Blockchain for drug traceability: Architectures and open challenges

Mueen Uddin
Khaled Salah
Raja Jayaraman
Khalifa University, UAE

Sasa Pesic
Arizona State University, USA

Samer Ellahham
Cleveland Clinic Abu Dhabi, UAE

Abstract
Pharmaceutical supply chain (PSC) consists of multiple stakeholders including raw material suppliers, manufacturers, distributors, regulatory authorities, pharmacies, hospitals, and patients. The complexity of product and transaction flows in PSC requires an effective traceability system to determine the current and all previous product ownerships. In addition, digitizing track and trace process provides significant benefit for regulatory oversight and ensures product safety. Blockchain-based drug traceability offers a potential solution to create a distributed shared data platform for an immutable, trustworthy, accountable and transparent system in the PSC. In this paper, we present an overview of product traceability issues in the PSC and envisage how blockchain technology can provide effective provenance, track and trace solution to mitigate counterfeit medications. We propose two potential blockchain based decentralized architectures, Hyperledger Fabric and Besu to meet critical requirements for drug traceability such as privacy, trust, transparency, security, authorization and authentication, and scalability. We propose, discuss, and compare two potential blockchain architectures for drug traceability. We identify and discuss several open research challenges related to the application of blockchain technology for drug traceability. The proposed blockchain architectures provide a valuable roadmap for Health Informatics researchers to build and deploy an end-to-end solution for the pharmaceutical industry.

Keywords
drug traceability, supply chain, blockchain architectures, healthcare IT, Hyperledger

Corresponding author:
Raja Jayaraman, Department of Industrial and Systems Engineering, Khalifa University, P O Box 127788, Abu Dhabi, UAE.
Email: raja.jayaraman@ku.ac.ae
Introduction

Counterfeit medications contribute to major public health concern that severely impact human lives and treatment outcomes. The World Health Organization (WHO) defines counterfeit medications as products that are deliberately and fraudulently mislabeled with respect to source and/or identity. Counterfeit drugs can contain insufficient, incorrect, erroneous ingredients, falsified information such as wrong labeling, and packaged incorrectly. WHO estimates that one out of ten medicines circulating in developing countries are either substandard or falsified, and approximately 1%–2% of all the drugs consumed are counterfeit in the developed nations.1,2

The global counterfeit drug trade impacts all pharmaceutical stakeholders including hospitals, pharmacies, wholesale distributors, global health programs, and regulatory authorities.3 The Illegal drug market contributes immensely toward producing fake and fraudulent medicines as its actors add contaminated, improperly stored, and falsified ingredients. This is enabled because there is a lack of technical and business solutions that offer adequate traceability and provenance solution.4,5 For example, a substandard version of the anti-cancer drug Avastin® was purchased and delivered to thousands of cancer patients in the U.S causing potential treatment complications for patients.6,7 The Asia Pacific, African, and Latin American regions are most vulnerable to counterfeit drugs with almost 30% of the drugs produced and consumed are counterfeit leading to almost 1.5 million deaths per year.8 In the European region the number of reported cases of counterfeit drugs have doubled compared to previous years.9 A recent report by a prominent European research project highlights that the counterfeit medication industry is considered more lucrative and profitable business than selling legal medicines and it estimates a revenue loss equals almost 4.5% in drug sales amounting to €10 billion every year.10–12

The increased access to medications via online pharmacies and unauthorized distribution channels makes it difficult to ensure product safety in the supply chain.13 In addition, limited data visibility about inventory and stock levels across the supply chain presents greater opportunities for counterfeits to enter the market.3,4 Drug traceability is the process of identifying the originality and legitimacy of the product that enables all stakeholders to track and trace the transactions at every stage in the supply chain.14,15 Regulations such as the US drug supply chain security act (DSCSA) requires all supply chain stakeholders to implement reliable measures that improve product traceability, the actual implementation of DSCSA will be in a phased manner by the year 2023.

Blockchain technology is a decentralized, distributed ledger system that provides an efficient and trusted solution for product traceability. Blockchain technology powers the crypto currencies and has been applied to variety of industries such as banking, supply chain, energy, commodities trading, healthcare and many businesses involving transaction processing. To deal with the issue of counterfeit drugs, blockchain technology has the potential to provide pragmatic solution for drug traceability and provenance in a secure and immutable manner. Blockchain technology enables the creation of a distributed shared data platform for storing and sharing the transaction data among various supply chain stakeholders ensuring the information remains accessible, immutable, transparent and secure via cryptographic techniques and accessible only to authorized parties. Thus, provides a proactive approach to track, detect, and manage counterfeits in pharmaceutical supply chains.

In this paper, we reflect on the potential and the limitations of blockchain technology for drug traceability. We describe the current blockchain enabled trends and describe two state of the art architectures, provide explanations on how these architectures are robust, secure, and scalable to provide better transaction privacy compared to existing solutions, and discuss potential opportunities for securing the pharmaceutical supply chain. The major contributions of our work are as follows:
• We discuss the reasons how the pharmaceutical supply chain benefits from a blockchain-enabled drug traceability solution.
• We highlight the key benefits of using blockchain solution for drug supply chain compared to existing solutions.
• We present two suitable blockchain architectures for drug traceability, Hyperledger Fabric and Besu private blockchains.
• We identify, enumerate, and discuss several future research challenges that may hinder the successful deployment of blockchain solutions in the drug supply chain.

