Proceedings of the 19th Conference on Computer Science and Intelligence Systems (FedCSIS) pp. 169–176
DOI: 10.15439/2024F5274
ISSN 2300-5963 ACSIS, Vol. 39

A Blockchain-based Transaction Verification Infrastructure in Public Transportation

Hidayet Burak Saritas[1 2]
0000-0002-0425-3051
[1] Ege University International Computer Institute,
[2] Ege Teknopark, Ege University
Erzene Mah., Ankara Cad.,
35100 Bornova - Izmir, Türkiye
Email: burak.saritas@kentkart.com

Geylani Kardas
0000-0001-6975-305X
Ege University International Computer Institute,
35100, Bornova – Izmir, Türkiye
Email: geylani.kardas@ege.edu.tr

***Abstract*—This paper proposes a new blockchain-based transaction verification infrastructure for co-payment and data verification for multi-modal public transportation systems. Our solution offers a decentralized platform that ensures secure co-payments and data integrity while addressing interoperability, data security and transactional transparency. With a private blockchain, transportation providers act as nodes and validated, consensus-approved transactions increase trust and transparency. A standardized data format and robust algorithms for data contribution by transport operators are developed as well as a model for operators, assets, and transactions. Including zero-knowledge proofs improves user privacy by allowing secure authentication without revealing sensitive data. We believe that this research may lead a closer collaboration between public transport operators and provide an enhanced user experience while enabling transport transaction security and data verification.**

***Index Terms*—Blockchain Technology, Public Transportation, Co-payment Systems, Data Verification, Interoperability, Transaction Security, Decentralized Networks, Zero-Knowledge Proofs, Standardized Data Format, Privacy Preservation.**

I. Introduction

With advancements in technology, the public transportation sector is expanding and offering a variety of options to a wider audience. In addition to the traditional methods, new alternatives like shared vehicles, scooters, and app-controlled taxis are becoming more popular [1]. Regulations in this field set limits to prevent unfair competition and encourage cooperation. Mobility partners have the freedom to make their own decisions. Various public transport providers need to work together on a common platform to manage this diversity and deliver an enhanced user experience. This can improve users' transportation experiences and reduce private vehicle usage. However, actors who offer different transportation methods have their own ticketing solutions. This may pose a significant challenge in the development process of a unified platform. These actors include ABT Kentkart [2], STIB-MIVB [3], MVV [4], and Whim [5]. Users need to adapt to various ticketing solutions, and each actor needs to offer features such as payment, personalization, and usability [6] [7]. Therefore, creating a unified and accessible platform within the public transportation ecosystem is considered a significant innovation and challenge for the sector [8].

It is not easy to combine different actors of the public transportation industry. But it can be made simpler and also efficient with following solutions like a single application, account management and a single card. To combine services and share profits, researchers are constantly exploring easy integration methods to create a common language that all transportation solution providers can use. They are also working to establish a method for verifying every user transaction [8]. To solve these problems, this study proposes developing a blockchain-based solution that processes and verifies data produced by different transportation actors. Blockchain is a ledger built from computers in a distributed structure that cannot be controlled by any central authority. [9]. In essence, Distributed Ledger Technology (DLT) is a type of encrypted database that is distributed, shared, and serves as an irreversible and incorruptible information store [10]. It enables trust in transactions between two parties and eliminates the need for a central intermediary to provide this service. This allows for the secure transfer of unique assets, such as money, title deeds, and identification information, without intermediaries. Two users can conduct a financial transaction without the need for an intermediary institution [11]. They can communicate directly without any trust issues [12]. The paper aims to solve integration problems in the public transportation sector by enabling different operators and businesses to work together more effectively and reliably. It examines how blockchain technology's decentralized and reliable structure can increase transaction transparency and security in the sector.

The standard message package format was developed on a private blockchain network. This format creates an environment where transportation operators can add data. The study considered parameters such as speed and assets that validating operators must have. This way, different operators in the public transportation sector can use blockchain technology to in-

Special acknowledgment is due to Kentkart A.Ş. Company for their generous support and guidance during the preparation of this paper.

tegrate with each other, trust each other, and query all transactions created with standard message format. Creating a trustworthy environment is crucial for this work. This can be achieved through a consensus mechanism and blockchain structure to confirm transactions. All businesses can join the blockchain network as validators, and data produced by any business can be added to the network after being approved by all nodes. The data added to the network in standard message format is trusted by everyone. To achieve this, a common data format and extensible approval mechanism have been created for the public transportation sector.

