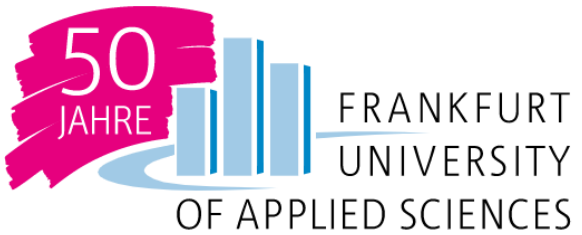


Frankfurt University of Applied Sciences

High Integrity Systems Project Report WS 20/21

Custody Transfer using Hyperledger Fabric 2.2

Safir Mohammad Shaikh (1322554)
Vidya Gopalakrishnarao (1323074)
Parag Tambalkar (1322596)
Pranay Raman (1321759)

Guidance:
Prof. Dr. Martin Kappes
Mr. Lukas Atkinson
Mr. Johannes Bouché

Table of Contents

Abstract

In the era of automation, Blockchain is an emerging and efficient technology as compared to traditional approaches in Oil and Gas industry. Custody Transfer in this industry is referred to as the transactions involved in the physical transportation of entities from one place to another. There are already several implementations of Custody Transfer in use, however, not using Hyperledger Fabric, which is an open-source, permissioned blockchain framework. And, this is what we aim at in this project, developing an end-to-end application for Custody Transfer using Hyperledger Fabric. To achieve this, we have built a Fabric network with five organizations, smart contracts, a client application and carried out ample amount of research. After successful implementation and evaluation, we have found out that, at each phase of the Custody Transfer process, Blockchain fits perfectly and no other technology can replace it with such efficiency.

Keywords: Blockchain, Custody Transfer, Hyperledger Fabric

1. Introduction

In oil and gas industry, custody transfer is the process of transferring large quantity of oil and gas from one party to another party [4]. There are three major stages of this process namely Upstream, Midstream and Downstream. Upstream process is related to oil and natural gas production. The Midstream stage includes storage and transportation of oil and gas. Downstream is the third stage, where crude oil and natural gas are refined into final products [5]. Several stakeholders are involved in this process – buyer, seller or oil producer, transportation service provider and governments from the buyer country and seller country. Every stakeholder plays an important role during end-to-end transfer of commodities. Buyer and seller are the two parties in which transfer of commodities take place. Transportation companies are responsible for moving these commodities from seller to customer. Ships, trains, and oil and gas pipelines are the most popular modes of oil and gas transportation. Transportation service providers get paid for the volume of commodities they move. Tax revenue generated from cross-border commodity trading is one of the most significant sources of revenue for any country's government [4] [6] [7].

Trading huge volumes of oil and gas involves a lot of money and taxes. High degree of transparency in the quantitative and quantitative measurements is required in this process. A small measurement error may result in a major financial difference, so measurement accuracy is important. Each stakeholder must have a clear understanding of the quantity and quality of the commodity being transferred. To keep buyers and sellers on the same page, both parties need to sign an agreement that defines the measurement requirements. Oil and gas measurements are performed in accordance with the industry standards. Metering systems used for measurements must be approved by global industry standards such as American Gas Association (AGA), American Petroleum Institute (API), or International Organization for Standardization (ISO), and national metrology standards such

as Physikalisch-Technische Bundesanstalt PTB (Germany), National Institute of Standards and Technology NIST (U.S.), and so on [4] [6].

It is clear from the process of custody transfer that trust and transparency must be built among the stakeholders in order to execute the end-to-end transfer process smoothly without any disputes. This can be achieved by incorporating blockchain technology into each phase of custody transfer process. A blockchain is a network of peer nodes that maintains an immutable transaction ledger. Each of these nodes holds a copy of the ledger, transactions that have been checked by a consensus protocol are added to the ledger and are arranged into blocks with a hash that connects each block to its previous block [8]. Bitcoin and Ethereum are well-known cryptocurrencies based on blockchain technology. Bitcoin utilizes decentralized ledger technique and Ethereum uses smart contracts for distributed applications. Bitcoin and Ethereum comes under the class of public permissionless blockchain. Public permissionless blockchains are public networks, open to all and participants interact anonymously. But, when using blockchain technology for enterprise-level applications such as custody transfer, few basic requirements must be considered. Some of the requirements of enterprise-level applications include identification of participants, permissioned networks, exceptional transaction throughput, minimum delay in transaction confirmation, privacy and confidentiality of transaction-related data. Since Hyperledger Fabric is explicitly built for enterprise use, it is one of the strongest blockchain applications to serve these requirements. We found below characteristics of Hyperledger Fabric that are best suited for our project [8],

- Distributed Ledger Technology (DLT)
- Highly modular and configurable architecture
- Permissioned Network
- Supports smart contracts
- Pluggable consensus protocols
- Privacy and confidentiality of transactions
- Performance and many more

2. Related Work

In real-world analogy, Custody Transfer is usually realized at an international level (among countries, continents etc.) with highest level of security mechanisms implemented. These security mechanisms include authentication and validation of Buyer and Seller parties, Buyer and Seller government, National and Global measurement standards of Buyer and Seller like ISO 8222 Standard, Physikalisch-Technische Bundesanstalt (PTB) Standard, American Petroleum Institute (API) Standard etc.

- **Custody Transfer using Blockchain [9]**
  Being such an important and high-level topic, many multinational firms have proposed and designed their own way of implementing Custody Transfer using Blockchain technology. Blockchain is being used for cost efficiency and improved user experience, in which a product i.e., oil or gas is transferred between endpoints. Moreover, it aims at ensuring transparency in the origin, possession, quality and quantity in the value chain. Blockchain provides a sturdy, reliable and cost-efficient solution to intractable problems in custody transfer like dilemma in contractual disputes among parties, costly rework, postponement, expenses of resolution management etc. According to Wipro, **adoption of Blockchain solutions is inevitable by the industry, however, it will happen sooner than later.** Also, with the fusion of Blockchain and IoT, the platform would have the potential to eliminate confusion and drive real-time rectifications. **FedEx** utilizes autonomous and distributed ledger potentialities of Blockchain effectively as a single solution for all consignments and to track expensive cargo and delivery services [10]. **Dior and Louis Vuitton** use it for tracking luxury goods [11]. Many organizations in other industries are illustrating how Blockchain addresses issues related to value transfer like authenticity, measurements, location, status of products, cross-border challenges, superior user experience and improved trust levels.

- **Getting to Value with Blockchain in Oil and Gas [12]**
  According to Accenture, Blockchain is becoming an important element in many industries utilizing secure distributed ledgers and smart contracts. For example, securing and simplifying energy trading, bills and payment, managing complex supply chains, responding to regulation requiring immense documentation. The Blockchain Track and Pay solution of Accenture allows the industry to realize cost reducibility in the form of increased visibility, transparency and accuracy of freight invoices. Moreover, this solution has the power to transform and streamline the shipment process. Throughout the whole process, transactions are logged, starting from the agreement till the delivery and remittance. And, when the shipment is in transit, the geolocation is logged to the Blockchain. When the consignment is reached, the invoice is generated using smart contracts. In case of traditional approach, even with detailed analysis and audit processes, many enterprises lose money due to invoice overpayments or repeated payments. Blockchain reduces this discrepancy by offering a single source of truth with a distributed ledger. Many companies in the Energy industry are using Blockchain for following reasons:

  - Hydrocarbon and Commercial Fleet Tracking
  - Commodity Trading and Trade Finance
  - Joint Venture Accounting (Shared Distributed Ledger) and Procure to Pay
  - Intragroup Billing (Cost Settlement) and Downstream (Bitcoin Payments) Payments

- **Maintaining Chain of Custody Using Blockchain [13]**
  In another research, the authors have implemented digital evidence (against criminals) handling using blockchain technology. They have used **Hyperledger Composer to transfer the digital evidences securely** using encryption techniques. Hyperledger Composer is an Hyperledger tool to model and build blockchain networks. Blockchain helps in secure transfer and maintaining integrity of the evidences. In this scenario, a chain of custody refers to recording and preserving an evidence i.e., the process starting from collection till presenting it in the court. Blockchain is the key factor for the evidence to remain original and authentic while storage, processing or in transit. The capability of Blockchain to secure transactions, giving authorized access, and other immutable features provides integrity and authenticity of digital evidence for its admissibility in court. The authors have built a system which is tamper-resistant, secure and more reliable chain of custody in digital forensics. **For encryption, they have used Base64 algorithm** in which, a hash of the evidence is generated and transferred and any participant can decode the hash and get the original evidence for verification purposes. Blockchain overcomes the drawbacks of traditional client-server architecture with its decentralized approach. Moreover, it provides transparency throughout the network for tracking the lifetime of evidences. Also, its feature of immutability makes it very difficult to tamper the data.

- **Summary**
  To infer, Blockchain provides following advantages in Oil industry:

  - Better transparency, visibility and sleek transactions across shareholders
  - Fewer disputes
  - System-driven affirmation and automation of remittance based on commodity volume exchange
  - Availability of whole logs of history for faster resolution in case of disputes

  The previous work in this field depicts that there has not been any implementation and end-to-end application of Custody Transfer using Hyperledger Fabric, a permissioned Blockchain framework. And this is what we aim at in this project, implementing an end-to-end application for Custody Transfer using Hyperledger Fabric.

3. Importance of Blockchain in Custody Transfer

3.1 Challenges in Custody Transfer Process

Overall, oil and gas custody transfer is a very complicated procedure. There are many difficulties that oil and gas companies face throughout the process. There is no simple understanding of how roles are delegated between organizations. This sometimes leads to confusion and distractions. For the handover of oil and gas, there is no standard protocol in place. Mismanagement, misunderstandings, and misjudgment are the common problems

that can have a noteworthy effect on custody transfer. Apart from these issues, there are several cases of cyber-attacks on oil and gas companies causing direct impact on custody transfer process. In 2008, Hackers breached the alarms and communications networks of Turkey's Baku-Tbilisi-Ceyhan pipeline. High pressure alarms were deactivated as a result of alarm system miscommunication caused by hackers. The pressure of crude oil surpassed the maximum limit, and this resulted in a huge explosion, resulting in the loss of 30,000 barrels of crude oil. In 2012, cyber-attacks were launched against Saudi Arabia's national petroleum and natural gas company. As a result of the cyber-attack, over 30,000 computers were damaged, and crude oil production had to be stopped until recovery [5]. Implementation of a firm and robust technological solution is need of an hour in oil and gas industry to overcome these challenges.