The rest of this paper is organized as follows, in the next section we present an overview of drug traceability in healthcare. In section 3 we present and discuss two blockchain based architectures for drug traceability, in section 4 we discuss several limitations and open challenges pertaining to adoption of blockchain technology that need to be addressed for efficient drug traceability. In section 5, we present the conclusions and future work.

Overview of drug traceability in healthcare

In this section, we highlight potential issues related to drug traceability in the pharmaceutical supply chain with an emphasis on counterfeit drugs. A pharmaceutical supply chain follows an end-to-end process from sourcing the active medication ingredients (source) to manufacturing the final product (medication) distributed and delivered to patients (end-users). It is the primary responsibility of the supply chain members to distribute authentic and high-quality products at the right time as it directly influences the health and safety of patients. The current drug distribution, and delivery systems have grown immensely in scale and complexity. In addition, limited data visibility, lack clear ownership structure, diversity of stakeholders makes transaction verification difficult. The lack of an integrated view of the entire supply chain often requires centralized third-party solutions to collect and validate information.

Pharmaceutical supply chain comprises of several stakeholders (supplier, manufacturer, distributor, retailer, pharmacy, and patient), and product distribution often requires intricate packing, unpacking and repacking process, which makes drug provenance and traceability very complicated. Figure 1 illustrates a high level overview of various stakeholders and their relationship in the pharmaceutical supply chain. There are several factors attributed to the availability of counterfeits in the supply chain, some examples include importing substandard medicines without the approval of regulatory authority, poor manufacturing and storage practices, theft, and infiltration of deficient drugs. Different technology driven approaches such as bar codes, RFID tags, IoT, serialization, and e-pedigree have been adopted to enhance trust among stakeholders to improve product visibility in the supply chains. However, these solutions are centralized and have serious limitations when it comes to security, interoperability, privacy, and scalability toward preventing counterfeits in the supply chains.

Blockchain solutions for supply chain and logistics have recently gained enormous acceptance as they provide an immutable and transparent way to record transactions between non-trusting stakeholders. The main feature of blockchain technology is the ability to track and trace transactions of an asset using decentralized distributed ledger with cryptographically secured timestamped records, thus enabling the direct digital transfer and storage of transaction records without the involvement of third-party intermediary service providers. It enables us to create an immutable ledger for transaction processing among untrusted and physically distributed stakeholders across the pharmaceutical supply chain. Blockchain technology ensures an efficient and cost-effective solution that underpins different drug traceability functions and procedures to ascertain proper
Blockchain technology has the potential to be integrated with existing anti-counterfeiting solutions including RFID, NFC, QRC, and e-pedigree to provide interoperable and better-integrated solutions. The wider acceptance of blockchain based solutions in the pharmaceutical industry is evident based on several recent pilot projects involving major stakeholders is shown in Table 1.

Table 1. Blockchain based drug traceability pilots.

| Product and pilot participants | Type of solution | Platform |
|-------------------------------|------------------|----------|
| IBM, KPMG, Merck, Walmart IDLogiq | Blockchain approach for track and trace, Blockchain based authenticated intelligent medication management | Hyperledger, Private platform |
| MediLedger—Amerisource Bergen, McKesson, and drug manufacturers Genentech, Pfizer, Gilead | Blockchain based product verification system for salable returns | Permissioned, Enterprise, Ethereum, Hyperledger |
| TraceLink—over 22 participants including manufacturers, wholesalers, distributors | Digital recalls and interoperable blockchain network solutions | Hyperledger |
| Indiana university health and Wakemed health and hospitals | Blockchain based solution to track specialty medicines within and outside the providers network | Private platform |
| LedgerDomain—University of California Los Angles health | Blockchain based solution for counterfeit detection | Hyperledger |
| SAP Multichain—Merck, Amerisource Bergen, GSK, Amgen, Boehringer Ingelheim, McKesson, Novo Nordisk | Blockchain based verification of counterfeits and tracking of salable returns | Multichain |

Source: https://www.fda.gov/drugs/drug-supply-chain-security-act-dcsca/dcsca-pilot-project-program; https://www.multichain.com/blog/2019/10/sap-pharma-case-study-interview/
collaboration between mutually untrusted stakeholders and creates an unassailable and immutable
decentralized drug traceability system. These benefits help in standardization and regulatory
oversight across multiple countries and drug regulatory authorities via shared data exchange, to
achieve interoperable solutions based on several regulators such as Food and Drug Administration
(FDA) and European Medication Agency (EMA). In the next section, we propose two private
blockchain architectures for product traceability in the pharmaceutical supply chain.