The rest of the paper is organized as follows: Section 2 reviews related work on blockchain applications in similar transportation sectors. In Section 3, we introduce the foundational elements and components of a blockchain environment optimized for public transportation. This section covers the architecture, roles, and interactions of transactions, as well as detailed descriptions of nodes, assets, and standardized message formats. In Section 4, we look at how to use decentralized technologies to keep people's information safe in public transportation. These technologies let people manage their digital identities without revealing sensitive information, which helps enhance people's privacy. We also look at how these technologies can be used with a single blockchain-based transaction verification system to verify user credentials. In Section 5, we summarize the contributions and implications of our blockchain-based infrastructure tailored for the public transportation sector.

II. Related Work

Some notable research has been done on using blockchain for public transportation. Jayalath et al. [13] propose a micro-transaction model based on blockchain to improve service in Sri Lanka's public transportation sector. They focus on a ticketing system using an Ethereum-based blockchain to reduce transaction fees and improve service quality. This approach creates QR-based tickets for users to make micro-payments without third-party intermediaries. It reduces transaction costs.

Wang et al. [14] introduce "InterTrust," an interoperable blockchain architecture to enhance interoperability and reliability across various blockchain systems. The InterTrust model is for communication and interoperability among existing blockchain systems, which is a broader scope. However, our study aims at providing a specialized blockchain network for the public transportation domain.

Yang et al. [15] suggest a blockchain and Edge Computing-based communication system for maritime transportation. Their work uses blockchain and Edge Computing to improve Internet of Things (IoT) device performance and security in maritime environments. This is different from our work, which focuses on public transportation.

Enescu et al. [16] discuss a blockchain application to promote ecological transportation and reduce traffic congestion. They imagine a system where blockchain records transactions and gives users digital currencies, which helps the environment and makes public transportation more popular.

Jabbar et al. [17] review blockchain applications in Intelligent Transportation Systems (ITS). They show how blockchain can improve transactional trust and efficiency. This supports various functionalities including automatic parking and fee payments.

Lastly, Chen et al. [18] describe a "Full-Spectrum Blockchain as a Service" (FSBaaS) approach with "Blockchain Lite" and "Hyperledger Fabric," focusing on providing blockchain services that cater to both centralized and decentralized frameworks. This study shows the flexibility needed in blockchain adoption.

Our study is different from the above mentioned noteworthy efforts because it suggests a way for public transport operators to trust each other. Each operator can check and verify data transactions without needing to ask anyone else. This makes sure that data is correct and that messages are the same across the network. It also makes easier to work together without having to rely on one person. Additionally, this study improves privacy and security in public transportation systems by using Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and Zero Knowledge Proofs (ZKPs) explained in later sections. It supports user privacy by authenticating users and transactions without exposing sensitive personal information. This approach not only secures digital identities and transactions but also sets a standard for using privacy-preserving technologies in public infrastructure. The proposed infrastructure helps advance blockchain technology and meets the needs of public transportation.

III. Defining Blockchain Model Elements And Basic Components

In this section, we introduce the main model elements and basic components of a blockchain-based transaction verification environment for public transportation.

A. High-Level Environment of Model Elements

In this study, we chose the Hyperledger Fabric blockchain environment and used the Raft consensus algorithm to establish a private blockchain environment. Hyperledger Fabric provides enhanced both control over transactions and privacy options. It allows for the creation of private channels, which limit visibility of specific transactions and data to certain network participants [19] [20]. Raft is known for efficiently handling high transaction volumes with low latency times [21]. This makes it ideal for verifying public transportation operations.

Figure 1 depicts the model elements operating in the high-level environment. These elements are defined as follows:

***Transaction**:* Represents actions such as buying tickets or making payments, performed across various transportation modes including buses, cars, and scooters.