3.2 Why Blockchain?

As already covered in the Motivation and Related Work, Blockchain not only overcomes the drawbacks of traditional approach, but also offers plethora of other features. In some fields, Blockchain has achieved remarkable results and no other technology could come up with such results. Specifically, in the oil and gas industry, Blockchain has come to the rescue and saved millions of dollars. Blockchain is already being used in this area by the biggest firms in the world and the results are already available in front of us. Blockchain is proved to be successful due to its features that don't let any drawbacks or vulnerabilities to enter the system. Moreover, there is a wide scope for the betterment of this technology, such as implementation of Consensus Mechanism, Private or Protected Blockchain Network, Implementation of Smart Contracts, Feasibility of Endorsement Policy etc. And with this, the strong becomes stronger and can be used with ease and efficiency in many fields. Blockchain has streamlined the complex process that passes through abundant number of stakeholders. Moreover, there are many kinds of challenges, such as technological challenges, procedural challenges, political challenges, camaraderie challenges etc. and Blockchain attempts to tackle all these challenges. Now, to answer the question, **"Why Blockchain in Custody Transfer?",** there is a process of evaluation, analysis and comparison of Custody Transfer and Blockchain. In Custody Transfer, there are 3 phases, namely, upstream, midstream and downstream.

- **Upstream:** In Upstream phase, several activities related to exploration and production are held. It is the initial and the most important phase, since all the checks are performed in this stage and a positive conclusion of this state is the green signal for the beginning of next phase. In this phase, Blockchain helps in authentication and agreement of the parties on a specific decision. So that, in future, if there is any conflict between the parties, immediately, the corresponding block can be referred to validate the actual truth and resolve the conflicts since all the steps are stored in the distributed ledger shared by the parties. And anyone cannot deny since both parties agreed on fact that was logged in the Blockchain. This maintains the trust issues between the governments of 2 parties. Therefore, there is also not any scope for the

fraud. In this phase, Blockchain helps to achieve Confidentiality, Non-Repudiation, Integrity and Authenticity and Authentication and Availability.

- **Midstream:** In this phase, the commodities are transferred, and thus, this phase is in principle the transport of the product. Now, there are many important factors related specifically to transportation such as location, quantity, time, rate etc. At each time, the rate is updated and it is dependent upon the time. Moreover, there are factors which could affect the quantity of the shipment. For example, the oil quality can be affected and the quantity can be reduced due to the high temperature, strong sun-rays etc. So, Blockchain helps to tackle such issues, from point to point, the location and quantity is updated and agreed by the entities, so that there is no conflict between the parties. This phase is all about transportation and Blockchain takes care of all of it. Therefore, there can be no fraudulent activity related to transportation due to Blockchain. The trustworthiness of the transporter is also important, however, with the implementation of Blockchain, there cannot be much scams in the transportation process.

- **Downstream:** The last and the final phase is the Refinery and End Product. In this phase, the shipment is received, evaluated against certain factors, refined and transformed into and end-product. Once the shipment is arrived, it the quantity and quality are cross-checked against the agreement which is available in the ledger of both parties. And upon confirmation, the commodities are processed and transfigured into the end-products which can be made available for the public to use. Blockchain again helps here to ensure that there is no activity related to swindling, deception, double-dealing, duplicity etc.

Therefore, at each phase of the Custody Transfer, Blockchain fits perfectly and no other technology can replace with such efficiency. Seeing above use-cases, we can conclude that Blockchain is made for Custody Transfer. However, Blockchain is helpful in many other fields. And to support our statement, many firms have already used and presented the efficiency and feasibility of Blockchain in the form of incredible results [1] [2]. Talking about a normal scenario, there exist 3 stakeholders. First, the producer/seller, who owns the oil. Second, the TSP (Transportation Service Provider), who transports the order from producer to consumer and third, the consumer/buyer, who receives the commodities. There also exist the authorities, involved at both sides (Buyer and Seller) and the authorities can be government officials as well that control the quantities of the transported oil. Every stakeholder involved in the process measures the volume individually with their respective measuring devices complying at least one national and global measurement standard. And upon measurement, they write the volume directly into the Blockchain so that, everyone is aware of the status of the shipment at each point in time. Moreover, Blockchain purveys Transparency, which is the best advantage this field can take. When one stakeholder writes into the ledger, others can also view the same and confirm whether its correct or not. There are no hidden actions and hence, there is no scope for fraudulent activities.

The extensive measuring at each phase by several stakeholders and logging of the results in the Blockchain almost vanishes the scope of ambiguity and helps in achieving a plane procedure. Hence, Blockchain has helped in smoothness and simplification of the process of Custody Transfer without any errors and with almost zero risks.

3.3 Blockchain in Metrology

Metrology is a very important component of custody transfer process. Due to the volatile nature of petroleum products and natural gas, temperature and all other parameters of oil and gas must be maintained at a constant value during the transfer process. All parameters must be measured precisely and unambiguously. As discussed in Introduction part of this report, metrological devices must adhere to national and international metrological standards. Measurement systems installed at large-scale custody transfer processes measure natural gas worth of $6 million every day which means these systems measure natural gas worth $2.2 billion annually. In such huge process, a very small mistake of 0.25% in the flow rate measurement of natural gas results into loss of $5.5 million in a single year for a company with defective devices [6]. To solve this problem implementation of blockchain certainly helps. Real-time parameter measurements at all transfer points, as well as metering device properties, are saved in a distributed ledger. Identical copy of ledger is provided to every stakeholder involved in the process. If there is confusion about measurement and quantity delivered, each stakeholder can refer to their ledger and find out the mistake [5].

3.4 Smart Contracts for Legal Aspects of Custody Transfer

Custody transfer is a linked process, every stage of custody transfer is tightly linked with other stage. Large volume of commodities with huge cost are being transferred in this process, which necessitates the use of various forms of legal contracts at each stage of custody transfer. Due to the complexity of oil and gas transfer process, there are chances of getting complicated contracts. It is always a massive and time-consuming job to keep track of all legal information from contracts. Smart contracts of Blockchain technology can be used to convert every detail in the legal contracts into electronic contract. All the transactions are evaluated against the legal requirements drafted in smart contract. This enables operators to adhere to all regulations and make quicker decisions about production, distribution, transportation, and several other tasks. Another advantage of smart contracts is that they minimize paperwork and make it easier to track legal details. On the other hand, smart contracts must be reviewed and revised regularly as per the change in the trade conditions. Small mistake in smart contract may cause significant loss [14].

3.5 Trading and Taxation

- **Trading Process**
  Oil and gas is a dynamic industry where oil and gas prices change continuously as per global demand and supply situations. Fluctuations in the rates may create confusion

and frauds. To avoid any confusions and fraudulent activities end-to-end process of custody transfer should be transparent. Use of Blockchain technology allows all parties involved in a transaction to record the same information about the prices fixed at the time of deal their ledgers. As a result, each party thus has a clear understanding about the details of the deal and there is no chance of conflicts regarding prices [14].

- **Benefits to Governments [7]**
  Oil and gas industry faces economic conflicts around the globe because of taxation policies and price fluctuations. As discussed in earlier sections, export and import of petroleum products is the major source of income for governments through foreign exchange and taxation. There are several examples where many governments have lost billions of dollars in terms of revenue because buyers and sellers found loopholes in the custody transfer process in traditional approach. Due to introduction of blockchain, governments can directly track the end-to-end process of custody transfer. Governments get details of commodities being transferred. By implementing legal aspects through smart contracts, governments can check adherence of participants towards the laws. As a result, fraudulent activities in trading and taxation process can be easily detected.

3.6 Scenario

As shown in Figure, we have taken a simple scenario for our project that involves at least one stage from each of the Upstream, Midstream, and Downstream stages of custody transition process. We set Germany as the buyer and America as the seller. When considering a purchase, the Buyer first places an order that includes order details such as volume, time, global and national measurement standards followed by the Buyer. Then, the order is processed, validated and sent to Seller. The Seller then checks if the deliverable quantity is available. If available, it accepts the order and updates the blocked quantity. Government one and Government two check national and global measurement system standards of both buyer and seller. Apart from metrological standards governments are specifically look for details of the deal such as date time cost and volume. Once the transaction is approved, the requested quantity is handed over to Transportation Service Provider which transports commodities from seller to buyer. Transportation Service Provider keeps updating its location time by time till it reaches to Buyer's country.

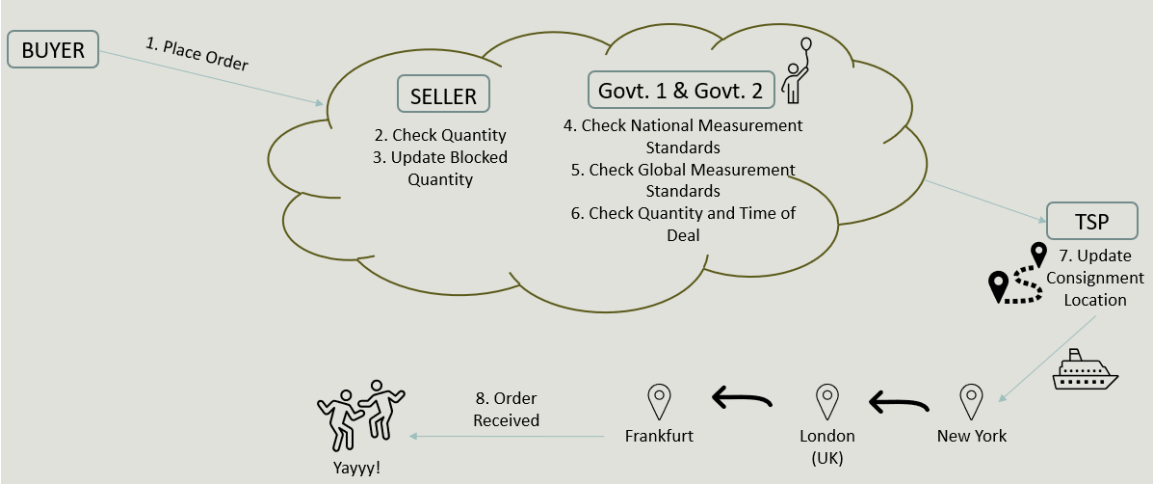


Fig. 1. A normal process in Custody Transfer

4. Architecture

Custody transfer architecture consist of five organizations namely seller, buyer, government from seller side, government from buyer side and transportation service provider. Every organization will have one peer node each, in which three peer nodes are endorsing peers and rest will be committing peer. Endorsing peer is the peer which provides an approval to the transaction when it is proposed, whereas committing peer will save or commit the traction into the ledger after the transaction was submitted by the endorsing peer. All these peers are connected through a single channel that provides transparency which means any modification or update in one organization will be notified to rest. The transaction request and the response will be maintained by orderer in the form of queue, it helps to order the transaction request/response from organization. To store this ledger record state database is used in Hyperledger fabric, which includes LevelDB and CouchDB. In our project, CouchDB is used to store the record instead of LevelDB because it accepts the Json format for data collection. The working flow of this architecture will be explained in the section. The figure 2 shows the architecture.

