PharmaSync: Optimizing Security and Transparency in Pharmaceutical Supply Chains using Decentralized Hybrid Blockchain

Jitesh Sureka
Institute of Information Technology
University of Dhaka
Dhaka, Bangladesh
bsse1115@iit.du.ac.bd

Mustahid Hasan
Institute of Information Technology
University of Dhaka
Dhaka, Bangladesh
bsse1114@iit.du.ac.bd

Ahmed Adnan
Institute of Information Technology
University of Dhaka
Dhaka, Bangladesh
bsse1131@iit.du.ac.bd

Samudra Gupta
Institute of Business Administration
University of Dhaka
Dhaka, Bangladesh
samudragupta06@gmail.com

Tasmia Zerin
Institute of Information Technology
University of Dhaka
Dhaka, Bangladesh
bsse1128@iit.du.ac.bd

Shafiq-us Saleheen
Institute of Information Technology
University of Dhaka
Dhaka, Bangladesh
bsse1125@iit.du.ac.bd

***Abstract*—The pharmaceutical industry depends on a complicated supply chain with numerous participants to make sure that pharmaceuticals are delivered to patients without a hitch. This supply chain, however, suffers a number of difficulties, such as a lack of confidence, drug fraud, sudden medicine shortages, product recalls and compliance problems. We suggest PharmaSync, a blockchain based solution that guarantees transparency for the general public while safeguarding the trade secrets of pharmaceutical companies involved in the pharmaceutical supply chain process. To address these issues-**

PharmaSync ensures privacy through zero-knowledge proof algorithms, establishes stakeholder transparency, prevents drug counterfeiting through traceability and regulatory compliance, improves product recall management, lowers costs, and improves compliance by utilizing blockchain technology. The solution makes use of a number of modules, including recall management, compliance data verification, fine-grained user access control, inter-supply chain participant verification, decentralized identity management, and data authenticity assurance using digital signatures. PharmaSync's deployment seeks to raise patient safety, protect brand reputation, and boost the pharmaceutical supply chain's overall effectiveness.

***Index Terms*—pharmaceutical supply chain, blockchain technology, transparency, privacy, drug counterfeiting, emergency drug shortages, product recalls, compliance**

I. Introduction

The pharmaceutical industry comprises a complex supply chain characterized by several stakeholders where the delivery of medical goods to end users must be seamlessly transferred through various entities. This involves the process of locating raw materials, producing, distributing, and delivering medications to patients. [1] Pharmaceutical supply chain management consists of the strategic coordination between the full value-added process of a product (pharma value chain) and logistics.

There's little margin for error in most supply chains, but none in the pharmaceutical supply chain. There are many challenges that the pharmaceutical supply chain faces, including a lack of trust and transparency among stakeholders. Patient safety is put at risk when drug counterfeiting occurs. Safeguarding privacy and protecting trade secrets pose significant challenges as well. During times of emergency, patients may not have access to essential medications. Product recalling costs money and reduces consumer trust. It is challenging to trace the source of problems inside the supply chain, which makes prevention measures tough. Poor cold storage management puts patients' safety and drug integrity at risk. It is essential to put in place reliable mechanisms that encourage accountability, traceability, privacy, and transparency throughout the pharmaceutical supply chain. Considering all the aforementioned challenges, we propose PharmaSync, a solution that ensures transparency for mass, and maintains trade secrecy for drug companies in the medicine supply chain process.

II. Objective

Blockchain technology can be effective in the pharmaceutical sector, where supply chain coordination, integrity, and transparency are crucial for the delivery of safe and efficient products. Blockchain systems have the ability to pinpoint the origin of data which makes them particularly suitable for ensuring traceability by effectively identifying the specific stakeholder responsible for a particular issue or problem. Therefore, the objectives of the project are:

- To ensure privacy and protect trade secrets using ZK proof using zkSnark algorithm and other efficient encryption techniques
- Establish transparency throughout the supply chain to improve the communications and coordination amongst the supply chain stakeholders
- Prevent drug counterfeiting by ensuring traceability and strict adherence to regulatory compliances
- Monitoring regulatory compliance in the supply chain by monitoring adherence to the laws, regulations, and guidelines so that the safety, efficacy, and quality of pharmaceutical products throughout the supply chain is assured.
- Implement strategies to mitigate emergency drug shortages, prevent product recalls, ensure effective cold chain management, and uphold optimal cost-effectiveness while maintaining brand equity.

III. Problems

The traded value of pharmaceutical supply chains has expanded over the past 20 years as a result of the globalization of the pharmaceutical sector, from $113 billion in 2000 to $629 billion in recent times [2]. According to Data Bridge Market Research, the pharmaceutical logistics market is predicted to grow from USD 227.45 billion in 2022 to USD 446.61 billion by 2030, at a CAGR of 8.8% from 2023 to 2030 [3]. In a survey conducted by Usp.org, 90% of doctors expressed concern that the global medicine supply chain might not be dependable and trustworthy in times of emergency [4]. The pharmaceutical supply chain has a number of difficulties that may have a big influence on patient safety and privacy, medication access, and overall healthcare delivery.

A. Privacy Concerns and Issues Surrounding Trade Secrets

A pharmaceutical supply chain can suffer severe damage from privacy and trade secret breaches because they can compromise sensitive patient data, undermine competitive advantage, and erode stakeholder confidence. On December 10, 2021, BioPlus reported a hacking breach on or around October 25, 2021, impacting a network server and exposing the PHI of 350,000 individuals, including names, contact information, dates of birth, medical record numbers, health insurance and claims information, diagnoses, prescription details, and Social Security numbers. [13]

B. Drug Counterfeiting

Drug counterfeiting is a serious threat to the pharmaceutical supply chain, which also jeopardizes patient safety, erodes public confidence in medicines, and compromises the reliability of the entire healthcare system. The annual sales of adulterated or substandard drugs in Bangladesh are estimated to exceed Tk1,500 crore, accounting for 20% of total sales. [5] In many developing countries, including those in Africa, Asia, and South America, counterfeit medicines constitute a significant portion, ranging from 10% to 30% of all medicines on the market. [6] (Fig. 1)

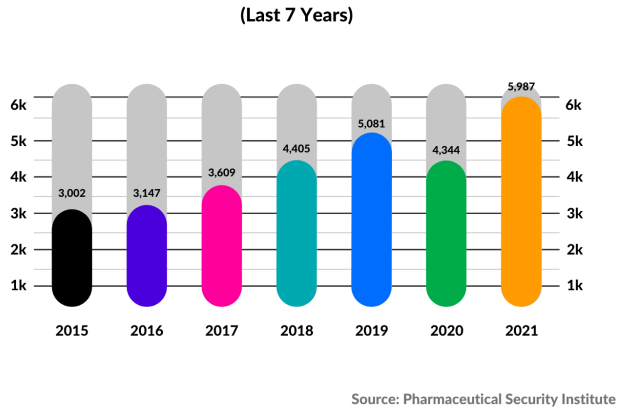

Fig. 1. Total number of counterfeit incidents concerning pharmaceuticals worldwide

C. Emergency On Drug Shortage

Emergency drug shortages pose serious problems for the pharmaceutical supply chain because they prevent timely access to life-saving drugs which jeopardizes patient health and safety. The following table is a case study on five drugs which shows the change in volume and price in comparison to substitutes during drug shortage. (Fig. 2)

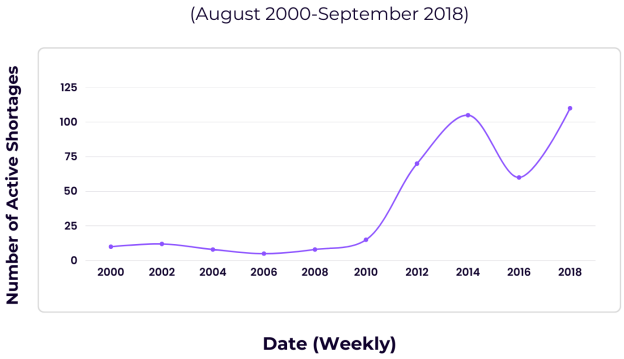

Fig. 2. FDA Active Drug Shortages

D. Product Recalling

Product recall in the drug supply chain refers to the process of removing and retrieving pharmaceutical products from the market due to safety concerns or regulatory violations. According to FDA (US Food and Drug Administration) statistics, 14,000 drug recalls happened in the last 4 years. That averages out to nearly four drug recalls a day. A consumer study found that 15% of consumers would never purchase a recalled product and 55% of consumers would switch brands after a recall, regardless of whether it was merely temporary. [8] (Fig. 3)

