privately and selectively on a shared ledger, while its endorsement policy system allows for fine-grained control over transaction validation. Fabric also supports the integration of off-chain data and smart contracts written in multiple languages, including Go, JavaScript, and Java. With its focus on security and privacy, Fabric has been adopted by various industries, including finance, healthcare, and supply chain management.

Figure 6 depicts the architecture and a sample transaction flow(as indicated by the red text in the figure) of the Hyperledger Fabric blockchain platform. The root Certificate Authority (CA) is responsible for issuing certificates to all member organizations, which in turn sign for their respective nodes. Upon initiating a transaction, the client collects endorsements from all involved organizations. The endorsement peers verify the transaction and sign for it upon receiving the request. After obtaining sufficient signatures, the client submits the transaction to the orderer cluster(Raft consensus). The order nodes determine the order of transactions and package them into the current block, which is then relayed to the peer node. Finally, the peer node notifies the client about the outcome of the specific transaction.

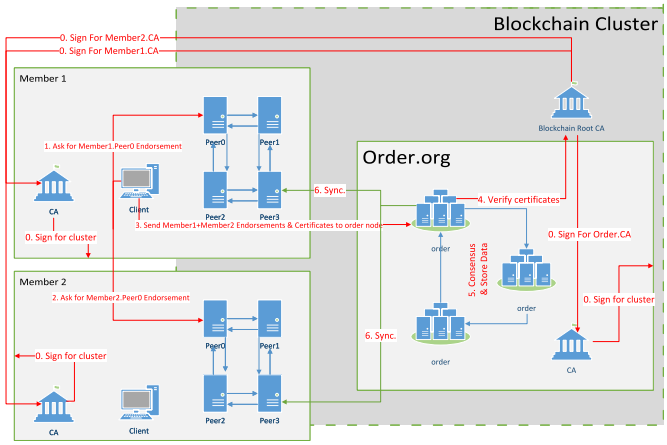


Figure 6: Hyperledger Fabric Architecture.

2) *Corda by R3:* Corda[29], developed by the software company R3, is a Distributed Ledger Technology (DLT) platform tailored for enterprise applications. Distinct from other blockchain platforms, Corda addresses specific challenges in business transactions, emphasizing privacy, security, and interoperability. Its design facilitates complex business logic, making it particularly suitable for supply chain management, where transparency, traceability, and efficient transaction processing are paramount. While R3 initially focused on financial services, the versatility of Corda has expanded its applicability across various industries. Figure 7 illustrates the architecture of Corda.

Corda employs various worker types, including:

- **Crypto Workers**: These are the sole workers capable of accessing sensitive cryptographic data, like private keys.
- **Database Workers**: They handle all persistence tasks (e.g., reading, writing, updating) within the cluster or for virtual nodes.
- **Flow Workers**: They run the CorDapp code defined by flows.
- **Membership Workers**: They offer membership functionalities, such as joining an app network or identifying other network members.
- **Gateway Workers**: They manage TLS connections with gateways from different clusters and handle message transmission via HTTPS, typically facing the internet.
- **P2P Link Manager Workers**: They ensure secure and dependable message delivery between two virtual nodes.

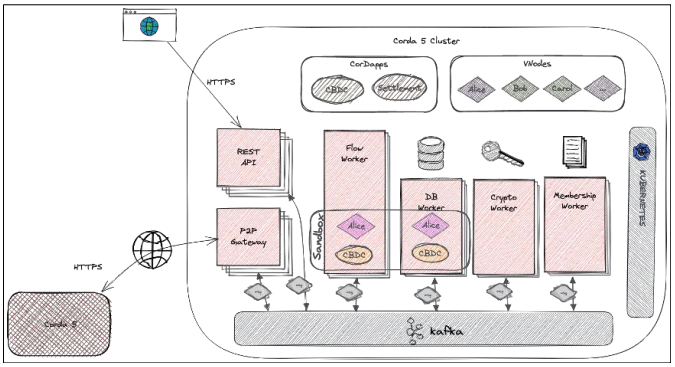


Figure 7: Corda Architecture. (Figure modified from Corda official document V5.0[29])

- **REST Workers**: They present the Corda REST API, which is utilized for management and flow operations.