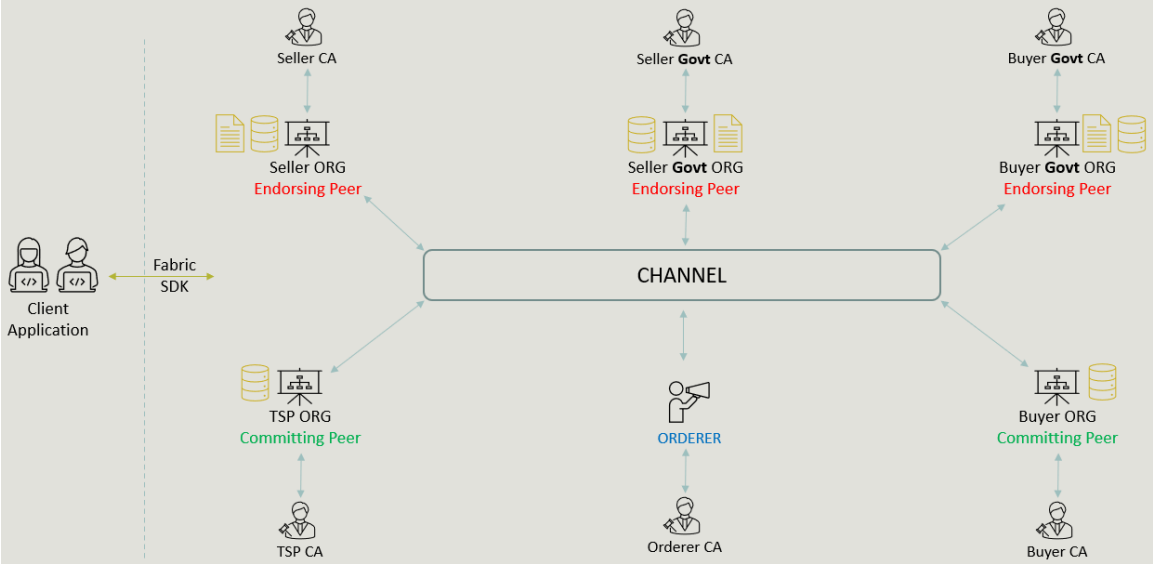


Fig. 2. Architecture of Custody Transfer using Hyperledger Fabric

4.1 Workflow of Custody Transfer architecture

The architecture gives an idea about the main components in the network and the use of each component. This section will explain the transaction flow in the blockchain of custody transfer. Initial step takes place when the buyer places an order, the request is sent to the endorsing peers i.e., Government from Buyer side, Government from Seller side and Seller. The governments verify the metrological credentials (standards) of both parties the buyer and seller to make sure that the transaction is legal and secure to trade. Later, the seller verifies the buyer's credential to make sure he/she is not threat before accepting the request. Once buyers credential is verified, seller checks for the availability of requested quantity. If the requested quantity is available, then the amount of crude oil is blocked. If the quantity is not available, then the request will canceled by the seller. Once the quantity is blocked it will be updated on the ledgers of all five organization Gov1, Gov2, seller, buyer, TSP along with other parameters. Then the crude oil is transferred to TSP (transportation service provider) for shipping. Once the TSP receives the oil that will update the ledger with the received quantity as well as the location at each checkpoint. Finally, when the crude oil is reached to the destination the buyer updates the ledger with the received quantity. By performing these transactions and updating the ledger at every step transparency is achieved. Trust factor is also improved. There is no scope for fraud because all the transactions and communication take place in the chain and it is constantly monitored by both the governments. As all the participants are constantly updating the ledger from time to time the governments ensure that the same quantity is delivered as requested by the buyer as a result there is no loss for both the governments.

5. Implementation

Hyperledger fabric is an open-source enterprise grade permissioned distributed ledger technology platform. This platform is designed to use in the context of enterprises, which provides different functionalities or capabilities over blockchain platform. Fabric is configurable architecture which means it is flexible for any modification in the network. The key elements to build a custody transfer using Hyperledger fabric are as follows,

- Network Setup
- Smart Contracts
- Database
- Client Application

5.1 Network Setup [1]

To setting up a custody transfer network using Hyperledger fabric, certain steps need to followed. These steps will helps to achieve network with five organization consists of one peer node each, which are connected to a single channel. Each organization will have a database to store records.

5.1.1 Prerequisites

Before starting the network setup in hyperledger fabric the following prerequisites needs to be installed on the platform where blockchain application development or operating hyperledger fabric takes place.

- Git
- cURL
- Docker and Docker Compose

5.1.2 Network setup in Hyperledger Fabric

After the installation of the prerequisites. Next step will be having hyperledger fabric on working platform by installing docker images, binaries and sample application, which will be modified based on the architecture of custody transfer in the following steps.

- **Docker containers for organization**
  The initial step of setting up a network is to create containers in docker for the orderer and organization peer nodes. The way to create a container is by specifying the volumes, network and services. The service consist of container name, working directory, environment, ports and docker image. In environment section enabling

of transport layer security(TLS) flags, setting up listening ports and peer specific variables takes place, where as working directory specifies the path of network. One of the important part in creation of docker container for five organisation is port number, which helps to allocate the volumes. By following the pseudo structure shown in figure 3, we can build the five organisation container. The figure 4 shows five organisation container achieved in docker.

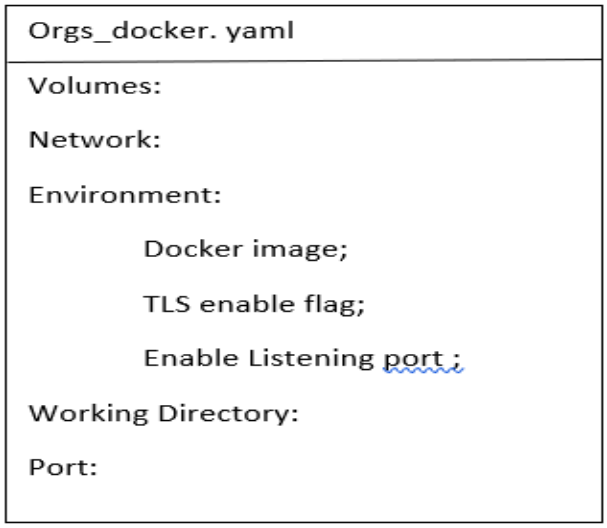


Fig. 3. Five Organisations Pseudo Structure

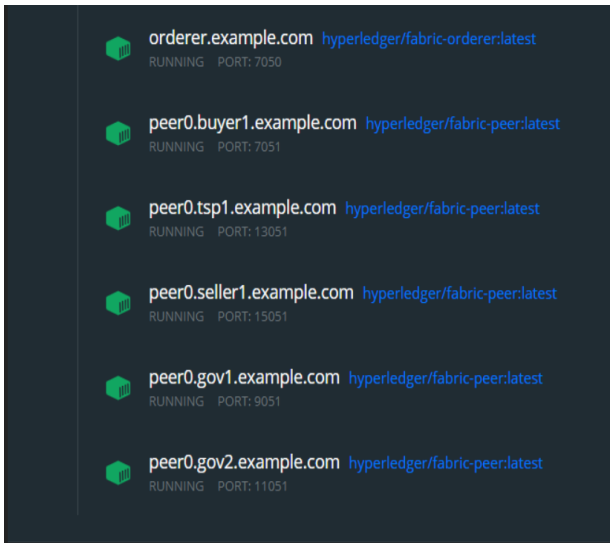


Fig. 4. Five Organisations Peer Nodes

- **Docker container for certificates**
  Every organization will be authenticated by certificates, so con- tainer needs to be created for every certificates. It specifies same components for creating container as organization, but in the environment section it will specifies the certificate server name, certificate server port number and TLS enabling flag. The following pseudo structure figure 5 helps to create certificate for all organisations. The figure 6 shows the container created for certificate in docker.

- **Docker container for Database [15]**
  In hyperledger fabric state database is used, to store the ledger records in the world state. Both LevelDb and CouchDb included in the state database for programmers or developers to verify the records. LevelDB stores the records in key value pair where as CouchDB in JSON format with rich query to the data collection. In custody transfer project the CouchDB is used for storing and verifying the record.

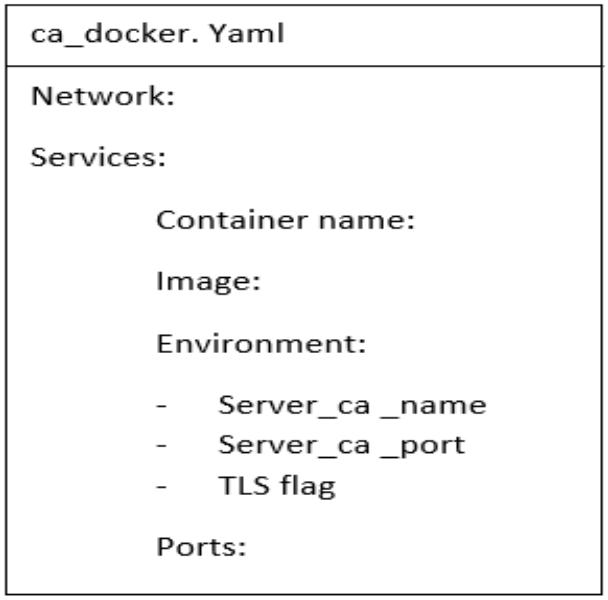


Fig. 5. Certification Pseudo Structure

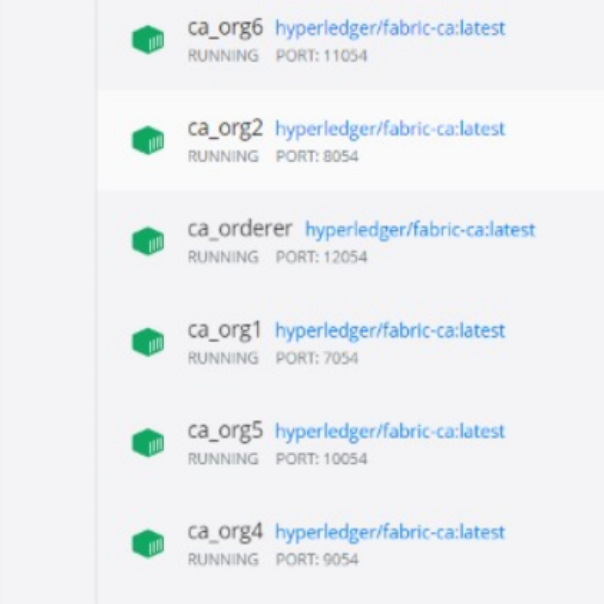


Fig. 6. Certification in Docker

Docker container creation for the CouchDB will also have same components as certificates and organization, where in the environment section it specifies the username and password for the database i.e., figure 7. The figure 8 shows couchDB container in docker.

