Grenze International Journal of Engineering and Technology, June Issue

A Blockchain-Based System for the Secure Transfer of Assets

Ramesh Cheripelli[1], Ambika Bongirwar[2], Varsha Myadam[3], Byri Sharanya[4] and Siri Mandadi[5]
[1]G Narayanamma Institute of Technology and Science, Dept of IT, Asst Professor, Hyderabad, India
[2-5]G Narayanamma Institute of Technology and Science, Dept of IT, Hyderabad, India
Email:chramesh23@gmail.com,{ambikabongirwar, varshamyadam, byrisharanya12, sirireddy.m01}@gmail.com

***Abstract*— The existing asset transfer mechanisms have several flaws, like high costs, slow processing, and a lack of transparency. The conventional approach used for asset transfer is based on complicated, manual, paper-based processes that involve a handful of intermediaries thereby scammers take advantage of them to mislead the public and the government due to which most buyers become victims. Even the settlement and clearing processes might take many business days from the transaction date, going through numerous intermediaries with separate systems. It causes delays in payment among stakeholders as well as cash flow difficulties. The asset management industry profits from distributed ledger technology (DLT), such as blockchain. In this project, with the help of blockchain technology, we reduce the expenses while increasing operational efficiency and transparency.**

***Index Terms*— Blockchain, Interoperability, Asset transfer, Cross-blockchain protocol, Decentralized asset transfers, Digital assets.**

I. INTRODUCTION

The property exchange system is flawed, so people use it to deceive the public and government. Blockchain majority consensus secures asset transfers in this project. Blockchain asset transactions aim to secure property deals and simplify recordkeeping.

The conventional approach used for asset transfer is complicated, manual, paper-based processes that involve a handful of intermediaries. Global asset transfers face difficulties like hefty costs, sluggish processing and lack of transparency. Many individuals and businesses are hesitant to transfer substantial amounts of money across borders due to lack of faith in an unknown party. The settlement and clearing processes might take up to three business days from the transaction date, going through numerous intermediaries with separate systems. It causes delays in payment among stakeholders as well as cash flow difficulties.

The solution avoids selling the same asset to numerous clients. This proposed solution requires minimal documentation and record-keeping and reduces transaction time, making it reliable. Current methods are difficult to record and assure. n nodes will check and add blocks to the distributed ledger for asset transactions. Thus, the blockchain-based secure asset exchange reduces record-keeping effort.

It can improve organizational efficiency and transparency while decreasing costs. It promotes transparent cooperation by: Blockchain is an integrated technology. A unified database serves as the hub for all assetmanagement processes, both those carried out internally and by external vendors. Since the blockchain handles all financial dealings, incorporating new partners is simplified. Because blockchain transactions are

Grenze ID: 01.GIJET.9.2.311

immutable, they can be relied upon by asset managers to provide transparent accounting of all financial dealings. This paves the way for safe and seamless communication between asset managers and their partners and service providers over topics like asset history. The nodes must verify each block through consensus using proof-of-work, which also helps with practical efficiency. Therefore, erroneous information is avoided.

II. Related Work

Blockchain for Central Banks: Systematic Mapping. This paper maps all scientific papers and identifies blockchain use-cases applicable to central banks, allowing the determination of what issues have already been investigated, yielding a theoretical knowledge or practical contribution.

Their study found that 1) Central Bank issued Digital Currency (CBDC), 2) Regulatory Compliance, and 3) Payment Clearing and Settlement Systems (PCS) operated by central banks are the most research-intensive use-cases, while 4) Assets Transfer/Ownership and 5) Audit Trail are the least.

Fewer papers address how blockchain could affect central bank asset transfer and ownership processes. Why blockchain for central bank asset movement and ownership? Nine periodicals discuss blockchain improvements. DLT is asset-agnostic because it can store, transfer, and record any form of asset [12]. Blockchain can provide, via a shared database [5], a time-ordered and immutable record of transactional history [6], [9], security ownership [4], [15], [16], and all transfers among all payment system participants [2], [18], which can be updated without multiple, specialized intermediaries or third-party infrastructure [19]. IBPS counterparties share the ledger when financial institutions deal. These include asset issuance and servicing [2], [16], enabling trading between partners, and liquidating holdings [17].