Blockchain based architectures for drug traceability

In this section, we present and discuss two blockchain-based architectures to fulfil important require-
ments for drug traceability. The proposed architectures are based on two blockchain platforms namely,
Hyperledger Fabric and Hyperledger Besu as they provide higher degree of trust, decentralization,
transparency, privacy, security, data integrity, deployment, modularity and scalability when compared
to other blockchain platforms such as Ethereum, Quorum, BigChain, etc. These architectures can be
key enablers for creating private permissioned blockchain ecosystems where pharmaceutical stake-
holders and their end-users are registered, controlled, and regulated by a regulating authority or a
group of authorities/stakeholders. The two proposed architectures and their respective transaction
flows are described in the following subsections, followed by in-depth technical comparison.

Hyperledger Fabric architecture

Hyperledger Fabric is a platform providing distributed ledger solutions, underpinned by a modular
architecture delivering high degrees of confidentiality, resiliency, flexibility and scalability. It is an
enterprise grade DLT based on blockchain technology that uses smart contracts to enforce trust
between multiple parties. Hyperledger Fabric eliminates the concept of mining, but still keeps the
good properties of a typical cryptocurrency blockchain (such as Bitcoin, Ethereum) like: block
immutability, order of events determinism, prevention of double spending, etc. Hyperledger Fabric
has been confirmed to offer superior transaction throughput, up to several thousand transactions
per second. These characteristics, among other that will be described below, make Hyperledger
Fabric a perfectly suitable candidate for complex supply chain systems with multiple physical and
logical processes and parties. By using general purpose programing languages (Java, Go, NodeJS)
to develop smart contracts, the adoption bar for this technology is lower than for others using dedi-
cated programing languages (e.g. Solidity in Ethereum).

The Hyperledger Fabric drug traceability architecture proposed in this paper provides an initial
design of an enterprise-level blockchain-based supply chain system, where different stakeholders in
the pharmaceutical supply chain are identified, their relationships established using different channels
to provide maximum privacy, confidentiality, and data security. A concept of channels is unique to
Hyperledger Fabric. Channels offer clear separation of business logic and data privacy policies
between different stakeholders operating in the same system. By default, Hyperledger Fabric provides
a secure and transparent crash –fault tolerant transaction ordering for ensuring deterministic recording
of events, secure communication and reliable exchange of medication related transactions amongst a
group of untrusted stakeholders. This helps to create a consistent track-and-trace provenance system
to ward off counterfeit medications in PSC. The proposed blockchain architecture introduces a new
modular approach to provide high levels of flexibility, resiliency, scalability, and privacy.

In the proposed Hyperledger Fabric architecture a permissioned private blockchain network is
created where all the participating organizations (pharmaceutical stakeholders) and their end-users
are identified and registered by the Health Authority using the membership service provider (MSP)
component of Hyperledger Fabric. The MSP component is pluggable—it can be the Certificate
Authority (CA) offered by Hyperledger Fabric by default (local), or external (e.g. generate and use OpenSSL certificates, integrate with Active Directory, etc.). To create a trusted environment between untrusted participants, Hyperledger Fabric requires usage of an MSP (local or external) that creates rules and regulations by which different stakeholders (identities) are governed, authenticated, validated, and authorized to access blockchain resources. This ensures privacy and confidentiality of every stakeholder throughout the network and enables easy activity tracing (e.g. malicious transaction occurs). The MSP is a comprehensive novel design that revamps the process of non-determinism, resource exhaustion, and performance attacks in the participating stakeholders in the pharmaceutical supply chain by decentralizing identity management.

Finally, at the core of the Hyperledger Fabric architecture there are Peer nodes (peers) and the Ordering Service (OS). Peers store ledger copies, execute smart contracts (also referred to as chaincode in Hyperledger Fabric), endorse, and commit transactions. The OS accepts the endorsed transactions from client applications, orders them into blocks with cryptographic signatures of the endorsing peers, and finally broadcasts these blocks to the committing peers in the blockchain network for validations against the endorsement policies.

Drug traceability flow with Hyperledger Fabric. In this section, we describe how transactions in the pharmaceutical supply chain are executed and communicated between different stakeholders using the execute-order-validate transaction processing methodology typical for Hyperledger Fabric. This is shown in Figure 2. The steps taken to complete a transaction processing cycle in this architecture are described in detail and numbered below.

In the proposed Hyperledger Fabric architecture, initially, an organizational user (client app) from a registered organization such as supplier or manufacturer, submits a transaction proposal (Step 1). The transaction proposal is a request to invoke a chaincode function with certain parameters, with the intent of reading and/or updating the ledger (Step 2). This proposal is submitted to all endorsing peers, as determined by the chaincode endorsement policy (Step 3). To clarify, for every chaincode there is an endorsement policy stating which organizations, and by extent which peers, must sign/check every transaction for that chaincode. The transaction proposal consists of different parameters such as client’s cryptographic credentials (obtained from an MSP), the transaction payload including the name of the chaincode function to be executed with input arguments, and the channel and chaincode identifiers. The client app sends this proposal to a set of endorsing peers to get a consensus that the transaction is valid. This phase is called the proposal phase.

The transaction proposal is executed by a specific number of endorsing peers determined by the chaincode’s endorsement policy (Step 4). These results (also called endorsements), will be encrypted, and recorded along with endorsing peers’ cryptographic signatures and RW sets (read-set and writeset), and sent back to the client app, as a response to the transaction proposal submitted (Step 5). It is important to highlight that the client app continues collect endorsements until it satisfies the chaincode’s endorsement policy. No updates are made to the ledger at this point. This phase is called the endorsement phase.