- **Configuration of organization**
  In this section the organisation identities will be defined, which means it defines membership service providers(MSP) in hyperledger fabric. MSP provides abstraction of membership operation. To create an identity for the organisation the given pseudo structure need to be followed as given in figure 9. The main elements in the organisation to configure are follows,
  - Name of the organisation
  - ID to load MSP defination
  - MSP directory, provides path of the file in the the system which contains the MSP configuration.
  - Policies defines set of policies namely Read, Write, Admins, endorsement
  - Anchor peer defines the location of peers , which can be used in cross organization gossip communication.

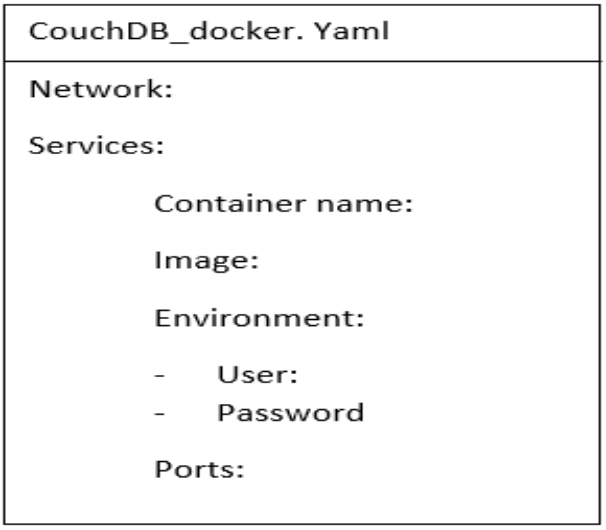


Fig. 7. CouchDB Pseudo Structure

Fig. 8. CouchDB in Docker

- **Single channel creation**
  The organizations are created for the network has to communicate with a single channel. The channel creation takes place by executing the create command, consist of orderer port number, channel name and orderer certificate in channel artifacts. The tool called configtxgen is used to create channel configuration transaction in the network. The following figure 10 helps to create channel for the organisations specifically based on the requirements. The following figure 11 shows the single channel created for all five organisation in docker.

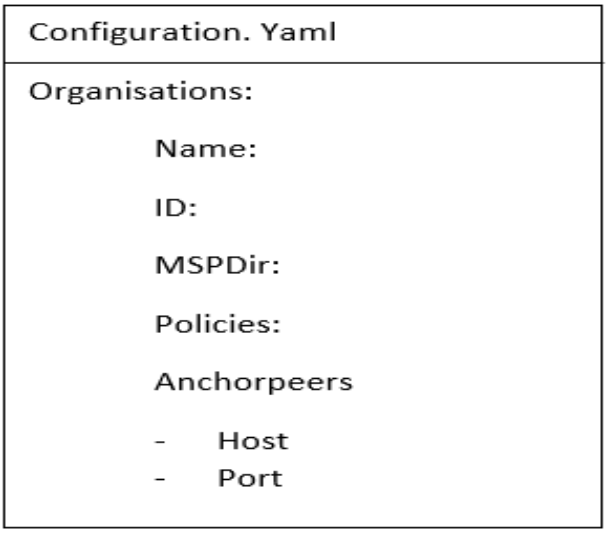


Fig. 9. Organization Configuration

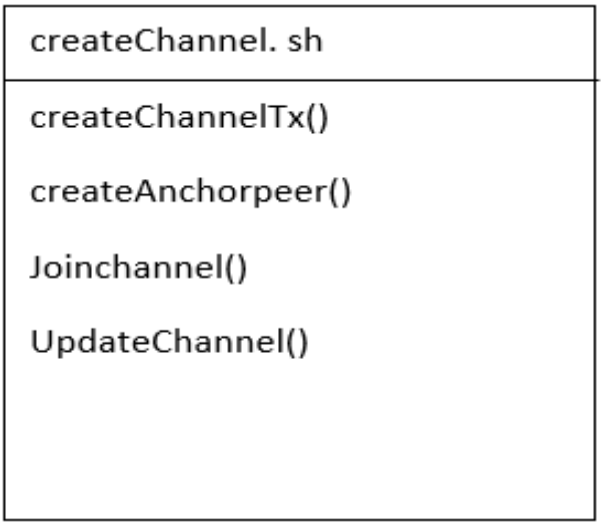


Fig. 10. Single Channel Pseudo Structure

- **Bring up the network**
  The final step to bring up the network is, executing the script file which consist of commands to create volume for organisations, database and the certificate and also to create identities and a channel for organisation. Basically this script will call all the files required to build a network as illustrated in figure 12. The command used for executing this script is as follows, which helps to bring up the network of five organisation consisting one peer node each.

Network Up

```
./network.sh up
```

After network is up these five organisation has to communicate through single channel, so to create a single channel the following command is used,

Create Channel

```
./network.sh createChannel
```

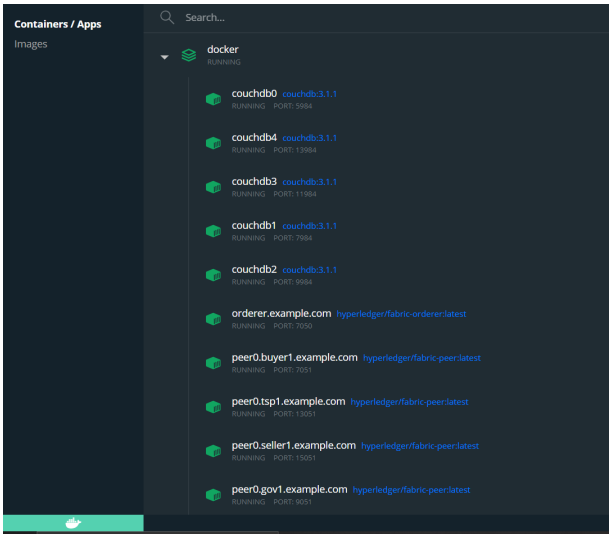


Fig. 11. Organizations with Single Channel

Finally, the last step is to bring down the network, to do that the following command is used,

Network Down

```
./network.sh down
```

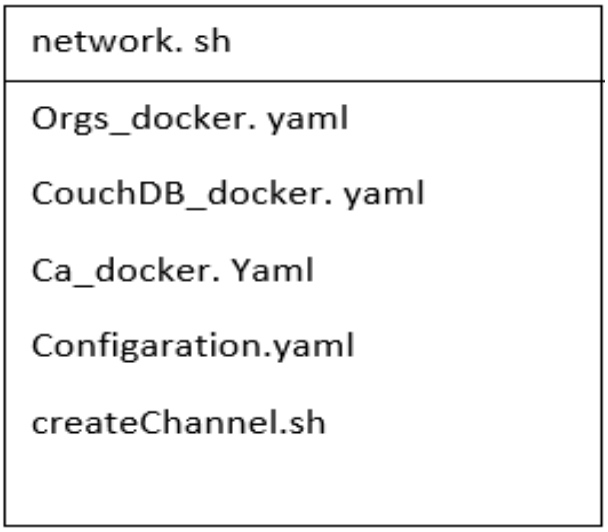


Fig. 12. Pseudo Structure to bring up the Network

5.1.3 Challenges in Network Setup

Many challenges occurred while creating network of five organizations using hyperledger fabric, some of them as related to theoretical understanding and some are occurred on creation of docker volume. In the following paragraph, the challenges and the solution will be explained briefly.

- Firstly, before starting of the network the binaries needs to installed properly. If the binaries are not installed, the network will not start to build. So installation of binary for hyperledger fabric is very much important part in network setup. To install the binaries the command command can be used.

Install Binaries

```
curl -sSL https://bit.ly/2ysbOFE | bash -s -- <
fabric_version> <fabric-ca_version>
```

- Next problem occurred related to orderer in the network, here the orderer was exiting while bringing up the network. By deleting the docker images and volumes from the docker application will resolve the problem of order immediate exit. The reason behind this problem is, if docker consist older version images or the network is corrupted. By restarting the desktop docker application the installation of the latest version of docker images takes place, with that it gives docker without any malware for network.

- Network will not start if the files in network folder has a syntax error. As .yaml file is case sensitive, have to make sure that there are no changes or modification occurred

in .yaml file before bringing up the network. To check the format of.yaml, there are many online websites present which are useful to resolve this issue.

- Last and the most important part in network setup is port number given to the docker containers. If the port is not correct then there will be an error on channel creation and deployment of chaincode in the network. So the most important thing before bring the network up is to provide correct port number to the container.

5.2 Smart Contracts [2] [3]

With traditional database systems, there exist queries to access the database, whereas, in Blockchain networks, there are smart contracts. A smart contract is at the heart of a blockchain. A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements exist across a distributed and decentralized blockchain network. The beauty of a smart contract is that they don‘t require any outside or third party to control transactions which results into cost and speed advantage. In Hyperledger Fabric, smart contracts are deployed in packages referred to as chaincode.

Let's have a small comparison between the smart contracts of Etherium and Hyperledger Fabric. Etherium has only one programming language called Solidity, whereas, in HLF, we are free to choose among languages that are supported by JVM and Node.JS. Moreover, HLF contracts are opensource and free to use. And the main reasons behind existence of HLF are we can have permissioned membership, whereas others are public and we do not need to spend money in mining process. The normal process is, Organizations that want to validate transactions or query the ledger need to install a chaincode on their peers. Then the peers can deploy the chaincode to the channel and use the smart contracts in it to assess assets on the ledger. A chaincode is deployed using Fabric chaincode lifecycle which consists of 4 steps,

- Package the smart contracts in a chaincode
- Install the chaincode package
- Approve a chaincode definition
- Committing the chaincode definition to the channel

For our project, We have automated these steps into one script called **deployCC** and We chose JavaScript as a language for Smart-contract development and therefore, we used fabric-contract-api. One important thing about the smart contracts of our projects is that, we have also implemented most of the methods for future scope in advance. Once the network is up and all the containers are running, execute following command:

Deplay Chaincode

```
./network.sh deployCC -cci InitLedger
```

Smart Contract is the only interface in Blockchains to access the database. The normal flow is, on each peer, there is a ledger and possibly a smart contract and whenever the peer receives any query, it has to go through smart contracts to access the database.