Four papers address potential DLT asset transfer and ownership issues. DLT entries are questioned as proof of title. After securities and cash change hands, there needs to be a formal, legally defined transfer of title for final and legal settlement [23]. Legal ownership of securities issued in a DLT is not defined by law [22] or ensured by regulators and regulators [24].

Permission less blockchain asset models use data types, and transactions transmit asset ownership. End-users use private keys in order for signing digital assets tied to their identity and transfer them to other identities with public keys. Miners ensure funds cannot be spent twice. This study proposes a worldwide asset management system that uses permissioned blockchains only to register complex assets in permission less blockchains. The permission less blockchain's smart contract object is the only record of asset title after registration. Additionally, only the permission less network trades this asset. Atomic swaps can sell the asset for additional securities and currencies in other permission less blockchains.

The term "Burn-to-Claim" refers to a procedure that consists of two parts: an exit Transaction that creates a proof that can be independently verified, and an entry Transaction that verifies the proof's validity before recreating the asset. The shipper starts the exit-transaction on the originating network. The author defines a function called export Verifier, which transfers the asset to the given burn-address if and only if both its sub functions spend Verifier and asset Verifier return true. The asset can be sent to the burn-address, but it can never be recovered from the address again because there is no private key associated with it. The recipient starts the entry-transaction on the destination network. When both spend Verifier and proof Verifier verify the asset's recreation, the author's defined import Verifier method will return true.

III. Solution Methodologies

Each block in the blockchain is a chronological record of transactions that reflect a request or update to the global state and are linked together. When blocks are first formed, a feature of the Hyperledger Fabric termed the ordering service determines the order of the blocks and the transactions within them. A hash of each block's transactions and a hash of previous block's header are both stored in the block's header. All ledger events are now cryptographically linked and sequentially ordered in this fashion. The data in the database is encrypted via hashing and linking. Due to the distributed nature of the blockchain, even if a single node holding the ledger were compromised, it would be unable to persuade the other networks that it possessed the "correct" blockchain. Let's take a closer look at the components that make up a blockchain. All seven of block B2's transactions (T5, T6, and T7) can be seen in block data D2 in the preceding image. Importantly, B2 also includes the block header H2 that

hashes H1 and includes a secure hash of all the events in D2. Blocks are linked in this manner in a way that cannot be undone, hence the name "blockchain."

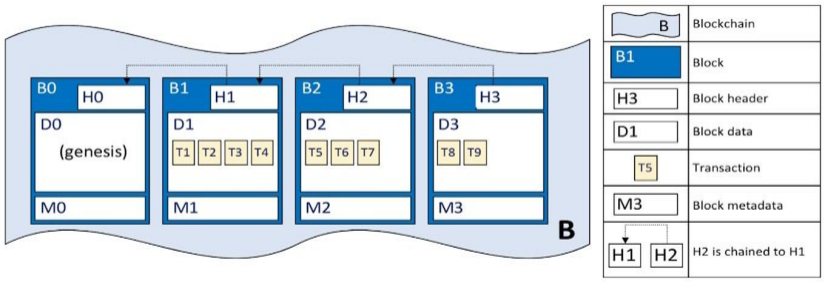


Fig. 1. A blockchain B containing blocks B0, B1, B2, B3

A.Create the org MSP needed to add an org to a channel

Fabric network structures are not equivalent to nodes in terms of real existence. Instead, they are represented on a channel's configuration as a hierarchy of files and certificates. Root CA, intermediate CA (if used), TLS CA, and administrative identities are all named in these certificates.

```
<location of msp>/msp
├── config.yaml
├── cacerts
│   └── cacert.crt
├── intermediatecerts
│   └── cacert.crt
├── tlscacerts
│   └── tlsca.<org-domain>.pem
└── tlsintermediatecerts
    └── tlsca.<org-domain>.pem
```