When the client app received enough endorsement responses, it inspect them to determine if RW sets are the same, making sure the chaincode ledger was not updated in-between proposal and endorsement phases (Step 6). Next, the client app assembles and broadcasts the transaction proposal and responses within a transaction message to the Ordering Service (Step 7). This message contains a transaction with RW sets, endorsing peer signatures and channel identifier. The decentralized Ordering Service uses a pluggable consensus protocol to calculate and establish the execution order of all the submitted transactions per channel. The Ordering service chronologically orders multiple drug transactions into blocks, chaining the blocks’ hashes to previous blocks (Step 8). This phase is called the ordering phase.
The final phase is the execution phase. The OS broadcasts the newly-formed blocks to the leading peers in the Hyperledger Fabric network (Step 9). The leading peers are then in charge of disseminating the blocks to other committing peers within the organization using gossip protocol (Step 10). Leading peers are elected per organization and they are known to the Ordering Service. Peers check if the endorsements are valid according to the chaincodes’ endorsement policies’ and verify that the RW sets have not been violated since last checked (Step 11). If any endorsement is invalid or the RW sets do not match the current world state, the transaction is marked as invalid. Alternately, the ledger is updated and all peers append the transactions to the channels’ ledgers in the predefined order, ensuring determinism (Step 12). Valid transactions will update the world state. Invalid ones are retained on the ledger but do not update the world state. Finally, the client app that submitted the transaction proposal will be notified by each peer on the network of transaction success (Step 13).

Hyperledger Besu architecture

The proposed Hyperledger Besu drug traceability architecture provides a fully compatible open-source distributed ledger solution for enterprises looking for Ethereum-compatible blockchain architectures. Hyperledger Besu is gaining popularity among enterprises as it supports building networks supporting both private transaction processing and integration with public blockchains.
(Ethereum), while maintaining architectural flexibility and high transaction throughput. The proposed Hyperledger Besu architecture bridges the gap between private and public blockchains and helps pharmaceutical supply chain organizations to build scalable, high-performance applications on peer-to-peer private networks that fully support data privacy and complex permissioning management. Hyperledger Besu supports business logic through Solidity smart contracts, and can take advantage of using ERC20 tokens and Ether cryptocurrency.

Hyperledger Besu is an open-source Ethereum client. It provides a simple JSON-RPC API for running and managing Hyperledger Besu nodes and executing transactions. The proposed Hyperledger Besu architecture supports storing both private and public drug transaction execution information, which is required to implement an efficient drug traceability across the pharmaceutical supply chain between different stakeholders. The core components of Hyperledger Besu architecture, as shown in Figure 3, are Ethereum Virtual Machines (EVMs), EtherSign, and Orion nodes. Although it is revolving around a public blockchain, privacy, and permissioning are the two key features of Hyperledger Besu architecture. To create a permissioned private blockchain for the pharmaceutical supply chain, Hyperledger Besu allows creating specific organizations (stakeholders) and their users (nodes) with their associated network accounts (wallets/addresses). Hyperledger Besu uses the inherent Public Key Infrastructure (nodes are issued a private/public key pair) to sign

Figure 3. Hyperledger Besu blockchain architecture.
and verify transactions, and the node’s address as a unique identifier for the node. To separate business logic from key storage/management procedures, EthSigner is recommended be used in combination with Hyperledger Besu as an external wallet service provider. Upon receiving a transaction, EthSigner will generate a signature using the stored private key, then forward the transaction with the fully valid signature to the Ethereum client for inclusion to the blockchain.

To keep transactions private between involved stakeholders, Hyperledger Besu uses a Private Transaction Manager (PTM) such as Orion. PTMs that conform to the Enterprise Ethereum Alliance (EEA) Client Specification allows shared business logic in smart contracts to be made private to a limited number of participants, thus making all transactions and state associated with those smart contracts private as well. Orion, that is, native to Hyperledger Besu is such a PTM. Configuring a network that supports private transactions requires starting an Orion node for each Hyperledger Besu node. Lastly, to give access permissions to different organizational users and their accounts, Hyperledger Besu offers both on-chain (via smart contracts) and off-chain permissioning (via configuration files). A permissioned network enables node and account permissioning, making access to the network restricted to only specified nodes and accounts. Alongside, permissioning features of Hyperledger Besu allow real-time account suspension, denying access to broken smart contracts, restricting actions based on organization/account details, etc. This further enables secure and transparent communication on the network by easing the management of access control.

Drug traceability flow with Hyperledger Besu. In this section, we describe how medication-related traceability transactions are executed and communicated between different stakeholders on a Hyperledger Besu network. In the proposed Hyperledger Besu architecture, when an organizational user (client) wants to perform a transaction (execute a specific smart contract function or transfer assets), it initially submits a signed private transaction request through a Distributed App (DApp) to a Hyperledger Besu EVM node (Step 1). The signed transaction includes the list of recipients’ addresses or privacy group ID, sender address, type of transaction (e.g. restricted), etc. To clarify, a privacy group is a group of nodes identified by a unique privacy group ID by Orion. Orion stores each private transaction with the privacy group ID. The Hyperledger Besu nodes maintain the public world state for the blockchain and a private state for each privacy group. The private states contain data that is not shared in the globally replicated world state. Privacy groups enable access to certain data only to a group of accounts/nodes.