5.3 Client Application

The client application is implemented based on Model View Controller (MVC) architecture, as it is the most commonly used industry standard framework for developing applications. For the development of this application Ember is used which is a JavaScript framework. The main reason for using Ember is that Ember.js tries to incorporate a variety of MVC architecture principles in order to create scalable JavaScript-heavy single-page web applications. Moreover, Ember can work with a larger application ecosystem and it focuses more on performance.

5.3.1 Overview of MVC with respect to Ember

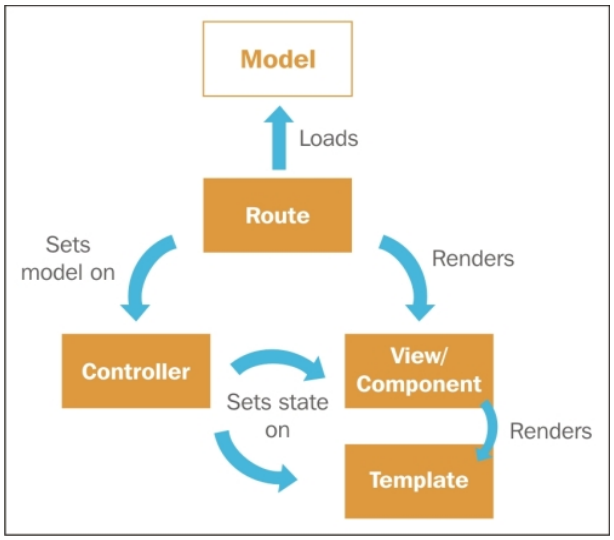


Fig. 13. Ember MVC Architecture [16]

- **Model Layer:** It is a combination of ember data and a model. This layer deals with the server-side communication and data formatting.
- **Controller Layer:** This layer is between model and view. It has routes and controllers built in it. The router is the mechanism that alerts when the URL is altered and updates the application's URL.

- **View Layer:** This layer mainly focuses on displaying elements on the screen. It is also responsible for reacting to user actions like scroll, click etc.

5.3.2 Prerequisites

The following things need to be installed properly:

- Git
- Node.js + NPM
- Ember CLI

5.3.3 Installation

To run our application, go through following steps:

- **Once the network is setup and smart contracts are deployed,** execute following commands from the **test-network** directory:

Start Backend Server

```
# Download all the dependencies
npm install
# Create an Admin Identity in the \textbf{wallet} directory
node enrollAdmin.js
# Create a User Identity in the \textbf{wallet} directory
node registerUser.js
# Start Backend API server on port 3000
nodemon apiserver.js
```

- Open another instance of Terminal and follow steps given below:

Install Dependencies and Start Front-End Server

```
# Clone the Git repository
git clone https://github.com/Safir-Mohammad-Mustak-Shaikh/Custody-Transfer-using-Hyperledger-Fabric.git
# Change to custody-delivery directory
cd custody-delivery-main
# Install the dependencies
npm install
# Start the front-end application server
ember serve
```

Now, to open the application, browse http://localhost:4200 and to view the tests, browse http://localhost:4200/tests.

5.3.4 Working

Currently we have developed only a static transfer i.e that is, there is only one fixed buyer country (Germany) and seller country (USA). Let us now look at how the transaction takes place from the client application.

- **Login Screen:** A simple user-friendly interface has been created. On the login screen there is a field called User Type that specifies the type of user. There are three different User Types:
  - Buyer
  - Seller
  - TSP (Transportation Service Provider)

  When a specific user is selected, the corresponding country is set by-default.

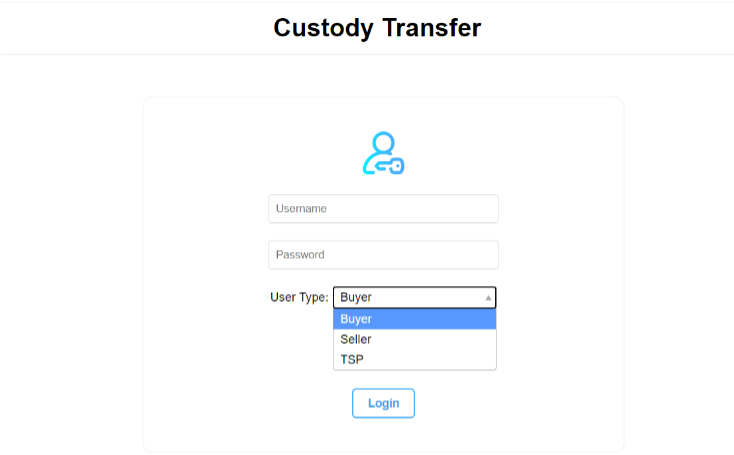


Fig. 14. Login Screen

- **Buyer Screen:** We have provided an important use-case for Buyer for placing an order. As we can see from the figure 16, there are three different fields. The first one is for the quantity of crude oil that has to be ordered. The second one is the Global

standard certificate and the third one is the Local or national Certificate of buyer. Once these details are filled the order is confirmed. The buyer gets a confirmation that the order is successful. If the buyer places an order with a quantity more than what seller has then the order will not be placed.

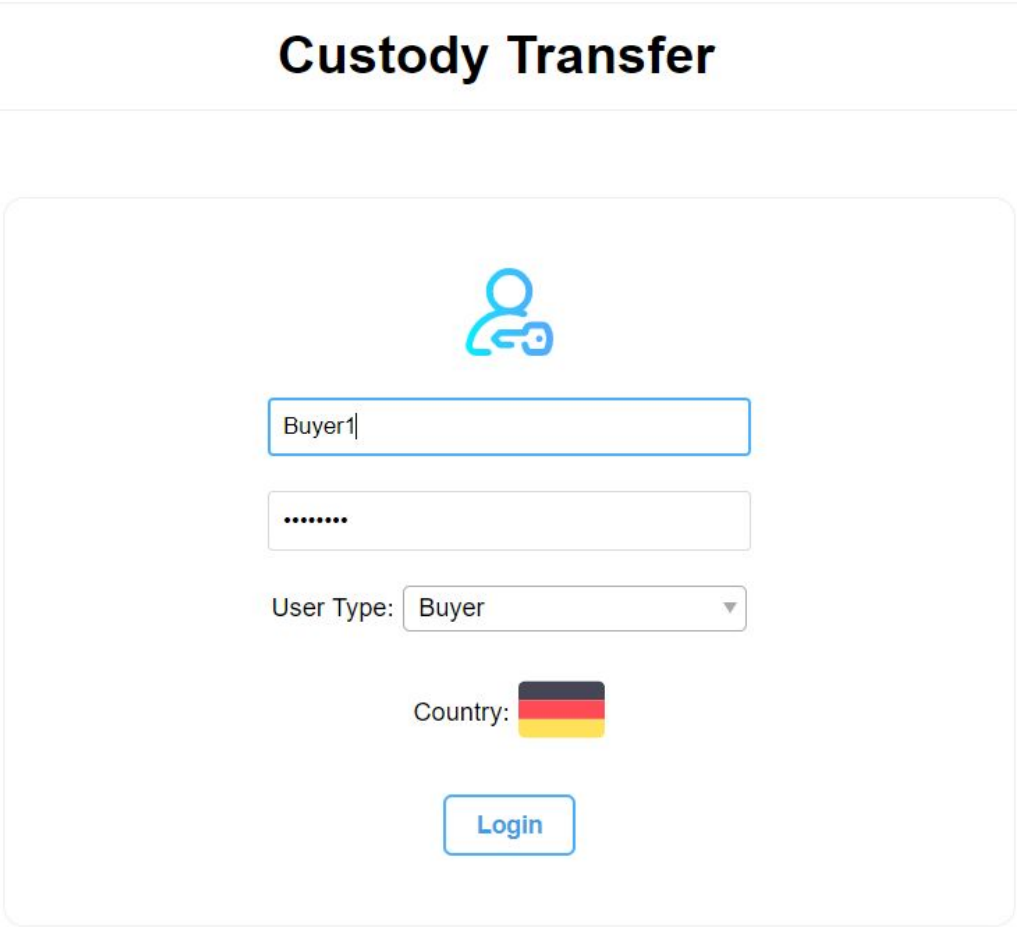


Fig. 15. Login Screen for Buyer

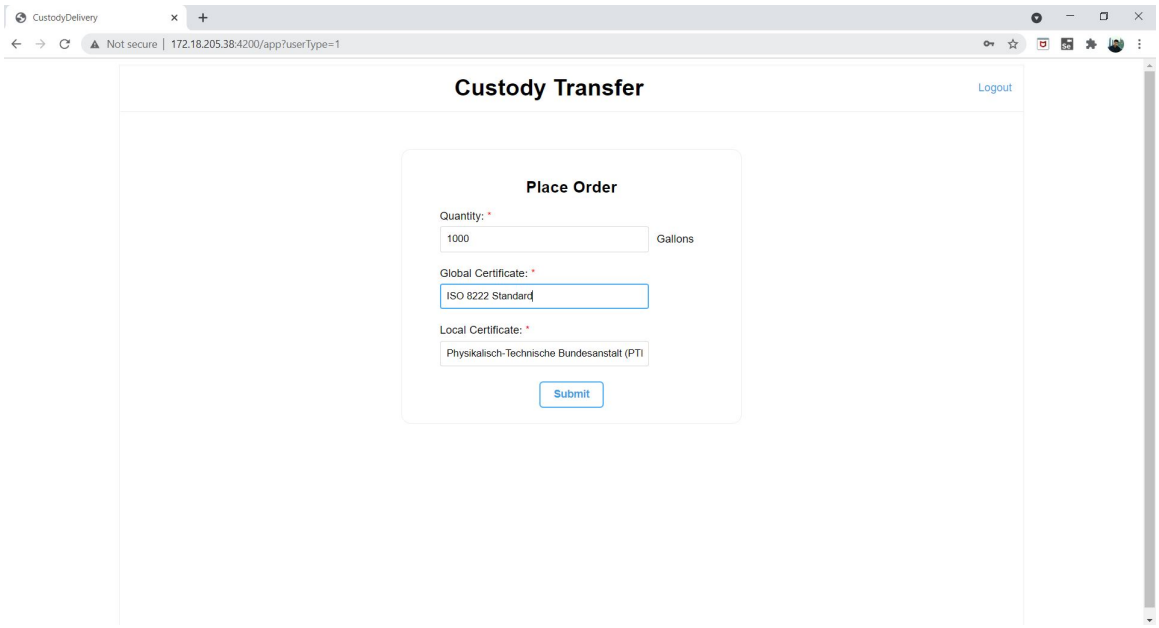


Fig. 16. Place Order

- **Seller Screen:** Figure 17 shows the login page for Seller. And, the country for Seller is automatically selected as USA according to our scenario.

