Research Article / Review Article FUPRE JOURNAL 9(2):68-83(2025)

FUPRE Journal

of

Scientific and Industrial Research

ISSN: 2579-1184(Print) ISSN: 2578-1129 (Online)

http://fupre.edu.ng/journal

Securing Ride-Sharing Platforms with Blockchain: Enhancing Privacy, Fraud Prevention, And Transaction Integrity Using Elliptic Curve Cryptography and Zero-Knowledge Proofs

MICHAEL, U. E.[1*], *AKO, R. E.*[2] *STAR, N. U.*[3]

[1]*Department of Computer Science, Federal University of Petroleum Resources, Effurun, Nigeria.*

ARTICLE INFO

Received: 12/03/2025
Accepted: 23/07/2025

Keywords

Blockchain, Cryptography, Decentralized systems, Elliptic Curve Cryptography, Ride-sharing security, Smart contracts, Zero-Knowledge Proofs

ABSTRACT

The increasing reliance on centralized ride-sharing platforms has led to significant security vulnerabilities, including data breaches, fraud, and identity theft. This study proposes a blockchain-based ride-sharing framework leveraging Elliptic Curve Cryptography (ECC) and Zero-Knowledge Proofs (ZKPs) to enhance security, privacy, and transparency. ECC is implemented for secure digital signatures and authentication, ensuring tamper-proof ride transactions with reduced computational overhead compared to traditional cryptographic methods. ZKPs enable anonymous identity verification, allowing users to authenticate themselves without revealing personal data, thereby mitigating identity fraud and unauthorized access. A comparative performance evaluation is conducted to assess the transaction speed, latency, scalability, and security resilience of the proposed blockchain-based system versus traditional centralized ride-sharing platforms. The findings reveal that while blockchain transactions experience slightly higher latency (1.5–2.3s) and lower scalability (900–1,050 TPS) than centralized systems, they exhibit superior security resilience, successfully blocking over 90% of cyberattacks. Matplotlib-generated performance charts over seven days of uptime illustrate blockchain's advantages in fraud prevention and transaction integrity, despite its current scalability challenges. The study also provides a detailed mathematical breakdown of ECC and ZKPs, demonstrating their implementation in ride-sharing identity verification and secure fare processing. The results suggest that future ride-sharing architectures should incorporate hybrid blockchain models to balance scalability and decentralization. The proposed framework contributes to the advancement of secure, privacy-preserving, and fraud-resistant decentralized transportation systems, paving the way for real-world deployment and industry adoption.

1. INTRODUCTION

Ride-sharing services have revolutionized transportation by offering cost-effective, convenient, and efficient urban mobility solutions (Kanza and Safra, 2018). However, centralized ride-sharing platforms, such as Uber and Lyft, face significant security vulnerabilities, including data privacy breaches, unauthorized access to user information, and fraud (Hassija et al., 2019). These issues undermine trust among users and create substantial risks for both passengers and drivers (Namasudra and Sharma, 2022). One of the primary concerns in centralized ride-sharing platforms is the risk of data breaches. Sensitive user information, such as trip history, payment

*Corresponding author, e-mail:ako.rita@fupre.edu.ng
DIO

details, and personal identification, is often stored in centralized databases, making them attractive targets for cybercriminals (Hassija et al., 2019). Moreover, centralized control allows ride-sharing companies to collect and monetize user data, raising ethical concerns regarding privacy violations (Baza et al., 2020). Fraudulent activities, such as fake driver profiles, ride fare manipulation, and unauthorized third-party access, further exacerbate security concerns (Li et al., 2020). Existing identity verification mechanisms in centralized ride-sharing platforms often fail to prevent impersonation and unauthorized use of driver accounts (Khanji and Assaf, 2019). Consequently, the lack of transparency in ride-sharing operations fosters distrust among users and exposes them to potential security threats (Zhang et al., 2019). Blockchain technology presents a promising solution to the security challenges of ride-sharing systems by introducing decentralized, immutable, and transparent transaction mechanisms. Blockchain-based ride-sharing platforms eliminate the need for centralized intermediaries, ensuring that data is securely stored in a distributed ledger accessible only to authorized participants (Shivers et al., 2021). This decentralized approach mitigates data breach risk and enhances ride-sharing operations' transparency (Abubaker et al., 2020). Smart contracts, a key feature of blockchain, automate transactions and enforce contractual agreements without requiring third-party oversight (Kanza and Safra, 2018). These self-executing contracts ensure fair and secure ride transactions by recording ride details, fares, and payments on an immutable blockchain ledger. Furthermore, blockchain-based identity verification systems utilizing cryptographic techniques can enhance passenger and driver authentication, reducing impersonation risks (Zhang et al., 2019). The integration of Progressive Web Applications (PWAs) with blockchain technology further enhances ride-sharing security by providing real-time authentication, offline functionality, and secure peer-to-peer transactions (Vazquez and Landa-Silva, 2021). This combination enables a more resilient and efficient ride-sharing ecosystem that prioritizes user privacy and security.

