LETTER

Blockchain-Based Pension System Ensuring Security, Provenance and Efficiency*

Minhaz KAMAL[†], **Chowdhury Mohammad ABDULLAH**[†], **Fairuz SHAIARA**[†], **Abu Raihan Mostofa KAMAL**[†], **Md Mehedi HASAN**[††], ***Nonmembers***, **Jik-Soo KIM**[†††a)], ***Member***, ***and*** **Md Azam HOSSAIN**[†b)], ***Nonmember***

SUMMARY The literature presents a digitized pension system based on a consortium blockchain, with the aim of overcoming existing pension system challenges such as multiparty collaboration, manual intervention, high turnaround time, cost transparency, auditability, etc. In addition, the adoption of hyperledger fabric and the introduction of smart contracts aim to transform multi-organizational workflow into a synchronized, automated, modular, and error-free procedure.

key words: *consortium blockchain, smart contracts, pension, traceability*

1. Introduction

Income security in retirement is essential for socio-economic stability. Both public and private employers around the globe provide pensions. By 2050, the dependency ratio (number of dependents to total working-age population) is projected to double due to the aging population [1]. This figure indicates a steady growth of the pension sector in near future. In addition, the intricate business process of the pension sector require multiparty collaboration, point-to-point coordination, and settlement, making it a perfect problem statement for consortium blockchain.

In the traditional pension system the well-defined transactions between the involved organizations are performed manually. As a result, administrative and operational expenses are elevated [2]. Moreover, different entities and user types inside the system need varied levels of permission and authentication, raising questions on data visibility and security. Auditability is another major issue due to the lack of data provenance and cost transparency. These shortcomings contribute to insufficient pension asset growth and poor savings returns, reducing pension accumulation and participation.

Taking the complete scenario into account, blockchain's inherent properties such as immutability, provenance, privacy, and security make it a promising technology for building a future proof pension system by overcoming all the aforementioned hurdles of the traditional system. Furthermore, the consortium blockchain has additional benefits like privilege and access controls, role-based definition of entities, and governance, giving it the capability of housing all the workflows and procedures as seen in the real life systems.

This paper presents a framework for the pension industry that leverages blockchain technology. It also addresses the key challenges that an integrated pension system faces and proposes the adoption of consortium blockchain a potential solution. To our best knowledge, this is the first study propose an architecture a consortium blockchain-based for pension system. Furthermore, smart contracts are employed in the proposed system to automate the process.

2. Related Works

There is a lack of research on the subject of blockchain-based pension funds. The authors [3] presented a life-based insurance concept for a pension fund, where participants pay a stream of value to join. Without central authority intervention, smart contracts will automatically provide retirement benefits to registered participants. This study just listed pension fund core activities and how they can be accomplished on distributed ledgers. It did not discuss system architecture or blockchain implementation. The authors of [4] envisioned a blockchain-based volunteer time bank (VOLTimebank) as a record-keeping mechanism for volunteer work. VOLTimebank allows volunteers to assist the elderly in exchange for future rewards. The purpose of this research is to enhance the collaboration between pension institutions and care providers.

A recent study [5] has uncovered the key prerequisites for the pension business to use permissioned blockchain technology. The emphasis of the study was on the business procedures inside the pension system. On the basis of the business model, a blockchain network architecture, an information systems model, and a technology model were developed. The study did not support consortium blockchains and did not address multiparty collaboration, cost, or design. The whitepaper [6] presented an Ethereum-based solution for a worldwide pension system. They proposed tokenizing assets for jurisdictional compliance. However, a

Manuscript received December 8, 2022.
Manuscript revised February 6, 2023.
Manuscript publicized February 21, 2023.

[†]The authors are with Network and Data Analysis Group, Department of Computer Science and Engineering, Islamic University of Technology (IUT), Gazipur 1704, Bangladesh.
[††]The author is with Department of Robotics and Mechatronics Engineering, University of Dhaka, Bangladesh.
[†††]The author is with Department of Computer Engineering, Myongji University, Yongin, Korea.

*This work was supported by the National Research Foundation of Korea (NRF) grant funded by Korea government (MIST) (No.NRF-2019R1A2C1005360).

a) E-mail: jiksoo@mju.ac.kr (Corresponding author)
b) E-mail: azam@iut-dhaka.edu

DOI: 10.1587/transinf.2022EDL8099

large tokenization initiative in a sensitive business like pensions is too risky. They cannot guarantee that authorities in diverse jurisdictions will permit their activity (i.e., some regions might not even have this service available).