E. Cold Chain Management

Due to the stringent temperature requirements for drug storage and transportation, cold chain management in the

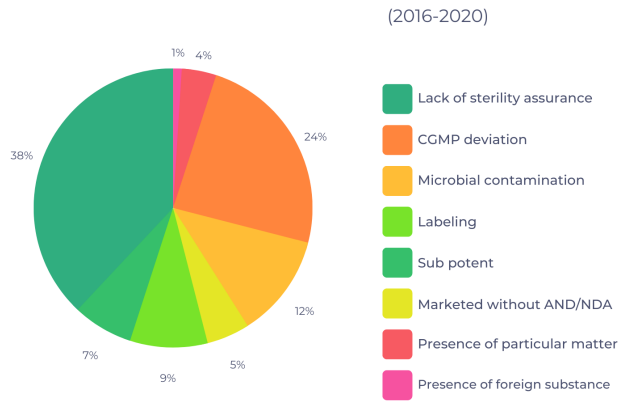

Fig. 3. Different causes of major recall in five years (2016-2020)

pharmaceutical supply chain presents a considerable challenge. According to SDCExecutive, CDC statistics from the first quarter of 2021 indicated a 20% loss of the Covid vaccine owing to problems with the cold chain. According to the IQVIA Institute for Human Data Science, supply chain temperature control issues cost the biopharmaceutical industry $34 billion yearly [10].

F. Cost and Compliance Issues

The pharmaceutical supply chain deals with many government compliance and cost-related issues. Regulation changes entail numerous compliance obligations that raise complexity and costs such as failure to follow written procedures, failures in laboratory controls, SOP(Standard Operating Procedures).

The conventional pharmaceutical supply chain systems face the following challenges:

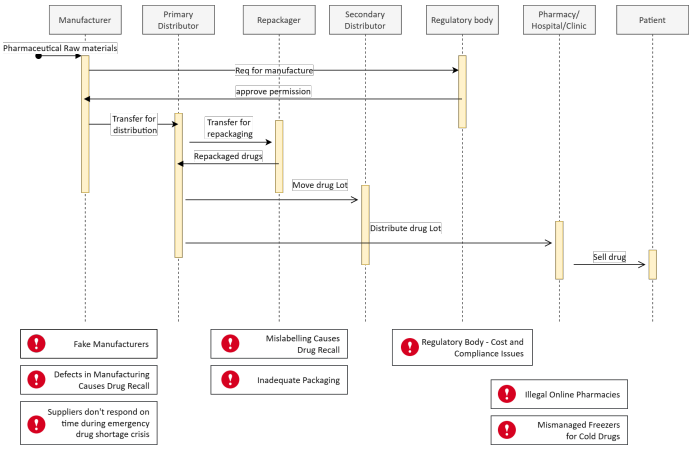

Fig. 4. Conventional pharmaceutical supply chain challenges

IV. Solution

Despite the fact that cutting-edge technologies have made exceptional progress against corruption and developing public transparency, the issues with the existing mechanisms still exist. We propose to apply blockchain technology within supply chain management procedures and contrast it to the current ones because blockchain technology has been developed and designed to achieve integrity, transparency, efficiency, and data accuracy, goals that are highly valued in supply chain management. We also aim to keep the integrity of the trade secrets within the supply chain.

A. Solution Overview

Our solution consists of a few modules, which are:

- Seamless end-to-end and secured data sharing pipeline for supply chain management system: Using Zero-knowledge proof, our solution aims to optimize the multi-party trust assurance, verification, and accessibility, thus tackling SDG Goal 17: Partnerships for the Goals, referring to the supply chain stakeholder collaboration.
- Fine-grained user access control: Using a Hybrid blockchain with public transparency and permissioned control, our solution meets SDG 9: Industry, Innovation, and Infrastructure. It issues and verifies credentials of supply chain stakeholders at operational levels with immutable certificates.
- Privacy-enhanced Decentralized Identity (DID) infrastructure solution using Hyperledger Aries, Indy, and Ursa: Decentralized identity is a type of identity management that allows people to control their own digital identity without depending on a specific service provider.
- ZkKYC submodule for inter-supply chain participant identification and verification: In 2021, financial institutions spent an estimated $37.1 billion on AML-KYC compliance technology and operations. This submodule also serves SDG 12: Responsible Consumption and Production.
- IoT integration to measure supply chain products, such as temperature and humidity: Our solution aims to provide an optimal recall management system with early fault detection and control counterfeiting. Since the value of the counterfeit drug market annually is $200 billion, our solution helps meet SDG 3: Good Health and Well-being.
- Recall management system to ensure efficient traceback and elimination of defective products from the market within minimum time and resources, meeting SDG Goal 8: Decent Work and Economic Growth. The number of U.S. products recalled this year has already surpassed 1 billion.
- Ensuring compliance data accessibility and verification by issuing soul-bound NFT (Non-Fungible Token) for the compliance data, ensuring SDG Goal 16: Peace, Justice, and Strong Institutions. Additionally, the total number of FDA warning letters referencing data integrity deficiencies has increased significantly in recent years.
- Ensuring authenticity of user-uploaded data using the Schnorr digital signature: The Schnorr digital signature is a highly efficient and compact digital signature enabling other users and the system to verify the authenticity and integrity of the data.

B. Current Issues and Proposed solution: PharmaSync

The traditional pharmaceutical supply chain system faces issues such as data privacy, lack of transparency, drug shortages, frequent recalls, inadequate temperature monitoring, and increased regulatory compliance burdens. Table-1 has given the issues with the current process along with the benefits of our proposed solutions.

V. Market

Inactive compounds, fluctuating active ingredients, or active ingredients that are more potent than the original constituents can all be found in counterfeit medications. Because these medications are so common, one of the biggest issues in the healthcare industry is the issue of counterfeit drugs. From 2022 to 2029, the global Counterfeit Drug Detection Device Market is anticipated to grow significantly at a 4.0% CAGR, with a projected market value of over US$1.14 Bn in 2022. According to Future Market Insights' predictions, counterfeit chemical composition detection devices will retain a sizable market share of roughly 60.6% in 2021. [16]

The anticipated market size for the global Counterfeit Drug Detection Device market in 2023 would be based on the supplied CAGR of 4.0%.

It is predicted that healthcare systems must spend at least $359 million annually on labor resources and $200 million annually on alternative therapies to manage or reduce shortages. The US market is the only one where this applies. This element could not be the subject of any workable study for low- and middle-income nations. We will therefore determine how much the US healthcare system spends on medicine shortages relative to the total amount spent on healthcare globally, which will provide us with a rough estimate and enable us to comprehend the gravity of this problem on a worldwide level. [17] The United States spent 17.8% of its GDP on health care in 2021, about twice as much as the typical OECD nation. [18] Global labor resource expenditure is equal to US labor resource expenditure multiplied by the US share of global healthcare expenditure. Spending on labor resources worldwide is $359,000,000 x 0.18 = $64.62,000,000 Global healthcare spending equals US healthcare spending plus the ratio of US healthcare spending to global healthcare spending. Spending on alternative medicine worldwide is $200 million times 0.18, or $36 million. We arrive at a net financial impact of $659.62 million after this calculation.

Drug development is a lengthy and time-consuming process that costs millions of dollars and takes, on average, 10 to 15 years of valuable time. If any drugs are later recalled, this reduces the company's market share and causes significant financial loss, as was the case with the recall of metformin extended-release use for type 2 diabetes mellitus due to lupin effects. is the sale of two generic drugs, Fortamet and Glumetza, for $25 and $15 million respectively to our FY21 and FY22. Analysts estimate that its sales in the USA were between $25 and $40 million in FY20, although accounting for only 3% to 5% of its overall revenue. [21] Sales losses of $25 million in FY21 and $15 million in FY22 are anticipated as a result of the recall of generic versions of Fortamet and Glumetza. Since the loss can differ from company to firm, we will use this example as a baseline in our calculations. Additionally, we do not accept the loss of having our brand's reputation destroyed as a result of such events, which may give rise to arguments. The average loss amount, which is $20 million for a single company, will be utilized in the calculation to show the size of the whole market for our product. 1039 drug recall instances were reported in 2020, bringing the total to roughly $20.7 billion. [19]

The cost of supply chain temperature control difficulties to the bio-pharmaceutical industry is $34 billion annually, according to the IQVIA Institute for Human Data Science.