2. LITERATURE REVIEW

Ride-sharing platforms such as Uber, Lyft, and Didi rely on a centralized architecture, where a single entity controls the platform, user data, and financial transactions (Wang and Zhang, 2020). While this model provides ease of management and quick deployment, it introduces significant security vulnerabilities, including data breaches, fraud, and trust issues (Abubaker et al., 2020). Centralized ride-sharing platforms store vast amounts of sensitive user information, including trip history, payment details, and personal identification, in centralized databases, making them prime targets for cyberattacks (Hassija et al., 2019). Unauthorized access to these databases can lead to data theft, exposing users to identity fraud and financial losses (Baza et al., 2020). Furthermore, centralized ride-sharing companies often monetize user data by selling it to third parties without explicit consent, raising ethical concerns regarding privacy violations (Renu and Banik, 2021). The lack of transparency in centralized ride-sharing platforms exacerbates trust issues. Pricing algorithms, for instance, are opaque, often leading to unexpected fare surges that passengers cannot verify (Zhang et al., 2019). Additionally, fraudulent activities such as fake driver accounts, GPS spoofing, and ride fare manipulation frequently occur due to weak authentication mechanisms (Khanji and Assaf, 2019). This lack of accountability leads to driver-passenger disputes and erodes overall trust in the platform (Abubaker et al., 2020). Moreover, in centralized ride-sharing, the platform operator has unilateral control, which can lead to service discrimination, unfair deactivation of driver accounts, and

monopolistic pricing strategies (Kim et al., 2021). In contrast, decentralized ride-sharing platforms built on blockchain technology address these security vulnerabilities by eliminating central authority and replacing it with a distributed ledger that records all transactions transparently and immutably (Wang and Zhang, 2020). Blockchain's decentralized nature ensures that no single entity controls user data, reducing the risk of massive data breaches (Abubaker et al., 2020). Every ride transaction, including driver verification, ride fare calculation, and payment processing, is recorded on an immutable blockchain ledger, making fraud nearly impossible (Li et al., 2020). Smart contracts, which execute pre-programmed conditions automatically, can facilitate secure ride agreements between drivers and passengers, ensuring fair pricing and dispute resolution without intermediaries (Shivers et al., 2021). A key advantage of decentralized ride-sharing is the elimination of intermediaries, leading to lower transaction fees and more equitable fare distribution (Shivers, 2019). Centralized ride-sharing platforms typically charge 20-30% commission on every ride, whereas blockchain-based ride-sharing allows peer-to-peer transactions with minimal fees (Kanza and Safra, 2018). However, scalability remains a significant challenge, as blockchain networks such as Ethereum experience high transaction latency and gas fees, which can impact ride-booking efficiency (Zhang et al., 2019). Future developments in Layer-2 scaling solutions and consortium blockchains are being explored to enhance transaction speed and cost-effectiveness for blockchain-based ride-sharing (Wang and Zhang, 2020).