The aforementioned studies do not address multiparty collaboration, data provenance, security, and, overall, fail to provide an umbrella platform to house all participants of the pension system. Acknowledging this gap in the existing literature body, we propose a consortium blockchain-based architecture for the pension system that is co-linear with the existing administrative framework and its business processes.

3. Challenges and Solutions

In this section, a number of challenges and possible solutions are provided that must be dealt with to realize a successful blockchain-based pension system.

The system must address the absence of trust among the different participants. A consortium blockchain is required for multiparty collaboration in a trust-less environment. Immutable ledgers provide data provenance and an audit trail. Every event that occurs inside the blockchain network is recorded in the distributed ledger. This prevents repudiation and establishes the ledger as the single source of the truth.

The pension system must have optimal record management and well-defined access privileges. For this purpose, proposed pension system data will be divided into two categories. Non-financial data: data about the identities of pensioners and organizations needing less throughput but higher security. Financial data: transactions and different pension schemes' information requiring more storage and less throughput. These two categories of data will be recorded on separate ledgers. This separation gets rid of the scalability issue, isolates the different types of data, and increases the cohesion of the relevant data.

The system must provide appropriate access control and support business process for participants to perform their responsibilities. Since consortium blockchain offers enhanced data access control within the network, they are more useful compared to public blockchains. In addition, the role-based description of participants will ensure the accurate execution of business processes inside the system.

The new system should minimize turnaround time and administrative costs. Smart contracts will automate the procedure, making it error-free and reducing the turnaround time. Ensuring smooth collaboration among the entities and automating the processes through smart contract adoption will ensure optimized resource utilization.

Therefore, the new solution will improve operational efficiency in the workflow and operation of the pension system through the automation and orchestration of the workflow of the involved entities in the consortium. Due to the solution's robust audit trail and traceability, if there is malpractice, pension fraud, or corruption, auditing will be much easier and faster than with the old system.

4. Proposed System

In this section, the proposed system is explained. First, we examine the application scenarios by analyzing the various actors and their interactions. The system architecture is then presented, followed by a description of its components.

4.1 System Application Scenario

The application scenario of the proposed pension system is shown in Fig. 1, illustrating the participants and their interactions.

Clients: The system supports a large number of pensioners, who are referred to as clients. A pensioner is, in essence, an employee working for a particular employer. They are able to initiate transactions inside the system. A client will be regarded as a pensioner upon retirement.

Enterprise: The system consists of three enterprises: Employers, Pension Trustees, and Banks. They will submit their information to join the system, enabling appropriate identification and authentication (e.g., registration documents, licensing, etc.). After validation, they will receive an e-certificate (a certificate ID against the listed attributes). This certificate will later be used to determine the roles of the organizations in the blockchain network.

Governors: Pension Regulators and Auditors are the two governing bodies. The Regulator is in charge of verifying the legitimacy of the enterprises and giving them with identification inside the system. The Auditor is in charge of pension fund account compliance.

Pension Ecosystem: It is the platform that allows enterprises to collaborate under the supervision of governors while offering distributed and secure services to their clients.

Blockchain: The blockchain network maintains a distributed ledger that records all transactions, guaranteeing their immutability, traceability, and security.

Figure 2 demonstrates a simplified system workflow, showing the pensioner's activities to submit a pension request to the employer and the governor's role in ensuring the accurate transfer of funds to the pensioner. The client requests a pension from the employer by submitting the required documents (Steps 1–2). The request is sent to the pension regulator after verification, where it awaits approval

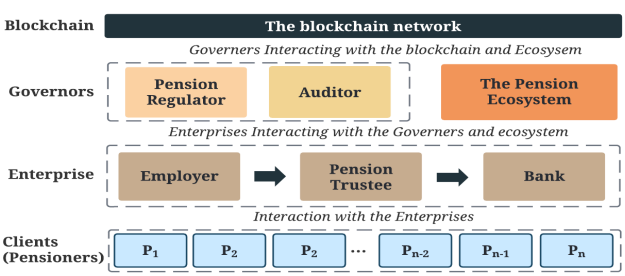

Fig. 1 System application scenario and interaction between various system entities.

(Steps 3–6). Upon getting a positive answer, the necessary amount (calculated by the auditor) is reported to the pension trustee (Steps 7–10), and the fund is wired to the client's designated bank account for the settlement with the client (Steps 11–14). This settlement procedure is further discussed in Sect. 5.2's algorithm 1.

4.2 System Architecture and Components

This section discusses the proposed system's components. Figure 3 depicts the proposed architecture of the consortium pension system.

