Design and Development of A Blockchain-Based Financial Aid Distribution System

Md. Raisul Hasan Shahrukh , Sifat Momen , Nafees Mansoor *

Posted Date: 11 March 2024

doi: 10.20944/preprints202403.0654.v1

Keywords: Blockchain; Financial Distribution; Process Automation; Smart Contracts; Hyperledger

Article

Design and Development of a Blockchain-Based Financial Aid Distribution System

Md. Raisul Hasan Shahrukh [1], Sifat Momen [2] and Nafees Mansoor [1,*]

[1] Department of Computer Science and Engineering, University of Liberal Arts Bangladesh, Dhaka, Bangladesh; raisul.hasan.cse@ulab.edu.bd
[2] Department of Electrical and Computer Engineering, North South University, Dhaka, Bangladesh; sifat.momen@northsouth.edu
* Correspondence: nafees@ieee.org

Abstract: Contemporary financial systems, despite their inherent complexity and resilience, face significant challenges related to transparency, efficiency, and security. Notable deficiencies in transparency and emerging security vulnerabilities underscore the pressing need for innovative solutions in current financial practices. Hence, this paper introduces a financial distribution system based on a consortium blockchain. Given organizations' preference for keeping sensitive data private, the partially decentralized nature of consortium blockchains plays a pivotal role in the proposed system's architecture. Moreover, within this system, the proposed smart contract serves a dual role. It functions not only as a transactional tool but also as a specialized solution designed to improve transactional procedures. Its multifaceted capabilities include ensuring data accuracy, facilitating swift execution, and ensuring adherence to regulatory requirements within the dynamic financial distribution landscape. Through rigorous testing and empirical analysis utilizing the Hyperledger Besu platform, it has been observed that the performance of the proposed system surpasses traditional blockchain frameworks. The results unequivocally demonstrate the proposed system's proficiency in handling high-frequency financial transactions with minimal computational burden.

Keywords: Blockchain; financial distribution; process automation; smart contracts; Hyperledger

1. Introduction

The swift advancements in various technologies, coupled with the evolving nature of financial activities, underscore the growing need for enhanced transparency, security, and efficiency in financial operations [1]. This is because traditional financial operations often grapple with inefficiencies, susceptibility to fraud, and a lack of immediate transparency [2]. Moreover, the dynamic landscape of financial technology (fintech) further amplifies the need for innovative solutions. Although blockchain technology is recognized as a promising tool to address these challenges, developing solutions with the appropriate blockchain platform remains an area of ongoing exploration. In the era of fintech, where agility and adaptability are paramount, these systems emerge as pivotal contributors to reshaping financial landscapes. However, seamlessly integrating these blockchain platforms into the financial distribution sector, ensuring compatibility, expandability, and maintaining security, poses a notable challenge [3,4].

On the other hand, blockchain technology, recognized for its decentralized, secure, and transparent characteristics, is driving innovation in various domains [5]. Within this technological realm, public, private, and consortium blockchains each play distinct roles and exert unique impacts. Consortium blockchain systems, particularly distinguished for their decentralized structure and integrated smart contract capabilities, stand out as powerful enablers of transformation [6]. Moreover, in tandem with this trend, Hyperledger Besu, an open-source client for the Ethereum blockchain, augments current advancements by offering greater flexibility and advanced features [7]. This synergy between blockchain's foundational strengths and the enhancements brought forth by Hyperledger Besu contributes to a more dynamic landscape of innovation. The industry's adoption of blockchain

 doi:10.20944/preprints202403.0654.v1

solutions is driven by the inherent advantages of the technology in terms of transparency, and security [8,9]. Furthermore, platforms such as Hyperledger provide enterprise-grade solutions for the financial sector, enabling the development of advanced financial applications [10]. This comprehensive integration of blockchain technology, coupled with specialized platforms, reflects a transformative shift in how industries approach and leverage cutting-edge solutions.

This research investigates the intricate architecture and functional capacities of integrating platforms like Hyperledger Besu [11,12], with a particular focus on addressing challenges inherent in traditional financial distribution systems [13]. The proposed financial distribution platform utilizes a consortium blockchain, combining its interoperability, scalability, and controlled access features with the robust functionalities of Hyperledger Besu. The incorporation of embedded smart contracts is expected to enhance procedural automation, reducing the need for manual intervention and minimizing the likelihood of human errors.

The architecture of the proposed blockchain-based system emphasizes adaptability and robustness while effectively addressing persistent issues in the financial distribution industry. This integration streamlines processes, facilitating advancements in the delivery of financial services and establishing the proposed system as an efficient solution. The research also aims to elucidate the distinct features of Hyperledger Besu, with a specific focus on its potential in financial distribution amid the growing discourse on the various applications of blockchain technology. The primary significance of this study lies in its comprehensive analysis of smart contract generation and its seamless incorporation into a private Hyperledger Besu environment. The study highlights the significant impact of smart contracts on streamlining operations, minimizing human involvement, and mitigating common issues like inefficiencies, susceptibility to fraud, and limited real-time visibility.

Therefore, this paper introduces a financial distribution system based on a consortium blockchain. The partially decentralized nature of consortium blockchains, catering to organizations' preference for keeping sensitive data private, plays a pivotal role in the proposed system's architecture. Within this system, the proposed smart contract serves a dual role as both a transactional tool and a specialized solution designed to improve transactional procedures. Its multifaceted capabilities include ensuring data accuracy, facilitating swift execution, and ensuring adherence to regulatory requirements within the dynamic financial distribution landscape. Rigorous testing and empirical analysis utilizing the Hyperledger Besu platform reveal that the proposed system's performance surpasses traditional blockchain frameworks. The results unequivocally demonstrate its proficiency in handling high-frequency financial transactions with minimal computational burden.

The subsequent sections of this article are organized as follows: Section 2 provides a discussion of existing blockchain-based systems, outlining their advantages and disadvantages. Section 3 outlines the architecture of the proposed system. The development and implementation of the proposed system, alongside a discussion of the envisioned smart contracts, are presented in Section 4. The performance evaluation of the proposed system is detailed in Section 5, and the paper concludes in Section 6.

2. Existing Systems

The potential of blockchain technology has not yet been completely recognized, and its implementation across numerous industries is still in its early stages [20]. Studies highlight how blockchain technology may greatly improve operations and provide transparent, reliable systems. This is especially helpful for senior citizens who need critical services [21]. Blockchain technology is known to provide better security and privacy, more efficiency, and lower prices in the service industry [4]. Self-executing contracts with embedded code, or "smart contracts," are emphasized for their ability to streamline authorization procedures and guarantee data integrity [7].

Challenges for blockchain-based service platforms include regulatory compliance, interoperability, and user adoption [10]. Notwithstanding these obstacles, additional research into the full potential and constraints of blockchain technology is imperative given its wide range of possible applications in the service industry [22]. To increase trading efficiency and security, an emphasis is focused on creating a

 doi:10.20944/preprints202403.0654.v1

decentralized stock market platform using consortium blockchain [1]. The underlying problems with traditional stock exchanges, namely their high costs, lack of transparency, and vulnerability to fraud, are suggested to be resolved by this platform.