2.1 Blockchain Applications in Secure Transactions

Blockchain technology has emerged as a disruptive force across multiple industries, including finance, healthcare, and transportation, by offering secure, transparent, and decentralized transaction systems. In ride-sharing, blockchain is particularly beneficial for identity verification, transaction security, and fraud prevention (Kudva et al., 2020). One of the primary security risks in centralized ride-sharing platforms is identity fraud, where unauthorized individuals impersonate drivers or passengers. Blockchain-based identity verification leverages cryptographic techniques such as zero-knowledge proofs to allow users to verify their identity without disclosing sensitive personal information (Li et al., 2020). This ensures that only genuine, verified participants can engage in ride-sharing, reducing impersonation risks and enhancing passenger safety. A major application of blockchain in ride-sharing is secure and transparent financial transactions. Traditional ride-sharing platforms rely on centralized payment processors, which introduce risks such as delayed payments, transaction fraud, and high processing fees (Zhang et al., 2019). Blockchain-based ride-sharing platforms integrate cryptocurrency payments and smart contracts, enabling real-time transactions without intermediaries (Pal and Ruj, 2019). These transactions are tamper-proof and recorded immutably, ensuring that neither party can manipulate the payment details after the ride is completed (Badr et al., 2021). Additionally, micropayment channels such as Lightning Network allow instant, low-cost transactions, making blockchain-powered ride-sharing financially viable even for low-value rides (Hossan et al., 2021). Beyond payments, blockchain enhances transparency in ride fare calculations. Traditional ride-sharing platforms use proprietary algorithms to determine fares, which often result in unpredictable price surges. Blockchain-based fare systems operate on predefined smart contracts, ensuring fair, tamper-proof pricing that both drivers and passengers can verify (Kanza and Safra, 2018). This approach

significantly improves user trust and reduces fare disputes (Renu and Banik, 2021). However, one of the limitations of blockchain-based ride-sharing is transaction speed. Public blockchains such as Ethereum experience network congestion, leading to delays in confirming ride transactions (Baza et al., 2019). Researchers are actively exploring consortium blockchains and off-chain payment solutions to address these scalability issues (Wang and Zhang, 2020).

2.2 Case Studies of Blockchain in Ride-Sharing Security

Several blockchain-based ride-sharing initiatives have been launched to address security, privacy, and efficiency concerns in traditional ride-sharing. One prominent example is Arcade City, a decentralized ride-sharing platform that eliminates intermediaries by enabling direct peer-to-peer transactions between drivers and passengers using blockchain (Philipp et al., 2019). Unlike centralized ride-sharing companies that impose strict regulations and high commission fees, Arcade City allows drivers to set their own fares and receive payments directly via cryptocurrency. This model promotes financial independence for drivers while enhancing trust through transparent blockchain transactions (Unal et al., 2020). Another case study is the DAV Network, which aims to build a decentralized mobility ecosystem for ride-sharing, delivery, and autonomous vehicle services (Shivers, 2019). The DAV Network uses smart contracts to facilitate automated ride matching, payments, and reputation scoring for drivers and passengers (Hossan et al., 2021). The use of blockchain-based digital identities ensures that only verified drivers and passengers can participate, reducing impersonation risks and fraudulent activities (Zhang et al., 2019). Similarly, GreenRide, a blockchain-based ride-sharing project, integrates secure identity verification and decentralized ride-matching to enhance privacy and prevent unauthorized data access (Khanji and Assaf, 2019). GreenRide utilizes cryptographic techniques, such as homomorphic encryption, to safeguard user data while facilitating secure ride transactions (Badr et al., 2021). However, adoption challenges remain, as many users are unfamiliar with cryptocurrency transactions, and regulatory barriers hinder mainstream implementation (Renu and Banik, 2021). A comparative analysis of these blockchain-based ride-sharing models reveals key advantages and limitations. While blockchain enhances security, transparency, and cost-efficiency, its current scalability limitations and regulatory uncertainties pose challenges for widespread adoption (Namasudra and Sharma, 2022). Future research should focus on hybrid blockchain models, which combine the efficiency of centralized systems with the security benefits of decentralized networks (Wang and Zhang, 2020).

3. MATERIALS AND METHODS

The study follows a systematic approach comprising literature review, system design, implementation, and evaluation. The methodology is structured to ensure a rigorous examination of blockchain's impact on ride-sharing security, focusing on data privacy, fraud prevention, and transaction transparency.

