The Chinese University of Hong Kong

FTEC5520 Applied Blockchain and Cryptocurrencies

Group 6 Project Proposal

Enhancing Transparency and Accountability:

Blockchain-Based Government Fund Allocation and Tracking System

Group Member:

Cen Baihui	*1155197612*
Chen Angyu	*1155197620*
Chen Yunfan	*1155198241*
Huang Shiqi	*1155204275*
Jiang Tianyun	*1155197611*
Liang Haojin	*1155200065*
Niu Xinyan	*1155201239*

06/Feb/2024

1. Project Background and Motivation

Within the public finance framework, governments serve as the managers of the nation's resources, overseeing and implementing fiscal programs through its various departments. To bolster the transparency and traceability of government funds, nations globally have adopted tailored regulatory measures. For example, the United States enacted the Digital Accountability and Transparency Act (DATA) in 2014, under which federal departments are required to disclose financials quarterly on government websites. However, solely depending on public disclosure to prevent fiscal mismanagement still leaves room for opacity and inefficiency in the allocation and tracking of government funds. Evident in the U.S., the Payment Protection Program (PPP), which initially aimed at supporting small businesses during economic downturns, has reportedly disbursed loans to unrelated entities. These incidents underscore a pressing need for a paradigm shift in government funding, one that transcends traditional disclosure mechanisms and introduces a more robust, transparent, and traceable system. Blockchain technology presents a promising avenue for realizing this transformation. By leveraging the inherent features of blockchain—immutability and transparency—this project aims to revolutionize government fund allocation and tracking, thereby enhancing the integrity and efficiency of public finance systems.

2. Objectives and Blockchain Applications

Our project aims to develop a blockchain-based government fund allocation and tracking system that ensures transparency and accountability. Main objectives and blockchain applications include:

1) **Develop a system for real-time tracking of government fund allocation.**

Every transaction on the blockchain is recorded on a ledger distributed across every participant in the network. This feature can create a transparent and immutable record of all government transactions, including contracts, disbursements, and receipts.

2) **Streamline government fund allocation process.**

Smart contracts can be programmed to release funds only when certain conditions are met. This automation can reduce the likelihood of overspending or misallocation of funds.

3) **Enhance data security and integrity in government financial transactions.**

The decentralized nature and cryptographic protection can offer robust security. Each block is linked to its predecessor through cryptographic hashes, ensuring the integrity of the entire chain.

3. Proposed System and Architecture

Our proposed system introduces an advanced architecture aimed at enhancing the transparency, efficiency, and accountability of government funding by various entities. Here's how the user-oriented and secure platform operates:

Upon the initial login, users are required to register in the system, subsequently requesting funds by uploading the necessary certification documents. These requests are then encrypted and stored on the blockchain as individual blocks, with each request assigned a unique ID. This allows users to easily review and track the status of their requests using this ID.

Fund allocators, including central and state governments, process and approve or reject requests by accessing the Requests List. Based on specifics like amount and project nature, approval types vary for different requests, including direct state approval, direct central approval, and dual government approval. Post-approval, smart contracts automatically allocate funds to requesters. Governments can monitor fund distribution and adjust budget schemes for optimal resource allocation.

Auditors are integral to maintaining financial propriety and accountability. The system grants them secure and transparent access to the entire fund allocation history, thereby streamlining their monitoring duties and aiding in the detection of any irregularities or corruption. Through this comprehensive and user-centric approach, our system aims to revolutionize the management and tracking of government funds.

