Turkish Journal of Computer and Mathematics Education *Vol.12 No.3(2021), 3762-3766*

Research Article

Application Of Permissioned Blockchain For Automated, Efficient, Secure Cross Border Trade

Sreedevi B[a], M.S. Bennet Praba[b]

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: There are lot of documents and confidential data involved in international trade. Banks offer financial services and also act as middleman for cross border trades. The verification process plays a vital role and it takes months to years, to complete. The major problem is to maintain integrity and confidentiality of the data shared, and to maintain fair trading process. Blockchain technology is introduced to increase the efficiency and security of the documents shared to the needed parties in the trade. Permissioned blockchain is used wherein the participants of the network are controlled and governed by the blockchain owner. Hyperledger fabric platform is used to implement the trade finance application. The main idea is to automate the verification processes in order to complete the trade financing within minutes to hours and to enhance security of the documents shared using Attribute Based Encryption (ABE) in cross border trades. The smart contracts in blockchain provides functionalities to assure that the information is tamper-free, auditable and verifiable.

Keywords: Attribute Based Encryption, Hyperledger fabric, Permissioned blockchain, Smart contracts, Trade finance

1. Introduction

Cross border trades generate huge amount of data and require thousands of people to verify the documents like letter of credit, bill of lading, etc. The verification process takes several months to years for completion and is a paper intensive task. The documents have to be shared with stakeholders, importer, exporter, banks, government and should be kept confidential. The documents involved in cross border trade are:

1. Commercial transaction documents like invoices, sales contract, packaging lists.
2. Transport documents like bill of lading, import and export licenses, etc.
3. Trade financing documents like letter of credit.

The whole process of verification and sharing of documents can be automated using blockchain technology. Permissioned blockchains like Hyperledger fabric platforms is used such that the participants of the network are controlled by the blockchain owner. This creates a private network and provides authenticity and authorization of the participants. What made blockchain so appealing is the fact that the network is so robust and runs well even in the presence of malicious nodes e.g., Byzantine nodes [5].

Blockchain contains a chain of blocks, which contains all the transactions occurred in the network and provides immutable data ledger with timestamp. The recorded transactions are tamper-free and is used, if any conflicts and confusion occur, in the court of law. Blockchain implemented in trade finance application increases the efficiency of the conventional trading process and reduces the high cost. Smart contracts are used to provide functionality to the participants and acts as a business logic. It implements intelligent programs which triggers actions according to the conditions and enable the transactions.

Blockchain has the potential to disrupt traditional business models described by FinTech Futures [3]. It completely eliminates the Trusted Third Parties (TTPs) and provides participants of the network to agree with each other, using consensus, before adding a block of transactions. In traditional cross border trading system consists of trusted third party intermediaries such as the banks. Banks of the respective importer and exporter acts as a middleman and manages the international trades. Such banks have world-wide connections and provides security to the clients. Importer's bank promise to send money to the Exporter's bank, after receiving the Proof of Delivery. Exporter dispatches the goods using a trusted international carrier like ships and planes. Traditional trading process is inefficient as it completely relies on documents and has lot of vulnerabilities as it is easy to defraud. Banks charges very high fees to their clients and it's difficult to track the goods or commodities.

2.Proposed System:

Using blockchain technology in trade finance, increases the efficiency as it speeds up the whole document verification process from minutes to hours. It guarantees data confidentiality, integrity and provides more secure international trading with less execution costs. All the parties involved are made as the members of the blockchain

network and the documents like letter of credit, invoices and bill of lading are stored in blockchain. The transactions are recorded in the blocks and are irreversible. All participants can view the recorded transactions and reach consensus to add a block to the chain. Smart contracts implemented in the blockchain, takes care of the functionality and conditions of the trading process.

3.System Architecture:

The system architecture showed in figure 1 is the permissioned blockchain network which consists of Importer, Exporter, Importer's Bank, Exporter's Bank and an international carrier like ships and airplanes. In the network, there exist a blockchain owner, who controls all the participants or members of the network. Only selected members are allowed to participate in the blockchain network and is not available for the public. All transactions are recorded in the ledger and viewed by all members. Each block in the blockchain contains transactions with timestamp and only after the network reaches consensus, a block is added to the chain. Each member act as a node in the private blockchain network and installs smart contract on the nodes. Smart contracts are programmed to automate the trading process. It is programmed such that, after goods sent to the Importer's country (destination), the Exporter's bank account will be credited with the payment money from Importer's bank account. Invoices and all other documents are encrypted and sent to the respective parties electronically.