Enhanced security is the main benefit of consortia blockchain use in stock exchanges. It lowers the possibility of market manipulation by making it easier to create smart contracts for crucial trading procedures like clearing and settlement and by offering a decentralized ledger with transparent transaction records [1]. It is advised to conduct more research to examine this platform's scalability and potential effects on the larger financial industry.

The HonestChain solution uses consortium blockchain to enable secure data sharing amongst health information systems in the healthcare industry [24]. Experiments and simulations show that this method improves data security and privacy while meeting regulatory requirements. HonestChain is a decentralized permission system that combines attribute-based encryption and access management to optimize security and efficiency in the sharing of healthcare data. A consortium blockchain method tackles security concerns, trust issues, and limited storage capacity for vehicular ad-hoc networks (VANETs) [25]. Improvements in capacity, data sharing, and storage security are shown, but problems still exist because of the dynamic nature of VANETs and the constrained resources of vehicles.

To solve high transaction costs and insufficient transparency in cross-border transactions, a consortium blockchain system is recommended [10]. Despite drawbacks including a small number of network users and technological limitations, an examination conducted in Shenzhen demonstrates that this system outperforms conventional approaches in terms of transaction speed, security, and cost-effectiveness. The scalability of consortium blockchain technology, its interaction with current systems, and its wider sectoral implications need more research [12]. Future studies will concentrate on enhancing the technology's ability to manage higher volumes and integrating it with other systems while looking at new applications across a range of industries.

The authors [34] suggest Mudrachain, a blockchain-based system intended to improve efficiency in financial institutions' current check clearance procedures. This study makes a significant contribution to the current discussion over blockchain's revolutionary potential for banking and finance. Although it greatly enhances this discussion, it does not adequately address the difficulties related to the general application of blockchain technology. Mudrachains's success and efficacy depend on this board's adoption. A thorough examination of workable plans for this adoption could strengthen the case even further.

Logistics may benefit from consortium blockchain, which combines elements of private and public blockchains [12]. It provides a decentralized, transparent, and secure platform to address logistics concerns. Through the use of a hierarchical consensus method, the T2L system improves supply chain transaction security and product traceability. Case studies demonstrate T2L's efficiency, affordability, and transparency in comparison to conventional systems; however, more investigation is required into its viability and scalability [12].

Ensuring secure data sharing and personalized services is essential for intelligent transportation systems [26]. A transparent and safe platform for sharing services and data is provided by the consortium blockchain system that is being suggested. To improve the efficiency and customization of transportation services, digital identities, and smart contracts both enable data sharing [26]. To promote a decentralized network for safe data exchange and service customization, a case study illustrates consortium blockchain's capacity to offer secure data sharing and customizable services.

A consortium blockchain system is suggested for smart homes to safeguard data privacy [21]. This system uses smart contracts to manage data sharing and homomorphic encryption to secure data. It also integrates aspects of both public and private blockchains. This technique safeguards the confidentiality and integrity of data by enabling computations on encrypted data without the necessity for decryption. According to recent studies, the consortium blockchain is known for creating a decentralized network of reliable companies, which lowers the danger of data breaches and illegal access.

 doi:10.20944/preprints202403.0654.v1

In particular, the authors [21] support a homomorphic consortium blockchain to improve data privacy in smart home systems. Conventional data privacy techniques are considered insufficient for smart homes, requiring a more comprehensive and adaptable strategy. To preserve the effectiveness and security of smart home systems, data privacy is to be protected by the proposed homomorphic consortium blockchain. Integrating homomorphic encryption into a consortium blockchain framework offers a practical method for safeguarding the privacy of sensitive data. Assessments validate its efficacy in preserving the confidentiality and integrity of data [21].

The study [11], which addresses mobile device security, lists obstacles to malware detection, including the absence of a centralized authority and the dynamic nature of malware. The suggestion is for a consortium blockchain as a safe, transparent, and decentralized malware detection system. Tests and simulations show that this technology lowers the expenses associated with traditional approaches while improving mobile malware identification and prevention. To facilitate collaborative malware detection and prevention, the authors [11] propose a unique consortium blockchain network that uses a consensus approach to store and distribute detection findings across numerous devices.

The authors [22] also look at efficiency and safety in the production of coal mines, and they suggest a consortium blockchain as a way to address issues with data management, such as accountability and transparency. A decentralized, transparent, and secure framework for managing data is provided by the blockchain, where digital identities guarantee participant authenticity and smart contracts automate the production process [22]. A consortium blockchain system for safe and adaptable access to medical data is suggested for the healthcare industry [23]. By addressing the industry's susceptibility to security threats, this technology preserves regulatory compliance while guaranteeing the privacy and accuracy of medical data. It has a dynamic permission function for ongoing data protection, limits access to medical data to authorized entities, and keeps an unchangeable log of all access attempts [23].

[24] examines data accountability and provenance tracing, emphasizing the advantages of consortium blockchain technologies in terms of automating these procedures and guaranteeing data integrity. The proposed architecture offers a decentralized, transparent, and secure alternative for data management, with implications for the government, banking, and healthcare industries that need to monitor data provenance and accountability [24]. In addition, the authors [24] discuss the difficulties associated with data management in smart grids and suggest a consortium blockchain as a decentralized, transparent, and safe platform. Authorized stakeholders can access a secure ledger that stores a variety of data sources that are integrated into the smart grid in this manner [24].

Akropolis, a worldwide pension scheme powered by blockchain, is unveiled in [8]. Evaluations of this system indicate advances in pension management and address issues of efficiency, transparency, and pension fund management. It provides a decentralized pension management system that makes safe access and effective fund management possible [8]. For Vehicle-to-Grid (V2G) networks, attribute-based signatures and consortium blockchains are suggested as ways to protect privacy [22]. A distributed, transparent, and secure architecture for protecting data privacy is ensured by this combination. With signatures that encode user properties for safe access and transactions, smart contracts and attribute-based signatures simplify procedures and preserve data integrity [22].

An analysis of Hawk, a smart contract privacy mechanism, can be found in [25]. It combines homomorphic encryption, multiparty processing, and zero-knowledge proofs to provide low latency and higher throughput than current blockchain models. Hawk protects participant and data privacy while guaranteeing safe smart contract execution [25]. In the research paper [26], a novel peer-to-peer blockchain-based system for file storing and sharing is introduced. With a file indexing technique for effective file retrieval and smart contracts for data transfer governance, this system tackles the problems of large-scale operations and security in file storage and sharing [26].

The authors in paper [21] discuss the use of consortium blockchain in smart grid systems, overcoming issues with consensus brought on by blockchain's decentralized structure. To improve system efficiency and take participant reliability into account, a hierarchical trust-based consensus

 doi:10.20944/preprints202403.0654.v1

mechanism is suggested. Traditional consensus algorithms like PoW and PoS have problems with scalability, latency, and fault tolerance that can be resolved with this method [21].