3) *FISCO-BCOS:* FISCO BCOS[30], developed by the Financial Blockchain Shenzhen Consortium, is a consortium blockchain platform designed for financial institutions. It is a permissioned blockchain(underpinned by public blockchain) that supports private and public deployment models. It utilizes a multi-chain architecture that enables the partitioning of data and services to meet different business requirements. FISCO BCOS also provides a pluggable consensus mechanism, allowing for easy configuration and customization of consensus algorithms. Its smart contract system supports multiple programming languages and provides a variety of pre-built contract templates for common financial transactions. FISCO BCOS has been adopted by numerous financial institutions, including banks and insurance companies[31]. Figure 8 illustrates the architecture of FISCO BCOS.

The key transaction flows are listed:

1. The transaction process in the system begins with a user initiating a transaction through the SDK or curl command, which is then sent to the connected node.
2. Upon receipt of the transaction, the node checks if the current transaction pool (TxPool) is full. If it is not full, the node adds the transaction to the TxPool and propagates it to connected nodes. However, if the TxPool is full, the node discards the transaction and issues a warning notification to the user.
3. Periodically, the sealer draws transactions from the TxPool and packages them into blocks, which are then sent to the consensus engine.

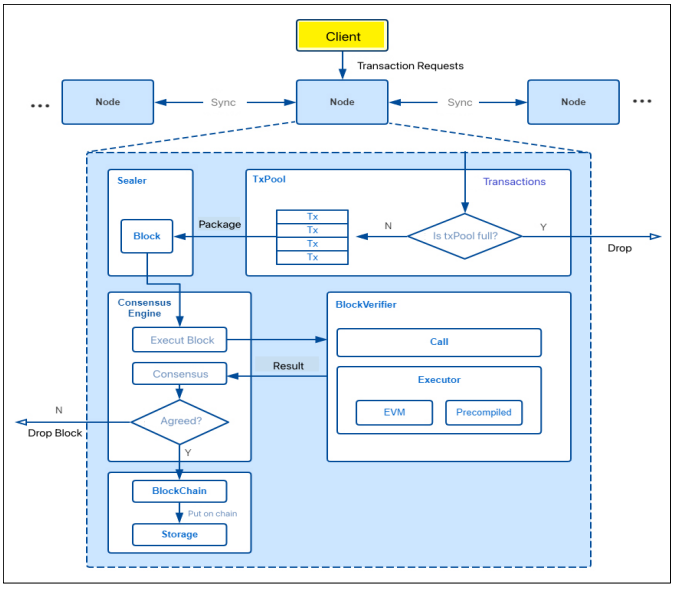


Figure 8: FISCO BCOS Architecture & Transaction Flow. (Figure modified from FISCO BCOS official document V2.x[30])

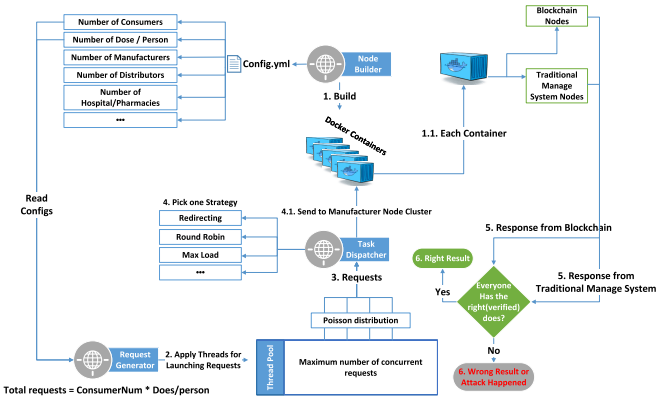


Figure 9: Functional Test Design.

4. The consensus engine is responsible for verifying the block and reaching a consensus on the block's contents among nodes in the network. To achieve this, the BlockVerifier is called to verify the block, and the Executor is called to execute every transaction within the block. Once the block is verified and agreed upon by nodes, the consensus engine sends it to the blockchain.
5. Upon receipt of the block, the blockchain checks the block information, such as block number, and inputs the block data and table data to the bottom storage. Finally, the block is appended to the blockchain.

### C. *Drug Lifecycle Simulator and Test Platform*

The testing platform, as shown in Figure 9, will cover the entire process from blockchain solution deployment to functional testing.

Firstly, Node Builder will generate various blockchain network nodes and traditional centralized information management system nodes (deployed in Docker containers) according to the configuration file. Then, the Request Generator will send requests, each request should contain the properties for drug production, distribution, consumption, and simulated attacks based on the configuration information, which will be processed by a thread pool and allocated to processing threads according to the pre-selected maximum request concurrency.

- Need 1/4 page more to present the drug lifecycle simulator properly.

