2024 IEEE International Conference on Computing, Applications and Systems (COMPAS), September 25-26, 2024, Bangladesh

Grainbee: A Quantum-Resistant Blockchain-Based Ration Distribution System with Hardware Security Modules

Sohel Ahmed Joni
Department of CSE
Bangladesh University of Business and Technology
Dhaka, Bangladesh
sohelahmedjony@gmail.com

Rabiul Rahat
Department of CSE
Bangladesh University of Business and Technology
Dhaka, Bangladesh
rabiulrahatt@gmail.com

Nishat Tasnin
Department of CSE
Bangladesh University of Business and Technology
Dhaka, Bangladesh
nishattasnin02@gmail.com

Partho Ghose
Department of CSE
Bangladesh University of Business and Technology
Dhaka, Bangladesh
partho.cse.jnu@gmail.com

Md. Mahbub-Or-Rashid
Department of CSE
Bangladesh University of Business and Technology
Dhaka, Bangladesh
mahbub@bubt.edu.bd

***Abstract*—In developing countries, subsidized food programs aimed at supporting the poor are often undermined by corruption and mismanagement, leading to food waste and unequal distribution. To overcome these challenges, we introduce GrainBee, a blockchain-powered ration distribution system designed to ensure secure, transparent, and efficient food supply distribution. By leveraging blockchain's inherent security and immutability, GrainBee addresses the major security and transparency issues that plague traditional and existing blockchain-based systems.**

Our proposed system employs a post-quantum secure, blockchain-based approach to combat corruption and fraudulent invoicing, guaranteeing integrity through a distributed, immutable ledger. To further fortify security, we integrate Hardware Security Modules (HSMs), providing an additional layer of protection for sensitive data and transactions. A built-in reservation and scheduling system streamlines the distribution process, while a user-friendly interface and machine translation services bridge language gaps, enhancing usability and accessibility. By harnessing the power of blockchain technology, GrainBee offers a robust solution to the complex challenges of food distribution.

***Index Terms*—Ration Distribution, Blockchain, Post-Quantum Cryptography, Hardware security modules, Automation**

I. Introduction

Food insecurity remains a significant global challenge, with an alarming number of individuals affected by hunger and malnutrition [1]. Ration distribution programs are crucial for supporting vulnerable populations. To ensure equitable access to essential food items, several nations have implemented rationing and price subsidies [2], [3]. However, the rising costs have pushed the least developed countries toward fiscal unsustainability, and current policies and distribution mechanisms have fallen short of fully assisting those in need [4].

The efficacy of these ration distribution programs is often undermined by challenges such as diversion, fraud, and delays, leading to waste and corruption due to inadequate supervision. [5] For instance, during the COVID-19 pandemic, collusion between government-authorized distributors and local merchants resulted in the diversion of essential goods. These issues not only hinder the delivery of critical support but also erode trust and transparency in the process [6].

In this paper, we address the question: Can a blockchain-based ration distribution system improve trust by being tamper-proof, publicly transparent, and privacy-preserving? We propose a novel approach, "Grainbee" that utilizes blockchain technology with a raft consensus-based permissioned blockchain for high-throughput and instant transactions [7] . Additionally, we integrate post-quantum secure asymmetric encryption methods (e.g., Dilithium-Kyber) to protect against potential quantum computing threats [8].

Manual processes in the current system, such as inventory stocking and selling, result in long overhead times for serving beneficiaries. To address this, we automate these processes using chain-code, which executes agreed-upon transactions when specific requirements are met. The transparency of chain-code enhances trust in the system [9].

To alleviate distribution bottlenecks, we propose a scheduling and reservation system [10]. Customers can use an app to purchase products and select a pickup time, streamlining inventory management and reducing waiting times. We also integrate a multilingual, multimodal translation model [11] into the app to cater to low-literacy and visually impaired customers, offering various translation options and automatic speech recognition.