The literature review highlights the growing significance of consortium blockchain in industries such as finance, healthcare, and logistics. It tackles important topics like data security and transparency whilst being distinct. These studies demonstrate blockchain technology's potential to revolutionize several industries and more importantly, financial distribution industries which can thrive on increased transparency and traceability that is enabled by blockchain. Thus the proposed system looks promising since it accommodates smart contracts and utilizes a private network that comes with increased security.

3. Proposed System

The structure of the proposed solution, which is designed to increase efficiency and transparency in the distribution of humanitarian aid, is laid out in the following section. To help readers better understand the architecture and workings of the system, subsequent parts will include detailed explanations accompanied by graphic representations.

3.1. System Overview

The system overview of the proposed solution is depicted in Figure 1. The proposed consortium blockchain network includes many parties, including a fund distribution organization, eligible pension recipients, and possibly financial service providers. Therefore, the major node, which is under the organizing body's control, is the hub of this system. To manage smart contracts, enroll beneficiaries, augment funds, and supervise their distribution, this node is essential. The organization node grants authorization to nodes representing pension-qualified beneficiaries to interact with the smart contract, allowing them to access their account information and make withdrawals.

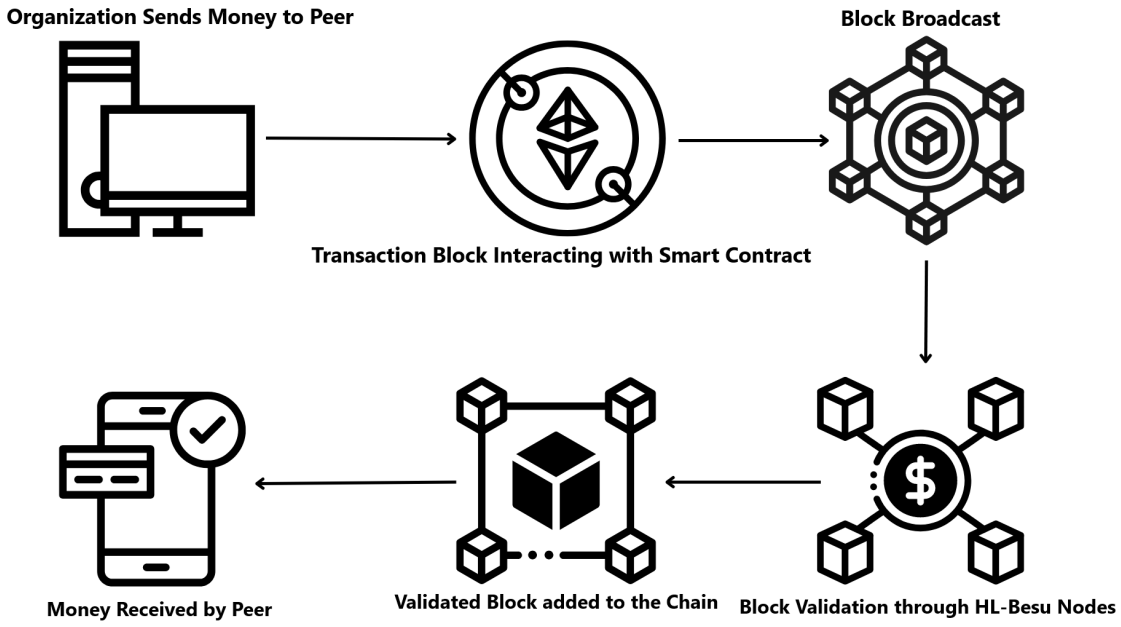

Figure 1. Proposed System Block Diagram

Contributions and distributions of funds made by the organization node are properly documented in this Consortium Blockchain Network. To carry out off-chain transactions, financial institutions, and other service providers may interact with the smart contract. When the smart contract is enabled, the receivers' bank information is included. The authorized organization node documents the pension disbursement procedure by verifying the recipients' status and account balance. By accessing

 doi:10.20944/preprints202403.0654.v1

blockchain data, financial service providers help with off-chain transactions, and these recipient nodes are able to confirm their balances. Elevated security, simple auditability, and unambiguous traceability are guaranteed by the transparency of every transaction. This system's consortium-based architecture improves control and efficiency.

3.2. Component Diagram

The component diagram in Figure 2 provides a detailed perspective of the financial distribution process. The diagram exhibits five key components, namely the User Interface (UI), Organization Interface, Hyperledger Besu Platform, Smart Contract, and Recipients. The user interface (UI) serves as the primary point of interaction for end users or beneficiaries, often taking the form of a user-friendly web or mobile application designed to facilitate straightforward engagement with the system. The Hyperledger Besu platform is directly interfaced with, enabling users to examine their balances and transaction histories. In a similar vein, the administrative point of contact is the Organization Interface. The company can administer the smart contract using this interface, which includes changing beneficiary information, adding money, and setting up bank accounts. Direct communication between this interface with the Hyperledger Besu platform is also possible.