We were unable to locate any relevant and practical studies to use as a frame of reference with regard to compliance and regulatory difficulties. However, if used, our technology will significantly advance the collection of accurate data about these problems. All of these figures and statistics add up to a

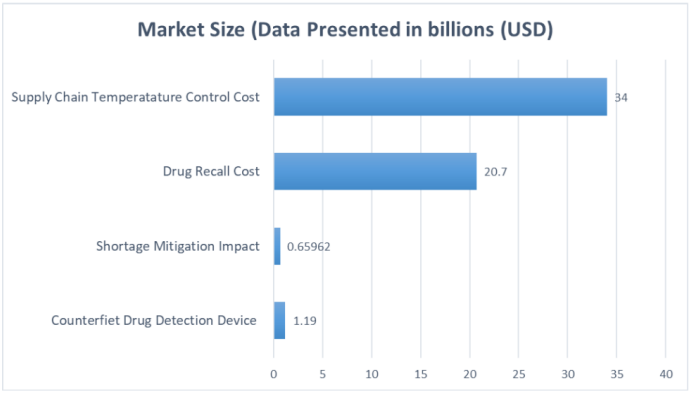

Fig. 5. Market size of issues in pharmaceutical supply chain

TAM (Total Addressable Market) of US$ 56.55 billion.

60% of experts in the pharmaceutical and life science fields are currently either using blockchain or experimenting with it, according to the non-profit organization The Pistoia Alliance. Companies who are prepared for blockchain technology would be our main focus. As a result, the size of our SAM (Serviceable Addressable Market), or around US$ 33.93 billion, would be 60% of US$ 56.55 billion. [20]

The SOM (Serviceable Obtainable Market) is US$1.0179 billion if we choose to take 3% of the market share.

It presently contributes approximately 1.83 percent of Bangladesh's GDP and has a market value of about $3 billion, which helps the nation's pharmaceutical sector. The Directorate General of Drug Administration (DGDA) said that Bangladesh now has 257 licensed pharmaceutical firms. As a result, 150 factories are carrying on as usual and satisfying around 98% of the nation's overall demand. Currently, local companies control 90% of the nation's overall pharmaceutical market, and global corporations control the remaining 10%. Currently, Bangladesh produces 4% of the nation's anti-cancer treatment needs and more than 450 generic medications for 5,300 registered brands. Approximately 80% of the pharma-

TABLE I
PHARMASYNC AS A SOLUTION TO CURRENT ISSUES

Steps	Current Process	Issues with Current Process	Proposed Process	Benefits of Proposed Process
1	Inadequate protection of private data	It results in numerous breaches over the years, causing privacy and security issues	PharmaSync proposes to use a private chain to secure trade secrecy and keep the internal transaction information safe	Stakeholders of the company get the security of their product formula, supply chain lifecycle, trade secrecy, and safe transformation
2	Insufficient transparency measures allow for the presence of adulterated or substandard drugs, costing 20% of total sales	It poses threats to patient safety, public trust with medications, and overall integrity	PharmaSync keeps track of the real-time data of supply chain transactions with hedera consensus service	Transparency with regulatory bodies, companies can make early damage control to the pharmaceutical supply chain. This could also reduce recall management issues
3	Due to a lack of monitoring activity, drug shortage occurs for essential medications	It compromises reliable access to necessary drugs, including supply chain disruption	Every supply chain stakeholder can access the real-time data of movement in the supply chain	Real-time and reliable access by stakeholders leads to proper inventory tracking
4	High frequency of drug recalls makes the current chain ineffective in resolving issues	It causes consumer distrust, as 15% of them refuse to buy products and 55% switch brands, even if the recall is temporary	Product quality data is public, and regulatory bodies and the general public can verify its authenticity	Since product quality data is updated at every chain movement, most defective products can be identified within the chain before launching them
5	No monitoring devices are available to track temperature-sensitive drugs whatsoever	Due to issues such as vaccines, failure to provide the required conditions leads to $34 billion in losses annually	IoT integration with the blockchain system enables the government and stakeholders to monitor the real-time condition of temperature and humidity of drugs	Companies can monitor their product's condition in real-time. Integration with the regulatory body reduces time, cost, complexity, and middlemen
6	Regulatory changes introduce complex compliance obligations and increased expenses	It forces the supply chain to struggle to balance cost management and regulatory adherence	The compliance and regulatory data are updated by the manufacturer, and regulatory bodies can verify its correctness	Verifying the correctness of compliance saves the company time by reducing approval processes, and regulatory bodies can also verify its authenticity

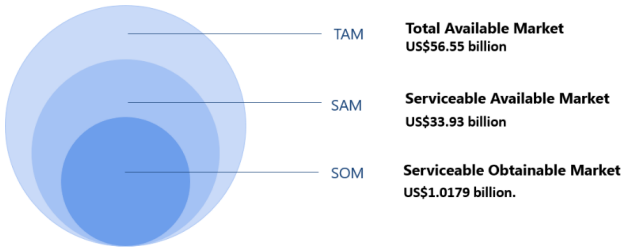

Fig. 6. TAM SAM SOM analysis of PharmaSync

ceuticals now produced in Bangladesh are generic medicines, with the remaining 20% being proprietary medicines. In addition, Bangladesh is the only LDC that fulfills approximately 98 percent of its own internal demand for pharmaceuticals. [22]

On the other hand, other calculations indicate that the volume of fake drugs being sold on the open market at any given moment may be as high as 2,500 crore taka, or around 233.64 million US dollars. Even if we factor in this amount, there is a sizable market for a product like PharmaSync, which may relieve businesses of the strain and support the saving of lives. [23]

As a result, it can be said that a blockchain system like PharmaSync has enormous potential and, if used, could completely transform the pharmaceutical sector in Bangladesh.

VI. PARTNERS

The key partners associated with PharmaSync are DGDA, BAPI, and Healthcare IT providers. This section discusses the organizational introductions, roles, and incentives of these partner organizations.

DGDA

The Ministry of Health and Family Welfare is home to Bangladesh's top drug regulation body, Directorate General of Drug Administration (DGDA). [24] With the primary regulatory authority, we shall collaborate. Since one of our services is assisting businesses in adhering to legal and regulatory requirements, collaboration with this organization will speed up the uptake and acceptance of blockchain solutions.

BAPI

The top organization for representing Bangladeshi pharmaceutical firms is the Bangladesh Association of Pharmaceutical Industries (BAPI). [25] The organization works to ensure that good manufacturing procedures (GMP) are understood and correctly applied to guarantee the quality of the medications. The goal of PharmaSync is to transform the pharmaceutical sector and bring about improvements for everyone. As a result, a relationship with BAPI will validate us and open doors to pharmaceutical firms. Since our visions are absolutely in line, they will also be interested in implementing PharmaSync.

Healthcare IT Providers

Healthcare businesses frequently use well-established systems and platforms that are provided by healthcare IT compa-

nies. By collaborating with them, PharmaSync is able to effectively incorporate its blockchain technology into the current healthcare IT infrastructure, facilitating data interchange and interoperability between various systems. PharmaSync may make use of its current clientele, knowledge, complementing features, and support abilities. The adoption, integration, and success of healthcare IT will be accelerated by this partnership.