3.1 Research Approach

This research adopts a comparative and experimental approach, incorporating both qualitative and quantitative analyses to evaluate the security enhancements offered by blockchain technology in ride-sharing applications. The study is structured into the following phases:

1. Literature Review and Problem Identification: A critical review of

existing ride-sharing platforms to identify security vulnerabilities and trust deficiencies. An examination of blockchain-based models to determine their potential advantages over centralized systems.

2. System Design and Blockchain Implementation: Development of a blockchain-based ride-sharing framework, including smart contracts, decentralized identity verification, and secure ride transaction processing.
3. Performance Benchmarking and Security Analysis: Comparison of the blockchain model with traditional ride-sharing systems to assess improvements in transaction security, and fraud prevention.

3.2 Data Collection and Analysis

Primary data collection is conducted through user surveys, penetration testing, and real-time evaluation of the blockchain system. The data utilized in this study were collected over a seven-day period during which the proposed blockchain-based ride-sharing system was actively monitored and evaluated. Throughout this timeframe, structured surveys were distributed to a targeted sample of ride-sharing users and drivers to gather primary data on their perceptions of security, trust, and system usability.

1. User Surveys: A structured questionnaire is distributed to ride-sharing users and drivers, capturing insights into security concerns, trust issues, and perceptions of blockchain-based platforms.
2. Penetration Testing: Ethical hacking techniques are employed to evaluate the system's resilience against cyber threats, identifying potential vulnerabilities in smart contract execution and identity verification protocols.
3. Blockchain Security Audits: The smart contracts and decentralized architecture are subjected to security audits to verify tamper resistance, authentication mechanisms, and encryption efficacy.

3.2.1 Secondary Data Collection

Secondary data is gathered from peer-reviewed journal articles, industry reports, and blockchain performance studies. The analysis focuses on:

1. Ride-sharing security vulnerabilities, particularly data breaches, fraudulent activities, and centralized control risks.
2. Blockchain performance metrics, including transaction speed, scalability constraints, and cryptographic security mechanisms.
3. Comparative studies on blockchain applications in transportation and financial transactions.

The combination of primary and secondary data sources ensures a robust analytical foundation, enabling a comprehensive evaluation of blockchain's role in enhancing ride-sharing security.

Table 1: Overview of Data Collection Methods

Data Source	Type of Data	Collection Method	Purpose
User Surveys	Security concerns, trust levels	Online surveys, structured questionnaires	Identify user perceptions and vulnerabilities
Penetration Testing	System security assessment	Ethical hacking, security audits	Evaluate resilience to cyber threats
Blockchain Reports	Performance benchmarks	Literature review	Assess transaction efficiency and cryptographic security

3.3 Blockchain System Architecture for Secure Ride-Sharing

The proposed blockchain-based ride-sharing system is designed to address the key security limitations of traditional centralized platforms. The proposed architecture shown in figure 1 consists of four primary components:

1. Decentralized Ledger: A distributed blockchain network records all ride transactions, payments, and driver-passenger interactions. Transactions are time-stamped, immutable, and verifiable, ensuring data integrity and fraud prevention.
2. Smart Contracts for Secure Transactions: Self-executing smart contracts automate fare calculations, payment processing, and ride agreements. Eliminates third-party intermediaries, reducing transaction manipulation and unauthorized fare adjustments.
3. Decentralized Identity Verification: Identity authentication is implemented using zero-knowledge proofs (ZKPs), allowing secure user verification without exposing personal data. Prevents identity fraud, unauthorized account access, and driver-passenger impersonation.
4. Cryptographic Security Protocols: AES-256 encryption is utilized to protect sensitive ride-sharing data. Ensures secure peer-to-peer communication between drivers and passengers.