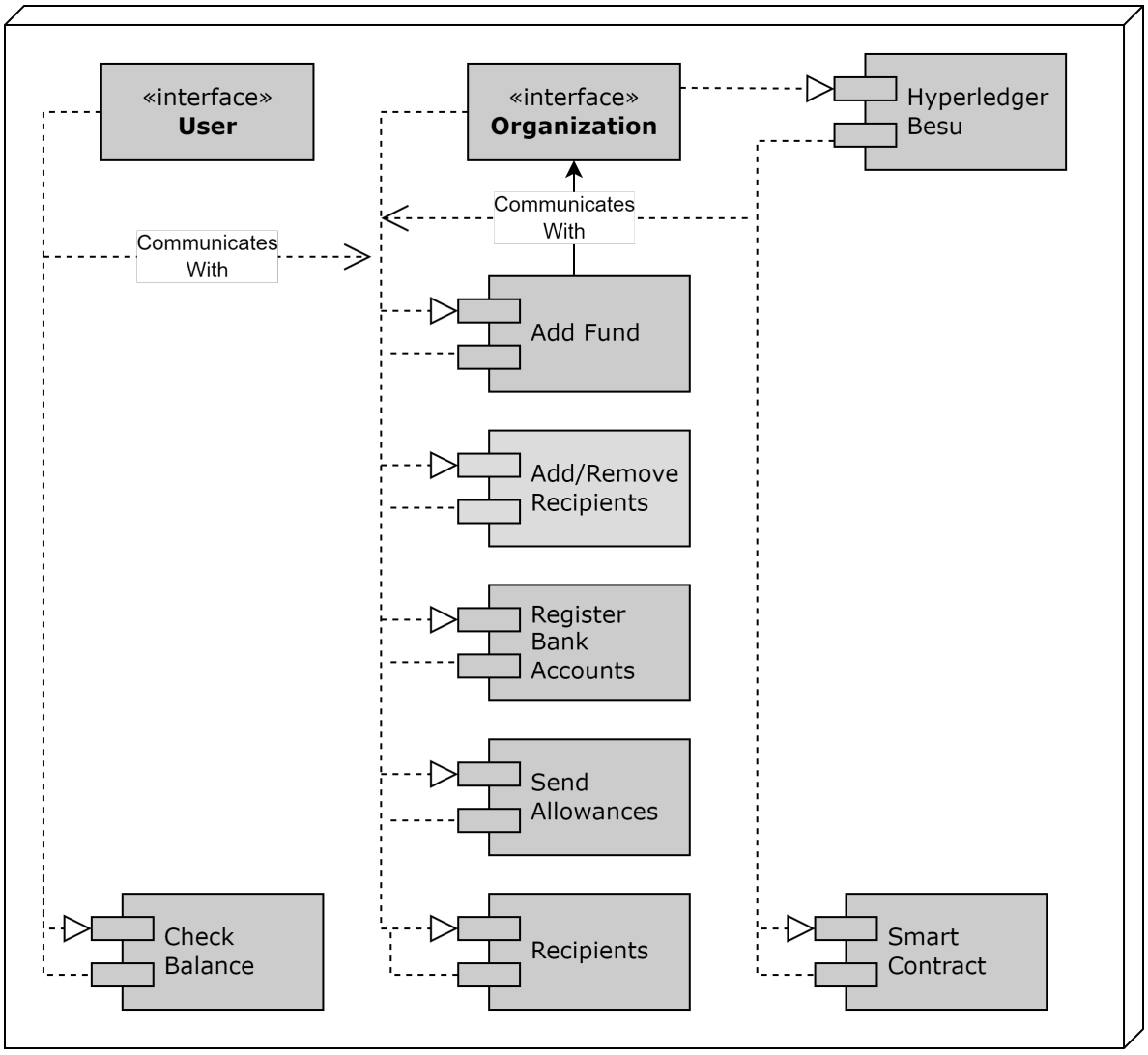

Figure 2. Proposed System's Component Diagram

 doi:10.20944/preprints202403.0654.v1

The Hyperledger Besu platform, which serves as a bridge between the smart contract and the User and Organization Interfaces to enable information sharing, hosts the smart contract. The operational logic of the system, which focuses on allocating cash and managing beneficiaries, is encapsulated in this smart contract. Through the User Interface, the recipients—fund beneficiaries—interface with the system. Last but not least, the Bank Accounts component represents the recipients' bank accounts that are connected to the system. Based on the replies from smart contracts, account information is shown on the user interface.

4. Development and Implementation of the Proposed Blockchain-based System

This section of the paper emphasizes the integration of Hyperledger Besu, a private network built on Ethereum, with an emphasis on the smart contract's design implementation and connection to the private network.

4.1. Smart Contract Overview

The smart contract is essential for facilitating authorization and transaction operations in the Hyperledger Besu consortium blockchain environment. A hierarchical access system is used in the contract to centralize power around the organization, which is the primary entity. This method is essential for controlling access rights and guaranteeing standardized transactions across a decentralized system.

The challenge of automating these operations is significant. Every function must work independently, but it also needs to blend in perfectly with the larger system architecture. Another layer of complication comes from the repeated emphasis on the msg.sender attributes to uphold transactional responsibility. Strong logic checks are necessary to address these complications and protect against security concerns, particularly in high-privilege operations.

Moreover, a crucial technical challenge is to guarantee the smart contract's operational effectiveness while also preserving its resistance against vulnerabilities. Considering the specific demands of financial systems within a consortium blockchain, the complexity of the situation is further heightened. To sum up, the smart contract illustrates how difficult it is to balance the operational needs of financial institutions in a consortium blockchain setting with technical precision.

4.2. Smart Contract

Using Solidity, a smart contract is created that provides dynamic control over beneficiary management and is a crucial tool for allocating funds in a consortium blockchain setting. Its main responsibility is to supervise and protect money distributions while following strict verification guidelines. By connecting beneficiary addresses to their banking information, this contract improves data confidentiality. By utilizing blockchain technology, the method ensures a safe, transparent, and effective way to distribute funds.

The smart contract in Algorithm 1 begins with a constructor function that creates the basic structure. $\mathcal{C}_{\text{addr}}$ [Table 1] is the address of the deployer during initialization, and it is the principal administrator. Important to the contract's administration, this body is in charge of beneficiary registration, which is represented by $\mathcal{M}$ [Table 1]. Through functions indicated by auth(m_i) [Table 1], the entity exerts control to confirm or deny the beneficiaries' status within $\mathcal{M}$ [Table 1]. Furthermore, keccak256 encryption is used by the H$(\cdot)$ [Table 1] function to securely link each beneficiary's identity, m_i [Table 1], with their financial information, represented by $\mathcal{A}_{\text{account}}$ [Table 1]. The overall security of the system is significantly improved by this centralized method of managing $\mathcal{A}_{\text{account}}$ [Table 1] under the supervision of $\mathcal{C}_{\text{addr}}$ [Table 1].

 doi:10.20944/preprints202403.0654.v1

Table 1. Descriptions of the symbols used in the Smart Contract algorithms.

Symbol	Name	Description
$\mathcal{M}$	Members Set	Set that contains all the individual members m_i
m_i	Individual Member	Represents users of system individually
addr(m_i)	Member Address Function	Wallet address of m_i
$\mathcal{A}$	Funds Allocation	Funds that are being allocated to m_i
$\mathcal{H}$	Bank Account Hash Mapping	Wallet address that is assigned to m_i with Name
$\mathcal{C}_{\text{addr}}$	Contract Creator Address	The main address wallet of the Organization
$\mathcal{B}$	Balance Mapping Function	Balance checker for Organization wallet
H$(\cdot)$	Hash Function	Hash generated combining m_i and addr(m_i)
$\mathcal{A}_{\text{account}}$	Bank Account Symbol	Account that represents the m_i for bank transfer
K_{m}	KeyManager Instance	A set which includes (keys,rcpUrl,gasPrice)
C_{a}	Contract Artifact	Smart contract that is being executed