VII. Competition

Since our product covers and addresses many issues currently faced by the pharmaceutical industry, there are competitors that we need to take into account before going further with our product. Here are some notable ones –

- MediLedger: In order to improve supply chain integrity and interoperability in the pharmaceutical sector, MediLedger is a blockchain-based platform. It emphasizes medicine tracking, verification, and regulatory compliance. [28]
- IBM Blockchain: IBM has been actively involved in blockchain solutions for the pharmaceutical industry. Their offerings include the IBM Blockchain Platform, which can be leveraged for supply chain transparency, drug provenance, and clinical trial data management. [29]
- FarmaTrust: FarmaTrust is a company that utilizes blockchain technology to address drug counterfeit issues. Their platform provides traceability and verification solutions to ensure the authenticity and integrity of pharmaceutical products. [30]
- Blockpharma: Blockpharma is a blockchain-based platform that aims to fight against counterfeit drugs by ensuring drug traceability and authenticity. They utilize blockchain technology to provide a decentralized and secure ledger for tracking pharmaceutical products. [31]
- Smart Software Solutions: It is a Bangladeshi startup that offers solutions to improve product sales features, inventory management, barcode generation, barcode scanning, retail management, return tracking, etc. [32]
- PharmaSolutions Bangladesh Ltd: PharmaSolutions is a Bangladeshi-based company that claims to utilize trade return management and relabeling management. Their services also involve product registration, patient order management, and consultancy [33].
- MediSoft Bangladesh Ltd: MediSoft is a Bangladeshi-based company that streamlines and automates the processes of wholesale trade and distribution companies. It facilitates seamless communication between manufacturers and retailers, optimizing business processes and enhancing customer relationships in the pharmaceutical supply chain [34].

It is important to note that while several existing blockchain solutions in the pharmaceutical industry address certain issues, none of them provide a comprehensive solution that encompasses all the challenges we aim to tackle with PharmaSync. Our revolutionary product, PharmaSync, offers a unique and comprehensive approach to addressing the various issues plaguing the pharmaceutical sector.

PharmaSync goes beyond existing solutions by providing a holistic platform that tackles multiple pain points in the industry. From drug traceability and supply chain management to authentication, anti-counterfeiting, data privacy, and compliance, PharmaSync offers an all-in-one solution that seamlessly integrates with existing systems and processes.

VIII. Risks

A. Business Risks

We applied the Porter Five Forces Framework to analyze PharmaSync's competitive environment. The following image shows how moderate the competitive rivalry for PharmaSync will be. It's likely that PharmaSync will face opposition from other blockchain-based solutions. The nature of this competition will vary depending on where in the world you are. PharmaSync will face less intense rivalry in nations where blockchain adoption is still at a low level. PharmaSync, on the other hand, will need to deal with competition before entering the market in nations where blockchain solutions are accessible.

Fig. 7. Porter's five forces analysis model

B. Technical Risks

Implementing a blockchain-based pharmaceutical supply chain solution introduces several technical and implementation risks. Firstly, utilizing blockchain technology carries inherent risks such as scalability limitations, the potential for network congestion, and the need for consensus mechanisms that may impact performance. These challenges can arise due to the distributed nature of the blockchain network and the computational requirements of cryptographic algorithms. Secondly, integrating various tools, technologies, and frameworks, such as Zero Knowledge Proofs, ZK-KYC, and Schnorr Digital Signature, the use of several identity management technologies and libraries may introduce complexity and compatibility issues, leading to development and integration challenges. Additionally, the reliance on external IOT devices, decentralized filed storage and management, the management of both on-chain and off-chain data, and maintaining a hybrid-chain approach poses risks such as network disruptions, latency, and potential vulnerabilities in the communication protocols. Moreover, if data privacy and security is not handled properly, any vulnerability or security breach could compromise sensitive information. Some other technical threats that may occur

include network and infrastructure reliability issues, adoption and interoperability-related challenges, legal and regulatory uncertainties, and technological obsolescence.

IX. Architecture

Our solution focuses on "Ensuring customer transparency while hiding the business secrets". For ensuring customer transparency, we are using a public permissioned blockchain approach where everyone from the general public to regulatory bodies can observe the product and its quality data. It is permissioned due to the level of access to the data an user is given. Some of the core technical features that our solution proposes in the architecture are:

- Zero Knowledge Proofs: Zero-knowledge proofs (ZKPs) are cryptographic protocols that allow one party (the prover) to prove the validity of a statement to another party (the verifier) without revealing any additional information beyond the truth of the statement itself. The solution implements one of the variations of Bulletproof algorithm to compute the zero-knowledge proof efficiently, which takes less space for ensuring zero-knowledge proof and is also one of the fastest prover algorithms with no trusted setup.
- ZK-KYC: The KYC module is required to register the supply chain stakeholders who directly participate in the workflow of the solution. Zero-knowledge proofs are applied to Know Your Customer (KYC) processes to enhance privacy while still providing necessary verification. The zero-knowledge standard applied to follow the protocol defined on Annoncreds implemented on the top of the W3C DID standard.
- Schnorr Digital Signature: The Schnorr digital signature scheme, based on elliptic curve cryptography, provides an efficient, secure, and linear method for creating and verifying digital signatures. It involves key generation, signing, and verification processes. Schnorr signatures offer advantages such as shorter signature lengths, faster computation, linearity for multi-signature schemes, and simplicity in implementation.

The sequence diagram of different stakeholders interacting with the provided solution will be in Fig. 8.

"PharmaSync" consists of different stakeholders. Manufacturers first make confirmation from regulatory bodies and store the verification information to the smart contract. After that, manufacturers upload blockchain information along with certificates using IPFS and store the hash in blockchain. Similarly, when distributors receive the confirmation of the receiving lot, they transfer it to the retailer by saving the storage information to the blockchain. While manufacturers, distributors and retailers store the information as a certificate to the blockchain, they need their decentralized identification and security via digital signature. When drug lots are transferred to the pharmacy or hospital, confirmations are also added to the blockchain via smart contract. Product quality related information are added to the public blockchain while lot quantity, other business related information are added in the private blockchain. Thus, on one hand, DIDs secure identity, while on the other hand, storing public data in decentralized file storage and trading information on a private chain create a hybrid chain infrastructure that enhances the overall security of PharmaSync.

The technical architecture can be discussed from two main high-level architecture view:

- Application Component Architecture
- Identity Information Architecture

A. Application Component Architecture

The application component architecture deals with the different parts of a node component and how they work together to form the application, blockchain, and data layer.

1) Application Layer: The application layer consists of three sub-layers, which involve end user interactions:

- End User Application (Mobile App and Web Portal)
- Development Portal (Node)
- Smart Contract Layer (Solidity)

2) Blockchain Service Layer: The distributed ledger layer with Hedera Hashgraph services consists of core modules, token, a smart contract engine, file services, and a transaction manager. The Network Services Module orchestrates efficient communication and networking protocols among nodes. The File Service Module offers secure and decentralized file storage capabilities, allowing users to manage their files using cryptographic keys. With the Identity Management Module, Hedera Hashgraph enables the establishment and administration of digital identities. Product management and quality assurance are handled with the Hedera smart contract service. The token service is used to create a soul-bound non-transferable NFT to issue QA certificates. The file itself is managed in the decentralized IPFS service. Finally, Hedera has a unique service called Hedera Consensus Service (HCS) which is a purpose-built tool for creating decentralized, auditable logs of immutable and timestamped events. Its pub-sub-based architecture is a perfect fit for tracking supply chain items throughout their lifetime. It also supports pulling data to private network setups for private transactions. We enable the storage and verification of data in a privacy-preserving way with ZK proof using Cairo to create and execute arithmetic bulletproof circuits.