Fig. 2. Folder structure to add organization to a channel

B. Register an identity

The registration command using the Fabric CA client looks like this:
./fabric-ca-client register -d --id.name <ID_NAME> --id.secret <ID_SECRET> -u <CA_URL> --mspdir <CA_ADMIN> --id.type <ID_TYPE> --id.attrs $ID_ATTRIBUTE --tls.certfiles <TLSCERT>

C. Enroll an identity

The CA administrator will need to get in touch with the individual who will be registering out of band once the account with the CA has been made up and profiles have been registered to provide the are enrolled ID and secret used during registration. Frequent Network Profiles Each of the Hyperledger Fabric Development Kit SDKs can join to a Hyperledger Fabric A network using the same Common Connection Profiles file format. A gateway can be set up with a connection configuration. There are many reasons why gateways are useful, but the main one is that they make it easier for applications to communicate over a network.

D. Chaincode

For the purpose of enforcing business rules, an application program can be written in Go, node.js, or Java and then executed atop an underlying infrastructure. Peer nodes execute Chaincode, or smart contracts, which manage the consensus-based business rules of the network. The state generated by a chaincode is private and cannot be viewed directly by any other chaincodes. It is a program that, through application transactions, initializes and maintains the ledger state within a protected docker container.

E.Wallet

A wallet is an application that allows you to keep and retrieve identity data using a persistent (or non-persistent) storage system of your choosing. Connecting to a Hyperledger Fabric network requires identity information, which can be kept in a wallet.

F. CouchDB

LevelDB and CouchDB are currently available as peer state databases. LevelDB is the peer process's built-in preset key-value state database. One other external state storage option is CouchDB. CouchDB, like LevelDB, is a key-value database, and it can save any chaincode-modeled binary data. (CouchDB attachments are used internally for

non-JSON data). CouchDB is a document object database that supports storing JSON documents, performing JSON queries on those documents, and using indexes to speed up those queries.

G. Ledger

A database in Hyperledger Fabric is made up of two separate but interconnected components: a global state and a blockchain. The global state is a database where all possible ledger states have their present values stored. blockchain, a distributed ledger of all the economic and other transactions that led to the present state of affairs

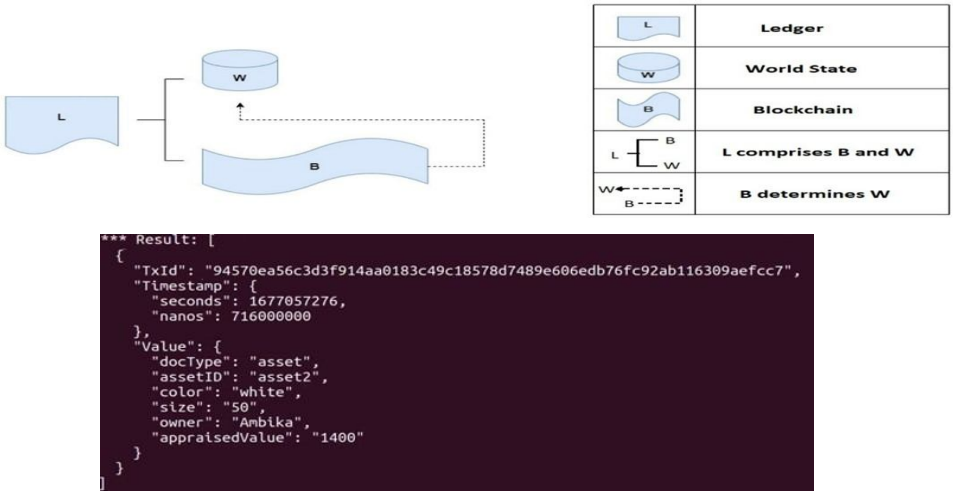


Fig. 3. Hyper ledger Fabric ledger

IV. Results Analysis

- Create Asset contract.submitTransaction('CreateAsset', 'asset2', 'white','50', 'Ambika', '1400');