Subsequently, Task Dispatcher will select a workload allocation strategy to distribute the requests to the corresponding service clusters of the supply chain nodes according to the Poisson distribution[32]. When these requests are received by the supply chain nodes, they will be processed separately using both the blockchain system and the traditional centralized system. Finally, the answers will be compared by the Discriminator, and if the results provided by the blockchain system are the same as those of the traditional solution, the request

will be deemed to be executed correctly; otherwise, it will be judged as a system error or illegal attack behavior.

In our test cases, a certain number of regular scenarios will be included, as well as attack simulation scenarios targeting various issues described in the previous chapter. This approach aims to evaluate the capability of the blockchain system to address all the issues described above.

## IV. Experiment Results

### A. *Functional Results and Analysis*

- Find a reasonable scale of supply chain participants and number of transactions.

### B. *Performance Results and Analysis*

System performance testing is also critical. Since blockchain systems add many security mechanisms compared to traditional database-oriented systems, we must ensure usable performance to avoid introducing additional security risks.

Based on Weyuker et al.[33] and Molyneaux et al.[34], we will collect Indicators listed for all three candidate consortium chain solutions.

1. Transaction Throughput (***TPS***): The number of transactions that can be processed per second.
2. Transaction Response Time (***TRT***): The time from submitting a transaction to its final confirmation.
3. Resource Utilization (***RU***): Measuring the utilization of resources such as CPU, memory, and network bandwidth in a blockchain system.

## V. Conclusions and Future Work

In this work, we summarized the main security challenges faced by the current pharmaceutical supply chain and reviewed some pioneering research. Subsequently, we proposed a blockchain-based pharmaceutical supply chain management solution with a unique DNA marker (physical-level anti-counterfeiting). We conducted functional and performance testing on several popular consortium blockchain frameworks to provide a highly valuable and feasible technical possibility. We hope to improve the quality and safety of drugs in the future.

## References


[1] Wikipedia, "Man-in-the-middle attack," 2023. [Online]. Available: https://en.wikipedia.org/wiki/Man-in-the-middle_attack

[2] S. Abdallah, and N. Nizamuddin, "Blockchain based solution for pharmacy supply chain industry," *Comput. & Ind. Eng.*, p. 108997, 2023.

[3] Food, and D. Administration(FDA), "Statement on the agency's ongoing efforts to resolve safety issue with arb medications," 2019. [Online]. Available: https://www.fda.gov/news-events/press-announcements/statement-agencys-ongoing-efforts-resolve-safety-issue-arb-medications

[4] J. Amankwah-Amoah, "Covid-19 and counterfeit vaccines: global implications, new challenges and opportunities," *Health Policy Technol.*, vol. 11, no. 2, p. 100630, 2022.

[5] B. B. Corporation(BBC), "Covid: police break up 'fake vaccine network' in china and south africa," 2021. [Online]. Available: https://www.bbc.com/news/world-africa-56270243

[6] A. Sahebi-Fakhrabad, A. H. Sadeghi, and R. Handfield, "Evaluating state-level prescription drug monitoring program (pdmp) and pill mill effects on opioid consumption in pharmaceutical supply chain," in *Healthcare*, vol. 11, 2023, p. 437.

[7] C. for Disease Control, and Prevention(CDC), "Understanding drug overdoses and deaths," 2022. [Online]. Available: https://www.cdc.gov/drugoverdose/epidemic/index.html

[8] P. Leach, M. Mealling, and R. Salz, "A universally unique identifier (uuid) urn namespace," RFC Editor, 2005. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4122.txt (Internet Requests for Comments)

[9] L. Jung, J. A. Hayward, and M. B. Liang, "Dna marking of previously undistinguished items for traceability," 2014. [Online]. Available: https://patents.google.com/patent/US20140272097A1/en

[10] T. M. Fernández-Caramés, and P. Fraga-Lamas, "A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories," *IEEE Access*, vol. 7, no. , pp. 45201–45218, 2019, doi: 10.1109/ACCESS.2019.2908780.

[11] B. Hammi, S. Zeadally, and J. Nebhen, "Security threats, countermeasures, and challenges of digital supply chains," *ACM Comput. Surveys*, 2023.

[12] Wired, "The untold story of notpetya, the most devastating cyberattack in history," 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[13] S. Sarkar, "Why pharmaceutical drug traceability in the us needs a centralized cloud-based platform," *Current J. Appl. Sci. Technol.*, vol. 42, no. 21, pp. 1–11, 2023.

[14] K. Zoughalian, J. Marchang, and B. Ghita, "A blockchain secured pharmaceutical distribution system to fight counterfeiting," *Int. J. Environmental Res. Public Health*, vol. 19, no. 7, p. 4091, 2022.