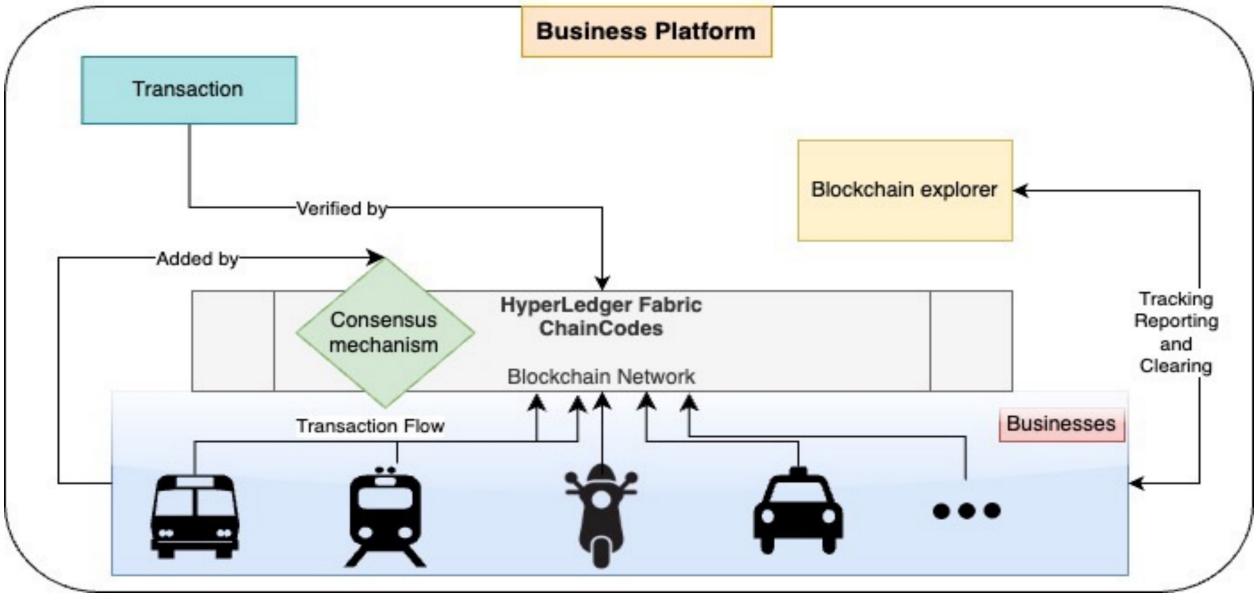

Fig. 1. High-Level System Design

Consensus Mechanism: Nodes (businesses) on the network verify transaction accuracy through a consensus mechanism [22]. This ensures that transactions are valid and their integrity is confirmed before being added to the blockchain.

Hyperledger Fabric Smart Contracts (Chaincodes): Transactions are processed using specific rules or smart contracts [19]. These smart contracts are utilized to automate, verify, and implement transaction logic.

Blockchain Network: Transactions take place and are recorded on the Hyperledger Fabric blockchain network.

Blockchain Explorer (Record Control Tool): An instrument utilized for visualizing and querying transactions, blocks, and other relevant data on the network. Users can track and report blockchain transactions with the help of this tool.

Businesses: Various enterprises serve as connected nodes on the network and participate in blockchain transactions.

The diagram in Figure 2 shows the defined classes for the fundamental components of the blockchain-based transaction verification system. The diagram demonstrates how a blockchain network is structured and how different components interact with each other. For example, a transaction executed by a node can trigger a smart contract, resulting in the addition of a block to the blockchain. The consensus mechanism verifies all processes and communicates using different data formats and messaging protocols. This plays a crucial role in maintaining the security and integrity of the blockchain network.

The “Node” class represents businesses and interacts with “SmartContract” and “Transaction”. The “Blockchain” and “Block” classes display the structural features of the blockchain, while the “ConsensusMechanism” details how the nodes on the network reach a consensus. Additionally, the “DataFormat” and “MessagingProtocol” classes represent the data formats and communication protocols within the blockchain-based infrastructure.

B. Definitions and Contents of Model Elements

This section describes the model elements and their roles that form the basis of a private blockchain environment customized for public transportation. The structures used clearly demonstrate how nodes, entities, and transactions on the blockchain are identified, processed, verified, and integrated into the public transportation system. Examples and scenarios are provided to concretize the use of the standard message format in practice.

Nodes (Businesses): Each node in the blockchain network represents a business. Businesses manage various transportation services, such as buses, trams, and scooters, and have the authority to control and approve transactions on the network. Businesses act as 'nodes' to carry out their transactions and verify those of other businesses. They also contribute to the consensus mechanism to maintain the network's integrity and security.

Incorporating nodes into the network involves authentication and authorization processes using the Trusted Platform Module (TPM) [23]. The TPM is a hardware-based security module that provides node authentication. Each operating node contains a TPM chip. TPM securely generates and stores the node's private keys. The TPM module is activated by the business during installation and the first key pair is generated. TPM securely manages business identity and other cryptographic operations.

