A Blockchain Framework for Investment Authorities to Manage Assets and Funds

P. C. Sherimon (ID), **Vinu Sherimon** (ID), **Jeff Thomas** (ID), **and Kevin Jaimon** (ID)

1 Introduction

State General Reserve Fund (SGRF) of Ministry of Finance (MoF) was established in 1980 under the Royal Decree 1/1980 [1] to manage the investment and financial matters on behalf of Government of Sultanate of Oman. It is the wealth deposit of the Sultanate of Oman. It is the body who manages and invests in public and private markets from the extra capital attained from oil and gas profits. Unlike other funds in Oman, this body mainly concentrates on investments outside the Sultanate. The IT department of OIA manages the development of the Information Systems used in the various departments. The targeted sectors in private investments include health sector, mining industry, food industries, logistics, and other diverse sources. Later in 1998, Tanmia, the Oman National Investment company was established [1].

In 2004, the company started investing in real estate, the first being the procurement of Regent Wharf property in London, UK [1]. The first direct investment in Private equity took place in 2006, with the acquisition of 6.1% of shares of AWAS, an Irish aviation company [1]. The investment of Oman in Vietnam happened with the establishment of Vietnam Oman Investment (VOI) in 2008 [1]. Later, a joint venture was established in the year 2010 with Uzbekistan, by the founding of

P. C. Sherimon
Faculty of Computer Studies, Arab Open University, Muscat, Sultanate of Oman
e-mail: sherimon@aou.edu.om

V. Sherimon (✉)
Department of IT, University of Technology and Applied Sciences, Muscat, Sultanate of Oman

J. Thomas · K. Jaimon
Department of Computer Science and Engineering, Saintgits College of Engineering, Pathamuttam, Kottayam, Kerala, India

Uzbek Oman Investment Joint Venture (UOI) [1]. Oman India Joint Investment Fund (OIJIF) was established in the year 2011 [1].

SGRF invests in more than 35 countries worldwide and allocates funds between 65–85% in public market shares and between 35–15% in private market shares [1]. The working of SGRF involves large number of transactions, which requires high level of transparency and governance between the involved stakeholders. In 2020, through a Royal Decree, SGRF have been transferred to Oman Investment Authority (OIA).

Generally transacted funds are recorded and tracked in the ledgers of the respective parties involved. To manage and allocate funds, organizations operate through various third parties to fulfil their objectives. This certainly comes with a cost of fee and more importantly, time. Like this, the OIA's work involves a plethora of transactions, which requires transparency and governance among their stakeholders, and all these are overcome with a general financial software. As of now, in the case of transparency, they operate through various manuals such as business conduct which sets a clear guide for all OIA staff concerning business ethics and behaviors and another whistle blowing system to report any sort of violations to preserve the rights of all parties. As mentioned above, all these are time-consuming, and the records may vary among the parties and may not create any consensus. Therefore, it is observed that it is mandatory to implement a better system or framework in OIA to manage the allocation of funds to public and private markets.

This research proposes a blockchain-based framework for OIA to achieve a better operational and investment performance, to track the funds allocated to different companies, and to ensure an effective system that enforce latest and best international practices. Blockchain technology will drastically improve the management of the distribution process of fund allocation. As per the survey of World Economic forum, September 2015, at least 10% of the global GDP will be stored on blockchain platforms by 2025 [2]. The fund sector involves lot of intermediate parties such as transfer agents, distributors, cash managers, and fund administrators [2]. With the use of blockchain technology, these intermediaries can be reduced, and the transactions can be secured at every stage, while maintaining the transparency. The data is encrypted using hash algorithms which is preserved and verified by every entity involved in the transaction.

Any framework based on blockchain eliminates third parties involved in the operations, reduces the transaction time and costs, and increases the transparency. When we consider a fund allocation body, its operations need to be done in a faster, efficient, and a transparent way. Because many organizations are looking forward to meeting the costs of their projects from OIA, it must be allocated at the earliest and in a fair manner [3]. Therefore, the proposed research is very significant in terms of usefulness. The proposed research uses IR4.0 technology, which is blockchain, a technological revolution of this era.

To achieve the main objective of the research, the following sub-objectives are formulated:

- Analyze similar use cases in blockchain technology.
- Propose an architecture for the prototype.

2 Background

This section includes information about the details of blockchain ledger, Hyperledger Fabric, the permission based private blockchain framework, and Hyperledger Minifabric, the web based tool used to set up a fabric network easily.