The key contributions of this research are as follows:

- Using blockchain technology to tackle issues in ration distribution authentication, inventory management, and security.
- This research propose a raft consensus-based permissioned blockchain for faster and more efficient transactions in ration distribution.
- Integrating post-quantum secure asymmetric encryption methods to create a Membership Service Provider (MSP), safeguarding against quantum computing threats.
- We introduce Hardware Security Module (HSM) to the ration distribution system to safeguard User and networks security.
- Automating manual processes with chaincode, enhancing transparency, and fostering trust.
- Introducing a scheduling and reservation system to streamline distribution and reduce waiting times.
- Catering to diverse customer needs with a multimodal machine translation model in the app.

The urgent need for innovation in ration management and distribution calls for exploring the potential of blockchain technology. "Ration" aims to

revolutionize the food distribution network, making it more efficient, reliable, and accessible while ensuring the privacy and security of beneficiaries.

The rest of this paper is organized as follows. Section II reviews the existing literature on blockchain-based ration distribution systems. Section III presents the methodology used to design and implement the proposed system. Section IV describes the implementation details of the proposed system. Section V presents the results and discussion of the proposed system. Section VI analyzes the security of the proposed system. Finally, Section VII concludes the paper and suggests future work.

II. Literature Review

The ration distribution system faces fraud and corruption challenges, causing inefficiencies and disruptions. Traditional centralized supply chains hinder data provenance tracking and traceability. Blockchain technology is proposed as a solution to provide traceability, trust, and delivery Shahid et al. [12] proposed Ethereum-based blockchain network featuring blockchain and smart contracts also used an Interplanetary File Storage System (IPFS) to upload the data of transactions in the blockchain system. P Thakare et al. [13] proposed suggested using blockchain technology in the Public Distribution System (PDS) to tackle fraud and corruption. They present a network of food transfers involving farmers, central and state governments, fair-price shops, and customers. To address corruption and fraud in the distribution chain C Devi Parameswari et al. [14] proposed blockchain technology using solidity language. G Baralla et al. [15] have proposed a blockchain-oriented platform to secure food data storage and origin provenance. To address corruption and transparency issues in the Public Distribution System (PDS) D Malathi et al. [16] proposed a blockchain technology-based smart ration shop system. The study finds that the proposed system achieves an average satisfaction level of 90% among users, with a notable response time of approximately 130 milliseconds. Mishra el at. [17] proposes a blockchain-based framework for the Public Distribution System (PDS) in India to manage food grain supply to targeted beneficiaries. Their proposed framework aims to prevent diversions and leakages of grains at the warehouse and Fair Price Shop (FPS) level. RS Pawar el at. [18] exploring the limitations of conventional food subsidy distribution systems proposed blockchain-based technology. S Dhanake el at. [19] proposed a blockchain technology-based prototype for a small website to address corruption in public ration distribution systems. D Nuševa el at. [20] explore the impact of digitalization on sustainable food supply chains, focusing on blockchain technology as a solution for traceability, safety, and sustainability issues. H Wu el at. [21] propose a parallel search algorithm to improve blockchain-based supply chain traceability efficiency. Their proposed algorithm replicates product records across multiple chunks and uses parallel search to reduce time overhead by up to 85.1% with minimal storage overhead.

Although existing research on ration distribution systems offers varying levels of security and transparency over traditional systems, most of them use DLT solely for transaction storage and fail to address the use case of integrated business logic and automation via chain-code. Additionally, some research relies heavily on Ethereum-based blockchain, resulting in slow throughput (only 25 TPS) and ever-increasing gas fees. Moreover, none of the existing research introduces post-quantum secure ration distribution systems or hardware secure modules (HSMs) for compliance with government standards such as FIPS 140-2 [9]. These persisting issues require serious attention to foster generational improvements on existing systems.

III. Methodology

The proposed ration distribution system address the critical aspect of secure ration distribution system. It's decentralize and each and every transaction is saved in blockchain ledger. and the chain-code mechanism automate the process for fast and efficient ration distribution experience.