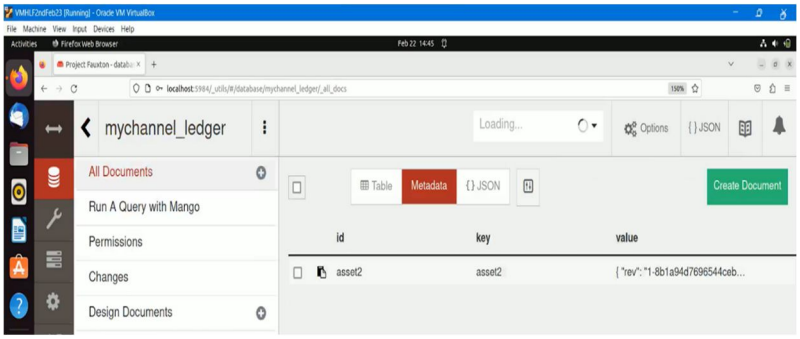


Fig. 4. Create Asset

- Read Asset contract.evaluateTransaction('ReadAsset', 'asset2');

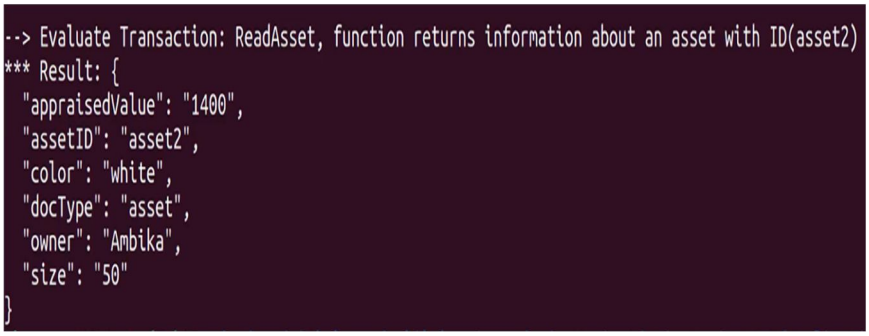
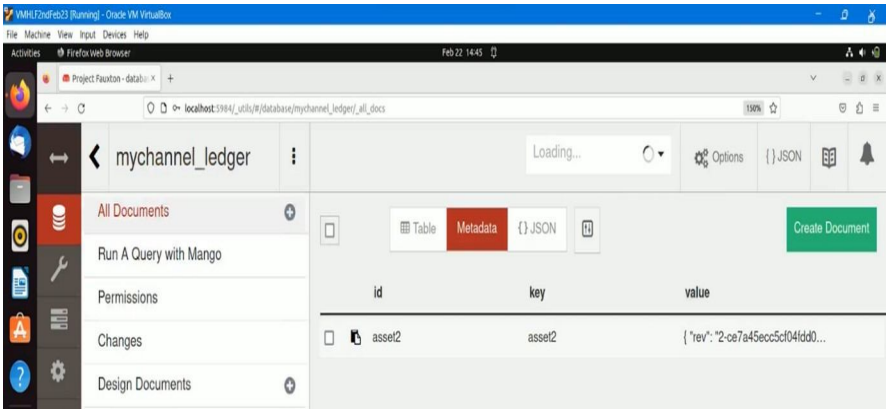


Fig. 5. Read Asset

- GetAllAssets: contract.evaluateTransaction('GetAssetsByRange', '', '');
  Fig. 6. GetAllAssets
- Transfer Asset contract.submitTransaction('TransferAsset', 'asset2', 'Sharanya');
  Fig. 7. Transfer Asset
- Query Assets By Owner contract.evaluateTransaction('QueryAssetsByOwner','Sharanya');




```
--> Evaluate Transaction: QueryAssetsByOwner, find all assets with owner(Sharanya})
*** Result: [
  {
    "Key": "asset2",
    "Record": {
      "appraisedValue": "1400",
      "assetID": "asset2",
      "color": "white",
      "docType": "asset",
      "owner": "Sharanya",
      "size": "50"
    }
  }
]
```