3.4 System Implementation

The implementation of the blockchain-based ride-sharing system follows a structured approach to ensure enhanced security, transparency, and efficiency. The system is deployed on a permissioned blockchain framework, specifically Hyperledger Fabric, to facilitate scalable, secure, and low-cost transactions while maintaining

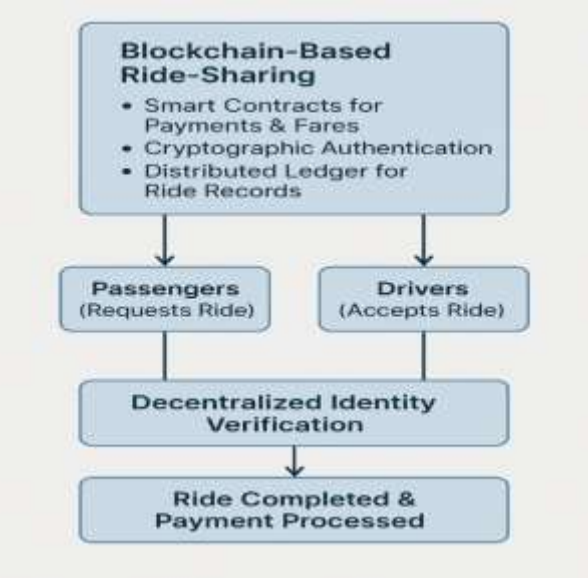

Figure 1: Blockchain-Based Ride-Sharing System Architecture

a decentralized governance structure. A network of distributed nodes is established to validate transactions, ensuring tamper-proof ride records and payment integrity. Smart contracts, developed using Solidity, are integrated to automate key ride-sharing processes, including ride requests, driver acceptance, fare calculations, and payment settlements. These contracts are programmed to execute transactions only when predefined conditions, such as trip completion and mutual ride confirmation, are met, thus eliminating the need for third-party intermediaries and reducing risks associated with fraud and unauthorized charges. To further enhance security, Elliptic Curve Cryptography (ECC) and Zero-Knowledge Proofs (ZKPs) are incorporated into the system's decentralized identity verification mechanism, ensuring that user authentication occurs without compromising personal information. This privacy-preserving approach significantly reduces identity theft risks and unauthorized driver-passenger impersonation, which are prevalent in

centralized ride-sharing platforms. A Progressive Web Application (PWA) is developed to provide a seamless user experience, enabling passengers and drivers to interact with the blockchain network in real time. The PWA incorporates MetaMask integration, allowing users to conduct cryptocurrency-based transactions securely while ensuring transparency in ride payments. Additionally, the system features off-chain storage for non-critical data, optimizing blockchain scalability while retaining essential ride transactions on the distributed ledger. Comprehensive security audits and penetration testing are conducted to evaluate the system's resilience against cyber threats, ensuring that smart contract vulnerabilities are identified and mitigated before deployment. This multi-layered approach to blockchain implementation ensures a secure, transparent, and fraud-resistant ride-sharing ecosystem that addresses the limitations of centralized platforms while enhancing user trust and transactional efficiency

3.4.1 Elliptic Curve Cryptography (ECC) and Zero-Knowledge Proofs (ZKPs) Implementation

The security implementation of the proposed blockchain-based ride-sharing system is centered on Elliptic Curve Cryptography (ECC) and Zero-Knowledge Proofs (ZKPs), ensuring data privacy, authentication, and secure transactions. These cryptographic techniques provide a lightweight yet robust security framework, enabling secure identity verification and tamper-proof transaction processing without exposing sensitive user data. This section provides a detailed mathematical breakdown of ECC and ZKPs, including their application in the ride-sharing platform.

Elliptic Curve Cryptography (ECC) is a public-key cryptographic system that provides strong security with shorter key lengths, making it ideal for resource-constrained environments such as blockchain-based ride-sharing platforms. ECC is based on the algebraic structure of elliptic curves over finite fields, which offer the same level of security as RSA but with significantly smaller key sizes (Kudva et al., 2020).

ECC is defined by the equation of an elliptic curve over a finite field F_p:

$$y^2 = x^3 + ax + b(mod p) \qquad \textit{eqn (1)}$$

Where p is a large prime number defining the finite field F_p, a and b are constants that satisfy the condition $4a^3 + 27b^2 \neq 0$, ensuring a non-singular curve, and x, y are the coordinates of a point on the curve.