A. System Design

The proposed system is built on a multi-organizational network that includes various types of organizations such as government agencies, distributors, sellers, NGOs, and logistics providers. All organizations in this network have access to certain components without restrictions, while some components are assigned to specific organizations via an independent node called the orderer service. Each organization in the network has multiple nodes, and each node can perform different logical functions. For example, some nodes may handle client requests, while others execute smart contracts, decide the order of transactions via a consensus algorithm, or validate blocks. This network architecture ensures that all organizations have the necessary access to the system while maintaining appropriate levels of security and privacy. By assigning specific components to certain organizations via the orderer service, we can ensure that sensitive information is only accessible to authorized parties.

The proposed system comprises several components as follows:

System: As Shown in Fig 1, each participant in the network will be a member of their respective organization and will be provided with relevant functionalities and business logic by their organization's dedicated super-nodes. For instance, government agencies can manage product sourcing, member card management, and related functionalities. Sellers may have access to scheduling, inventory management, and order-related functionalities. The client app can have stock management, scheduling, and payment-related functionalities. This structure enables each organization to have control over its specific functions, while still maintaining the integrity and security of the overall network. Additionally, this approach allows for better data privacy and access control, as each organization only has access to the data and functionalities that are relevant to their specific role in the network.

HSM: The cryptographic operations performed by blockchain nodes can be delegated to an HSM. An HSM protects your private keys and handles cryptographic operations, allowing your peers and orderer nodes to sign and endorse transactions without exposing their private keys.

External Entities: The proposed Ration Distribution System integrates external services such as payment gateways, MSP service, and other organizational entities to ensure a secure, transparent, and reliable distribution process.

Participants: The primary participants in the Ration Distribution System are government agencies, ration distribution points or sellers, and customers. Each participant is provided with a dedicated user interface panel tailored to their specific functionalities, task, and access level, enabling efficient task execution and seamless communication across various blockchain systems.

B. Ration Distribution

The ration distribution process starts with identifying the type of asset. If the rations come in individual packets, they can be serialized and added to the blockchain as non-fungible tokens (NFTs). For example, 5000 serialized packages of 5kg grains could be tokenized as unique NFTs. On the other hand, if the rations are in bulk, such as 10,000 liters of vegetable oil, they can be added as fungible tokens, allowing for easy portioning during transactions.

The distribution process involves multiple stakeholders, as shown in Fig 1.

Customers can use their mobile app to purchase rations, make payments, and schedule a convenient time to collect their rations from their chosen distributor. This eliminates the need for long queues and provides certainty about the quality and quantity of the products they receive.

At the distribution points, sellers receive rations and use custom instructions via chaincode to automatically reserve and secure customer orders. This enables them to efficiently provide rations to each customer. The sellers obtain their supplies from government and logistics agencies, and these rations are added to their balance as fungible or non-fungible tokens. When a customer purchases a ration, the corresponding asset is deducted from the distributor's balance and burned to prevent reuse.

Various government, NGO, and logistics agencies play crucial roles in the process. They manage the initial collection of rations, supply them to distribution points, identify and enroll needy individuals for membership, and handle membership status and cards.

All data and functionality are executed through smart contracts, ensuring automation and transparency. The system also includes a monitoring mechanism that detects data abnormalities or irregularities in customer purchases, sales data, and distributor inventory. If any issues are identified, an alert is automatically triggered, along with a detailed report on the transaction, asset, distributor, and customer. This monitoring function is embedded within a self-executing chaincode program.

IV. Implementation

From an implementation standpoint, the proposed system consists of multiple sub-systems. Here are the implementation details:

Network: To set up a multi-organization permissioned blockchain network, we utilized Hyperledger Fabric. In this research, we used the CC-Tools to create relational definitions of asset types, data type validation, and many custom types. We also used Fabric events management and transaction definitions with built-in argument's validation, CRUD mechanism and callers restriction via chain-code for the Fabric network. Additionally, we used the CC-tools-demo to monitor the blockchain network and test the developed chain-code, as well as create a gateway API.