Fig. 6. Query Assets By Owner

- Delete Asset contract.submitTransaction('DeleteAsset', 'asset2');

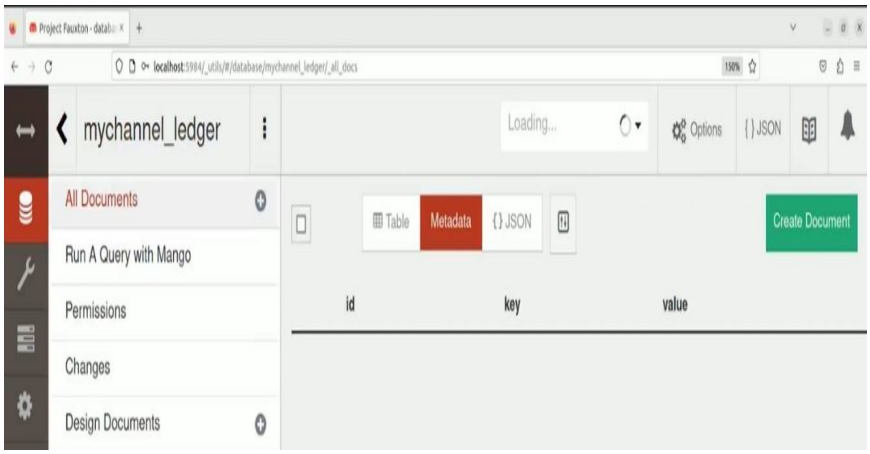


Fig. 7. Delete Asset

- AssetExists contract.evaluateTransaction('AssetExists', 'asset2');

Result: false

- Get Asset History contract.evaluateTransaction('GetAssetHistory','asset2');

Fig. 8. Get Asset History

V. CONCLUSIONS

This project uses blockchain and majority consensus to carry out secure asset transactions. The implementation of asset transactions utilizing blockchain has two main goals: to simply preserve records and to secure property transactions against flaws. The suggested remedy tries to prevent situations in which the same property is sold more than once to various clients. The time needed to complete a transaction is also reduced because relatively little work is needed to maintain records and document transactions. N nodes will be involved in the asset transaction, and they will oversee verifying transactions and adding new blocks to the blockchain.

REFERENCES

[1] Michael Borkowski, Daniel McDonald, Christoph Ritzer,and Stefan Schulte. To- wards atomic cross-chain token transfers: State of the art and open questions within tast. Distributed Systems Group TU Wien , Report, 2018.

[2] Michael Borkowski, Christoph Ritzer, Daniel McDonald,and Stefan Schulte. Caught in chains: Claim-first transactions for cross-blockchain asset transfers. Technische Universit¨at Wien, 2018.

[3] Ittay Eyal, Adem Efe Gencer, Emin G¨un Sirer, and Robbert Van Renesse. Bitcoin- ng: A scalable blockchain protocol. In 13th symposium on networked systems design and implementation, pages 45–59, 2016.

[4] Jianxi Gao, Daqing Li, and Shlomo Havlin. From a single network to a network of networks. National Science Review, 1(3):346–356, 2014.

[5] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In Annual International Conference on the Theory and Applications of Cryptographic Techniques.

[6] Thomas Hardjono, Alexander Lipton, and Alex Pentland. Towards a design philos- ophy for interoperable blockchain systems. arXiv preprint arXiv:1805.05934,2018.

[7] Ghassan O Karame, Elli Androulaki, and Srdjan Capkun. Double-spending fast payments in bitcoin. In Proceedings of the 2012 ACM conference on Computer and communications security, pages 906–917, 2012.

[8] Kostis Karantias, Aggelos Kiayias, and Dionysis Zindros. Proof-of-burn. In Inter- national Conference on Financial Cryptography and Data Security, 2019.