The DApp user interface uses JSON-RPC to send transactions to Orion (Step 2) through the Private Transaction Handler (PTH). Orion distributes the transactions to other Orion nodes specified by the privacy group ID or recipient addresses (Step 3). After receiving the transactions, Orion nodes will store them in the state database, and return the transaction hash value to the PTH (Step 4). Alongside private transactions, the PTM creates Privacy Marker Transactions (PMT) which are also mined into blocks and broadcasted (Step 5). The Mainnet Transaction Processor on every Hyperledger Besu node will process PMT, and on nodes that contain the corresponding private precompiled smart contract, the transactions are passed to the contract for execution (Step 6). This contract queries the Orion for the private transaction using the transaction hash value, and passes the transaction to the Private Transaction Processor, which executes the transaction and commits the read-write operations to the private world state to update all the participating nodes (Step 7). Nodes without the precompiled contract will ignore the marker transaction.

Technical comparison: Ethereum, Hyperledger Fabric and Hyperledger Besu

We present an in-depth technical comparison of the three blockchain platforms, highlighting their advantages and disadvantages. Although Ethereum can be setup as a private network, in this
comparison we will focus on it as a public network. Features for comparison were collected empirically, based on evidence from past research and development, as well as actual documentation and several ongoing projects. Table 2 aims to offer deeper insights into outcome of the comparison.

Compared to Ethereum, both Hyperledger Fabric and Besu are aimed to be used as private, permissioned Business-2-Business networks. Ethereum is rather Business-2-Customer oriented, with no inherent support for privacy groups or private data/transactions. Hyperledger Fabric and Besu support faster state reconciliation and offer superior transaction execution speed. Smart contracts in Hyperledger Fabric might be easier to develop since they use general-purpose programming languages, as opposed to Besu and Ethereum that use a domain-specific language. However, Hyperledger Fabric lacks a proper smart contract development framework that is available in both Besu and Ethereum (e.g. Truffle). Network configuration, setup, and deployment complexities are higher for Hyperledger Fabric, however it is easy to manage/update/upgrade since all components are Dockerized. Using Hyperledger Fabric also comes with increased client application responsibility, but increases the amount of control on the client side. Hyperledger Fabric is superior to both Besu and Ethereum for identity management and access control by having both physical (channels) and logical (chaincodes, certificate attributes) enablers to manage them. For the pharmaceutical traceability application both Hyperledger Fabric and Besu provide the best alternatives and features for effective trace and trace solution.

Discussion and open challenges

In this section, we briefly outline notable challenges in adopting blockchain based provenance, track and trace solutions in the pharmaceutical industry.

Stakeholder agreement

A blockchain network is a distributed ledger where all pharmaceutical supply chain stakeholders store their core business data and everyone has access to this sensitive private data on the platform. Potential stakeholders might be reluctant to participate in such networks since it could lead to losing their competitive advantage, especially when multiple business competitors exist in the same supply chain.38

Interoperability

Interoperability is defined as a mass adoption of business software and platforms across multiple organizations to provide efficient integration strategies. It serves as a means for users of different platforms and software’s to interact and conduct meaningful businesses seamlessly. The existing drug traceability solutions such as serialization, barcodes, RFID tags, and e-pedigree as well as blockchain-based solutions and platforms lack full interoperability as there are no standardized solutions to make integration, adaptability and implementation easier.39 Further, different blockchain platforms under the Hyperledger umbrella are coping with issues to provide interoperability, ensure maximum scalability and adaptability for enabling internal and external communication between business organizations.

Implementation cost

Designing the perfect blockchain application is not an easy task, since majority of the existing solutions are under development. The privacy, scalability, and interoperability challenges
Table 2. Comparison of Blockchain Platforms.