Benchmark: To measure the performance of a specific blockchain implementation, we employed Hyperledger Caliper along with Go's built-in

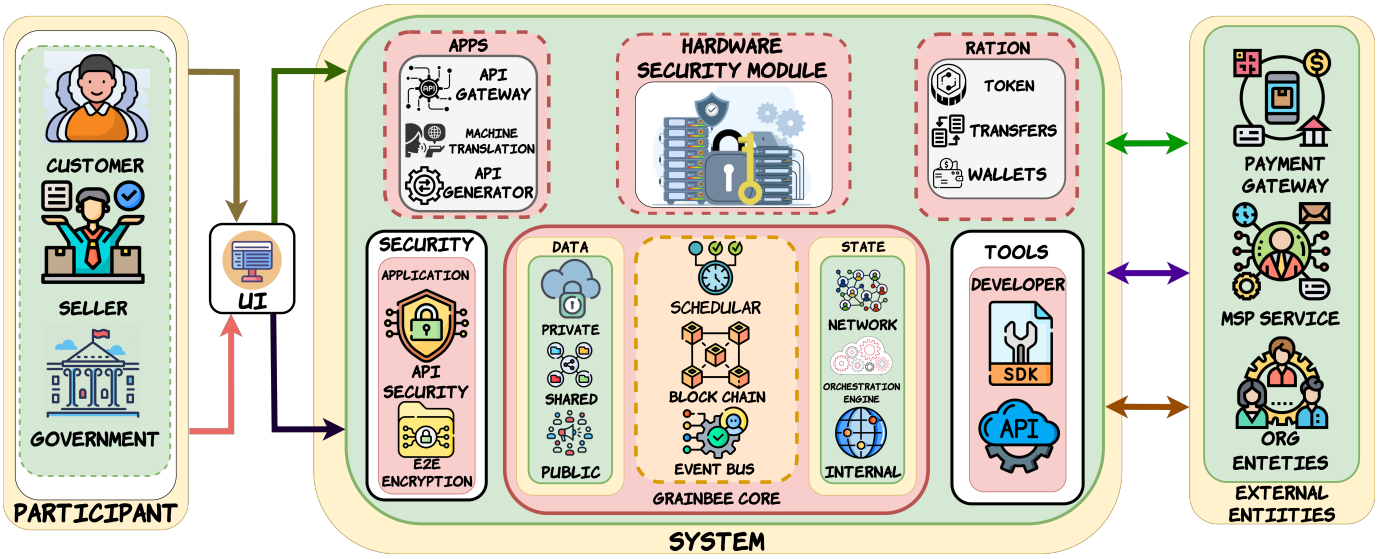

Fig. 1. The diagram illustrates how various participants (customers, sellers, government agencies, etc.) and system components (security system, event bus, blockchain, payment gateway, etc.) interact with the proposed ration distribution system through APIs provided for SDKs, tokens, wallets, and mobile apps.