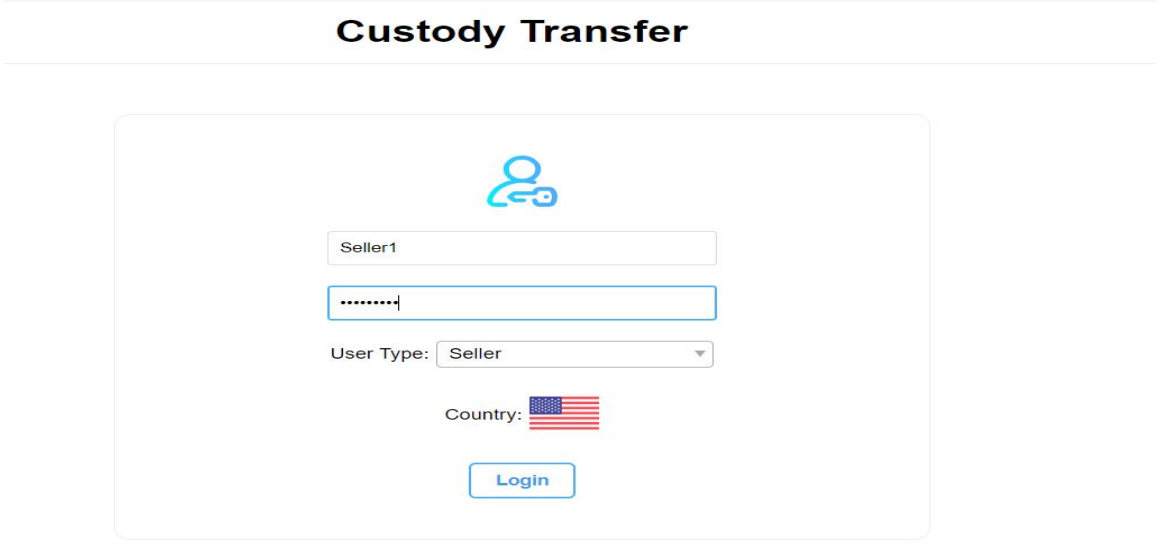


Fig. 17. Login Screen for Seller

Once the seller is logged in there are three different fields that appear on the screen.

– **Display Asset Information**
There are different attributes in display asset info such as assetid, rate, coun-

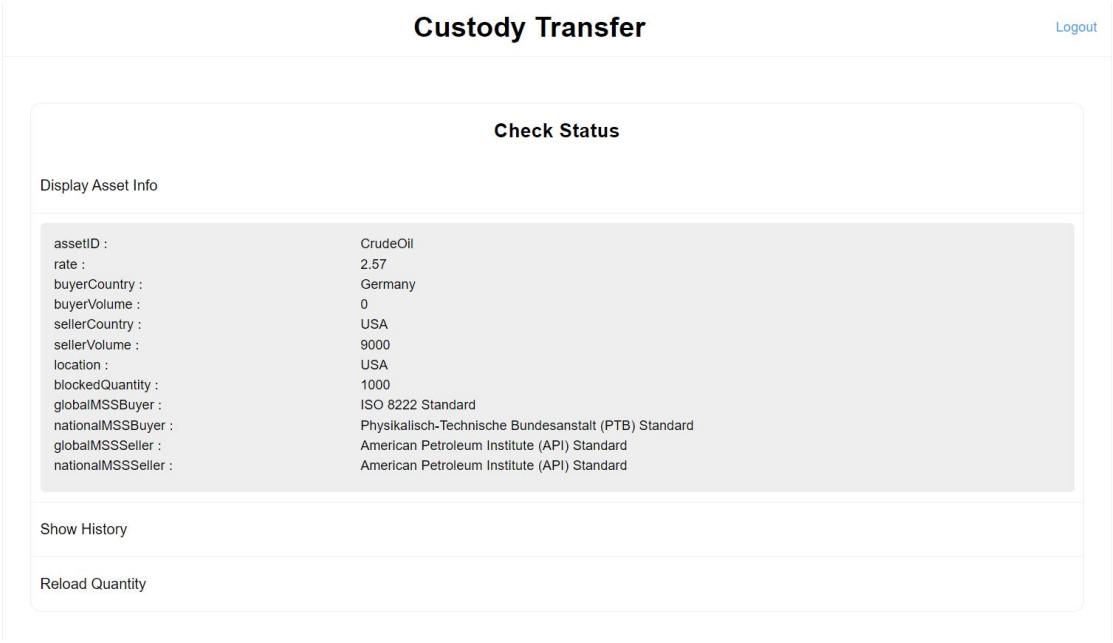


Fig. 18. Display Asset Information

try etc. But the important thing is to look at buyerVoulume, sellerVolume, blockedquantity. Initially the buyer volume is set to 0 even though there was an order placed with some quantity. This is because the order is not delivered yet. Once the order is delivered it will be changed to the original amount of placed quantity. Blocked quantity tells the quantity of crude oil ordered by the buyer (i.e., 1000 from the above image). This is important because it will block the quantity of 1000 or it will reduce the seller's volume by 1000 so that the next person who places an order will have limited quantity to order and also it will notify the TSP that the required quantity has to be shipped so that the TSP can prepare accordingly.
Let us now look at how display asset changes when the order is delivered.

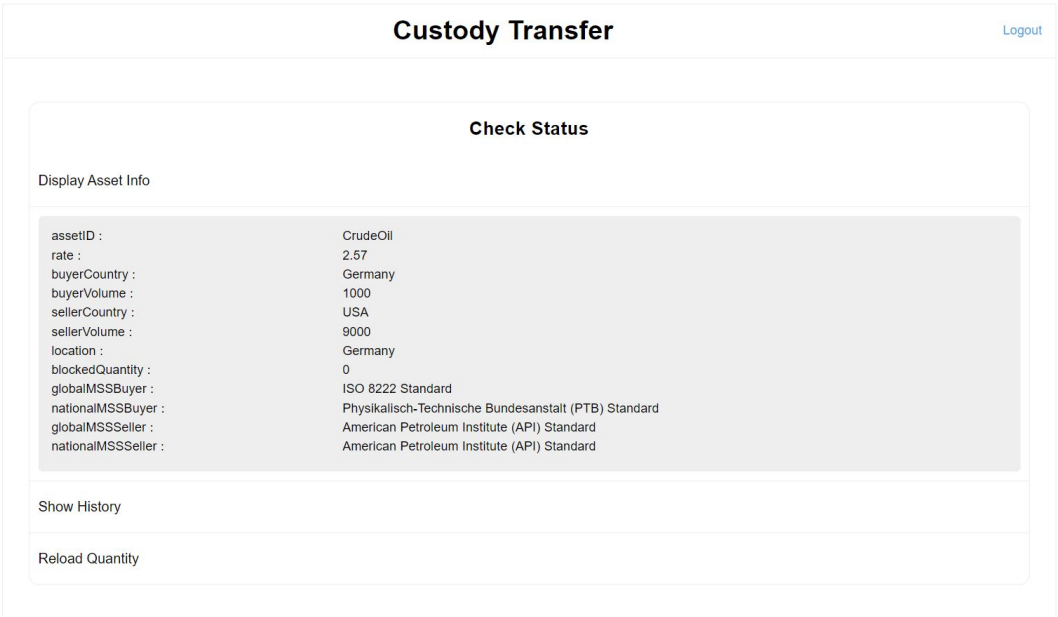
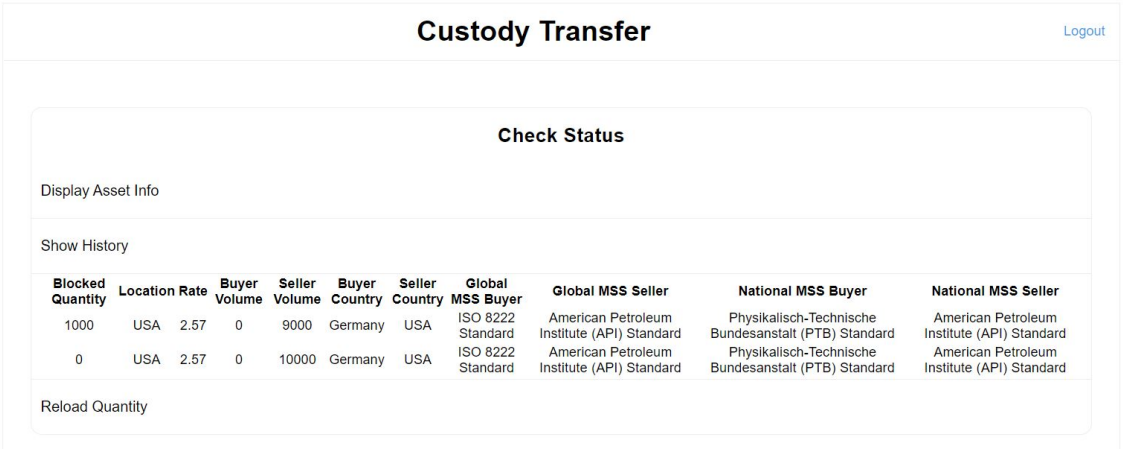


Fig. 19. Seller Order Completion Status

As we can see in figure 19, once the order is delivered, buyer volume changes to 1000 and blocked quantity changes to 0.