3) Data Layer: The data layer is the storage layer and consists of on-chain and off-chain storage services. For on-chain data service, the Hedera private network is used for managing government and industry-compliant data, and the public Hedera chain supports the supply chain flow. Hedera public chain is one of the most suitable enterprise-level chains out there because of its extremely fast transaction time and TPS (Transactions Per Second). Also, unlike any other mainstream public blockchain platform, it has a fixed transaction fee rate, and that fee is among the cheapest. For identity DID (Decentralized Identifiers) of stakeholders, they are stored on the Hyperledger Indy chain. For off-chain service, the API layer and application hosting service off-chain regular

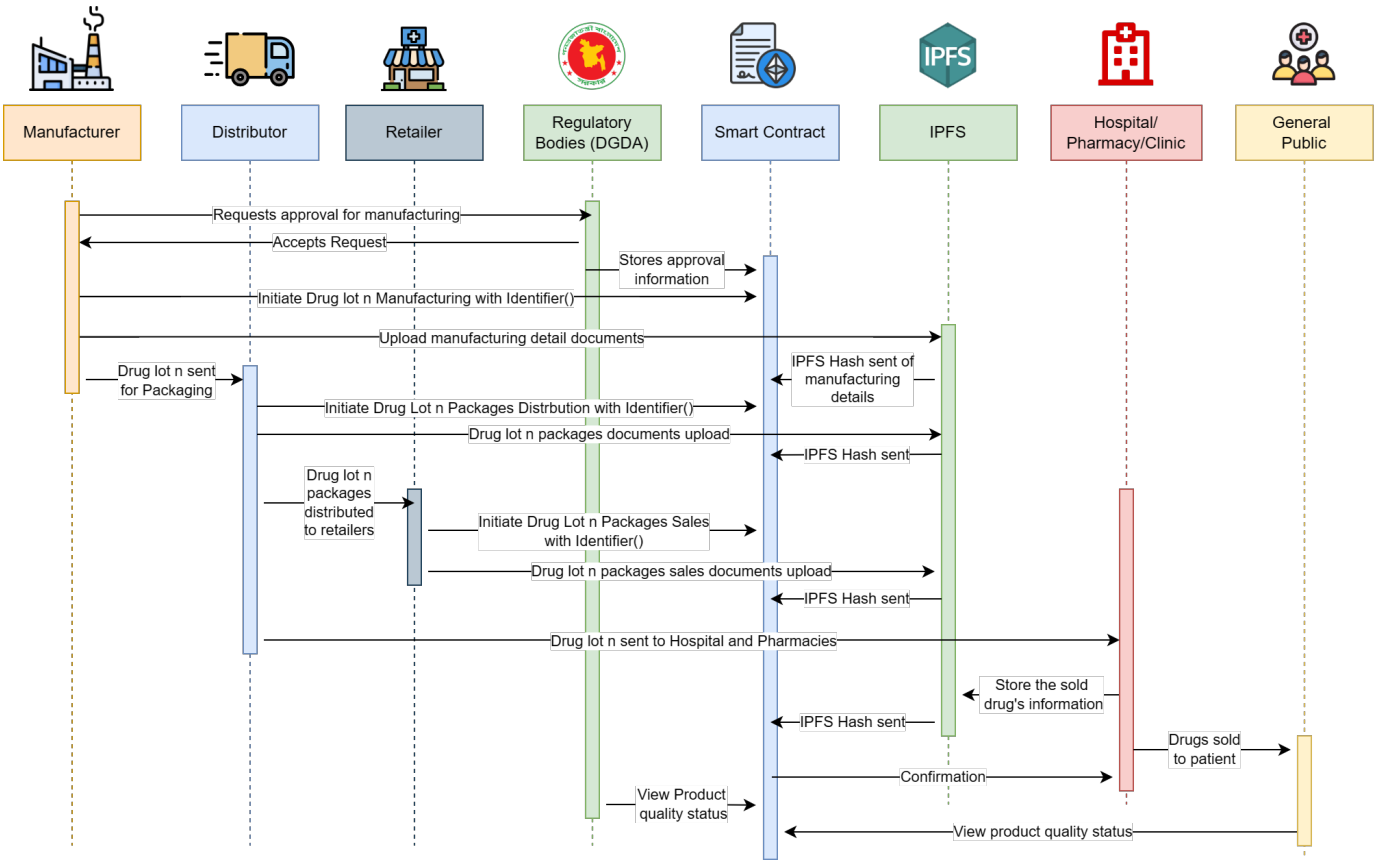

Fig. 8. Sequence diagram of proposed solution

web3 service are used, and IPFS (InterPlanetary File System) is the decentralized data storage for storing and retrieving documents.

B. Identity Information Architecture

The proposed identity information architecture combines Hyperledger Ursa, Aries, and Indy to form a Self-Sovereign Identity (SSI) system based on Decentralized Identifiers (DID). With interoperability and pluggability at the infrastructure level, users can achieve secure supply chain transactions, leveraging Aries' open-source wallets for digital credentials and the DKMS (Decentralized Key Management System) architecture [15]. Aries utilizes agent and wallet components, powered by Ursa's cryptographic library, while running the DID communications protocol on the Indy ledger. The Indy ledger encompasses multiple ledger types, including pool, audit, domain, and config ledgers, each maintaining its transaction logs and Merkle trees for added security and functionality. This architecture provides a robust framework for SSI, enabling secure, flexible, and privacy-enhanced identity management in supply chain ecosystems.

Here is an example DID of a supply chain stakeholder following the W3C standard with custom implementation:

C. Zero Knowledge Proof construction

In Pharmasync, Bulletproofs algorithm is used to provide zero-knowledge proofs for statements related to the authenticity and integrity of drug transactions. Below is illustrated how Bulletproofs can be applied to verify the validity of a drug transaction:

Let's consider a scenario where a manufacturer (M) sells a batch of drugs to a distributor (D). The transaction includes the following information:

Manufacturer's public key: P_M Distributor's public key: P_D Batch ID: B Quantity of drugs: Q Price per unit: P

To prove that the transaction is valid without revealing any sensitive information, we can construct the following equations using Bulletproofs:

Equation for Quantity:

$$C_Q = (P_M \cdot Q) + (P_D \cdot (-Q))$$

Equation for Price:

$$C_P = (P_M \cdot P) + (P_D \cdot (-P))$$

In these equations, C_Q and C_P represent the commitments to the quantity and price respectively. P_M and P_D are the public keys of the manufacturer and distributor, and Q and P are the quantity and price values of the transaction.

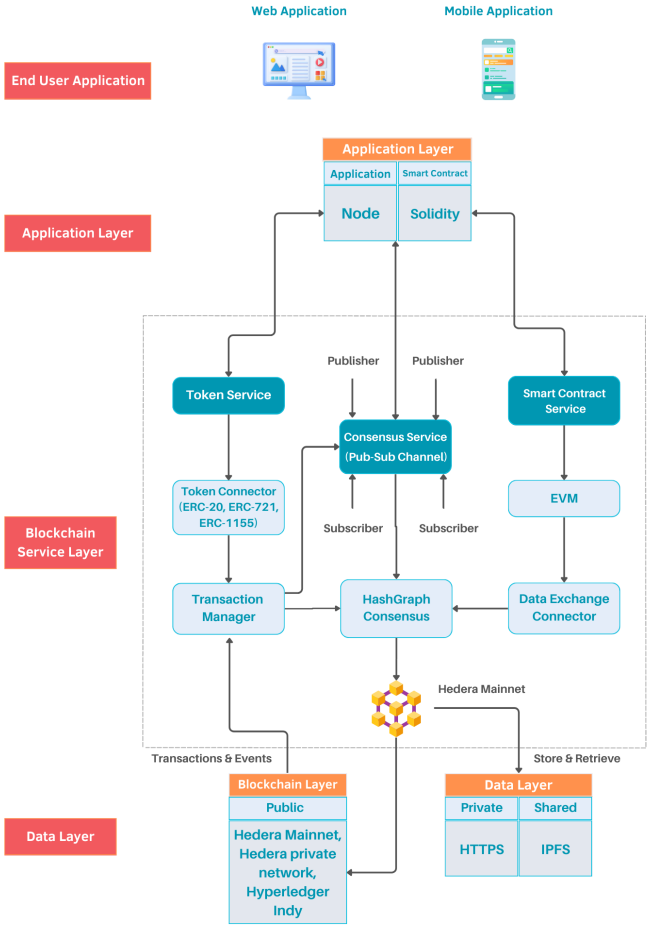

Fig. 9. Application Component Architecture of PharmaSync

With Bulletproofs, we can generate a zero-knowledge proof to demonstrate that the commitments C_Q and C_P satisfy the following conditions:

- The sum of the manufacturer's commitment and the distributor's commitment equals zero ($C_Q + C_P = 0$).
- The manufacturer's commitment is correctly multiplied by the quantity and price values, and the distributor's commitment is correctly multiplied by the negative of the quantity and price values.

By constructing and verifying these equations using Bulletproofs, it is possible to prove the validity of the drug transaction without revealing any specific values of the quantity or price.

D. Schnorr Digital Signature

For further fortifying the authentication and verification process within the infrastructure of the blockchain, the Schnorr digital signature algorithm scheme is incorporated. The data exchange between two stakeholders of the application can be signed with Schnorr digital signature to strengthen the verification process.