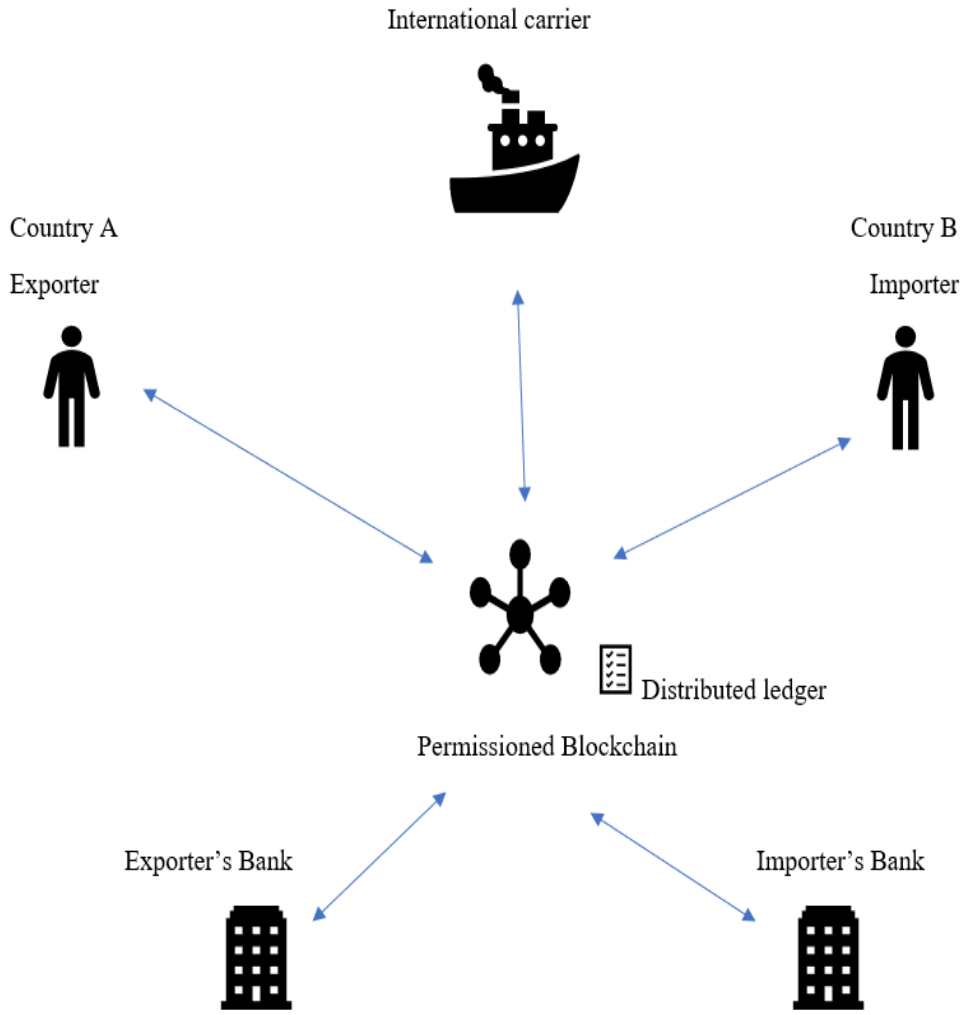

Figure 1. System Architecture

4.Details Of The Process:

Stages:

The stages are:

1. Instantiating of the private blockchain

2. Initializing the network members
3. Invoking the smart contract.

In the first step, instance of the blockchain or the distributed ledger is created. Instance of the blockchain is known as channel. Thus, the network is bootstrapped and the service is made available by the genesis block. In the second step, the participants join the particular channel and maintain records in the ledger. All the members are able to view the ledger and have privileges to commit the updates to the ledger. Next step is to install the smart contract on the members' nodes and it is invoked by running the code, which either updates or queries the ledger.

5.Features:

The important properties involved are:

1. Efficiency:

As the verification of the trade documents is automated and last from minutes to hours, the efficiency increases.

2. Fairness:

Fairness is maintained through out the trading process. Money from the Importer's bank account is transferred only after goods reaching the destination. This provides fairness and secure transactions.

3. Transferring the evidence:

Documents like bill of lading, invoices and other proofs are transferred more securely through blockchain. The concerned parties view the proofs for avoiding any conflicts.

4. Non-repudiation:

The proof of transaction origin and recipient is provided by the ledger, as all the transactions with timestamp is recorded and can be used as a proof in any court of law.

5. Confidentiality:

It is the most basic and important property provided by blockchain technology. All the documents and data are secured and confidential, as international trade contains sensitive data.

6. Implementation:

6.1. Hyperledger Fabric Platform:

It is a permissioned blockchain framework which is used by enterprises, business and hospitals to support private transactions. This platform is modular in nature and also allows to reuse the existing features and modules. The identities of the members in the network are already known. It allows asynchronous transactions and the distributed ledger is viewed by all the participants of the network. Channels are created and the details and data are available only to certain parties involved. Smart contracts are used to update the ledger according to process that takes place eventually.