[9] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Annual In- ternational Cryptology Conference, pages 357–388. Springer, 2017.

[10] Pascal Lafourcade and Marius Lombard-Platet. About blockchain interoperability. Information Processing Letters, page 105976, 2020.

[11] Babu Pillai, Kamanashis Biswas, and Vallipuram Muthukkumarasamy. Cross- chain interoperability among blockchain-based systems using transactions. The Knowledge Engineering Review, 35, 2020.

[12] C. Prybila, S. Schulte, C. Hochreiner, and I. Weber, “Runtime Verification for Business Processes Utilizing the Bitcoin Blockchain,” Future Generation Computer Systems, vol. 107, pp. 816–831, 2020.

[13] S. Schulte, M. Sigwart, P. Frauenthaler, and M. Borkowski, “Towards Blockchain Interoperability,” in Business Process Management: Block-chain and Central and Eastern Europe Forum, ser. LNBIP, vol. 361, 2019, pp. 1–8.

[14] A. Zamyatin, M. Al-Bassam, D. Zindros, E. Kokoris-Kogias, P. Moreno-Sanchez, A. Kiayias, and W. J. Knottenbelt, “SoK: CommunicationAcross Distributed Ledgers,” IACR Cryptology ePrint Archive, 2019.

[15] Cheripelli, R., Ch, S., Appana, D.K. (2022). New Model to Store and Manage Private Healthcare Records Securely Using Block Chain Technologies. In: Islam, A.K.M.M., Uddin, J., Mansoor, N., Rahman, S., Al Masud, S.M.R. (eds) Bangabandhu and Digital Bangladesh. ICBBDB 2021. Communications in Computer and Information Science, vol 1550. Springer, Cham. https://doi.org/10.1007/978-3-031-17181-9_15

[16] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng,“Decentralized Applications: The Blockchain-Empowered ,”IEEE Access, vol. 6, pp. 53 019–53 033, 2018.
[17] R. Belchior, A. Vasconcelos, S. Guerreiro, “A Survey on Blockchain Interoperabil- ity: Past, Present, and Future Trends,” arXiv:2005:14282, 2020.
[18] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller,A. Poelstra,
[19] J. Tim´on, “Enabling blockchain innovations with pegged sidechains,” 2014,
[20] J. Poon and V. Buterin, “Plasma: Scalable Autonomous Smart Con- tracts,”www.plasma.io/plasma.pdf, 2017, 2021-06-29.
[21] M. Di Angelo and G. Salzer, “A Survey of Tools for Analyzing Ethereum Smart Contracts,” in 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), 2019, pp.69–78.
[22] P. Frauenthaler, M. Sigwart, C. Spanring, M. Sober, and S. Schulte,“ETH relay: A cost-efficient relay for ethereum-based blockchains,” in 2020 IEEE International Conference on Blockchain. IEEE, 2020, pp. 204–213.
[23] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” ethereum.github.io/yellowpaper/paper.pdf , 2020-03-26.
[24] Cramesh, Teja A Framework for E-Auction Scheme Using Hyperledger Fabric International Conference on Recent Advancements in Artificial Intelligence and Soft Computing ICAISC 2nd–3rd Dece, 2022
[25] Cramesh , New Challenges and its Security, Privacy Aspects on Blockchain Systems, International Conference on Recent Advancements in Artificial Intelligence and Soft Computing ICAISC 2nd–3rd Dece, 2022
[26] M. Herlihy, “Atomic Cross-Chain Swaps,” in 2018 ACM Symposium on Principles of Distributed Computing (PODC), 2018, pp. 245–254. [20] B. Pillai, K. Biswas, and V. Muthukkumarasamy, “Blockchain interoperable digital objects,” in 2019 International Conference on Blockchain (ICBC), 2019, pp. 80–94.
[27] P. Cuffe, “The role of the erc-20 token standard in a financial revolution: the case of initial coin offerings,” in IEC-IEEE-KATS Academic Challenge, 2018.