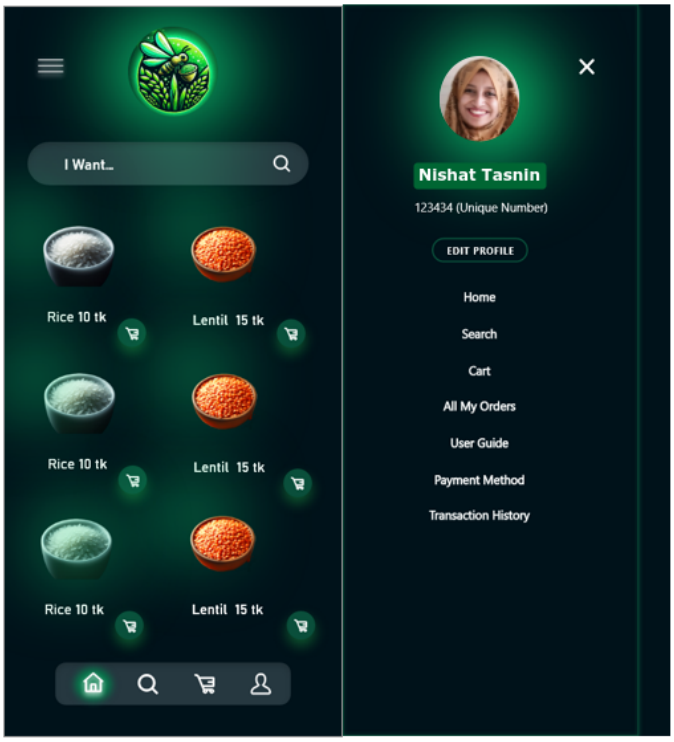

Fig. 2. Visual representation of the front-end implementation of the home page, showcasing the user interface and experience for the application's users.

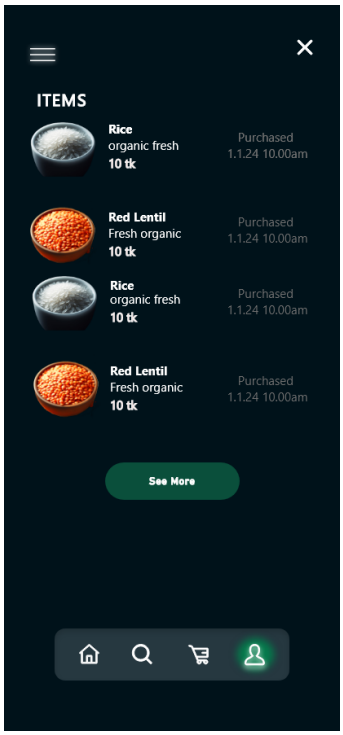

Fig. 3. This image presents the front-end implementation of the ordering mechanism and experience for the application's users.

benchmarking tool set. We tested the network with various workloads to measure throughput and resource utin the processlization, enabling us to evaluate the performance and scalability of the blockchain network.

Backend: We developed a backend system using Go and the Gin web framework to handle API requests, maintaining effective communication between the blockchain network and the frontend system. We also used Protocol Buffers to create a platform-neutral, extensible, and serialized data structure to manage and serve the distributed ledger.

Frontend: To deliver a seamless and intuitive user experience, we leveraged Flutter, a Dart-based framework, to develop cross-platform applications for Android, iOS, and the web. As illustrated in Figure 2 and 3, our application's user interface is designed to be visually appealing, easy to navigate, and accessible to a wide range of users, ensuring a hassle-free experience for customers.

Machine Translation: To accommodate blind or visually impaired users and those who are illiterate, we integrated SeamlessM4T v2, a multilingual multimodal machine translation model, to support speech-to-text, text-to-speech, and automatic speech recognition.

Post Quantum Secured MSP: Implementation of Post-Quantum Secured MSP using Dilithium-2 algorithm from CIRCL for secure certificate issuance, validation, and user authentication against classical and quantum computers.

HSM: To enhance the security of the ration distribution system, we integrated the PICO-HSM hardware security module and implemented the PKCS11 standard to facilitate communication with the HSM, enabling secure key storage and cryptographic operations.

V. Result and Discussion

In our proposed architecture, we conducted a comparative analysis with existing blockchain systems, including Ethereum, Corda, and Quorum, to evaluate their scalability in terms of throughput and latency as the number of peers increases. The results, illustrated in Fig. 4 (marked as A and B), demonstrate that our proposed system achieves a significant performance advantage. Initially, our system processes approximately 3000 transactions per second (TPS) with 5 peers, which is 50% higher than Quorum's initial 2000 TPS and 17.6 times higher than Corda's initial 170 TPS. Moreover, our system maintains a higher throughput as the number of peers increases, scaling down to 150 TPS with 50 peers. In contrast, Quorum's throughput decreases by 50% to 1000 TPS, while Corda's decreases by 23.5% to 130 TPS. Ethereum performs the worst, with an initial throughput of 30 TPS that decreases by 33.3% to 20 TPS. Overall, our proposed system outperforms the existing blockchain systems, achieving a 5-20 times higher throughput and demonstrating its potential for large-scale deployment.