Key Generation:


```
{
 "@context": "https://www.w3.org/ns/did/v1",
 "id": "did:pharmasync:123456789",
 "authentication": [
  {
   "type": "Ed25519SignatureAuthentication2018",
   "publicKey": "did:pharmasync:123456789#keys-1"
  }
 ],
 "publicKey": [
  {
   "id": "did:pharmasync:123456789#keys-1",
   "type": "Ed25519VerificationKey2018",
   "controller": "did:pharmasync:123456789",
   "publicKeyBase58": "7nCn9RAcQBeNcMQH76v2kKRTmCqAS1b91jJfXAzBvXQ8"
  }
 ],
 "service": [
  {
   "id": "did:pharmasync:123456789#service-1",
   "type": "VerificationService",
   "serviceEndpoint": "https://pharmasync.com/verification"
  }
 ],
 "created": "2023-05-18T10:00:00Z",
 "updated": "2023-05-18T10:00:00Z"
}
```


Fig. 10. DID of a supply chain stakeholder following the W3C standard with custom implementation

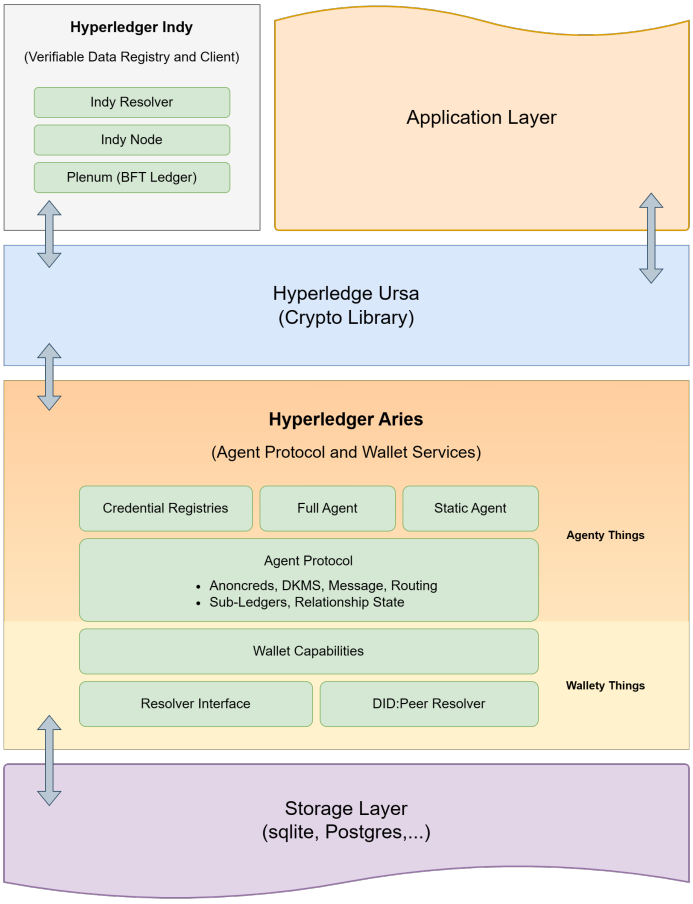

Fig. 11. Identity Information Architecture of PharmaSync

1) The distributor generates a private key (random secret integer) represented by 'd'.
2) The distributor computes the public key by performing elliptic curve point multiplication: $D = d \cdot G$, where 'G' is a predefined base point on the elliptic curve.

Signature Generation:

1) The distributor selects a random nonce (another secret integer) represented by 'k'.
2) The distributor computes the nonce's corresponding public key by performing elliptic curve point multiplication: $K = k \cdot G$.
3) The distributor generates a commitment value, 'e', by hashing the message to be signed along with the public key: $e = \text{Hash}(message||D||K)$.
4) The distributor computes the response, 's', by combining the private key, the nonce, and the commitment value: $s = (k + e \cdot d) \mod n$, where 'n' is the order of the elliptic curve's base point.
5) The distributor creates the signature consisting of the response 's' and the commitment value 'e'.

Signature Verification:

1) The manufacturer receives the signature (s, e), the message, and the distributor's public key (D).
2) The manufacturer computes the commitment value 'e' by hashing the message along with the distributor's public key: $e = \text{Hash}(message||D)$.
3) The manufacturer verifies if $K = s \cdot G - e \cdot D$ by performing elliptic curve point addition and multiplication.
4) If 'K' matches the computed value, the signature is valid, indicating that the distributor is the authentic signer; otherwise, it is considered invalid.

X. Governance

A. Network Membership Governance

Network Membership Governance indicates a discipline that ensures effective network operations, including on-boarding and off-boarding of participants, permissions, regulatory oversight provisioning, support services, risks, and equitable costs distributed fairly based on participants' activities. The key stakeholders of this project include manufacturers, distributors, retailers, regulatory bodies (DGDA), hospitals/pharmacies/clinics, and general consumers. The on-boarding process of any stakeholder will be done formally upon agreeing to comply with the existing regulatory compliance. These stakeholders have the opportunity to switch from conventional account management systems to a blockchain-based SSI-enabled identity management systems. A fee is associated with every stakeholder registering to the system. The on-boarding stakeholders will keep the trust in IP architecture intact by allowing an authorized issuer to provide access. The access control and permissions of the stakeholders would be defined in the smart contract and all the accessibility, verifications and validations would be done accordingly. The rules and regulatory compliances would be strictly maintained and monitored by the regulatory bodies (DGDA). To uphold the regulatory guidelines for using the system, eligibility would be confirmed via hyperledger consensus nodes and laws encoded in smart contracts. Any stakeholder flagged by any lawmaker/ auditor/ regulator/ law enforcement agency would be deprived of access controls and permissions according to the smart contract. The on-chain application and server of the network will be maintained by the monitoring body and the off-chain part will be maintained by the respective stakeholders. Network Operations will be performed by internal networking staff/ Pharmars Team (the blockchain team) to monitor, manage and communicate throughout the network. Some third party IOT devices will also be integrated in order to perform some operations. The sequence of the operations are described in the sequence diagram given in the solution section.

B. Business Network Governance

Business network governance includes the underlying dynamics and structure of a multiorganizational operation that is particular to a sector or use case. It includes essential elements including the business model, shared services, cost distribution, incentives, compliance controls, and regulatory frameworks that drive and oversee how the network operates. The objective of this pharmaceutical supply chain project is to create a transparent, secure, and decentralized network for ensuring traceability and protecting privacy and trade secrets of the stakeholders. The participants in the network would be the manufacturers, distributors, retailers, regulatory bodies (DGDA), hospitals/clinics/pharmacies, general consumers and the Pharmars team. The physical assets would belong to the stakeholders of the supply chain and the intangible assets such as the smart contracts, compliance rules, IoT device integration, operational information, etc. would be developed and maintained by the Pharmars team along with the regulatory bodies. The founding members would be the registered stakeholders in the centralized database. Although the procedure would be mostly automated, it would still undergo an additional audit phase before switching to the new system. As our solution is aimed at handling six major problems (discussed in the Problem section), the stakeholders would get a more controlled, secured, and efficient ecosystem in the network than the conventional systems. As for the non-founding members, the identity management process of the system would be much easier with the cloud based agent for the stakeholder organizations and the mobile app based agent for the general consumers of Hyperledger Indy, Aries and Ursa. The SLA (Service Level Agreement) regarding availability, auditing, tracking, and tracing of assets would be monitored off-chain according to the Hyperledger consensus nodes with built-in automated penalty system.