Algorithm 1: Smart Contract

Input : A set $\mathcal{M}$ of members m_i, each with an address addr(m_i) and a bank account
Output: Allocation of funds $\mathcal{A}$ and registration of $\text{A}_{account}$ *hashes* $\mathcal{H}$
$\mathcal{C}_{\text{addr}} \leftarrow$ Address of the contract creator
`// Initialize` $\rightarrow \mathcal{C}_{\texttt{addr}}$
while *contract is active* **do**
  foreach $m_i \in \mathcal{M}$ **do**
    if *auth*(m_i) **then**
      $\mathcal{B}(\mathcal{C}_{\text{addr}}) \leftarrow \mathcal{B}(\mathcal{C}_{\text{addr}}) - \alpha$
      $\mathcal{B}(\text{addr}(m_i)) \leftarrow \mathcal{B}(\text{addr}(m_i)) + \alpha$
      `// Deduct` α `from` $\mathcal{C}_{\texttt{addr}}$ `and add` α `to` m_i
    else
      `// No action if` m_i `is not authorized`
  if *new funds* ϕ *are received* **then**
    $\mathcal{B}(\mathcal{C}_{\text{addr}}) \leftarrow \mathcal{B}(\mathcal{C}_{\text{addr}}) + \phi$
    `// Add funds` ϕ `to the contract's balance`
  foreach $m_i \in \mathcal{M}$ **do**
    $\mathcal{H}(\text{addr}(m_i)) \leftarrow \text{H}(\mathcal{A}_{\text{account}})$
    `// Register bank account hash` $\text{H}(\mathcal{A}_{\texttt{account}})$ `for` m_i
  foreach $m_i \in \mathcal{M}$ *requesting balance* **do**
    `// Return the balance of member` m_i
    return $\mathcal{B}(\text{addr}(m_i))$
  foreach $m_i \in \mathcal{M}$ *submitting account for validation* **do**
    `// Validate the submitted account against the stored hash for` m_i
    return $\text{H}(\mathcal{A}_{\text{account}}) = \mathcal{H}(\text{addr}(m_i))$

The operational core of the smart contract makes it possible for crucial financial transactions to be completed for a blockchain-based financial distribution system. Key functionalities are involved in this area, which is distinguished by automated, secure tracking and certification of fund balances and distributions. By using the $\mathcal{B}$ [Table 1] function, $\mathcal{C}_{\text{addr}}$ [Table 1] can increase its balance by a given amount, ϕ [Table 1], provided that $\mathcal{C}_{\text{addr}}$ [Table 1] initiates it first. The CapitalIncremented event is triggered upon a successful fund increment, recording the transaction value.

The allocation process, denoted as α [Table 1], streamlines the beneficiary allowance allocation procedure. It requires that the recipient m_i [Table 1] be authorized in $\mathcal{M}$ [Table 1] , that the action be started by $\mathcal{C}_{\text{addr}}$ [Table 1], and that the $\mathcal{B}(\mathcal{C}_{\text{addr}})$ [Table 1] be sufficient for the suggested allocation. When these conditions are satisfied, an AllocationDisbursed event is logged, indicating the recipient and the transferred amount, and the allotted α [Table 1] is subtracted from $\mathcal{C}_{\text{addr}}$'s balance [Table 1].

 doi:10.20944/preprints202403.0654.v1

To keep the system transparent, the function $\mathcal{B}$ [Table 1] to verify balances is essential. It makes the framework more transparent and accountable by enabling entities to determine their financial situations. To summarize, the smart contract's transaction features guarantee the careful, open, and safe management of money in this blockchain-based system. They are the best example of the efficiency and accuracy found in smart contract-driven financial systems.

4.3. Platform Integration

An open-source Ethereum client that works well in both public and private environments is called Hyperledger Besu. Besu usually employs consensus methods like as Ethash in public networks and is getting ready for Ethereum 2.0 to switch to Proof-of-Stake. It uses consensus techniques like Clique Proof-of-Authority and IBFT 2.0 in private networks, emphasizing efficiency and enhanced privacy. To secure network agreement even with possibly hostile nodes, the system in issue uses Hyperledger Besu with the IBFT 2.0 consensus protocol [27], set with four validators.

The environment in which the IBFT 2.0 mechanism functions is a mixture of Byzantine and honest nodes. In this case, honest nodes carefully follow the protocol, but Byzantine nodes may behave strangely. This system's notion of quorum is crucial. The protocol needs a quorum to reach a consensus, which is determined by the equation $F(n) = \frac{N-1}{3}$ [27].

This formula states that agreement from more than two-thirds of the nodes is required to reach a consensus. The system can therefore support up to $F(n)$ Byzantine nodes; however, the consensus is only preserved if $n - F(n) > 2F(n)$ [27]. IBFT 2.0 operates in a network that finally reaches synchronization, leveraging Ethereum's ÐΞVp2p for message delivery [27]. The global stabilization time (GST) is a crucial factor to take into account, as it determines when the message transmission delays, denoted by Δ, become consistent. Before GST, messages may be subject to erratic delays and possible losses. The capacity of IBFT 2.0 to effectively reach consensus in a heterogeneous network environment is largely dependent on the combination of Byzantine fault tolerance, the requirement for a quorum, and synchronization considerations [27].

While both use the IBFT 2.0 PoA consensus, there are differences in how smart contracts are deployed on Hyperledger Besu in public (P_{pub}) and private (P_{priv}) networks. Deployment to a fixed validator group ($V = 4$) in a private setting (DP_{priv}) provides faster deployment times (DT_{priv}) and consistent consensus. On the other hand, lengthier deployment durations (DT_{pub}) may result from a larger and more dynamic validator group in a public setting (DP_{pub}). While the public deployment is open to a larger range of users, the private deployment is concentrated on better control and restricted access. As a result, the deployment process and governance vary greatly based on the kind of network.

Using the IBFT 2.0 consensus mechanism; implementing a smart contract through the Truffle Suite within the private network contains various variables such as, The network URL, an array of keys, and a range for key selection; lowerLimit and upperLimit are the four key inputs needed for the setup. The K_{m} [Table 1], which is the process's output, is essential to preserving safe network transactions.

KeyManager (K_{m}) [Table 1], guarantees a safe connection to the blockchain node. It becomes part of the network configuration, allocating a unique network ID, usually referred to as '8001', which is a standard identification for private Ethereum networks. Additionally, parameters that determine the amount of computational labor needed and the cost per unit of that effort are set, such as maxGas and gasPriceUnit.

Then setup function, which activates the configured private (IBFT2.0) [27] network, completes the configuration. The Truffle Suite is then used to get ready for the implementation of a Solidity-based smart contract. To deploy smart contracts on the designated private network, the configuration file, needs to include network attributes such as host, port, and network ID.