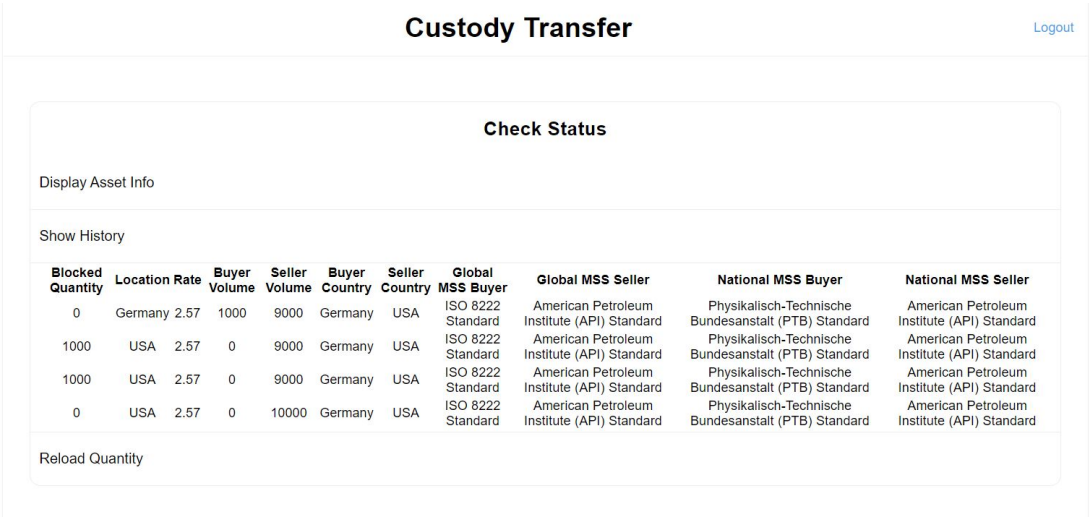
– **Show History**
This will show the entire history of the transaction. As and when the TSP updates the location it will be notified in show history.



Blocked Quantity	Location	Rate	Buyer Volume	Seller Volume	Buyer Country	Seller Country	Global MSS Buyer	Global MSS Seller	National MSS Buyer	National MSS Seller
1000	USA	2.57	0	9000	Germany	USA	ISO 8222 Standard	American Petroleum Institute (API) Standard	Physikalisch-Technische Bundesanstalt (PTB) Standard	American Petroleum Institute (API) Standard
0	USA	2.57	0	10000	Germany	USA	ISO 8222 Standard	American Petroleum Institute (API) Standard	Physikalisch-Technische Bundesanstalt (PTB) Standard	American Petroleum Institute (API) Standard

Fig. 20. Show History

From the above figure 20, we can see that the recent location updated by TSP is USA and also the blocked quantity is 1000. It will be turned to 0 as and when TSP updates the location to the buyer country i.e., Germany.



Blocked Quantity	Location	Rate	Buyer Volume	Seller Volume	Buyer Country	Seller Country	Global MSS Buyer	Global MSS Seller	National MSS Buyer	National MSS Seller
0	Germany	2.57	1000	9000	Germany	USA	ISO 8222 Standard	American Petroleum Institute (API) Standard	Physikalisch-Technische Bundesanstalt (PTB) Standard	American Petroleum Institute (API) Standard
1000	USA	2.57	0	9000	Germany	USA	ISO 8222 Standard	American Petroleum Institute (API) Standard	Physikalisch-Technische Bundesanstalt (PTB) Standard	American Petroleum Institute (API) Standard
1000	USA	2.57	0	9000	Germany	USA	ISO 8222 Standard	American Petroleum Institute (API) Standard	Physikalisch-Technische Bundesanstalt (PTB) Standard	American Petroleum Institute (API) Standard
0	USA	2.57	0	10000	Germany	USA	ISO 8222 Standard	American Petroleum Institute (API) Standard	Physikalisch-Technische Bundesanstalt (PTB) Standard	American Petroleum Institute (API) Standard

Fig. 21. History after Delivery

As TSP has updated the location to Germany the blocked quantity has become 0 and the buyers volume has changed to 1000. This states that the crude oil is delivered to the buyer.

– **Reload Quantity**
If the seller receives new stock, it can be updated via reload quantity. In figure 22, we can see that the seller has reloaded 2000 gallons.

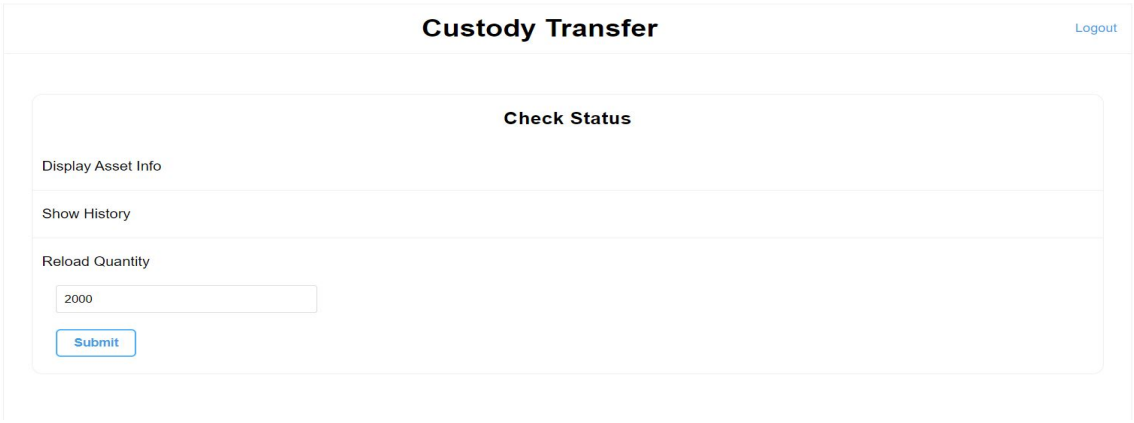


Fig. 22. Reload Quantity for Seller

As the quantity is reloaded, sellers volume is also updated. Initially the sellers volume was 9000 (In display asset) now we can see in figure 23 that, the volume has changed to 11000.

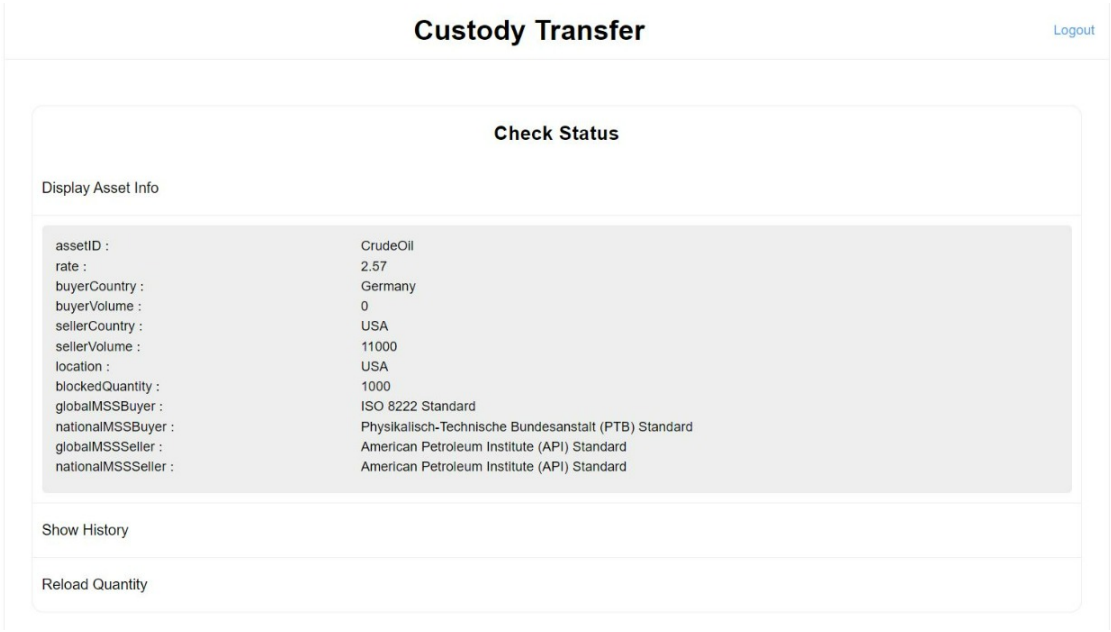


Fig. 23. Seller Volume after Reload

- **TSP Screen:** TSP has two fields one is show blocked quantity and the other is update location. Initially the blocked quantity is 1000. As the location is updated to Germany the blocked quantity is changed to 0. This is because the blocked quantity becomes zero when the order or commodity is delivered to the buyer.