| Category        | Sub-category                    | Hyperledger Fabric                                                                 | Hyperledger Besu                                                                 | Ethereum Enterprise Alliance |
|-----------------|---------------------------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|------------------------------|
| General         | Governing bodies                | Originally contributed by IBM and Digital. Now governed by Linux Foundation         | Originally contributed by ConsenSys (PegaSys). Now governed by Linux Foundation  | Announced 2015, ~100 Geth client releases, nine hard forks, high-level maturity |
|                 | Maturity                        | Announced 2017, ~60 version improvements, high-level maturity                      | Announced 2019, ~30 version improvements, middle-level maturity                  | Public                       |
|                 | Intended manner of usage        | Private, permissioned                                                                | Semi-private                                                                    |                              |
|                 | Community of contributors       | ~200                                                                                 | ~60                                                                             | ~450                         |
|                 | Cryptography                    | Pluggable (ECDSA with secp256r1 and secp384r1 built-in)                             | secp256k1                                                                      | secp256k1                    |
| Network         | Network configuration complexity | Cryptographic materials dynamically grow with number of organizations, peers, and users | Requires configuring a genesis file and Orion configuration file per node (EthSigner optional). | Network is ready to be used immediately |
| management      |                                 | User-friendly command line libraries: cryptogen, configtxgen, configtxlator. High-complexity | Middle-complexity                                                              |                              |
|                 | Network deployment              | Using Docker and Docker Compose                                                     | Requires starting every Besu and Orion node through a simple command line command. Can be configured via Docker and Docker Compose | Network is publicly available |
|                 | Multiple ledgers                | Yes, via channels                                                                   | No concept of a chain (shared ledger)                                           | No concept of a chain (shared ledger) |
|                 | Running costs                   | Dynamic ledger size (storage inside Docker container).                                | Dynamic ledger size.                                                           | Archive – >4TB, 4GB RAM      |
|                 | breakdown                       | 1GB RAM per Peer                                                                    | 4GB for private network usage, 8GB for usage with public Ethereum networks (e.g. Ropsten) |
|                 |                                 | 2GB RAM per Certificate Authority                                                   |                                                                                  | Full node – 350GB SSD, 4GB RAM, Light node – 10GB, 4GB RAM |
|                 |                                 | 256MB RAM per CouchDB                                                              |                                                                                  |                              |
|                 |                                 | 512MB RAM per chaincode container                                                   |                                                                                  |                              |
|                 |                                 | 256MB RAM per Ordering Service node (RAFT)                                          |                                                                                  |                              |
|                 | Storage options                 | LevelDB                                                                             | File storage                                                                    | File storage                 |
|                 |                                 | CouchDB                                                                            |                                                                                  |                              |

(Continued)
| Category                     | Sub-category                      | Hyperledger Fabric | Hyperledger Besu                                                                 | Ethereum                                                                                     |
|-----------------------------|-----------------------------------|--------------------|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Transaction Execution       | Transaction consensus             | Unique Execute-Order-Validate methodology. Tolerating, instead of eliminating non-determinism | Order-Execute methodology. Every transaction execution must be deterministic. Clique and IBFT 2.0 Proof of Authority (Byzantine Fault Tolerance) | Order-Execute methodology. Every transaction execution must be deterministic. Ethash Proof of Work (Byzantine Fault Tolerance) |
|                             | Applied consensus protocols       | Kafka/Raft (Crash Fault Tolerance with trusted leader)     | Clique and IBFT 2.0 Proof of Authority (Byzantine Fault Tolerance)               | Fee is paid in Ether for smart contract deployment or transaction execution. Cost different for different networks Besu nodes are integrated with (public Ethereum, Ropsten, etc.) |
|                             | Cost/Fee                          | Only network running costs exist                           | Only network running costs exist                                                | Fee is paid in Ether. Higher fee indicates faster mining/confirmation time. $2.71 per transaction for September 24th, 2020 |
| Secure communication        | TLS support                       | Yes                                                            | Yes                                                                            | Yes                                                                                         |
| Identity and privacy        | Data privacy                      | Private data collections                                      | Privacy groups that can access private transactions                           | No support                                                                                   |
|                             | User and Node Permissioning       | Organization level: channels                                 | On-chain through smart contract                                                | No support                                                                                   |
|                             | Identity generation and management| Based on PKI. Organizational identity rather than individual identities used in consensus and permissioning. Management through Certificate Authority Or third party certificate provider | Of-chain through configuration files                                            | No support                                                                                   |
| Business logic              | Client application responsibility | Coordinating with other participants to obtain endorsement, managing optimistic concurrency locking on state, signature, and submission | Sending signed transactions to a single node in the network                     | Sending signed transactions to a single node in the network                                   |
| implementation complexity    | Smart contract execution engine   | Isolated inside Docker container                              | EVM (sandbox)                                                                 | EVM (sandbox)                                                                               |
|                             | Smart contract languages          | General purpose: Java, Go, NodeJS. Non-determinism is tolerated | Domain specific (Solidity), guaranteed deterministic. Frameworks: Truffle, Embark, OpenZeppelin, etc. | Domain specific (Solidity, Viper), guaranteed deterministic. Frameworks: Truffle, Embark, OpenZeppelin, etc. |
|                             | Smart contract lifecycle          | Requires installation on peers, instantiation in coordination with Ordering Service. Stored off-chain | Immutable, easy to deploy, and stored on-chain                                 | Immutable, easy to deploy, and stored on-chain                                              |
|                             | Smart contract upgrade            | Replacing code via an upgrade transaction (versioning), similar to initial contract deployment | Programing schemes to extend/migrate code and data                            | Programing schemes to extend/migrate code and data                                           |
|                             | Tokenization of digital assets    | No native support. FabToken token management system in Hyperledger Fabric 2.0 | Native feature with several token standards (ERC20, ERC721, ERC777 etc.)         | Native feature with several token standards (ERC20, ERC721, ERC777 etc.)                     |
| Integration with            | Services interaction              | Service interacts with an SDK (NodeJS, Java, Python, Golang) | Distributed Apps (DApps) interact with nodes. JSON-RPC over HTTP or WebSockets  | Distributed Apps (DApps) interact with nodes. Web3.js Ethereum JavaScript API. HTTP or IPC connection |
| Third party services        |                                   |                                                                                                           |                                                                                             |                                                                                             |
also contribute severely toward this issue. Implementation and energy costs are one of the leading challenges faced by majority of enterprises, including the pharmaceutical supply chain. The existing platforms and legacy software systems are inefficient and centralized when executing transactions, causing enormous implementation and maintenance costs. For example, Hyperledger Fabric can execute more than 3500 transactions per second and its power consumption is significantly reduced compared to Ethereum, due to different consensus protocols.