C. Technology Infrastructure Governance

Technology Infrastructure Governance sheds light on IT infrastructure and its distribution, technological assessment, and adoption of resources, performance, security, cost structures, and the associated risks that come along with it. In

PharmaSync, Hedera Hashgraph's Network Services Module facilitates efficient communication and networking protocols among nodes. This ensures a robust foundation for developing and executing smart contracts and a secure and decentralized File storage. A hybrid-chain architecture consisting of a public chain and a private chain is used in this project. The private chain node hosting is done by the manufacturing company in the supply chain. The read-only data of various stakeholders that ensure the transparency in the system, transaction history, and the verification and validation data of the stakeholders that requires monitoring would be stored in the public chain (Hedera Mainnet). The operational data, confidential transactions, private information, and trade secrets would be stored in the private chain (utilizing Hedera Consensus Service). As a public permissioned chain Hyperledger Indy ensures that everyone has read access to the ledger but only selected authorized persons can have write access. The credentials for identity management is held with an Aries agent/cloud Aries agent. The data ownership, accessibility (read, write permissions), and storage type (on-chain, off-chain) of all data are discussed in the access control matrices. To achieve secure and efficient consensus among participants in private and permissioned networks, Hedera Consensus Service is used which ensures agreement on the order and validity of transactions. The identity management system of this project would include a privacy-enhanced Decentralized Identity (DID) infrastructure solution using Hyperledger Aries, Indy and Ursa. The verification and validation-related data on the public chain that will be governed and monitored and encrypted using Zero-Knowledge proof. Some other algorithms and techniques that are used to make this solution standalone are ZkKYC technique for inter-supply chain participant identification and verification, Iot integration for the measurement and quality control of supply chain product, the compliance data accessibility and verification by issuing soul bound NFT and the Schnorr digital signature scheme for an efficient, secure, and linear method for creating and verifying digital signatures. As for the deployment of the project, The core technical team (Team Pharmars) would be in charge of the project's gradual deployment, and each subteam within the main team would be in charge of its own on-site server maintenance and other hardware-related issues. The technical staff would also keep an eye on and take care of any network and protocol level issues. The risk mitigation of this project involves implementing strategic policies to mitigate IT infrastructure risks, including secure management of Hedera Hashgraph's hybrid-chain architecture, adherence to access control matrices, utilization of privacy-enhancing technologies, continuous monitoring of network and protocol-level issues and having proper contingency and backup plans for all possible situations. Proper maintenance and hardware management would be ensured for minimizing risks and ensuring the smooth operation of the pharmaceutical supply chain system.

XI. Value Proposition

In business plans, this is usually called a revenue model or business model, but the value may not always be money. Show that the solution generates value and can capture it. Make sure it is measurable. Another way to think about it is key performance metrics: what defines success and failure? It has to be quantifiable. A subjective mission cannot fail, and also cannot succeed. No financial projections are expected.

PharmaSync's value proposition lies in its ability to revolutionize the pharmaceutical supply chain through advanced blockchain technology, ensuring efficiency, transparency, security, and accountability, while simultaneously reducing costs, errors, and corrupt practices.

Point of Parity (POP) - Our blockchain solution, PharmaSync, offers a streamlined registration process and ensures compliance with regulatory standards, delivering a user-friendly experience on par with existing solutions.

Point of Difference (POD) - Unlike other blockchain solutions, PharmaSync incorporates a ZkKYC submodule for secure participant identification and verification, reducing fraud risks and enhancing trust. It also provides an added layer of trust and verification using the Schnorr digital signature algorithm during data exchange between two parties.

Overall, our solution, PharmaSync, presents a comprehensive array of advantages within the pharmaceutical supply chain management system:

- Enhanced Compliance with Regulatory Standards: Our solution enables pharmaceutical companies to maintain compliance with regulatory standards, reducing the risk of non-compliance and associated penalties. This aligns with the need to address the increasing number of FDA warning letters referencing data integrity deficiencies.
- Improved Traceability and Recall Management System: Our solution incorporates a recall management system that ensures efficient traceback and swift removal of defective products from the market, minimizing the impact on consumers and resources.
- Increased Accountability: The real-time monitoring and tracking capabilities of PharmaSync ensure accountability across the supply chain, fostering responsible practices and adherence to quality standards.
- Elimination of Single Point of Failure: With no centralized entity storing related data, PharmaSync eliminates the risk of a single point of failure, enhancing the resilience and reliability of the system.
- Cost Savings: The automation, elimination of intermediaries, and streamlined processes offered by PharmaSync result in cost savings for pharmaceutical companies, reducing operational expenses.
- Faster Operations: Through automation and digitization, PharmaSync expedites operations, reducing lead times and enabling faster delivery of pharmaceutical products to market.
- Increased Public Trust: By promoting transparency, security, and accountability, PharmaSync builds public trust in

the pharmaceutical industry, bolstering the reputation of companies and improving customer confidence.

To establish PharmaSync in the market and to be a dominant player in the years to come, it is of utmost importance to identify revenue streams and ensure a stable cash flow into the business. Having such cash flow would help PharmaSync keep afloat and help us make continuous improvement into the market. As we intend to form partnerships with regulatory bodies to gain access to the market and establish validation in the market, we will charge a subscription fee from these regulatory bodies. This fee would be payable annually. This annual subscription fee would be competitive and discounted since both parties would be benefitted from this partnership. Now the question may arise that why would these regulatory bodies pay a subscription fee? These regulatory bodies aim to make the pharmaceutical industry better and establish transparency. PharmaSync will help them achieve just that. With the help of PharmaSync, they will be able to solve problems of different magnitudes.

As for pharmaceutical companies, the revenue stream will be twofold. First of all, implementation of PharmaSync would require significant cost and labor. To cover this, we will charge companies an implementation fee firstly. This would be a one-time payment, and a discount will be provided if a large conglomerate wants to implement our solution for other purposes. Secondly, an annual maintenance fee will be charged to pharmaceutical companies to ensure smooth operation and output from our solution. In the initial stages, we will earn our revenue from these three sources. When we explore different horizons and implement our solutions in different countries, we will surely come across different avenues that will help us to earn from additional sources of revenue.

XII. Distribution

Demonstrate that not only does the project have value, but it can be brought into reality. Distribution is about how the project will go to market and what the next steps would be. What is a plan to get it launched, and even better if there are immediate next steps or short term roadmap. No financial projections are expected.

In terms of distribution, PharmaSync will first concentrate on seizing the local market because there isn't much competition there. In the first two years, we'll concentrate on expanding the local market and enhancing the state's pharmaceutical sector. In the first six months of our adventure, which will start in 2024, we will do everything we can to develop the solution. The following six months will be spent to assess our offering and uphold the highest caliber.

As they will be crucial in gaining access to and validation in the market, we will move our focus in the upcoming year to developing collaborations with national regulatory bodies. We will begin operating in the neighborhood market after we prove our superiority to them and win them over. To increase our market share, we'll keep growing, provide excellent service, and forge connections inside the sector.

Fig. 12. Short Term Distribution Timeline of PharmaSync

XIII. Conclusion

The current supply chains of the pharmaceutical industries faces numerous challenges and complexities, ranging from lack of transparency, breach of privacy and drug counterfeiting to product recalls and regulatory compliance issues. PharmaSync presents a robust blockchain-based solution that addresses the critical challenges that modern pharmaceutical supply chains face. By leveraging the power of blockchain technology, PharmaSync ensures transparency for the general public while safeguarding the privacy and trade secrets of the stakeholders. Through modules such as recall management, compliance data verification, fine-grained user access control, decentralized identity management, and data authenticity assurance, PharmaSync delivers a comprehensive and efficient system. This solution enhances patient safety, protects brand reputation, and improves overall supply chain effectiveness. By tackling issues like privacy, drug counterfeiting, product recalls, and regulatory compliance, PharmaSync paves the way for a secure, transparent, and reliable pharmaceutical supply chain ecosystem. In conclusion, the decentralized nature of blockchain makes it the upgraded choice compared to traditional supply chain solutions.