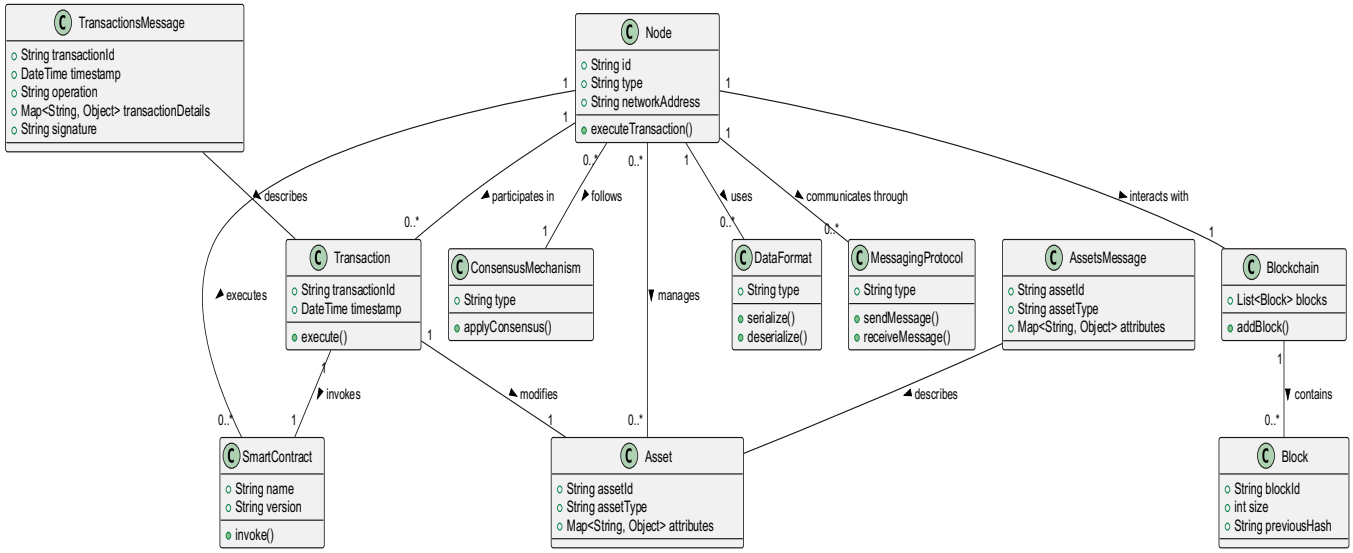

Fig. 2. Interactions between Components of Blockchain-based Transaction Verification System

Assets: Assets represent physical or digital items such as tickets, memberships, or payment records. For example, a ticket sales transaction creates an asset, while a boarding transaction represents the use of a ticket asset. An asset can be any item defined on the blockchain. Each entity has its own attributes, such as those given in the Table I defining the attributes of the Assets model element.

Each asset has an Asset ID and Asset Type, along with other predefined or optional attributes. Additional attributes may include time information, journey details, or any definition attributes necessary for verifying operations.

An extensible JSON structure for how assets are represented and used on the blockchain can be designed as shown in Listing 1. The initial design includes mandatory fields, and new fields can be added as needed.

TABLE I.
MESSAGE STRUCTURE OF ASSETS MODEL ELEMENT

Attribute Name	Attribute Detail
Asset ID (assetId)	Each asset has a unique identifier
Asset Type (assetType)	The category into which the asset is classified (for example, ‘ticket’, ‘membership’)
Other Attributes	Other information that defines the properties of the asset (for example, validity period, price)

Transactions: Transactions are defined as actions that create a change in the state of assets. Transaction types can include creating, updating, and deleting assets. Attributes of the Transactions model element are defined in Table II.

Transactions record all movements that users and businesses make on the network. Every transaction must be verified by other nodes in the network. Any unique transaction must contain the Transaction ID, which is a unique identifier, the timestamp of the transaction, and the type of transaction.

With the transaction examples given in Listing 2, it can be explained in detail how a transaction is initiated, how it progresses on the network and how it is concluded. For example, scenarios such as purchasing a ticket and boarding can be handled this way.

Listing 1. Message Structure of Assets Model Element

```
{
  "assetId": "123456",
  "assetType": "ticket",
  "attributes": {
    "issueDate": "2024-05-05 12:00:00",
    "expiryDate": "2024-06-05 12:00:00",
    "passengerId": "21412",
    "journeyDetails": {
      "origin": "Station A",
      "destination": "Station B",
      "departureTime": "2024-05-05 15:00:00"
    }
  }
}
```

TABLE II.
MESSAGE STRUCTURE OF TRANSACTIONS MODEL ELEMENT

Attribute Name	Attribute Detail
Transaction ID (transactionId)	Each transaction has a unique identifier
Timestamp	Indicates the time when the transaction took place
Operation Type	Indicates what type of action the operation is (for example, 'create', 'update', 'delete')

Listing 2. Message Structure of Transactions Model Element

```
{
    "transactionId": "tx123456789",
    "timestamp": "2024-05-05 12:00:00",
    "operation": "create",
   "transactionDetails": {
      "assetId": "123456",
      "assetType": "ticket",
  "attributes": {
        // Detailed information about the asset
  }
 },
    "signature": "DigitalSignatureOfTheUser"
}
```

Examples of transaction-specific data (payload) to be added to the message for different transactions in the standard message format to be sent over the network are given below. Listing 3 shows the ticket creation process, Listing 4 shows the membership update process, and Listing 5 shows sample "payload" information for fee payment. These payload samples represent the information required for various public transport operations and can be customized according to the needs of the transaction. Payload content may vary depending on the transaction type and the characteristics of the asset being processed.