In terms of latency, our proposed system also outperforms the other blockchain systems, as shown in the bar chart. Notably, Ethereum exhibits the worst performance, with a latency of 14,000 ms (milliseconds) for 5 peers and 17,000 ms for 50 peers. In contrast, our proposed architecture achieves a latency of 170 ms to 500 ms, which is 98.8% lower than Ethereum's latency for 5 peers and 97.1% lower for 50 peers. Corda and Quorum have similar latencies, ranging from 500 ms to 700 ms and 400 ms to 600 ms, respectively. However, our proposed system still outperforms them, with a latency that is 66% to 83% lower than Corda's and 57% to 75% lower than Quorum's.

These results demonstrate that our proposed architecture is more scalable and efficient in handling an increasing number of peers compared to Ethereum, Corda, and Quorum. Our system's superior performance in terms of both throughput and latency highlights its potential for large-scale deployment and real-world applications.

VI. Security analysis

- **Denial of Service (DoS) Attacks:** Our system only allowed for member to access and continuously monitors performance (throughput, latency) with automated alerts to counter DoS attacks and maintain network stability.
- **Consensus Manipulation:** Raft consensus with logging, anomaly detection, and ordering service redundancy safeguards against consensus manipulation, ensuring network integrity.
- **MSP Compromise:** Robust key management (secure generation, storage, rotation) and Hardware Security Modules (HSMs) safeguard against compromised MSPs, preventing unauthorized access and identity spoofing.
- **Chaincode Exploitation:** Secure development lifecycle (SDLC) with static/dynamic analysis, along with regular audits and penetration testing, fortifies our Chain-code against vulnerabilities.
- **Sybil Attacks:** Sybil attacks (single adversary, fake identities) are mitigated by our system's robust identity management (MSP) and strict peer node authentication. Additionally, Raft consensus limits individual node influence, further reducing this risk.
- **Data Privacy:** Our system safeguards data privacy with encryption (at rest & in transit), access controls (MSPs), and regular audits to ensure compliance with privacy regulations.

VII. Conclustion

In conclusion, this research presents GrainBee, a blockchain-powered ration distribution system, which offers a novel solution to the challenges of food distribution in developing countries. GrainBee introduces a post-quantum secure, blockchain-based approach that utilizes a distributed immutable ledger to uphold integrity and mitigate corruption and fraudulent invoicing. The system also incorporates a user-friendly interface, machine translation services, Post Quantum Secured MSP, and Hardware Security Modules (HSM) to improve security, usability, and ensure swift and robust distribution. Notably, our proposed architecture significantly outperforms Ethereum, Corda, and Quorum in both throughput and latency as the number of peers increases. It achieves a 50% higher initial throughput than Quorum and 17.6 times higher than Corda, maintaining a throughput 5-20 times higher with 50 peers. Additionally, our architecture exhibits a latency that is 97.1%-98.8% lower than Ethereum's and 57%-83% lower than Corda's and Quorum's. These results highlight the system's superior scalability and efficiency, making it ideal for large-scale deployment and real-world applications. making it well-suited for high-performance distribution networks. The research demonstrates that blockchain technology has the potential to revolutionize the food distribution network, making it more efficient, reliable, and accessible while ensuring the privacy and security of beneficiaries. In terms of future work, further research can be done to explore the scalability and adaptability of GrainBee, as well as its potential integration with other emerging technologies, such as the Internet of Things (IoT), distribution-based sharding, and multi-party computation.

References

[1] W. H. Organization *et al.*, *The state of food security and nutrition in the world 2022: Repurposing food and agricultural policies to make healthy diets more affordable*. Food & Agriculture Org., 2022, vol. 2022.