An essential component of the implementation of the proposed system's smart contract inside the Truffle framework. The smart contract artifact (C_{a}) [Table 1], which contains the necessary deployment parameters and opcode, is the input for this deployment process. The functioning smart contract uses deploy function, which also marks the deployment outcome. In order to guarantee the contract's

 doi:10.20944/preprints202403.0654.v1

successful integration into the blockchain network, this method either generates a new contract instance or retrieves an existing one. By turning on the network capabilities of the contract, it opens the door to a safe and open system for money distribution and management inside the blockchain network. The contract's successful implementation on the Hyperledger Besu network [Shown in Figure 3], marks the beginning of a safe and effective financial management and distribution system.

```
Starting migrations...
======================
> Network name:    'besugo'
> Network id:      1337
> Block gas limit: 16777216 (0x1000000)


2_deploy_aNp.js
===============

   Replacing 'aNp'
   ---------------
   > transaction hash:    0x50588ad89d8e7edde2f671611e56c8e9f8f84404c446cf123eaaae71b5aabd94
   > Blocks: 0            Seconds: 0
   > contract address:    0xa50a51c09a5c451C52BB714527E1974b686D8e77
   > block number:        2033
   > block timestamp:     1688969782
   > account:             0xFE3B557E8Fb62b89F4916B721be55cEb828dBd73
   > balance:             4266
   > gas used:            930121 (0xe3149)
   > gas price:           0.000001 gwei
   > value sent:          0 ETH
   > total cost:          0.000000000930121 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:     0.000000000930121 ETH

Summary
=======
> Total deployments:   1
> Final cost:          0.000000000930121 ETH
```

Figure 3. Deployment of Smart Contracts on the Private Network

5. Performance Evaluation

The performance evaluation of the proposed system focuses on assessing the efficiency and responsiveness of a smart contract deployed on a custom network via the Hyperledger Besu platform. Conducted on a robust system with an AMD RYZEN 5600X processor and 16GB DDR4 RAM, the test, executed on the Fedora Workstation using the Caliper tool, measures throughput, latency, and resource usage. This evaluation aims to comprehend the system's performance and reliability under diverse transaction loads.

5.1. Benchmark Configurations & Metric

The benchmarking setup for the proposed system's smart contract, using Hyperledger Caliper, targets three specific functions: addRecipient, sendAllowance, and registerBankAccount. Each function undergoes five runs of transaction tests, ranging from 50 to 500 transactions in increments of 50. Employing a fixed-rate control for each transaction level, mirroring the transaction number for transactions per second (tps), the tests utilize specific JavaScript modules for each function with consistent arguments: initialMoney set at 10,000 and moneyToTransfer at 100.

The Hyperledger Caliper Framework provides parameters and their respective data based on the set benchmark configuration. The observed metrics from the test benchmark framework include:

 doi:10.20944/preprints202403.0654.v1

- Throughput (TPS): TPS, refers to the number of transactions a blockchain network can process per second. It's a key metric for gauging the scalability and efficiency of the system (TPS = Total Number of Transactions / Total Time in Seconds).
  In blockchain, high throughput is desirable, especially for public chains, to accommodate large numbers of users and applications. However, achieving high TPS often requires trade-offs with decentralization and security.
- Latency(s): Latency is the time taken from when a transaction is submitted until it's added to the blockchain. It's a measure of how quickly the network can confirm and commit transactions (Latency = Timestamp of Block Confirmation - Timestamp of Transaction Submission).
  Low latency is crucial for applications that require real-time or near-real-time settlements. However, like TPS, there's often a trade-off between low latency, security, and decentralization in blockchain networks.

5.2. Performance Analysis

The performance of various function components of the smart contract for the proposed system is illustrated in Figure 4. These functions are categorized into two groups: Transactional and Event where the figure highlights the throughput of these TPSs concerning varying send rates within a 4-Validator configuration.

The initial send rate is set at 50 and gradually increased to 250 for this analysis. It is observed that both Transactional TPS and Event TPS are similar at low rates. However, the curves diverge with increasing send rates. Transactional TPS shows an initial steep ascent followed by a plateau, suggesting a saturation point or system constraint. In contrast, Event TPS exhibits a more consistent and almost linear growth, indicating adaptability to higher send rates until it also plateaus. These nuanced differences in trajectories underscore distinct capacities and optimization levels between the two systems.

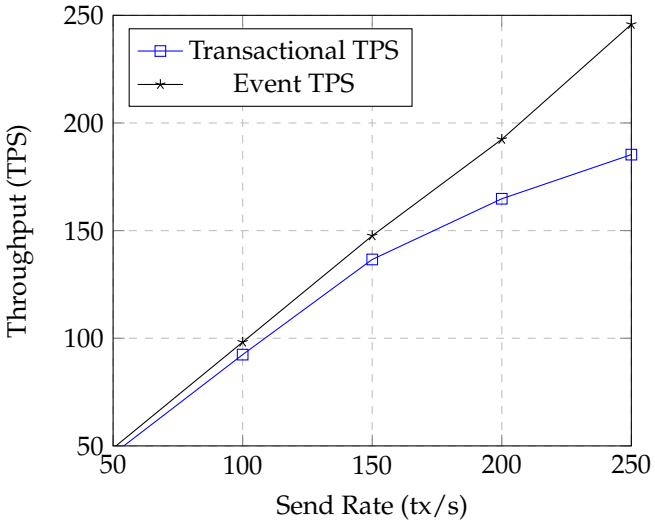

Figure 4. Smart contract function performance (Transactional TPS and Event TPS) in the proposed system, demonstrating throughput variations with increasing send rates in a 4-Validator configuration

Figure 5, depicts the performance dynamics of three distinct smart contract functions—AddRecipient, SendAllowance, and RegisterBankAccount—within a 4-Validator environment. Hence, the figure highlights the performance of these functions in terms of latency. To evaluate the performance of these functions, relatively higher send rates are considered. Thus, the initial rate is set at 250 and gradually increased to 500 for this purpose. The graph provides a comprehensive exploration of the intricate equilibrium within the system. Notably,

 doi:10.20944/preprints202403.0654.v1

RegisterBankAccount consistently displays heightened latency, hinting at its computationally intensive nature or the possibility of encountering execution bottlenecks. Upon observation, SendAllowance emerges as the most optimized for higher throughputs, while RegisterBankAccount lags in terms of efficiency. Moreover, the escalating latency beyond the optimal point for all functions underscores the critical importance of avoiding network overload, emphasizing the intricate relationship between throughput and latency.

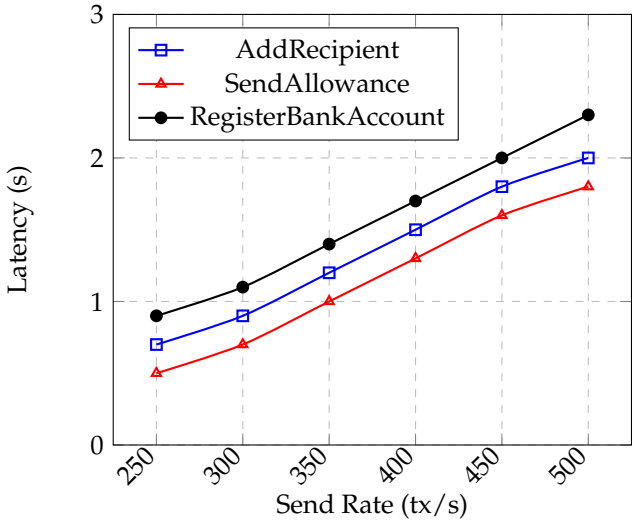

Figure 5. Exploration of System Equilibrium: Latency Dynamics Across Smart Contract Functions.