C. Standardized General Message Format

It is necessary to determine a general message format to use all the message contents that we defined specifically for assets and transactions in the previous headings on the network. In this way, messages sent on the network can be standardized by using a common message format to produce transaction-specific data. Sample JSON structure and descriptions for the standard message format that can be used among all models in public transportation is defined as in Listing 6.

Listing 3. Payload of Ticket Creation Process

```
"payload": {
    "ticketNumber": "1234567890",
    "issueDate": "2024-01-01 10:00:00",
    "expiryDate": "2024-01-02 10:00:00",
    "passengerName": "Hakan Demir",
  "journeyDetails": {
      "origin": "Station A",
      "destination": "Station B",
      "departureTime": "2024-01-01
11:00:00"
  }
}
```

Listing 4. Payload of Membership Update Process

```
"payload": {
    "membershipId": "MEMB1234567",
    "memberName": "Hakan Demir",
    "validFrom": "2024-01-01",
    "validTo": "2024-01-01",
    "membershipType": "Gold",
    "additionalBenefits": ["Extra
Luggage", "Priority Boarding"]
}
```

Listing 5. Payload of Fee Payment

```
"payload": {
    "fareId": "FARE12345",
    "amountPaid": "15.00",
    "currency": "USD",
    "paymentMethod": "Credit Card",
    "transactionDate": "2024-01-01
12:30:00",
    "serviceType": "Tram"
}
```

This format is designed to encapsulate all necessary details for executing and verifying transactions, such as payments or asset transfers. It standardizes data for all parties involved in the transaction and maintains the system's integrity and reliability. Moreover, it supports various transportation modes and is versatile in different scenarios. The message's key components are the transaction type, transaction ID, timestamp, and invoked by, as well as transportation details. This part of the transportation message contains information about the mode of transport and route, including membership details for discounts or special fares.

Additionally, digital signature and consensus details are also present in general message format. Digital signature is used to authenticate the user's identity. The transaction's endorsing nodes, namely information, consensus timestamp, and consensus algorithm used are provided in the consensus detail part. Digital signatures and consensus details are pivotal for security, allowing for authenticated and verified transactions on the blockchain.

Listing 6. Standardized General Message Format

```
{
"transactionType":
"PaymentorAssetTransfer",
    "transactionId": "UniqueTransactionID",
    "timestamp": "2024-01-01 12:00:00",
    "invokedBy": "UserIDorBusinessID",
  "transportationDetails": {
       "modeOfTransport":
"bus/tram/scooter/minibus/metro",
       "routeId": "RouteID",
       "startLocation": "StartingLocation",
       "endLocation": "EndLocation",
    "fare": {
          "amount": "Amount",
          "currency": "Currency"
    },
    "membershipDetails": {
          "membershipId": "MembershipID",
          "validity": "MembershipValidity"
    }
  },
  "transactionDetails": {
       "assetId": "AssetID",
       "assetType": "AssetType",
       "operation": "create/update/delete",
    "payload": {
          // Customized data fields
     "journeyDetails": {
             "origin": "Station A",
             "destination": "Station B",
       "departureTime": "2024-05-05 15:00:00"
     },
     "fareDetails": {},
     "seatAllocation": {},
    }
  },
    "signature": "DigitalSignatureOfTheUser",
  "consensusDetails": {
       "endorsedBy": ["NodeID1",
"NodeID2"],
       "consensusTimestamp": "2024-01-01
12:00:10",
       "consensusAlgorithm":
"ConsensusAlgorithmUsed"
  }
}
```

IV. Enhancing User Privacy In Public Transportation Through Decentralized Technologies

This section explains how decentralized technologies can help protect user privacy in public transportation. It also looks at the challenges in digital systems that affect personal data security and how blockchain technology can help protect user privacy. This study looks at how these technologies can be used to improve privacy in public transportation.

A. Privacy Challenges in the Digital Era

In today's world, it is crucial to securely store and process personal data due to the significant impact of social media and digitalization. Despite existing laws and regulations to protect user data, data breaches still occur, highlighting significant vulnerabilities. Storing personal data on company or institution servers is often the main cause of security breaches [24]. This is because central storage of personal data can be vulnerable to attacks and single point of failure can make it susceptible to cyber-attacks and unauthorized access. Personal data must be stored securely, and access should be restricted to authorized personnel only.