2.1 Basic Ledger in a Blockchain

A ledger is a centralized repository that records information of a business object's current state and provides its attribute value and transaction history. These entries could include investments, accounts receivable/payable, and customer deposits.

Figure 1 depicts a blockchain ledger. It is divided into two separate yet related segments: a "blockchain" and "world state (state database)." World state stores the current state of data in the network, whereas the blockchain keeps the entirety of the transaction log (the endorsed transactions) in a blockchain data structure. Unlike other ledgers, these are, however, immutable. This means that in blockchain, once a block is created, i.e., added to the chain, it is almost impossible to modify it. In comparison, the global state might be a database that contains the set of key-value pairs that are added, changed, or removed by the set of blockchain transactions that have been verified and committed [5]. For every channel created within the network, there is a separate ledger belonging to the respective channel.
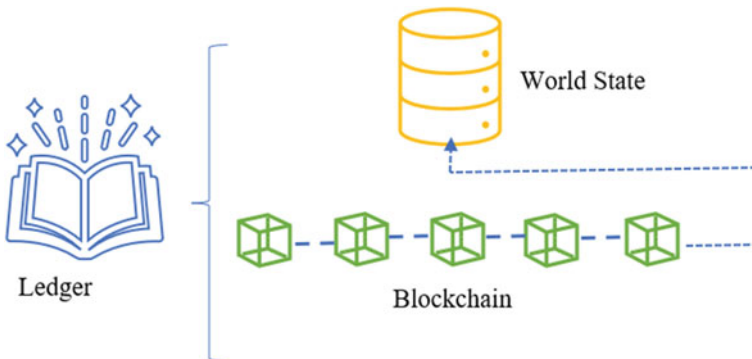

Fig. 1 Basic leger in a blockchain [4]

2.2 Hyperledger Fabric

It contains a ledger, implements smart contracts (chaincode), and functions as a system by which members control and store their transactions. However, it differs from other blockchain technologies in that its transactions are private and permissioned. It uses plug-and-play components that are aimed for use within private enterprises.

The most basic Hyperledger Fabric network is shown in Fig. 2 with two organizations (Org1 and Org2) sharing the same channel [6, 7]. A channel could be thought of as a pipeline through which one organization can communicate privately with other involved stakeholders that have joined the same channel [5]. The concept of channels brings a new dimension within the network as it allows the participating organizations to form and join their own network for various reasons and each channel would have its own ledger. Organizations outside the channel will not be involved in any sort of transactions and do not query about any information related with that channel. A single organization can participate in several channels at once.

A peer is a node on the blockchain that records every transaction on a participating channel. Each peer has the option to join one or more channels as needed. The task of organizing transactions, establishing a new block containing ordered transactions, and distributing the newly generated block to all peers on a pertinent channel fall under the purview of the Orderer service. The management of user credentials, including user registration, user enrolment, user revocation, and other actions, is the responsibility of the certificate authority, or CA. To describe rights, responsibilities, and properties to each user, Hyperledger Fabric employs an X.509 standard certificate [5]. An application that communicates with the Fabric
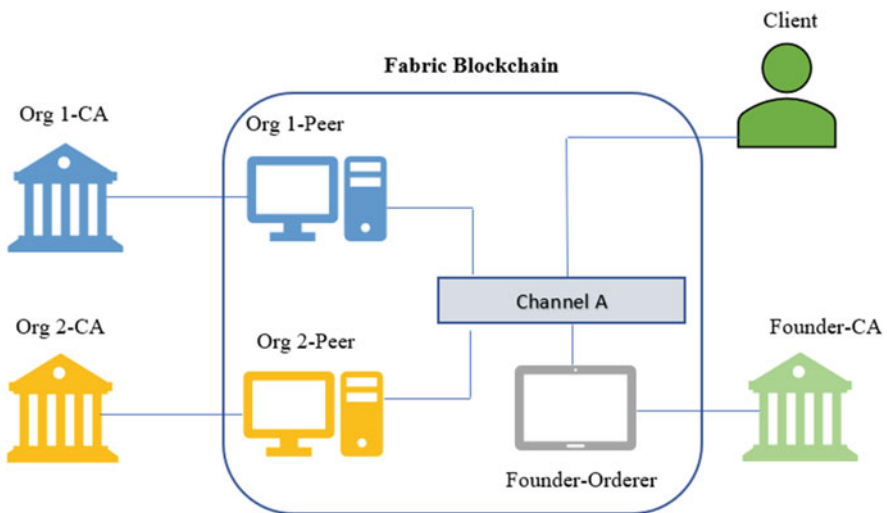

Fig. 2 Simple Fabric Network with two organizations joining same channel A [5]

blockchain network is referred to as a client. That is, the Client can communicate with the Fabric network in accordance with the permissions, roles, and attributes listed in the certificate it obtained from the CA server of the associated company. The entities given inside the blue box are part of the blockchain network, and the outside entities are off chain.