[15] M. Rehman, I. T. Javed, K. N. Qureshi, T. Margaria, and G. Jeon, "A cyber secure medical management system by using blockchain," *IEEE Trans. Comput. Social Syst.*, 2022.

[16] T. Hardin, and D. Kotz, "Amanuensis: provenance, privacy, and permission in tee-enabled blockchain data systems," in *2022 IEEE 42nd Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2022, pp. 144–156.

[17] M. Uddin, K. Salah, R. Jayaraman, S. Pesic, and S. Ellahham, "Blockchain for drug traceability: architectures and open challenges," *Health Inform. J.*, vol. 27, no. 2, 2021, doi: 10.1177/14604582211011228.

[18] A. El Azzaoui, H. Chen, S. H. Kim, Y. Pan, and J. H. Park, "Blockchain-based distributed information hiding framework for data privacy preserving in medical supply chain systems," *Sensors*, vol. 22, no. 4, p. 1371, 2022.

[19] L. Cui, Z. Xiao, F. Chen, H. Dai, and J. Li, "Protecting vaccine safety: an improved, blockchain-based, storage-efficient scheme," *IEEE Trans. Cybern.*, 2022.

[20] Y. Long, S. Rampazzi, T. Sugawara, and K. Fu, "Protecting covid-19 vaccine transportation and storage from analog cybersecurity threats," *Biomed. Instrum. & Technol.*, vol. 55, no. 3, pp. 112–117, 2021.

[21] FOLEY, "Types of blockchain: public, private, or something in between," 2021. [Online]. Available: https://www.jdsupra.com/legalnews/types-of-blockchain-public-private-or-5282575/

[22] S. Jabbar, H. Lloyd, M. Hammoudeh, B. Adebisi, and U. Raza, "Blockchain-enabled supply chain: analysis, challenges, and future directions," *Multimedia Syst.*, vol. 27, pp. 787–806, 2021.

[23] B. Kaur, M. Dugré, A. Hanna, and T. Glatard, "An analysis of security vulnerabilities in container images for scientific data analysis," *Gigascience*, vol. 10, no. 6, 2021.

[24] K. A. Clauson, E. A. Breeden, C. Davidson, and T. K. Mackey, "Leveraging blockchain technology to enhance supply chain management in healthcare:: an exploration of challenges and opportunities in the health supply chain," *Blockchain Healthcare Today*, vol. 1, Mar. 2018. [Online]. Available: https://www.blockchainhealthcaretoday.com/index.php/journal/article/view/20

[25] H. Howard, "Arc: analysis of raft consensus," University of Cambridge, Computer Laboratory, 2014.

[26] F. Muratov, A. Lebedev, N. Iushkevich, B. Nasrulin, and M. Takemiya, "Yac: bft consensus algorithm for blockchain," *Arxiv Preprint Arxiv: 1809.00554*, 2018.

[27] Hyperledger, "Fabric documents," 2023. Accessed: 2023. [Online]. Available: https://hyperledger-fabric.readthedocs.io/

[28] E. Androulaki, A. Barger, et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proc. Thirteenth Eurosys Conf.* in Eurosys '18, Porto, Portugal, 2018, doi: 10.1145/3190508.3190538. [Online]. Available: https://doi.org/10.1145/3190508.3190538

[29] Hyperledger, "Corda documents," 2023. Accessed: 2023. [Online]. Available: https://docs.r3.com/en/platform/corda/5.0.html

[30] FISCO, "Fisco-bcos documents," 2019. Accessed: 2019. [Online]. Available: https://fisco-bcos-documentation.readthedocs.io/en/latest/docs/design/architecture/transaction_stream.html?highlight=transaction\%20flow

[31] F. Ma, M. Ren, et al., "Security reinforcement for ethereum virtual machine," *Inf. Process. & Manage.*, vol. 58, no. 4, p. 102565, 2021, doi: https://doi.org/10.1016/j.ipm.2021.102565. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306457321000674

[32] Wikipedia, "Poisson distribution," 2023. [Online]. Available: https://en.wikipedia.org/wiki/Poisson_distribution

[33] E. J. Weyuker, and F. I. Vokolos, "Experience with performance testing of software systems: issues, an approach, and case study," *IEEE Trans. Softw. Eng.*, vol. 26, no. 12, pp. 1147–1156, 2000.

[34] I. Molyneaux, *The Art of Application Performance Testing: From Strategy to Tools*, " O'Reilly Media, Inc.", 2014.