B. Emerging Solutions for Data Protection

To tackle the challenges addressed in Sect. IV.A, innovative technologies have been developed. These include the Decentralized Identifiers (DID) protocol [25], Verifiable Credentials (VC) [26], and Zero Knowledge Proof (ZKP) [27]. These technologies promote secure and digital storage of user data on individuals' devices, departing from traditional centralized systems. The DID protocol enables users to create and manage their digital identities without relying on central authorities. Verifiable Credentials enhance the dependability of digital identities and claims presented by users. They only include necessary data for a transaction. ZKP enables mathematical verification of information while maintaining privacy by not revealing personal details.

C. Application in Public Transportation Systems

A unified infrastructure allows users to securely access various public transportation services. The proposed study is different from conventional systems because users do not have to repeatedly share sensitive personal information with each service provider. Instead, it uses Verifiable Credentials stored in digital wallets, backed by the DID protocol. The claim information is stored in a data structure called the Sparse Merkle Tree [28]. This ensures data integrity by updating the root hash value, which is critical for verifying proofs. The root hash value is stored immutably on the blockchain.

D. Implementing a Privacy-Centric Approach

Users prove their eligibility to service providers by presenting ZKP-generated proofs alongside their credential information. These proofs can demonstrate eligibility as a student, teacher, elderly person, or person with a disability. Personal information is not required to be disclosed. Service providers verify these claims by referencing the proof and the root hash value on the blockchain. This model promotes a secure environment that minimizes personal data exposure and prioritizes privacy. Figure 3 shows how users can manage their digital identities securely and provide verification to service providers without revealing personal information. This is done by using technologies such as DID, VC, ZKP, and blockchain.

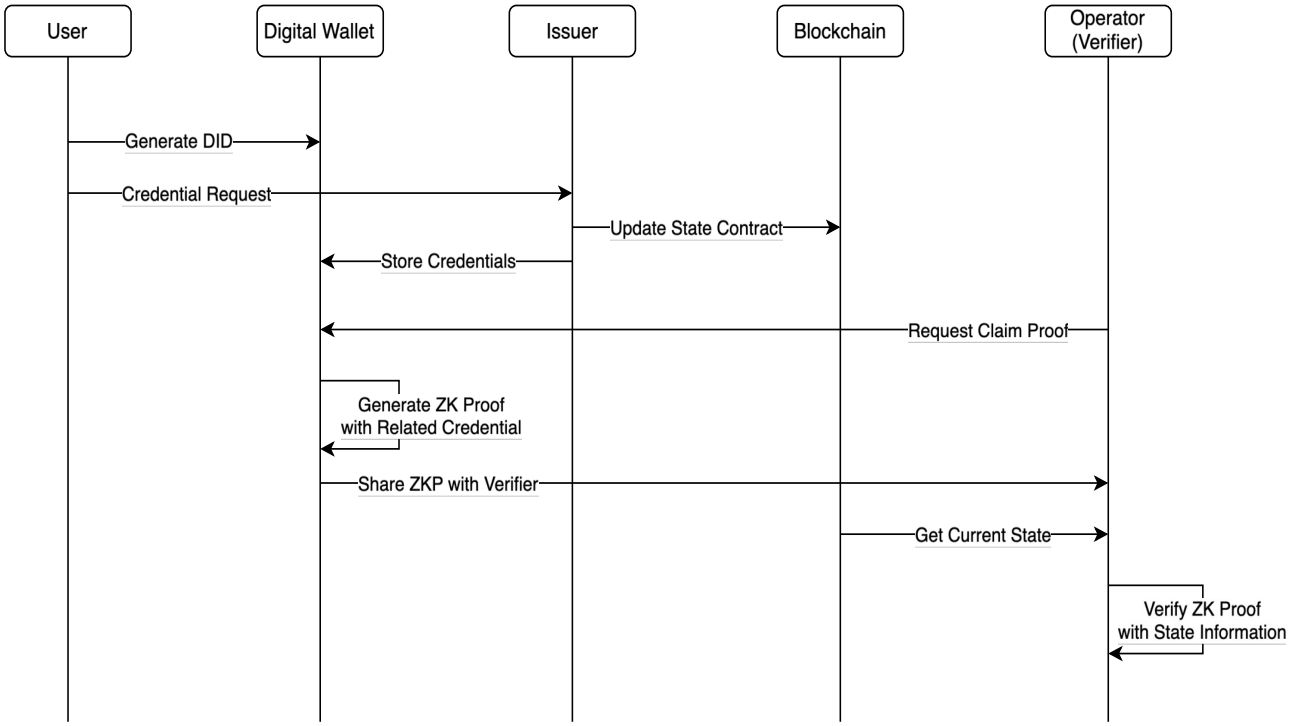

Fig. 3. User Privacy Protection in a Blockchain-Enabled Public Transportation System

Figure 3 shows how data and interactions flow between users, their digital wallets, issuers, the blockchain, and operators (verifiers) in a blockchain-based public transportation system. The system is designed to protect user privacy, and the user initiates the process by creating a Decentralized Identifier (DID) in their digital wallet. The issuer updates the relevant state contract on the blockchain and returns the approved credentials to the user's digital wallet for storage after requesting credentials.