[2] B. Rowland, K. Mayes, B. Faitak, R. M. Stephens, C. R. Long, and P. A. McElfish, "Improving health while alleviating hunger: best practices of a successful hunger relief organization," *Current developments in nutrition*, vol. 2, no. 9, p. nzy057, 2018.

[3] H. Mohajan, "Food and nutrition of bangladesh," *Peak Journal of Food Science and Technology*, 2013.

[4] W. Bank, "Food security update," 2024, accessed: 2024-07-10. [Online]. Available: https://www.worldbank.org/en/topic/agriculture/brief/food-security-update

[5] I. S. of Supreme Audit Institutions (ISSIA), "Issai - 5530 - adapting audit procedures to take account of the increased risk of fraud and corruption in the emergency phase following a disaster," 2019, accessed: 2024-07-10. [Online]. Available: https://www.issai.org/wp-content/uploads/2019/08/issai-5530-e.pdf

[6] S. Roy, "TCB Oil found under Trader's bed in Rangpur — Dhaka Tribune," 2020, the edible oil were to be sold at a higher price in the upcoming Ramadan. [Online]. Available: https://archive.dhakatribune.com/bangladesh/nation/2020/04/16/tcb-oil-found-under-trader-s-bed-in-rangpur

[7] I. Surjandari, H. Yusuf, E. Laoh, and R. Maulida, "Designing a permissioned blockchain network for the halal industry using hyperledger fabric with multiple channels and the raft consensus mechanism," *Journal of Big Data*, vol. 8, pp. 1–16, 2021.

[8] S. A. Joni, R. Rahat, N. Tasnin, P. Ghose, and L. Gaur, "Hac-bchain: A secure and scalable blockchain-shard based e-voting system," in *2023 IEEE Technology & Engineering Management Conference-Asia Pacific (TEMSCON-ASPAC)*. IEEE, 2023, pp. 1–6.

[9] L. Foschini, A. Gavagna, G. Martuscelli, and R. Montanari, "Hyperledger fabric blockchain: Chaincode performance analysis," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, 2020, pp. 1–6.

[10] C. Curino, D. E. Difallah, C. Douglas, S. Krishnan, R. Ramakrishnan, and S. Rao, "Reservation-based scheduling: If you're late don't blame us!" in *Proceedings of the ACM Symposium on Cloud Computing*, 2014, pp. 1–14.

[11] L. Barrault, Y.-A. Chung, M. C. Meglioli, D. Dale, N. Dong, P.-A. Duquenne, H. Elsahar, H. Gong, K. Heffernan, J. Hoffman *et al.*, "Seamlessm4t-massively multilingual & multimodal machine translation," *arXiv preprint arXiv:2308.11596*, 2023.

[12] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, "Blockchain-based agri-food supply chain: A complete solution," *Ieee Access*, vol. 8, pp. 69 230–69 243, 2020.

[13] P. Thakare, N. Dighore, A. Chopkar, A. Chauhan, D. Bhagat, and M. Tote, "Implementation of block chain technology in public distribution system," in *International Conference on Hybrid Intelligent Systems*. Springer, 2019, pp. 210–219.

[14] C. Devi Parameswari and V. Mandadi, "Public distribution system based on blockchain using solidity," in *Innovative Data Communication Technologies and Application: Proceedings of ICIDCA 2020*. Springer, 2021, pp. 175–183.

[15] G. Baralla, S. Ibba, M. Marchesi, R. Tonelli, and S. Missineo, "A blockchain based system to ensure transparency and reliability in food supply chain," in *Euro-Par 2018: Parallel Processing Workshops: Euro-Par 2018 International Workshops, Turin, Italy, August 27-28, 2018, Revised Selected Papers 24*. Springer, 2019, pp. 379–391.