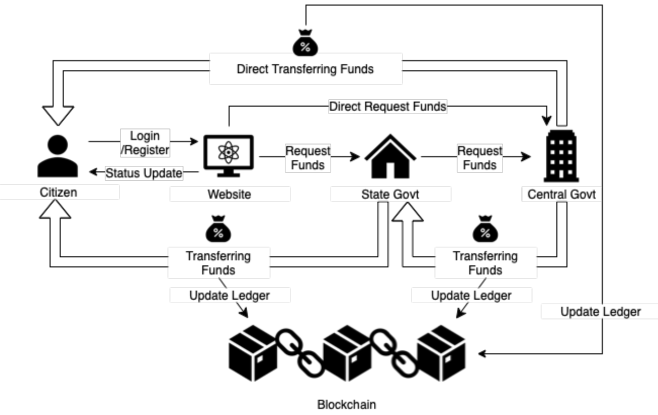

Fig. 1 Flowchart of funding process

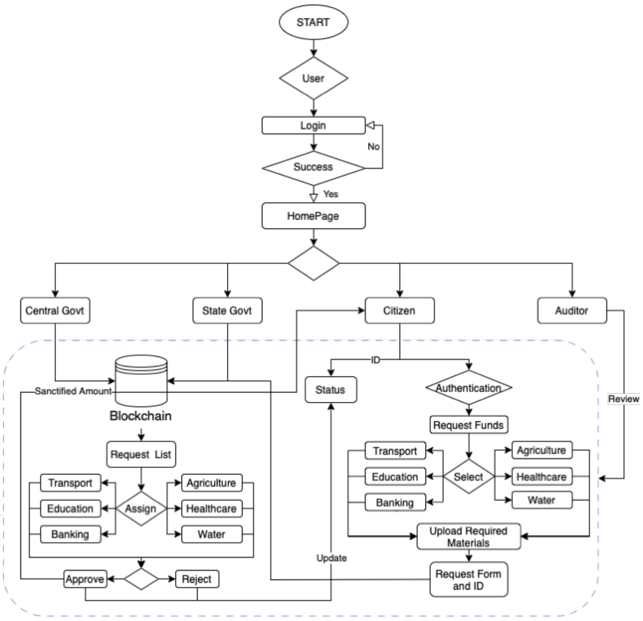

Fig. 2 Architecture diagram

4. Technical Framework

4.1 Blockchain Selection

In government fund allocation and tracking, we regard consortium chains as superior to both public and private chains: the former offers excessive transparency that risks sensitive financial data, while the latter lacks the necessary transparency for public accountability (Swan, 2015). Among consortium blockchain platforms, Ethereum stands out for its advanced technology, vast developer ecosystem, and robust smart contract capabilities compared to other consortium chains such as Hyperledger and R3 Corda (Gatteschi et al., 2018). Ethereum's smart contract capabilities enable the creation of self-executing agreements that can automate budget allocation and tracking, reducing the potential for human error and corruption (Christidis & Devetsikiotis, 2016). Moreover, Ethereum's extensive developer community and established tools and frameworks make it easier to build, deploy, and maintain the necessary blockchain solutions for budget tracking (Mougayar, 2016). Thus, the Ethereum-based consortium chain stands out as the optimal choice, for its balanced approach to privacy and transparency, and its comprehensive ability for system development.

4.2 Consensus Mechanism

We compared three consensus mechanisms that are suitable for an Ethereum consortium chain: Proof of Authority (PoA), Practical Byzantine Fault Tolerance (PBFT), and Quorum Chain (a variation of PoA). PoA is highly efficient and provides low-latency transaction processing, which is crucial for systems requiring quick and reliable updates, like financial tracking systems (Dai, H. K., & Vasarhelyi, M. A., 2017). It is characterized by its reliance on trusted, pre-approved validators, making it an appropriate choice for a consortium of known entities, such as government agencies. Meanwhile, the energy efficiency and low latency of PoA also contribute to a more sustainable and responsive system, addressing governmental priorities of operational cost-effectiveness and environmental responsibility. While PBFT provides a robust fault tolerance mechanism, its complexity and scalability issues make it limiting in a large-scale government system that requires both responsiveness and simplicity in operations (Castro & Liskov, 1999). On the other hand, Quorum Chain, though shares the centralization characteristics of PoA, lacks the same level of maturity and community support.

In our project, the centralization aspect of Proof of Authority (PoA) is not a considerable disadvantage, given our focus on ensuring transparency and traceability. Validators in PoA, usually government departments or auditors, inherently act as third-party scrutinizers. Consequently, PoA emerges as the ideal consensus mechanism for a government fund allocation and tracking system, adeptly balancing the requirements for control, efficiency, and accountability.

4.3 Smart Contract Development

Smart contracts, with robust encryption and automated execution, form the core of our funding allocation and tracking system. Our team plans to develop a Fund Allocation Contract to distribute funds under specific conditions, featuring a multi-signature approval mechanism for enhanced security, dynamic budget allocation for flexibility, and real-time anomaly detection for financial integrity.

The multi-signature mechanism ensures funds are released only after obtaining approvals from a predetermined number of stakeholders, reducing risks of unauthorized access. Unlike traditional approaches, our smart contract also allows dynamic redistribution of resources across departments or projects, adapting to performance changes or shifting priorities. Additionally, anomaly detection mechanisms will be implemented to automatically identify unusual spending patterns, potential discrepancies, or deviations from approved budget norms. Alerts will be triggered when anomalies are detected, allowing for timely investigation and corrective action. Overall, this contract embodies our commitment to financial accountability, efficiency, and transparency in budget management.

References

Castro, M., & Liskov, B. (1999). Practical Byzantine Fault Tolerance. Proceedings of the Third Symposium on Operating Systems Design and Implementation, 173-186.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292-2303.

Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. Journal of Information Systems, 31(3), 5-21.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough?. Future Internet, 10(2), 20.

Mougayar, W. (2016). The business blockchain: Promise, practice, and application of the next Internet technology. John Wiley & Sons.

Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.