The user's digital wallet generates a Zero-Knowledge Proof (ZKP) for the credential and shares it with the verifier, who is typically a transportation operator. The operator requests proof of claim and retrieves the current state from the blockchain to validate the transaction. The operator checks the ZKP using the state information from the blockchain. This process confirms the user's claim without compromising their privacy.

The verification flow ensures that the user's sensitive data remains secure. The Zero Knowledge Proof (ZKP) enables the user to demonstrate ownership of a valid credential without disclosing the credential itself. This use case shows how privacy-enhancing technologies can be used in public transportation systems. It utilizes blockchain technology to securely manage identities and verify transactions in a decentralized manner.

E. Outlook for Privacy Enhancement

The adoption of DID, VC, and ZKP represents a significant change in personal data protection and privacy enhancement. It is a positive development for the protection of personal data and privacy. Service providers can conduct necessary verifications without compromising privacy, while users have greater control over their data. The study sets a new precedent for a digital ecosystem focused on security and user control [29].

V. Conclusion

A blockchain-based infrastructure for co-payment and data verification in the public transportation sector is presented in the paper. Our solution addresses interoperability, data security, and transactional transparency through a private blockchain. Transportation providers are nodes in this architecture and confirm transactions by consensus.

We analyze guarantee and reward systems to encourage participation and compliance across the network. Proposed infrastructure may also lead to implement systems carefully to establish trust among stakeholders and foster collaboration across multiple transportation services.

Design and deployment of smart contract APIs for network nodes are also discussed in the paper. These APIs are essential for running agreements autonomously, allowing fare settlements, service level agreements and more. They constitute the foundation of the system and enable smooth, scalable, and flexible services across the transportation network.

In addition, the paper addresses the strategic use of zero-knowledge proofs. This technology supports user privacy by authenticating users and transactions without revealing sensitive information. It meets today's digital privacy demands.

In conclusion, we believe that the proposed infrastructure is a significant step forward for public transport. It claims efficiency gains, enhanced security, and a user-centered approach. The system creates an environment for smart contract automation with advanced guarantee and reward mechanisms. This enables a seamless and secure public transportation experience. The presented research provides a roadmap for a harmonized, user-centric transportation network that respects privacy. This is especially relevant as urban mobility patterns change and require sophisticated solutions.

As the future work, we plan to develop and implement smart contracts for the public transportation system. These contracts will be tailored to the specific needs of the system. Additionally, the transaction verification mechanism will be operationalized within the blockchain environment. Transactions designed to guarantee user data confidentiality will be verifiable through the use of smart contracts.

REFERENCES

[1] G. Oeschger, P. Carroll, and B. Caulfield, "Micromobility and public transport integration: The current state of knowledge," *Transportation Research Part D: Transport and Environment*, 2020. https://doi.org/10.1016/j.trd.2020.102628.

[2] ABT Kentkart, "Automated fare collection system," Kentkart, 2022. https://www.kentkart.com/solutions/automated-fare-collection-system.

[3] STIB-MIVB, "Ticket information," STIB-MIVB Ticket, 2022. https://www.stib-mivb.be/article.html?l=en&_guid=80bb5be7-429c-3810-a795-dfe836d62585.

[4] MVV, "Online and handy ticket," MVV Ticketing, 2022. https://www.mvv-muenchen.de/en/tickets-and-fares/online-und-handyticket/index.html.

[5] MaaS Global, "Whim - All your journeys," Whim, 2022. https://whimapp.com.

[6] S. Kazi, M. Bagasrawala, F. Shaikh, and A. Sayyed, "Smart e-ticketing system for public transport bus," in *Proc. 2018 International Conference on Smart City and Emerging Technology (ICSCET)*, 2018, pp. 1-7. https://doi.org/10.1109/ICSCET.2018.8537302.

[7] T. Khedekar, V. Jamdar, S. Waghmare, and M. L. Dhore, "FID automatic bus ticketing system," in *Proc. 2021 International Conference on Artificial Intelligence and Machine Vision (AIMV)*, 2021, pp. 1-6. https://doi.org/10.1109/AIMV53313.2021.9670957.

[8] G. D. Pasquale, J. D. Bie, and J. Singh, "Ticketing in Mobility as a Service," International Association of Public Transport (UITP), 2022. https://cms.uitp.org/wp/wp-content/uploads/2022/07/Report-Ticketing-MaaS-JULY2022-web.pdf.