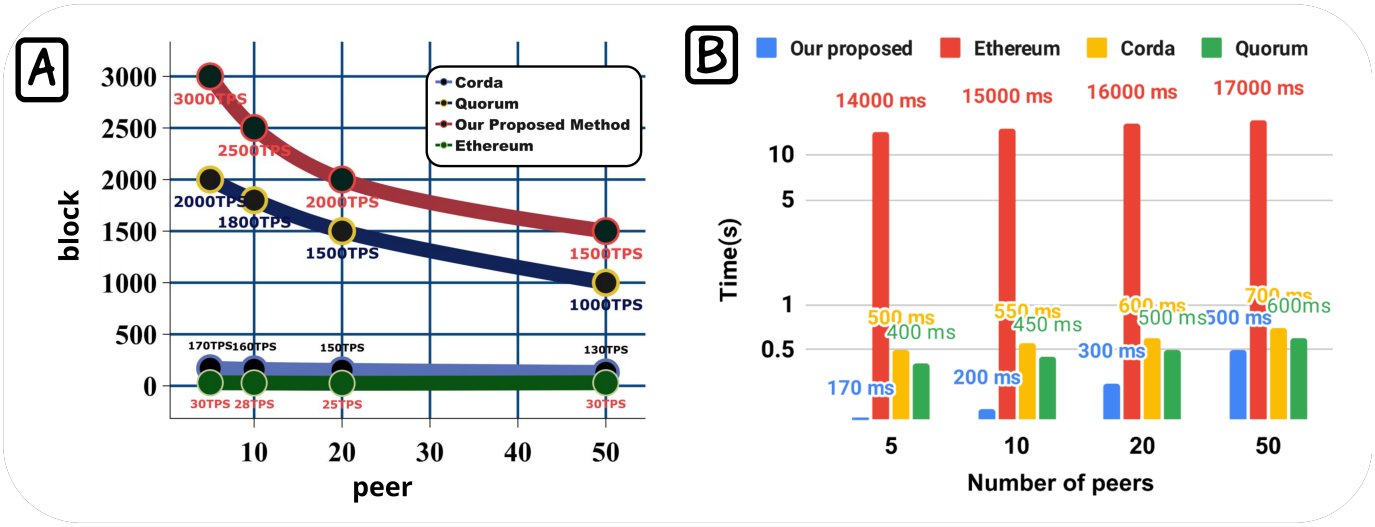

Fig. 4. The diagram illustrates how various participants (customers, sellers, government agencies, etc.) and system components (security system, event bus, blockchain, payment gateway, etc.) interact with the proposed ration distribution system through APIs provided for SDKs, tokens, wallets, and mobile apps.

[16] D. Malathi, V. Ponnusamy, S. Saravanan, D. Deepa, and T. A. Ahanger, "A design framework for smart ration shop using blockchain and iot technologies." *Intelligent Automation & Soft Computing*, vol. 32, no. 1, 2022.

[17] H. Mishra and P. Maheshwari, "Blockchain in indian public distribution system: a conceptual framework to prevent leakage of the supplies and its enablers and disablers," *Journal of Global Operations and Strategic Sourcing*, vol. 14, no. 2, pp. 312–335, 2021.

[18] R. S. Pawar, S. A. Sonje, and S. Shukla, "Food subsidy distribution system through blockchain technology: a value focused thinking approach for prototype development," *Information Technology for Development*, vol. 27, no. 3, pp. 470–498, 2021.

[19] S. Dhanake, S. Desale, P. Pawar, G. Patil, and S. Shende, "Blockchain technology in public ration distribution," *Int Res J Eng Technol*, vol. 8, no. 3, pp. 732–736, 2021.

[20] D. Nuševa, K. Leković, S. Vučenović, R. Marić, D. Marić, and G. Vukmirović, "The impact of digitalization on sustainable food supply chain management," in *International Scientific Conference Strategic Management and Decision Support Systems in Strategic Management*, 2024, pp. 198–206.

[21] H. Wu, S. Jiang, and J. Cao, "High-efficiency blockchain-based supply chain traceability," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 4, pp. 3748–3758, 2023.