**Attacks and vulnerabilities**

One of the greatest advantages and selling points of blockchain technology is its resilience against various types of attacks, including cyberattacks. A recent cybersecurity report highlights several security risks, such as bad actors and man in the middle attacks, being involved in the blockchain network and exposing the vulnerabilities of the network. The current blockchain implementations are leaving inherent vulnerabilities and bugs due to the development of immature processes and systems. Phishing scams, technology vulnerabilities, implementation exploits, and malware, due to lack of standards and procedures, present serious challenges to be addressed in moving forward.

**Lack of standardized regulations**

The role of drug regulatory authorities includes quality checks and monitor the quality, safety, and efficacy and post market surveillance of pharmaceutical products. They often oversee the manufacturing, distribution, and storage of pharmaceutical products so that illegitimate manufacturing and trade of counterfeit medicine can be detected quickly and adequately sanctioned. In blockchain-based solutions, the role of regulatory agencies becomes more pertinent and complex as it becomes hard for these agencies to define the legal boundaries and environment for blockchain technology. For instance, when a new transaction is executed in the network, it is difficult for these authorities to clearly define the jurisdiction and correct legal obligations of the stakeholders involved. Another challenge is to cope with the requirements of upcoming legislations such as FDA DSCSA, sterilization, and GDPR in blockchain networks. Therefore, blockchain technology is still incompatible with recent laws and regulations regarding the pharmaceutical supply chain.

**Conclusions**

In this paper, we discuss how blockchain technology can be leveraged for drug traceability application in the pharmaceutical supply chain. We proposed two blockchain architectures based on Hyperledger Fabric and Hyperledger Besu. Such architectures provide a shared, trusted, permissioned and decentralized platform for storage and communications among different pharmaceutical supply chain stakeholders, and in a manner that can fulfill key requirements and features that include security, privacy, accessibility, transparency, and scalability. We present a comparison of the two platforms, and outlined a number of implementation challenges that hinder the wide spread adoption of blockchain technology for effective drug traceability. As future work, we plan to develop smart contracts, deploy the overall system components, and build user interface DApps of the proposed architectures.

**Declaration of conflicting interests**

The author(s) declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.
Funding
The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This publication is based upon work supported by the Khalifa University of Science & Technology under Award# CIRA-2019-001.

ORCID iDs
Raja Jayaraman https://orcid.org/0000-0002-2749-2688
Sasa Pesic https://orcid.org/0000-0003-4916-6506

References
1. Mackey TK and Liang BA. The global counterfeit drug trade: patient safety and public health risks. *J Pharm Sci* 2011; 100(11): 4571–4579.
2. Bichell RE. Fake drugs are a major global problem, WHO Reports. *NPR*, 29 November 2017, www.npr.org/sections/goatsandso/2017/11/29/567229552/bad-drugs-are-a-major-globalproblem-who-reports (2017, accessed 12 January 2020).
3. Venhuis BJ, Keizers PH, Klausmann R, et al. Operation resistance: a snapshot of falsified antibiotics and biopharmaceutical injectables in Europe. *Drug Test Anal* 2016; 8(3–4): 398–401.
4. Rosenthal ET. The “gray market” raises concerns about cost, safety, and ethics. *J Natl Cancer Inst* 2012; 104(3): 168–170.
5. Hemalatha R and Rao AS. Electronic solutions for combating counterfeit drugs. *J Pharm Bioallied Sci* 2015; 7(3): 230–232.
6. Mackey TK, Cuomo R, Guerra C, et al. After counterfeit Avastin—what have we learned and what can be done? *Nat Rev Clin Oncol* 2015; 12(5): 302–308.
7. Mackey TK, Kohler JC, Savedoff WD, et al. The disease of corruption: views on how to fight corruption to advance 21st century global health goals. *BMC Med* 2016; 14(1): 149.
8. Kovaes S, Hawes SE, Maley SN, et al. Technologies for detecting falsified and substandard drugs in low and middle-income countries. *PLoS One* 2014; 9(3): e90601.
9. European Alliance for Access to Safe Medicine-ESSAM. Counterfeit medicines, eaasm.eu/en-gb/counterfeit-medicines (2007, accessed 15 January 2020).
10. Parker RG and Sommer M (eds). *Routledge handbook of global public health*. Abingdon: Routledge, 2011.
11. Pharmaceutical Security Institute Website. Incident trends, www.psi-inc.org/incident-trends (2002, accessed 20 January 2020).
12. Plotnikov V and Kuznetsova V. The prospects for the use of digital technology “blockchain” in the pharmaceutical market. In: *MATEC web of conferences*, 2018, vol. 193, p.02029. EDP Sciences.
13. Clark F. Rise in online pharmacies sees counterfeit drugs go global. *Lancet* 2015; 386(10001): 1327–1328.
14. Alonso-Roris VM, Álvarez-Sabucedo L, Santos-Gago JM, et al. Towards a cost-effective and reusable traceability system. A semantic approach. *Comput Ind* 2016; 83: 1–11.
15. Haq I and Esuka OM. Blockchain technology in pharmaceutical industry to prevent counterfeit drugs. *Int J Comput Appl* 2018; 975: 8887.
16. Bocek T, Rodrigues BB, Strasser T, et al. Blockchains everywhere—a use-case of blockchains in the pharma supply-chain. In: *2017 IFIP/IEEE symposium on integrated network and service management (IM)*, Lisbon, Portugal, 8–12 May 2017, pp.772–777. New York, NY: IEEE.
17. Yang K, Botero U, Shen H, et al. A split manufacturing approach for unclonable chipless RFIDs for pharmaceutical supply chain security. In: *2017 Asian hardware oriented security and trust symposium (AsianHOST)*, Beijing, China, 19–20 October 2017, pp.61–66. New York, NY: IEEE.
18. Tseng JH, Liao YC, Chong B, et al. Governance on the drug supply chain via Gcoin blockchain. *Int J Environ Res Public Health* 2018; 15(6): 1055.
19. da Silva RB and de Mattos CA. Critical success factors of a drug traceability system for creating value in a pharmaceutical supply chain (PSC). *Int J Environ Res Public Health* 2019; 16(11): 1972.
20. Su S, Wang K and Kim HS. SmartSupply: smart contract based validation for supply chain blockchain. In: 2018 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018, pp.988–993. New York, NY: IEEE.