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Technical Report, 2008. https://bitcoin.org/bitcoin.pdf.

[10] H. Kakavand, N. Kost De Sevres, and B. Chilton, "The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies," *SSRN Electronic Journal*, 2016. https://papers .ssrn.com/sol3/papers.cfm?abstract_id=2849251.

[11] I. Nath, "Data exchange platform to fight insurance fraud on blockchain," in *Proc. 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)*, 2016, pp. 821–825.

[12] S. Gupta, S. Sinha, and B. Bhushan, "Emergence of blockchain technology: Fundamentals, working and its various implementations," *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*, 2020. http://dx.doi.org/10.2139/ssrn.3569577.

[13] S. A. Jayalath, C. Rajapakse, and J. M. D. Senanayake, "A microtransaction model based on blockchain technology to improve service levels in the public transport sector in Sri Lanka," in *Proc. 2020 International Research Conference on Smart Computing and Systems Engineering (SCSE)*, 2020, pp. 82-89. https://doi.org/10.1109/SCSE49731.2020.9313037.

[14] G. Wang and M. Nixon, "InterTrust: Towards an efficient blockchain interoperability architecture with trusted services," in *Proc. 2021 IEEE International Conference on Blockchain*, Melbourne, Australia, 2021, pp. 150-159. https://doi.org/10.1109/Blockchain53845.2021.00029.

[15] T. Yang, Z. Cui, A. H. Alshehri, M. Wang, K. Gao, and K. Yu, "Distributed maritime transport communication system with reliability and safety based on blockchain and edge computing," in *IEEE Transactions on Intelligent Transportation Systems*. https://doi.org/10.1109/TITS.2022.3157858.

[16] F. M. Enescu, N. Bizon, G. Serban, and I. C. Hoarcă, "Environmental protection - Blockchain solutions for intelligent passenger transportation of persons," in *Proc. 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2021, pp. 1-6. https://doi.org/10.1109/ECAI52376.2021.9515026.

[17] Y. Jabbar, E. Dhib, A. B. Saıd, M. Krichen, N. Fetais, E. Zaidan, and K. Barkaoui, "Blockchain technology for intelligent transportation systems: A systematic literature review," in *IEEE Access*, vol. 10, 2022, pp. 20995-21031. https://doi.org/10.1109/ACCESS.2022.3149958.

[18] Y. Chen, J. Gu, S. Chen, S. Huang, and X. S. Wang, "A full-spectrum blockchain-as-a-service for business collaboration," in *Proc. 2019 IEEE International Conference on Web Services (ICWS)*, 2019, pp. 219-223. https://doi.org/10.1109/ICWS.2019.00045.

[19] Hyperledger Foundation, "Hyperledger Fabric Documentation," 2023. https://hyperledger-fabric.readthedocs.io/.

[20] B. Reddy and P. S. Aithal, "Blockchain based service: A case study on IBM blockchain services & Hyperledger Fabric," *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, vol. 4, no. 1, May 2020, pp. 94-102. https://ssrn.com/abstract=3611876.

[21] D. Ongaro, "In search of an understandable consensus algorithm (Extended Version)," Stanford University, 2014. https://raft.github.io/raft.pdf.

[22] R. Awati, "Consensus algorithm," TechTarget. https://www. techtarget.com/whatis/definition/consensus-algorithm.

[23] Trusted Computing Group, "TPM Main Specification," Trusted Computing Group, 2019. https://trustedcomputinggroup.org/resource/tpm-library-specification/.

[24] Proceedings of the 17th Conference on Computer Science and Intelligence Systems, M. Ganzha, L. Maciaszek, M. Paprzycki, D. Ślęzak (eds). ACSIS, Vol. 30, pages 685–694 (2022)

[25] W3C, "Decentralized Identifiers (DIDs) v1.0," Jul. 19, 2022, W3C Recommendation. https://www.w3.org/TR/did-core/.

[26] W3C, "Verifiable Credentials Data Model v2.0," World Wide Web Consortium. https://www.w3.org/TR/vc-data-model/.

[27] Hyperledger Foundation, "Hyperledger AnonCreds: Anonymous Credentials with Zero-Knowledge Proofs," Hyperledger Wiki. https://wiki.hyperledger.org/display/anoncreds.

[28] F. Haider, "Compact Sparse Merkle Trees," Oct. 6, 2018. https://doi.org/10.31219/osf.io/8mcnh.

[29] A. Sherriff, K. Young, and M. Shea, "Editorial: Establishing Self Sovereign Identity with Blockchain," in *Front. Blockchain*, vol. 5, Art. no. 955868, Aug. 19, 2022. https://doi.org/10.3389/fbloc.2022.955868.