References

[1] https://www.researchgate.net/publication/326785031/
[2] https://timesofindia.indiatimes.com/blogs/voices/pharmaceutical-supply-chain-management-crises-and-innovations/
[3] https://www.databridgemarketresearch.com/reports/global-pharmaceutical-logistics-market
[4] https://www.usp.org/news/physician-survey-supply-chain-vulnerabilities
[5] Adulterated and counterfeit drugs are worse than fake Covid-19 reports' — The Business Standard (tbsnews.net)
[6] Countering counterfeit medicine in Bangladesh — The Daily Star
[7] https://www.statista.com/chart/30067/worldwide-counterfeit-pharmaceuticals-incidents/
[8] https://www.pharmacy.biz/understanding-the-impact-of-pharma-recalls-on-the-industry-and-consumers/
[9] https://www.supplychainbrain.com/articles/34798-five-critical-challenges-facing-pharma-supply-chains

[10] https://aspe.hhs.gov/sites/default/files/documents/87781bc7f9a7fc3e6633199dc4507d3e/aspe-rtc-costs-drug-shortages.pdf
[11] https://www.researchgate.net/publication/353396425
[12] https://healthpolicy.duke.edu/sites/default/files/2020-02/
[13] https://www.uspharmacist.com/article/pharmacies must take steps to protect against data breaches
[14] https://www.hipaajournal.com/healthcare-data-breach-statistics/
[15] https://www.evernym.com/blog/hyperledger-aries/
[16] https://www.futuremarketinsights.com/reports/counterfeit-drug-detection-device-market
[17] https://www.fiercepharma.com/pharma/drug-shortages-cost-u-s-care-providers-at-least-200-million-annually-pose-patient-safety
[18] https://www.commonwealthfund.org/publications/issue-briefs/2023/jan/us-health-care-global-perspective-2022: :text=In 202021 2C 20the 20U.S. 20spent,higher 20than 20in 20South 20Korea.
[19] https://www.lightfootlawdc.com/blogs/fda-drug-recall-statistics/
[20] https://pharmaphorum.com/news/60-of-pharma-companies-using-or-trying-blockchain-survey
[21] https://www.livemint.com/market/mark-to-market/lupin-s-recall-of-metformin-formulations-in-the-us-to-hit-profitability-in-q2-11594274825091.html
[22] https://businessinspection.com.bd/pharmaceutical-industry-of-bangladesh/
[23] /urlhttps://www.thedailystar.net/health/news/countering-counterfeit-medicine-bangladesh-2971806
[24] https://dgdagov.info/: :text=The 20Directorate 20General 20of 20Drug,Regulatory 20Authority 20of 20the 20country.
[25] http://www.bapi-bd.com/index.html
[26] https://fisher.wharton.upenn.edu/wp-content/uploads/2020/09
[27] https://hedera.com/hh whitepaper v2.1 20200815
[28] https://www.mediledger.com/
[29] https://www.ibm.com/blockchain
[30] https://www.farmatrust.com/
[31] https://www.blockdata.tech/profiles/blockpharma
[32] https://www.smartsoftwareinc.com/
[33] https://www.pharmasolutions.com.bd/
[34] https://mediasoftbd.com/wholesale-distribution-management

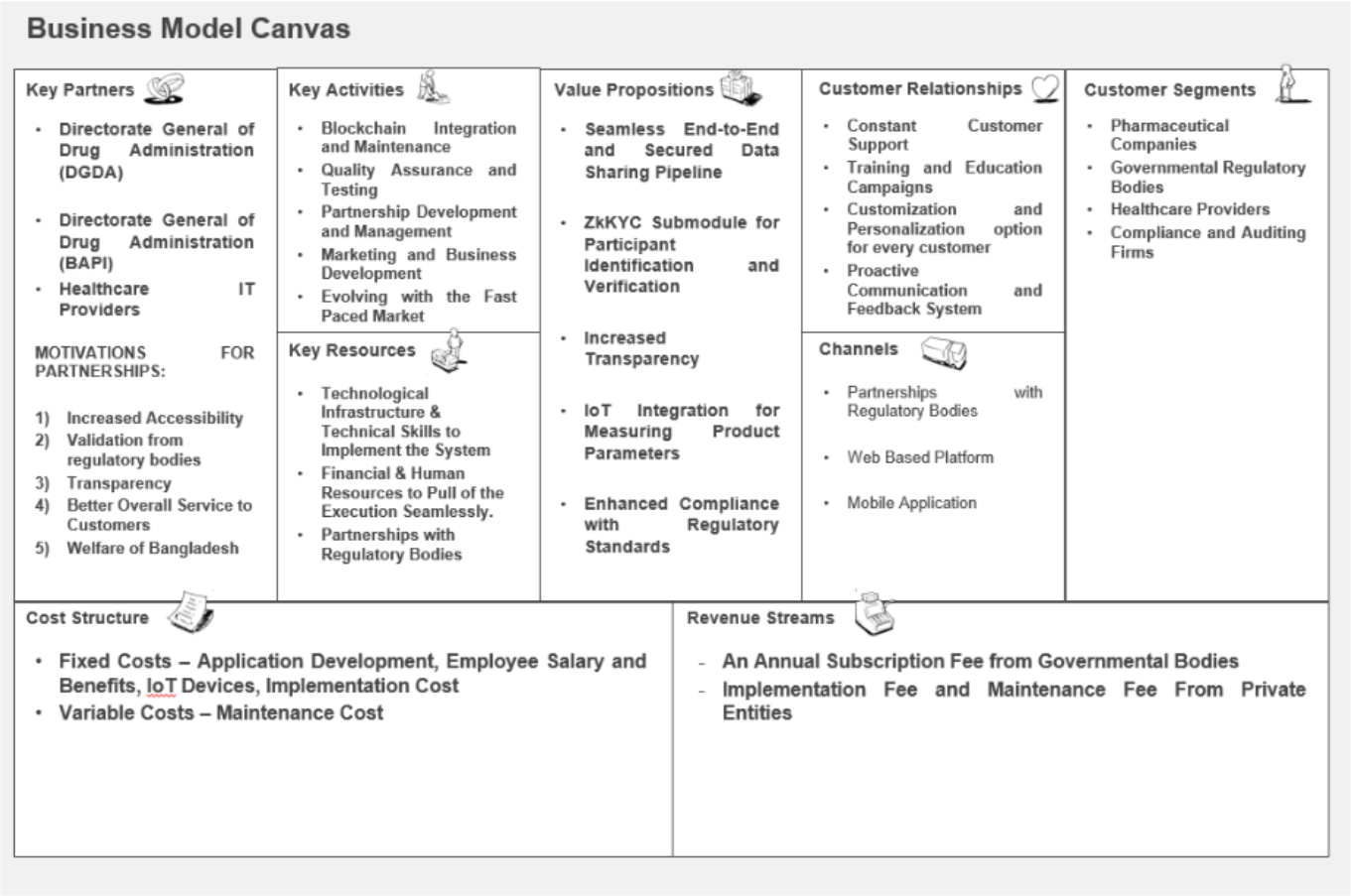

Fig. 13. Appendix A: Business Model Canvas

Read access control matrix chart

Entity:	Product	Product Quality Status	Product flow from M to D	Product flow from D to R	Product flow from R to P	Purchase Orders and Invoices	Compliance and regulatory data	MF Identity	Supply chain entities identity
Storage type:	On chain	On chain	On chain	On chain	On chain	On chain	On Chain	Off chain	Off chain
Stakeholder									
Manufacturer	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Distributors	Yes	only if involved	Yes	Yes	Yes	Only if involved	With restriction	Yes	Only own
Retailers	Yes	only if involved	No	Yes	Yes	Only if involved	With restriction	Yes	Only own
Pharmacies	Yes	only if involved	No	No	Yes	Only if involved	With restriction	Yes	Only own
Pharmars Team	Yes	Yes	Yes	Yes	Yes	No	With restriction	Yes	Only own
Regulatory Bodies	Only global data	Yes	No	No	No	No	Yes	Yes	Global data
General public	Only global data	Only global data	No	No	No	No	WIth restriction	Yes	No

Fig. 14. Appendix B: Access Control Matrix [Read]

Write access control matrix chart									
Entity:	**Product**	**Product Quality Status**	**Product flow from M to D**	**Product flow from D to R**	**Product flow from R to P**	**Purchase Orders and Invoices**	**Compliance and Regulatory Data**	**MF Identity**	**Supply Chain Entities Identity**
Storage type:	On chain	On chain	On chain	On chain	On chain	On chain	On Chain	Off chain	Off chain
Stakeholders									
Manufacturer	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No
Distributors	No	Yes	Yes	Yes	No	Yes	No	No	Only own
Retailers	No	Yes	No	Yes	Yes	Yes	No	No	Only own
Pharmacies	No	No	No	No	Yes	Yes	No	No	Only own
Pharmars Team	No	No	No	No	No	No	No	No	Only own
Regulatory Bodies	No	No	No	No	No	No	Yes	No	No
General public	No	No	No	No	No	No	No	No	No

Fig. 15. Appendix B: Access Control Matrix [Write]