21. Mamoshina P, Ojomoko L, Yanovich Y, et al. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget 2017; 9(5): 5665–5690.

22. Han S, Bae HJ, Kim J, et al. Lithographically encoded polymer microtaggant using high-capacity and error-correctable QR code for anti-counterfeiting of drugs. Adv Mater 2012; 24(44): 5924–5929.

23. Clark B and Burstall R. Blockchain, IP and the pharma industry—how distributed ledger technologies can help secure the pharma supply chain. J Intellect Prop Law Pract 2018; 13(7): 531–533.

24. Benatia MA, Remadna A, Baudry D, et al. QR-code enabled product traceability system: a big data perspective. In: Thorvald P and Case K (eds) Advances in Manufacturing Technology XXXII. IOS Press, 2018, pp.323–328.

25. Metcalf DS, Bass J, Hooper M, et al. Blockchain in healthcare: innovations that empower patients, connect professionals and improve care. Boca Raton, FL: CRC Press, Taylor & Francis Group, 2019.

26. Hölbl M, Kompara M, Kamišalić A, et al. A systematic review of the use of blockchain in healthcare. Symmetry 2018; 10(10): 470.

27. Cachin C. Architecture of the hyperledger blockchain fabric. In: Workshop on distributed cryptocurrencies and consensus ledgers, 25 July 2016, vol. 310, no. 4. Zurich, Switzerland: IBM.

28. Alangot B and Achuthan K. Trace and track: enhanced pharma supply chain infrastructure to prevent fraud. In: International conference on ubiquitous communications and network computing, 2017, pp.189–195. Cham: Springer.

29. Francisco K and Swanson D. The supply chain has no clothes: technology adoption of blockchain for supply chain transparency. Logistics 2018; 2(1): 2.

30. Dai H, Ge L and Zhou W. A design method for supply chain traceability systems with aligned interests. Int J Prod Econ 2015; 170: 14–24.

31. Gorenflo C, Lee S, Golab L, et al. Fastfabric: scaling hyperledger fabric to 20,000 transactions per second. In: 2019 IEEE international conference on blockchain and cryptocurrency (ICBC), May 2019, pp.455–463. New York, NY: IEEE.

32. Sousa J, Bessani A and Vukolic M. A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. In: 2018 48th annual IEEE/IFIP international conference on dependable systems and networks (DSN), Luxembourg, 25–28 June 2018, pp.51–58. New York, NY: IEEE.

33. Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the thirteenth EuroSys conference, 2018, pp.1–15. New York, NY: Association for Computing Machinery.

34. Hyperledger. Hyperledger/fabric. GitHub, 21 January 2020, github.com/hyperledger/fabric (2020, accessed 21 January 2020).

35. Hyperledger Besu. Besu Enterprise Ethereum client, besu.hyperledger.org/en/stable/ (2020, accessed 15 January 2020).

36. Hyperledger Besu. Using wallets for key management, https://besu.hyperledger.org/en/stable/HowTo/Send-Transactions/Account-Management/ (2020, accessed 25 September 2020).

37. Nevele C and Polzer G (eds). Enterprise Ethereum alliance client specification v6. https://entethalliance.github.io/client-spec/spec.html (2020, accessed 10 September 2020).

38. Zhang A and Lin X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. J Med Syst 2018; 42(8): 140.

39. Dagher GG, Mohler J, Milojkovic M, et al. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain Cities Soc 2018; 39: 283–297.

40. Blockchain Threat Report-Mcafee.com. www.mcafee.com/enterprise/en-us/assets/reports/rp-blockchain-security-risks.pdf (2018, accessed 21 January 2020).