2.3 Hyperledger Minifabric

With the help of this web-based tool, developers can easily become familiar with Hyperledger Fabric, model their business network, test it, and then deploy it to a live instance of a blockchain network.

The easiest method to utilize Fabric technology is via Mini Fabric. Unlike Fabric, with the help of just a docker environment, we can smoothly run our first minifab command, regardless of if it is a production server or is a VirtualBox virtual machine. The network can be set up in a few minutes. Minifabric is small but it allows to experience the full skills of Hyperledger Fabric.

The highlighted features are as follows:

- Establishing a fabric network and growing it by incorporating additional organizations.
- Establish, join, query, and update channels.
- Installation, approval, instantiation, invocation, inquiry, and gathering of private data for chaincode.
- Support for block queries, ledger heights, and Hyperledger Explorer.
- Monitoring, evaluation, and identification of nodes.
- Minifabric is only a single little script and a docker container image, thus the ecosystem is not polluted (Fig. 3).

A simple "minifab" command would be enough to start up a fabric network in the provided working directory. Upon its completion, a Fabric network will be running normally using the latest Fabric release on your machine. An application channel named "mychannel" will be created, all peers defined in the network specifications file will be joined to that channel, and a chaincode will be installed and instantiated. The above command will execute most of the Fabric network operations, and the process will take approximately a couple of minutes to complete with respect to the network connection provided to the system in which it is running as the process downloads the Hyperledger Fabric official images from Docker Hub [9].

Business network fundamental data, such as the business model, transaction logic, and access restrictions, are captured by the Business Network Archive (BNA), which then bundles and distributes these parts to a runtime. Fabric also includes a Loopback connector for business networks that provides an active network as a REST API that client apps can use to easily interact with non-blockchain applications. Basic smart contracts are simply stored programs that execute when certain conditions are satisfied. They are frequently used to streamline
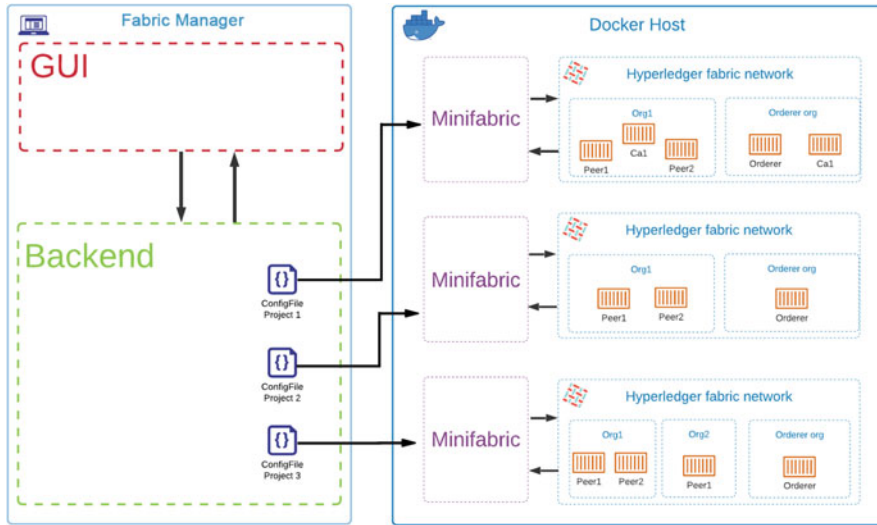
Fig. 3 Basic Mini Fabric architecture [8]

the implementation of an agreement so that each person can instantly be certain of the outcome, without the involvement of a go-between or a waste of time. They can also automate a procedure at work by triggering the subsequent action when certain criteria are fulfilled [10].

3 Related Works

In 2018, Indian researchers proposed a blockchain-based architecture for allocating government funds and increasing transparency. The system's prototype was built using Hyperledger composer [11]. Calastone, an investment technology firm, has unveiled a blockchain-based infrastructure for the trading and settlement of investment funds. In this platform, 1800 service providers from 41 countries are connected through a live distributed ledger. These participants have real-time access to trade, service, and monitor their investments [12]. The Internal Revenue Service of Kogi is responsible for collecting and managing domestic revenues that form the state's financial backbone [13]. There are several inherent problems in the present system. The challenge in recognizing tax dodgers, computational errors, a high level of duplication and discrepancies in records, a low level of data security, and the failure to extract and gather pertinent data for timely decision-making rapidly and correctly were just a few of the issues highlighted.