The transmit rate and latency rate have a proportional relationship, as seen in Figure 5. AddRecipient, SendAllowance, and RegisterBankAccount all exhibit a noticeable increase in latency as the transmit rate increases from 250 to 500 transactions per second (tx/s). This Pattern indicates a system that scales in terms of handling load but at the same time has decreased processing efficiency. The rise in latency is not just a result of increased demand; rather, it is a reflection of the inefficiencies in the underlying system's ability to handle concurrent transactions. It becomes clear that there is a fundamental trade-off between throughput and latency in distributed system design. Although the system shows excellent throughput scalability, it does so at the cost of higher latency. This occurrence highlights a common problem in distributed systems architecture; throughput optimization frequently leads to compromised latency and vice versa.

5.3. Performance Comparison

In this section, we evaluate and compare the overall efficiency of the proposed system, with throughput serving as the primary performance metric. The results are juxtaposed against two benchmark systems: Traditional Blockchain and Hyperledger Fabric. The selection of these systems is strategic—Hyperledger Fabric represents a contemporary benchmark, while Traditional Blockchain serves as a representation of legacy systems. This comparative analysis discerns the strengths of the proposed system, shedding light on its potential and prospective contributions to the industry.

 doi:10.20944/preprints202403.0654.v1

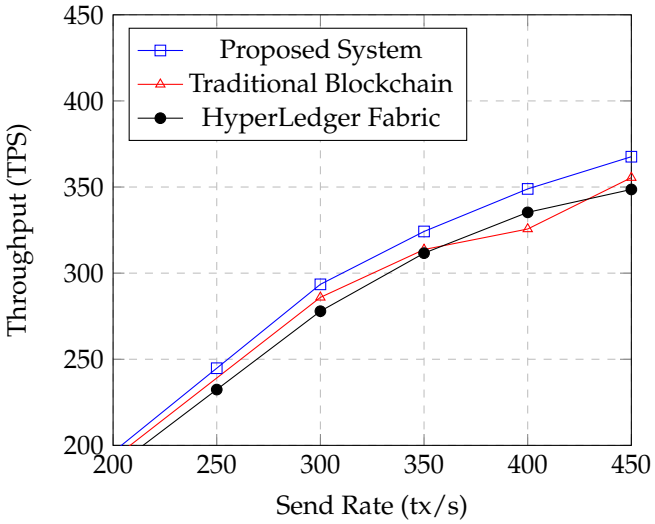

Figure 6. Throughput Efficiency: Comparison of Proposed System, Traditional Blockchain, and Hyperledger Fabric.

Therefore, Figure 6 presents the throughput performances of these three systems. The initial rate is set at 200 and progressively increased to 450 for this analysis. Examining a range of transmission rates, the graph distinctly underscores the advantages of the proposed system over its conventional counterparts. Graph [Figure 6] showcases the enhanced efficiency and scalability of the proposed solution. The system maintains significant throughput performance, even with an increase in the transmission rate. This trend is particularly noticeable at higher send rates, where the proposed system exhibits a less pronounced decline in throughput growth. This suggests a heightened emphasis on efficiency and scalability in the system's architecture, potentially leveraging improved consensus techniques, sophisticated algorithms, or more effective data structures.

In contrast, despite demonstrating excellent performance, conventional blockchain systems like Hyperledger Fabric fall short of the proposed system's efficiency, especially when dealing with larger transaction volumes. This variation points to possible bottlenecks or inherent inefficiencies in conventional blockchain layouts that could impede performance under high loads. Even well-established blockchain networks can face scalability issues, as indicated by Hyperledger Fabric's performance trajectory, which roughly aligns with those of other systems.

Considering the performance of the proposed system, the implementation of creative solutions or optimizations beyond the constraints of traditional blockchain architectures becomes imperative. Progress in these areas is crucial not only to increase transaction throughput but also to address more general scalability issues that have long been a focus of blockchain systems and their development.

6. Conclusion

The exploration of a financial distribution system based on a consortium blockchain reveals its potential to address challenges in contemporary financial systems. Addressing transparency, efficiency, and security concerns in traditional practices, the proposed system leverages the partially decentralized nature of consortium blockchains, ensuring vital data privacy for organizations handling sensitive information. The embedded smart contract plays a dual role, serving as both a transactional tool and a specialized solution to enhance procedural efficiency. Rigorous testing on the Hyperledger Besu platform validates the system's proficiency in handling high-frequency financial transactions with minimal computational burden. Successfully addressing transparency, efficiency, and security concerns, the proposed system emerges as a robust solution, supported by rigorous empirical testing.