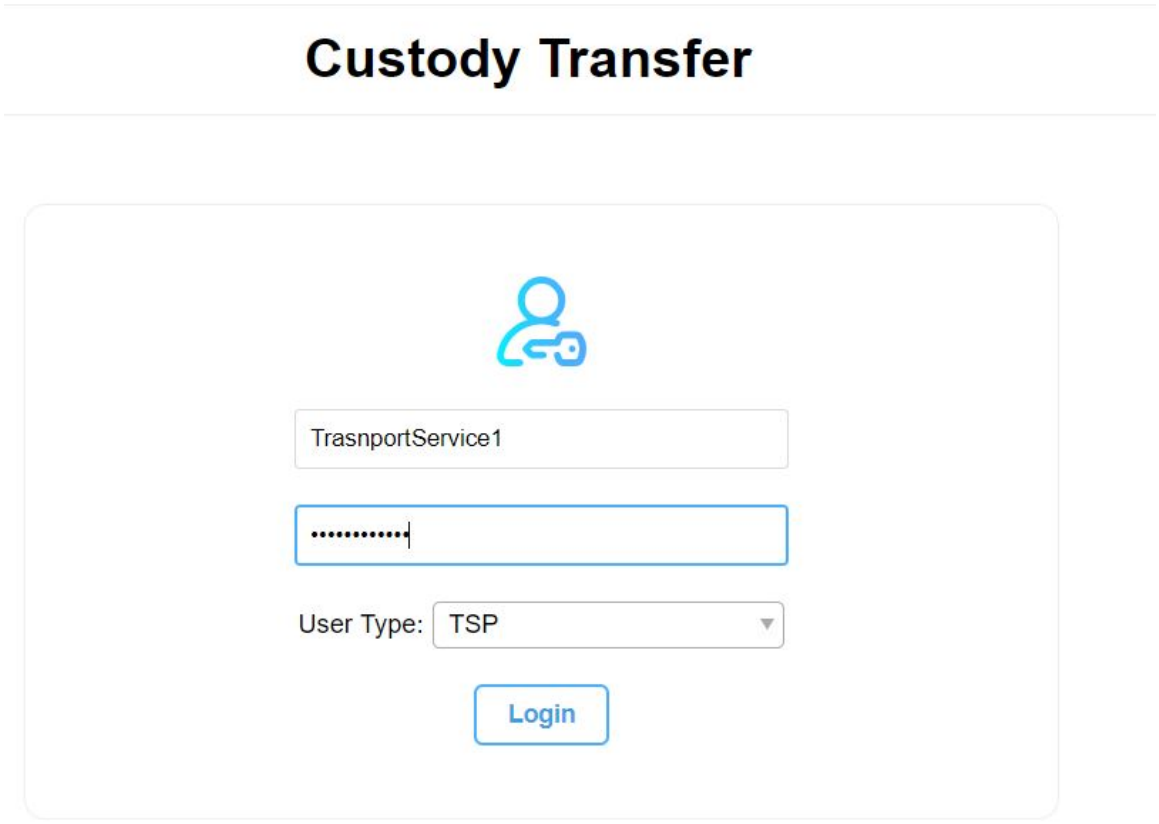


Fig. 24. Login Screen for TSP

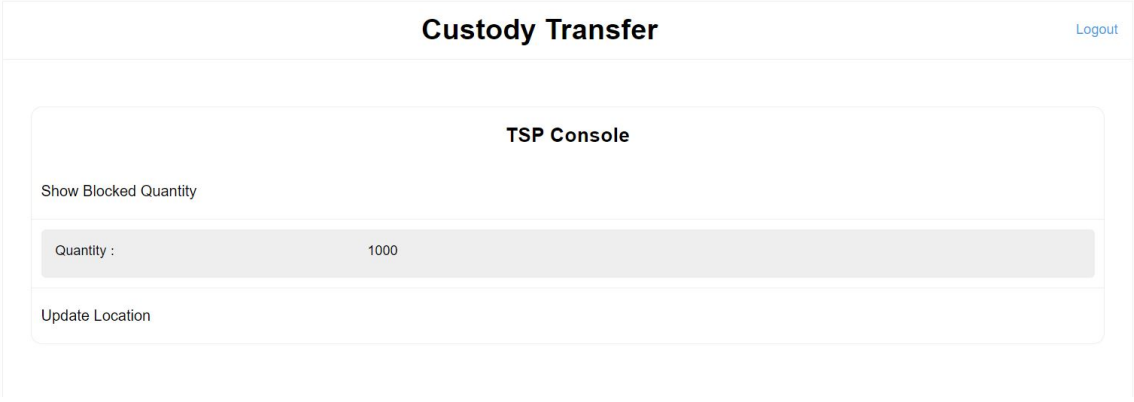


Fig. 25. Blocked Quantity before Delivery

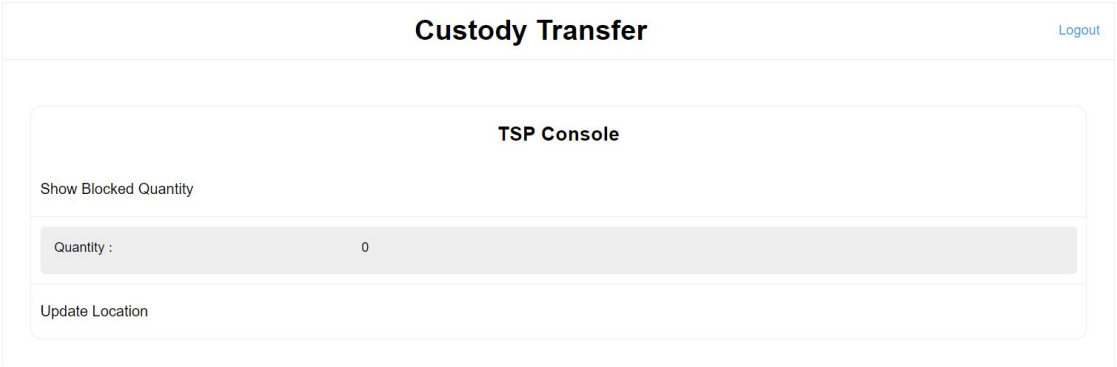


Fig. 26. Blocked Quantity after Delivery

6. Results and Discussion

The use of blockchain in the custody transfer process creates a transparent and reliable platform. Since identical ledger copies are shared by all stakeholders, all stakeholders are on the same page. Legal aspects such as metrological standards are verified using smart contracts before start of the process. Transactions are approved only if the legal requirements are met by the stakeholder submitting the transaction. All transactions are approved based on common consensus hence transaction data that is stored in the ledger is unambiguous. Stakeholders are identifiable, network is private and unauthorized access is restricted. Users having valid CA get access to the network and can submit transactions over the channel. Thus, we can conclude that, using Hyperledger fabric in this project we achieved all basic the requirements for implementation of blockchain technology in custody transfer application.

7. Conclusion

The oil and gas industry has a lot of potential for blockchain technology, but it's only been around for two years, so there are a lot of possibilities, obstacles, and risks. Blockchain technology has the potential to transform the oil and gas sector by lowering transaction costs and increasing transparency. However, it also faces many challenges and needs to address many technical and regulatory issues. Talking about Hyperledger Fabric, it is the cutting edge framework for Blockchain having features like open-source, free-to-use and permissioned membership. Moreover, due to few reasons such as,

- Automation of payments based on commodity volume exchange,
- Fewer disputes,
- Availability of entire exchange history for faster resolution etc.

we have come to a conclusion that the topic which we have chosen, i.e. Custody Transfer best suits this technology.

8. Future Scope

Custody transfer is a wide domain. It includes numerous processes. In our project we implemented a simple scenario where we provided specific features and functionalities to each stakeholder. When it comes to features and functionality, there is undoubtedly a lot of room to provide stakeholders a variety of options. The following are some potential features we would like to include,

- Login and display transaction history for governments
- Additional features to buyer such as display asset and asset track location
- Provision of cost and taxation details to all stakeholders
- Display metrological data (Temperature, Pressure, Flow Rate, Density, etc.) from measurement devices during transfer

Apart from features, we would like to make this application dynamic. As of now, buyer and seller are fixed and communicating on single channel. The advancement in this scenario could be having multiple buyers and sellers along with their respective governments. This will result in a multi-channel architecture in which transaction data on one channel is limited to the participants communicating on the same channel.

Acknowledgments

This project was possible under the guidance and direction of Prof. Dr. Martin Kappes and tutors, Mr. Lukas Atkinson and Mr. Johannes Bouché. We sincerely acknowledge the contribution of our project group members in development of blockchain network using Hyperledger fabric. We are really grateful to have managed to complete the implementation of this project within the time frame provided by Prof. Dr. Martin Kappes. This report is the final submission for the course High Integrity Systems Project taught in the Master's programme High Integrity Systems (HIS).

References

[1] Creative Commons Attribution 40 International License Revision 222fbc83 Install Samples, Binaries, and Docker Images. Available at https://hyperledger-fabric.readthedocs.io/en/release-2.2/install.html.

[2] JAKE FRANKENFIELD (2021) Smart Contracts. Available at https://www.investopedia.com/terms/s/smart-contracts.asp#:~:text=A%20smart%20contract%20is%20a,a%20distributed%2C%20decentralized%20blockchain%20network.

[3] Creative Commons Attribution 40 International License Revision 222fbc83 Deploying a smart contract to a channel. Available at https://hyperledger-fabric.readthedocs.io/en/release-2.2/deploy_chaincode.html.

[4] Wikipedia (2020) Custody transfer. Available at https://en.wikipedia.org/wiki/Custody_transfer#:~:text=Custody%20Transfer%20in%20the%20oil,and%20ships%20and%20other%20transactions.
[5] Maximilian Enthoven Tokenized Custody Transfer. Available at https://www.maximalwert.com/projects/tokenized-custody-transfer.
[6] DUPUIS E, HWANG G Custody Transfer: Flowmeter as Cash Register. Available at https://www.controleng.com/articles/custody-transfer-flowmeter-as-cash-register/.
[7] Prast, William G (1964) The Role Of Host Governments In International Petroleum Operations. https://doi.org/10.2118/1035-MS. sPE-1035-MS https://onepetro.org/SPEERM/proceedings-pdf/64ERM/All-64ERM/SPE-1035-MS/2086888/spe-1035-ms.pdf Available at https://doi.org/10.2118/1035-MS
[8] Creative Commons Attribution 40 International License Revision 222fbc83 Introduction. Available at https://hyperledger-fabric.readthedocs.io/en/release-2.2/whatis.html.
[9] Muneeb, Shah Oil custody transfer: Blockchain comes to the rescue. Available at https://www.wipro.com/blockchain/oil-custody-transfer-blockchain-comes-to-the-rescue/.
[10] Precision Software COULD BLOCKCHAIN REVOLUTIONIZE PARCEL SHIPPING?. Available at https://bit.ly/347EEXp.
[11] THOMAS SIMMS Louis Vuitton and Christian Dior Owner Unveils Blockchain Platform to Verify Luxury Goods. Available at https://bit.ly/2XyTcNa.
[12] Accenture Getting to Value with Blockchain in Oil and gas. Available at https://www.accenture.com/us-en/service-getting-value-blockchain-oil-gas.
[13] Chopade M, Khan S, Shaikh U, Pawar R (2019) Digital Forensics: Maintaining Chain of Custody Using Blockchain. *IEEE Xplore* .
[14] Lu H, Huang K, Azimi M, Guo L (2019) Blockchain Technology in the Oil and Gas Industry: A Review of Applications, Opportunities, Challenges, and Risks. *IEEE Access* 7:41426–41444. https://doi.org/10.1109/ACCESS.2019.2907695
[15] Deeptiman Pattnaik (2020) CouchDB as a State Database in Hyperledger Fabric. Available at https://www.maximalwert.com/projects/tokenized-custody-transfer.
[16] Packt The Ember.js MVC pattern. Available at https://subscription.packtpub.com/book/web_development/9781784395841/1/ch01lvl1sec10/the-ember-js-mvc-pattern.

A. Task Distribution of Report Writing

Our project can be found at this link: https://github.com/Safir-Mohammad-Mustak-Shaikh/Custody-Transfer-using-Hyperledger-Fabric. The following listing shows the parts of this report written by each individual:

- **Safir Mohammad:**
  - Abstract
  - Related Work (Section 2)
  - Importance of Blockchain in Custody Transfer (Section 3.2 and Section 3.5)
  - Implementation (Section 5.2)
  - Conclusion (Section 7)
  - Acknowledgements
  - References
  - Appendix
- **Parag:**
  - Introduction (Section 1)
  - Importance of Blockchain in Custody Transfer (Section 3.1 and Sections 3.3 - 3.6)
  - Results and Discussion (Section 6)
  - Future Scope (Section 8)
- **Vidya:**
  - Architecture (Section 4)
  - Implementation (Section 5.1)
  - Acknowledgements
- **Pranay:**
  - Implementation (Section 5.3)
  - Conclusion (Section 7)