To bring trust to the donors in an NPO in Russia, a system was developed to track the flow of funds and increase transparency. This system was made using Ethereum. The Smart contract was developed using solidity programming language. The server

side is developed using Node.js platform and express framework. MySQL is used for centralized off chain data storage. This project is being carried out because of funding provided by the government of the Russian Federation for applied research [14]. After closely analyzing the above-mentioned research, we were not able to identify many projects that use blockchain technology to achieve our use case.

4 Proposed Framework

Figure 4 illustrates the proposed framework.

There are various entities present in this system like the Oman Investment Authority and various other organizations that are receiving investments from OIA.

- *Oman Investment Authority*: With the help of the proposed blockchain network, the OIA can easily allocate and track funds. This system will also increase the transparency and Immutability which thereby will increase the efficiency of the Oman Investment Authority.
- *Organizations*: Every organization falls under the receiver side of the application. They receive investments from the OIA through the application. Since the middlemen are cut off from the system, the system can be trusted. These organizations can also track the transaction made to them.
- *Auditor*: They are responsible for keeping account of the transactions that happened in the network. Each organization in the system has an auditor. An
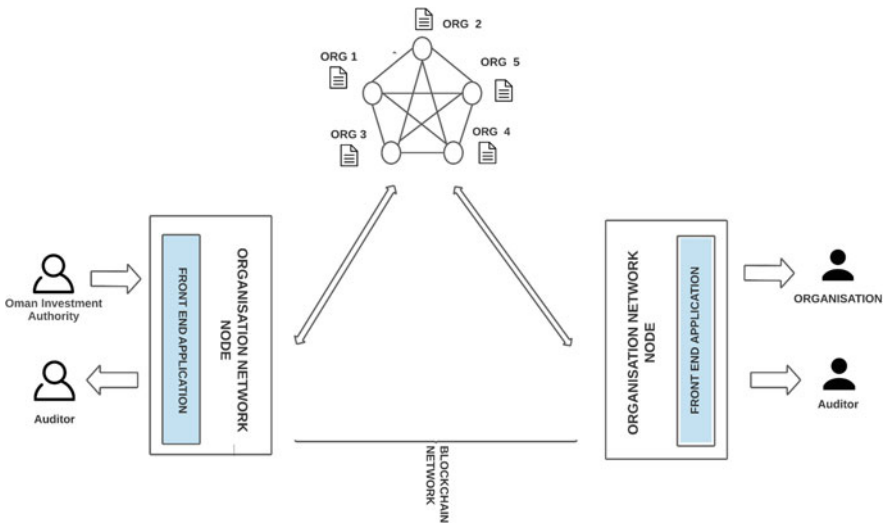

Fig. 4 Proposed framework

auditor cannot look to get more details about the agreement. But he can have access to information like the name of sender and receiver, the amount that is being transferred and the transaction date and time.

The actors are the frontend application, the backend, and the decentralized network. Each user will have two keys, one to login to the application and the other key to submit a transaction. The details regarding the user's profile are stored in the off-chain database whereas the information regarding the transaction is stored as blocks in the blockchain. Whenever the user wants to view the ledger in which the transactions are stored, a fetch request is given, and the details are retrieved using REST API.

The processes involved in completing a transaction are as follows:

- Log-in to the Decentralized Application: In order to conduct a transaction, the user needs to login to the Dapp using his private key. Every user has a different interface depending on the roles given to them by the organization.
- Create Smart Contract: The Oman Investment Authority (OIA) needs to create a Smart Contract such that the contract may include the details about the sender and the receiver, fund that is being transferred, and set of conditions that needs to be met. Every network has a maintainer/validator who is responsible for reviewing, verifying, and uploading the smart contract into the network.
- Notify the Receiver: The organization that is receiving investments is notified about the Smart Contract and the organization can review the agreement (Fig. 5).
- Agree to the Contract: The OIA and the organization must mutually agree on the agreement by signing the smart contract with a digital signature (Fig. 6).
- Publishing on the blockchain: When the OIA and the organization sign the Smart Contract, it becomes an official document that is shared on the blockchain.
- Viewing the smart contract: Once the transaction is made, anybody with access can view the ledger and evaluate the transaction. Decisions like who can see and what can be seen are made by the organization.