Applications: The applications are the interfaces via which users interact with the blockchain network through a server using application programming interfaces (APIs). Regulators and auditors need their own application because they are fundamentally different and play different important roles in the system. The non-governing entities only need a single enterprise API. A user-friendly application is finally incorporated into the system to facilitate clients engagement with the system. Using this API, enterprises and pensioners can use the blockchain network to execute necessary tasks.

Server: It acts as a middleware, accepting requests from the application and relaying them as compatible interactions to the blockchain network.

Organizations: Entities such as regulators, auditors, and enterprises are defined as organizations. Each organization has its own Certification Authority (CA), which manages the certificates required to communicate with the network and determine the peers and nodes within itself. There are different types of peers: endorsing and committing peers are two of the most important types. Endorsing peers store the smart contracts and execute them. Upon getting a correct output, they digitally sign the output to be committed into the ledger. Whereas, the committing peers commit a transaction to be embedded into the ledger.

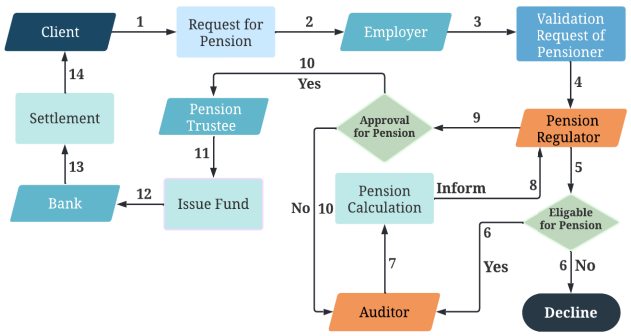

Fig. 2 Pensioner on boarding and transaction settlement.

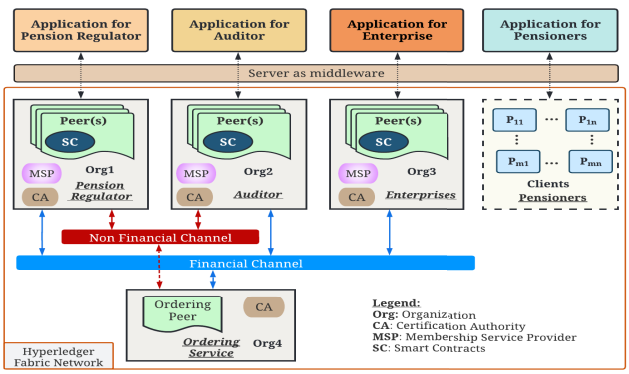

Fig. 3 System architecture of consortium pension system

Clients: Clients do not host any nodes. Instead, they function as "submitting clients" of the blockchain network, using different APIs directly. A large number of clients interact with the platform using web access points.

Ordering Service: Collects the transactions and verifies them through the defined consensus protocol to be committed into the ledger irreversibly.

Channels: A subset of the participants in the network can be privately connected through a bridge called a channel. The two channels in the network are independent and parallel with respect to each other. They decouple two different types of data requiring different throughput, latency, and security, and ensures optimum management of records.

Membership Service Providers (MSP): It enforces the prerequisites for a node to join the blockchain network by verifying their identity (given by CA) and enabling them to communicate with the network. It transforms an individual's identity into roles within the network of their peers.

Smart Contracts (SC): Smart contracts specify business logic and agreements between entities in code to ensure transparency. They allow automated transactions between entities, resulting in an error-free and fast system.

5. System Design

For ensuring a purposeful blockchain based framework, an efficient design plan is necessary. This section addresses the structure of information and a relevant algorithm, thereby outlining the smart contract for the system.

5.1 Data Structure

The system's participants are recorded through lists of attributes, which are also represented as data structures. For instance, the information of a pensioner is shown in Table 1 for identification purposes within the system. The attributes are used as inputs to different functions in the smart contracts, such as the pension scheme, eligibility, audits, and so on. The attributes shown in Table 1 are reflected in the data

Table 1 Basic information about pensioner

BASIC_INFORMATION_OF_PENSIONER
Name: Pensioner Name
DOB: Date of Birth
Contact: Contact Information
Employer: Employer Name
Joining Date: Date of Joining
Retirement Date: Date of Retirement
Designation: Last designation in working
Leave Taken: Number of leaves taken

Table 2 Data structure of pensioner

Prefix	PENSIONER
Key	Certificate_ID
	{
	id: Certificate_id
Value	BASIC_PENSIONER_INFORMATION
	pension_amount: Amount of pension
	transaction_state: 'applied'/'in process'/'approved'
	}

structure presented in Table 2. These data structures are kept in a key-value pair, where the key is the certificate ID and the value is the information recorded during registration.