Author Contributions: Conceptualization, N.M. and R.H.S.; methodology, R.H.S.; software, R.H.S. and S.M.; validation, N.M., R.H.S. and S.M.; formal analysis, N.M. and R.H.S.; writing—original draft preparation, N.M., R.H.S. and S.M.; writing—review and editing, N.M., R.H.S. and S.M.; visualization, N.M. and S.M.; supervision, N.M. and S.M.; project administration, N.M. and S.M.; funding acquisition, S.M. All authors have read and agreed to the published version of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bai, Yuhao, Qin Hu, Seung-Hyun Seo, Kyubyung Kang, and John J. Lee. "Public participation consortium blockchain for smart city governance." IEEE Internet of Things Journal 9, no. 3 (2021): 2094-2108.
2. Praitheeshan, Purathani, Lei Pan, and Robin Doss. "Private and trustworthy distributed lending model using hyperledger Besu." SN Computer Science 2 (2021): 1-19.
3. Fu, Zhengtang, Peiwu Dong, Siyao Li, and Yanbing Ju. "An intelligent cross-border transaction system based on consortium blockchain: A case study in Shenzhen, China." Plos one 16, no. 6 (2021): e0252489.
4. Mansoor, Nafees, Kaniz Fatema Antora, Priyata Deb, Tarek Ahammed Arman, Azizah Abdul Manaf, and Mahdi Zareei. "A Review of Blockchain Approaches for KYC." IEEE Access (2023).
5. Al-Shaibani, Hamed, Noureddine Lasla, and Mohamed Abdallah. "Consortium blockchain-based decentralized stock exchange platform." IEEE Access 8 (2020): 123711-123725.
6. Al Omar, Abdullah, Abu Kaisar Jamil, Amith Khandakar, Abdur Razzak Uzzal, Rabeya Bosri, Nafees Mansoor, and Mohammad Shahriar Rahman. "A transparent and privacy-preserving healthcare platform with novel smart contract for smart cities." Ieee Access 9 (2021): 90738-90749.
7. Zeng, Xueyun, Ninghua Hao, Junchen Zheng, and Xuening Xu. "A consortium blockchain paradigm on hyperledger-based peer-to-peer lending system." China Communications 16, no. 8 (2019): 38-50.
8. Andrianova, A. N. A. S. T. A. S. I. A., P. A. U. L. Hauner, D. K. Mcdonald, D. A. Manning, and M. E. H. D. I. Zerouali. "AKROPOLIS: A Global Blockchain Pensions Infrastructure." (2022).
9. Rahman, Tasfia, Sumaiya Islam Mouno, Arunangshu Mojumder Raatul, Abul Kalam Al Azad, and Nafees Mansoor. "Verifi-chain: A credentials verifier using blockchain and IPFS." In International Conference on Information, Communication and Computing Technology, pp. 361-371. Singapore: Springer Nature Singapore, 2023.
10. Ariffin, Nizamuddin, and Ahmad Zuhairi Ismail. "The design and implementation of trade finance application based on hyperledger fabric permissioned blockchain platform." In 2019 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), pp. 488-493. IEEE, 2019.
11. Gu, Jingjing, Binglin Sun, Xiaojiang Du, Jun Wang, Yi Zhuang, and Ziwang Wang. "Consortium blockchain-based malware detection in mobile devices." IEEE Access 6 (2018): 12118-12128.
12. Hao, Yue, Yi Li, Xinghua Dong, Li Fang, and Ping Chen. "Performance analysis of consensus algorithm in private blockchain." In 2018 IEEE Intelligent Vehicles Symposium (IV), pp. 280-285. IEEE, 2018.
13. Vinayak, Muskan, Saulo dos Santos, Ruppa K. Thulasiram, Parimala Thulasiraman, and Srimantoorao S. Appadoo. "Design and implementation of financial smart contract services on blockchain." In 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 1023-1030. IEEE, 2019.
14. Oliveira, Nicollas Rodrigues de, Yago de Rezende dos Santos, Ana Carolina Rocha Mendes, Guilherme Nunes Nasseh Barbosa, Marcela Tuler de Oliveira, Rafael Valle, Dianne Scherly Varela Medeiros, and Diogo M. F. Mattos. 2024. "Storage Standards and Solutions, Data Storage, Sharing, and Structuring in Digital Health: A Brazilian Case Study" Information 15, no. 1: 20. https://doi.org/10.3390/info15010020
15. Zhang, Lihua, Qianqian Yang, Yi Yang, Shihong Chen, and Jinguang Gu. 2024. "Data Sharing Scheme of Smart Grid Based on Identity Condition Proxy Re-Encryption" Electronics 13, no. 1: 139. https://doi.org/10.3390/electronics13010139
16. Ansar, Kainat, Mansoor Ahmed, Markus Helfert, and Jungsuk Kim. 2024. "Blockchain-Based Data Breach Detection: Approaches, Challenges, and Future Directions" Mathematics 12, no. 1: 107. https://doi.org/10.3390/math12010107
17. Ahmed, Istiaque, Kai Fumimoto, Tadashi Nakano, and Thi Hong Tran. 2024. "Blockchain-Empowered Decentralized Philanthropic Charity for Social Good" Sustainability 16, no. 1: 210. https://doi.org/10.3390/su16010210

18. Kufo, Andromahi, Ardit Gjeci, and Artemisa Pilkati. 2024. "Unveiling the Influencing Factors of Cryptocurrency Return Volatility" Journal of Risk and Financial Management 17, no. 1: 12. https://doi.org/10.3390/jrfm17010012
19. Hajian Berenjestanaki, Mohammad, Hamid R. Barzegar, Nabil El Ioini, and Claus Pahl. 2024. "Blockchain-Based E-Voting Systems: A Technology Review" Electronics 13, no. 1: 17. https://doi.org/10.3390/electronics13010017
20. He, Ming, Haodi Wang, Yunchuan Sun, Rongfang Bie, Tian Lan, Qi Song, Xi Zeng, Matevz Pustišek, and Zhenyu Qiu. "T2L: A traceable and trustable consortium blockchain for logistics." Digital Communications and Networks (2022).
21. Jiang, Xingguo, Aidong Sun, Yan Sun, Hong Luo, and Mohsen Guizani. "A trust-based hierarchical consensus mechanism for consortium blockchain in smart grid." Tsinghua Science and Technology 28, no. 1 (2022): 69-81.
22. Wei, Guochen, and Yonghong Ma. "Privacy protection strategy of vehicle-to-grid network based on consortium blockchain and attribute-based signature." In IOP Conference Series: Earth and Environmental Science, vol. 661, no. 1, p. 012027. IOP Publishing, 2021.
23. Agrawala, Devendra, Anurag Shrivastavab, and Rishi Kumar. "A survey on vulnerabilities and performance evaluation criteria in blockchain technology." Advances in Distributed Computing and Artificial Intelligence Journal 9, no. 2 (2020): 91-105.
24. Purohit, Soumya, Prasad Calyam, Mauro Lemus Alarcon, Naga Ramya Bhamidipati, Abu Mosa, and Khaled Salah. "HonestChain: Consortium blockchain for protected data sharing in health information systems." Peer-to-peer Networking and Applications 14, no. 5 (2021): 3012-3028.
25. Zhang, Xiaohong, and Xiaofeng Chen. "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network." Ieee Access 7 (2019): 58241-58254.
26. Wang, Di, and Xiaohong Zhang. "Secure data sharing and customized services for intelligent transportation based on a consortium blockchain." IEEE Access 8 (2020): 56045-56059.
27. She, W. E. I., Zhi-Hao Gu, Xu-Kang Lyu, Q. I. Liu, Zhao Tian, and Wei Liu. "Homomorphic consortium blockchain for smart home system sensitive data privacy preserving." IEEE Access 7 (2019): 62058-62070.
28. Qiang, Zilin, Yingsen Wang, Kai Song, and Zijuan Zhao. "Mine consortium blockchain: the application research of coal mine safety production based on blockchain." Security and Communication Networks 2021 (2021): 1-10.
29. Xu, Boyi, Li Da Xu, Yuxiao Wang, and Hongming Cai. "A distributed dynamic authorisation method for Internet+ medical & healthcare data access based on consortium blockchain." Enterprise Information Systems 16, no. 12 (2022): 1922757.
30. Neisse, Ricardo, Gary Steri, and Igor Nai-Fovino. "A blockchain-based approach for data accountability and provenance tracking." In Proceedings of the 12th international conference on availability, reliability and security, pp. 1-10. 2017.
31. Kosba, Ahmed, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts." In 2016 IEEE symposium on security and privacy (SP), pp. 839-858. IEEE, 2016.
32. Peng, Shaoliang, Wenxuan Bao, Hao Liu, Xia Xiao, Jiandong Shang, Lin Han, Shan Wang, Xiaolan Xie, and Yang Xu. "A peer-to-peer file storage and sharing system based on consortium blockchain." Future Generation Computer Systems 141 (2023): 197-204.
33. Saltini, Roberto, and David Hyland-Wood. "Ibft 2.0: A safe and live variation of the ibft blockchain consensus protocol for eventually synchronous networks." arXiv preprint arXiv:1909.10194 (2019).
34. Kabra, Naman, Pronaya Bhattacharya, Sudeep Tanwar, and Sudhanshu Tyagi. "MudraChain: Blockchain-based framework for automated cheque clearance in financial institutions." Future Generation Computer Systems 102 (2020): 574-587.