The following explains how smart contracts are used to manage the fund:

A smart contract takes up the role of a lot of intermediaries. Simple "if/else . . . then . . . " statements are written on a blockchain to make smart contracts work. If the conditions mentioned by the organization are met, the

Fig. 5 Creating smart contracts and notifying the organizations

Fig. 6 Reaching consensus and signing of agreement

smart contract is executed, and the funds are released from the sender's account to the receiver's account. If the receiver does not follow the conditions mentioned in the contract, then the transaction can be reversed or kept in hold. Only parties who have been granted permission can view the results. The entities will be provided a set of rules/guidelines that will ensure the network's integrity. The entities can only change these rules or guidelines through voting, and a vote of 75% of the total network is required to change or add a new rule or guideline.

5 Conclusion

Oman Investment Authority fund allocation and tracking currently uses primitive methods to transfer funds. They now use publications like the Authorities and Responsibilities manual, the Investment Manual, the Code of Business Conduct, and others to ensure transaction transparency. However, these methods are not efficient to ensure the transparency of the transaction. This research paper discusses the architecture of a blockchain network to transfer funds based on the Industrial Revolution 4.0 standards. The transaction is transparent, traceable, and immutable due to this technology. The user interface provided by the front-end application will allow users to effortlessly transfer funds and view transactions. The collection of rules supplied will ensure that the network runs smoothly. The development of the network and the user interface, as well as the addition of entities and system testing, will be the emphasis of future work on this project.

References

1. Oman State General Reserve Fund (Oman SGRF) – Sovereign Wealth Fund, Oman – SWFI [Online]. Available: https://www.swfinstitute.org/profile/598cdaa60124e9fd2d05ba27. Accessed 19 Jun 2022
2. Deloitte: Impacts of the Blockchain on Fund Distribution, p. 24

3. Oman Investment Authority [Online]. Available: https://oia.gov.om/Index.php?r=en%2Fsite%2Fpages&slug=governance&csrt=10462007450093286215# GOVERNANCE. Accessed 19 Jun 2022

4. Hyperledger Fabric: Ledger—Hyperledger-fabricdocs main documentation, https://hyperledger-fabric.readthedocs.io/en/release-2.2/ledger/ledger.html. Accessed 20 Jun 2022

5. P. Thummavet, *Demystifying Hyperledger Fabric (1/3): Fabric Architecture* (Coinmonks, 28 Aug 2020), https://medium.com/coinmonks/demystifying-hyperledger-fabric-1-3-fabric-architecture-a2fdb587f6cb. Accessed 20 Jun 2022

6. Hyperledger Foundation: Hyperledger fabric, https://www.hyperledger.org/use/fabric. Accessed 20 Jun 2022

7. Hyperledger Fabric: Using the Fabric test network—Hyperledger-fabricdocs main documentation, https://hyperledger-fabric.readthedocs.io/en/latest/test_network.html. Accessed 20 Jun 2022

8. K. Siripatkerdpong, Fabric-Manager (2021) [Online]. Available: https://github.com/new4761/Fabric-Manager. Accessed 20 Jun 2022

9. T. Li, IBM Open Technology: *Minifabric: A Hyperledger Fabric Quick Start Tool (with Video Guides)* (Hyperledger Foundation, 29 Apr 2020), https://www.hyperledger.org/blog/2020/04/29/minifabric-a-hyperledger-fabric-quick-start-tool-with-video-guides. Accessed 20 Jun 2022

10. IBM: What are smart contracts on blockchain?, https://www.ibm.com/in-en/topics/smart-contracts. Accessed 20 Jun 2022

11. A. Mohite, A. Acharya, Blockchain for government fund tracking using Hyperledger, in *2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)*, (IEEE, 2018), pp. 231–234. https://doi.org/10.1109/CTEMS.2018.8769200

12. N. Reeve, *Technology Roundup: Blockchain-Based Fund Trading System Launches* (IPE, 2019), https://www.ipe.com/technology-roundup-blockchain-based-fund-trading-system-launches/10031307.article. Accessed 20 Jun 2022

13. S.F. Ayegba, Automated internal revenue processing system: A panacea for financial problems in Kogi state. West Afr. J. Ind. Acad. Res. **7**(1), 56–69 (2013)

14. H. Saleh, S. Avdoshin, A. Dzhonov, Platform for tracking donations of charitable foundations based on blockchain technology, in *2019 Actual Problems of Systems and Software Engineering (APSSE)*, (IEEE, 2019), pp. 182–187