5.2 Smart Contracts (SC)

The business process and orchestration of a real-time, multi-party pension system can be turned into a simple, error-free digital workflow. Algorithm 1 presents the smart contract that was developed to automate the pensioner workflow shown in Fig. 2. Initially, a pensioner's information is retrieved from the blockchain and mapped to the certificate id (key). Following that, an eligibility check is performed. For an affirmative outcome, the transaction state is modified and the computation of the pension amount begins. The auditor does the required computation for the eligible pensioner, which is then subject to a second review. Through these checks in the SC, a pension is given out, and the pensioner gets it through the pension trustee and designated banks.

Algorithm 1 Pension Transaction Settlement

Inputs:
PFK: Key Value of Pensioner;
Outputs:

```
for Key in PFK do
    pensioner = GetState(Key);
    VPI = pensioner.BASIC_PENSIONER_INFORMATION;
    if Eligibility(pensioner) = True then
        pensioner.transaction_state = 'in process';
        pension_amount = CalculatePension(auditor, pensioner);
        if PensionApproval(pensioner, pension_amount) = True then
            pensioner.pension_amount = pension_amount;
            IssueFund(pensioner, pension_trustee, bank);
        else
            pension_amount = CalculatePension(auditor, pensioner);
        end if
    else
        Pension Declined;
    end if
end for
```

There is a dedicated smart contract (presented in algorithm 2) that automates a retiree's pension calculation from a set of inputs (pension scheme, number of years before retirement, etc.). The calculation differs according to the industry, organization, job type, geography, and so on. This function can only be invoked by a verified auditor in the network, ensuring integrity.

Algorithm 2 Pension Calculation

Inputs:
auditor: the person who is responsible to calculate pension;
pensioner: the person whose pension is to be calculated;
Outputs:

```
if verification(auditor) = verified then
    VPI = pensioner.BASIC_PENSIONER_INFORMATION;
    scheme = pensioner.PENSION_SCHEME_INFORMATION;
    remainingLeave = pensioner.LEAVE_INFORMATION;
    pension_amount = pensionCalc(VPI, scheme, remainingLeave)
    return pension_amount;
else
    Auditor is not verified;
end if
```

6. Conclusion and Future Work

The pension industry contributes significantly to the socioeconomic stability of a nation. The current systems suffer from a number of limitations, including multiparty cooperation, manual intervention, high turnaround time, cost transparency, security, and auditability issues. This study analyzes the challenges, and existing technical solutions and presents a blockchain based future solution. This paper also discusses a governance model for the proposed architecture, taking prospective participants into account. Furthermore, the study proposes using smart contracts to convert a manual, multi-organizational workflow into a synchronized, automated, and error-free procedure. This article will serve as a blueprint for future industrial-scale blockchain implementation in the pension industry, ensuring provenance, transparency and operational efficiency. In the future, we will extend this research to include details about system implementation on Hyperledger Fabric as well as performance analysis.

References

[1] K. Christensen, G. Doblhammer, R. Rau, and J.W. Vaupel, "Ageing populations: the challenges ahead," The Lancet, vol.374, no.9696, pp.1196–1208, 2009.
[2] A. Benish, H. Haber, and R. Eliahou, "The regulatory welfare state in pension markets: Mitigating high charges for low-income savers in the united kingdom and israel," Journal of Social Policy, vol.46, no.2, pp.313–330, 2017.
[3] P. Sestoft, "3.7 autonomous pension funds on the blockchain," Opportunities and Risks of Blockchain Technologies, p.121, 2017.
[4] S. Cheng, W. Shi, and H. Zhang, "Voltimebank: A volunteer system for mutual pension based on blockchain," Proceedings of the 2019 International Conference on Blockchain Technology, ICBCT, New York, NY, USA, pp.75–79, Association for Computing Machinery, 2019.
[5] I. Sarker and B. Datta, "Re-designing the pension business processes for achieving technology-driven reforms through blockchain adoption: A proposed architecture," Technological Forecasting and Social Change, vol.174, p.121059, 2022.
[6] A. Andrianova, P. Hauner, D.K. Mcdonald, D.A. Manning, and M. Zerouali, "AKROPOLIS: A Global Blockchain Pensions Infrastructure," https://crebaco.com/planner/admin/uploads/whitepapers/7198745akropolis-whitepaper.pdf, 2018. [Online; accessed 01 December, 2022].