6.2.Attribute Based Encryption (Abe):

Attribute-based encryption is a kind of algorithm of public key cryptography in which the private key is used to decrypt data is dependent on certain user attributes such as position, place of residence, type of account [2]. Here, Ciphertext-policy Attribute-based encryption (CP-ABE) is used in order to encrypt and decrypt the sensitive documents involved in cross border trade. The private keys and the ciphertext is associated with a policy and can be decrypted only when the user's private key matches with the ciphertext. Thus, it provides authorization as default property. The methods or functions used in CP-ABE are Setup, Encrypt, Key Generation, Decrypt.

6.3. Smart Contract:

Smart contract helps speed up the trading process and increases efficiency of export and import process. It automates the verification process in a secure way. The main components are:

1. The hash of the content is generated by the data owner.

2. The data is signed using the private key of the data owner.

3. The hash of the signed data is returned and signed data is stored.

4. The members in the network are authorized and public key is provided.

5. Verification of the trade documents are done by the members.

6. Real time updates of the goods are recorded.

7. Payment is triggered as soon as the goods arrive the destination.

6.4.Module Description:

The implementation is done using JavaScript, NodeJS, React and Express. The private blockchain is developed from the scratch. The modules are:

1. Creation of block:

In this module, blocks are created and parameters like timestamp, lastHash, hash and data are defined. The hashes of the blocks are created using SHA-256.

2. Creation of blockchain:

In this module, methods or functions are defined for adding blocks to the blockchain. Validation of the incoming chain is also done in this module. The Proof of Work is done using difficulty and nonce values.

3. Creation of peer Network:

Here, Express API is set up for interacting with the backend with HTTP requests. GET and POST requests are created for reading and writing new blocks to the blockchain respectively. Real time messaging in the network is implemented using Redis. Peers nodes are started and broadcast is made.

4. Wallets, keys and transactions:

Core wallet class is created and cryptographic algorithms like Attribute based Encryption is implemented. Signature generation and verification is made to make transactions official. Smart contracts are implemented in this module and developed functionality to actually validate the transactions.

5. Frontend:

It is completed using JavaScript, HTML, CSS. Built React in the frontend using parcel-bundler. Visualized blocks from the backend.

7. Conclusion

International trade requires a highly secure application or system to store sensitive documents. Blockchain technology completely eliminates the Trusted Third Parties and provides immutable, irreversible, distributed ledger to store all the transactions across the network. Permissioned blockchain allows only known identity people to join in the network. This eliminates anonymity and used widely in enterprises, businesses, hospitals, etc.. There are many unexplored platforms which provide private blockchain capability like Corda, Hyperledger Fabric, etc. Each platform have their own features and performances. They can be explored and further performance can be increased in the future works.

References

M. Mut-Puigserver, and M. A. Cabot-Nadal, M. M. Payeras-Capella, “Removing the Trusted Third Party in a Confidential Multiparty Registered eDelivery Protocol Using Blockchain”, IEEE Access, June 8, 2020.

Attribute based Encryption, 2015, http://cryptowiki.net/index.php?title=Attribute-based_encryption

G. Eason, B. Noble, and I. N. Sneddon, “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchain” Eurosys 2018.

Nizamuddin Ariffin, Ahmad Zuhairi Ismail, “The Design and Implementation of Trade Finance Application based on Hyperledger Fabric Permissioned Blockchain Platform”, IEEE, 2019.

Leslie Lamport, Robert Shostak and Marshall Pease, “The Byzantine General Problems” ACM Transactions on Programming Languages and Systems, vol. 4, Dec. 1982.

FinTech Futures, Why blockchain could revolutionise trade finance documentation, June 2018 (on web page https://www.fintechfutures .com/2018/06/why-blockchain-could-revolutionise-trade-financedocumentation/)

H. R. Hasan and K. Salah, ‘‘Proof of delivery of digital assets using blockchain and smart contracts,’’ IEEE Access, vol. 6, pp. 65439–65448, 2018.

J. A. Onieva, J. Zhou, and J. Lopez, ‘‘Multiparty nonrepudiation: A survey,’’ ACM Comput. Surveys, vol. 41, no. 1, pp. 5:1–5:43, Jan. 2009.

M. M. Payeras-Capella, M. Mut-Puigserver, and M. A. Cabot-Nadal, ‘‘Blockchain-based system for multiparty electronic registered delivery services,’’ IEEE Access, vol. 7, pp. 95825–95843, 2019, doi: 10.1109/ACCESS.2019.2929101.

H. R. Hasan and K. Salah, ‘‘Blockchain-based solution for proof of delivery of physical assets,’’ in Blockchain—ICBC (Lecture Notes in Computer Science), vol. 10974. Cham, Switzerland: Springer, Jun. 2018, pp. 139–152.

A.V.Baguscharkov, I.E.Pokamestove, K.R.Adamova and Zh.N Tropina: Adoption of Blockchain Technology in Trade Finance, Nov 2018.

Xiwei Xu, Ingo Weber, Liming Zhu, Jan Bosch, Cesare Pautasso, Paul Rimba: A Taxonomy of Blockchain-Based Systems for Architecture Design, April 2017.