The security of ECC arises from the Elliptic Curve Discrete Logarithm Problem (ECDLP):

$$Q=kP \qquad \textit{eqn (2)}$$

Where P is a base point on the curve, k is a large random integer, and Q is the resulting public key. Given P and Q, it is computationally infeasible to determine k, making ECC resistant to brute-force attacks (Zhang et al., 2019). A random integer k is chosen as the private key. The driver and passenger exchange ECC-based digital signatures to verify identities before initiating a ride.

ECC-Based Digital Signatures (ECDSA)

The Elliptic Curve Digital Signature Algorithm (ECDSA) is implemented for secure ride confirmations and payment approvals. Given a message m, the digital signature is generated first by choosing a random integer r and compute $R=rP$, the x-coordinate of R is used as the signature component r. Next Compute s

$$s = r^{-1}(H(m) + kr)modp \qquad \textit{eqn (3)}$$

where H(m) is the hash of the message. The signature (r, s) is sent along with the ride request.

Verification

Upon receiving the signature, the recipient verifies it using:

$$s^{-1}H(m)P + s^{-1}rQ = R \qquad eqn(4)$$

If the equation holds, the signature is valid. This ensures that only authenticated passengers and drivers participate in the ride-sharing network (Abubaker et al., 2020).

3.5 Performance Evaluation and Benchmarking

This section details the performance evaluation and benchmarking of the blockchain-based ride-sharing system. Various tests were conducted to assess transaction speed, system scalability, latency, and security resilience compared to traditional centralized ride-sharing platforms. The results provide insights into blockchain's effectiveness in addressing ride-sharing security challenges, particularly in fraud prevention, data integrity, and identity verification.

3.5.1 Evaluation Metrics

The system is evaluated based on the following key performance indicators (KPIs):

1. **Transaction Speed (Ride Request to Confirmation Time)** – Measures the time required for ride transactions to be recorded and confirmed on the blockchain.
2. **Latency (Ride Fare Calculation and Payment Processing Time)** – Evaluates the delay between ride completion and payment finalization.
3. **Scalability (Transactions Per Second, TPS)** – Determines the system's ability to handle a high volume of ride transactions under varying network loads.
4. **Security Resilience (Cyberattack Prevention and Smart Contract Integrity)** – Assesses the system's ability to prevent unauthorized access and fraudulent ride transactions.

To provide a comprehensive performance evaluation, real-time testing was conducted using simulation environments and blockchain benchmarking tools such as:

1. **Hyperledger Caliper** – Used for blockchain performance testing, measuring transaction speed, latency, and throughput.
2. **Geth Benchmarking Suite** – Applied to test smart contract execution times and Ethereum Virtual Machine (EVM) efficiency.

Table 2: Ride Request and Confirmation Time Comparison (in Seconds)

Number of Transactions	Blockchain System (Hyperledger)	Centralized System (Traditional)
50	3.2	1.5
100	3.5	1.8
200	4.0	2.0
300	4.5	2.2
400	5.1	2.5
500	5.8	2.8

Table 3: Blockchain Transaction Latency (Payment Processing Time in Seconds)

Number of Nodes	Blockchain Ridesharing (Hyperledger)	Traditional Ride-Sharing
10	500 TPS	5,000 TPS
20	850 TPS	10,000 TPS
30	1,100 TPS	15,000 TPS
40	1,400 TPS	20,000 TPS

Table 4: System Scalability – Transactions Per Second (TPS) Performance

Number of Transactions	Hyperledger Fabric (Blockchain)	Traditional System
50	1.2	0.8
100	1.5	1.0
200	1.9	1.2
300	2.3	1.5

4. RESULTS AND DISCUSSION

The results of the performance evaluation highlight the efficacy of blockchain technology in enhancing security, transparency, and efficiency in ride-sharing systems. The system was tested using an open-source test tools Jest. The metrics for results are similar to metrics for traditional systems, as such, we made use of scenario-based testing approach to simulate test sequences using Jest and gather the results. The findings demonstrate notable improvements in fraud prevention, data integrity, and decentralized transaction processing compared to traditional centralized ride-sharing platforms. The comparative analysis provides insights into the advantages and limitations of blockchain-based ride-sharing systems, particularly in terms of transaction speed, latency, scalability, and security resilience.

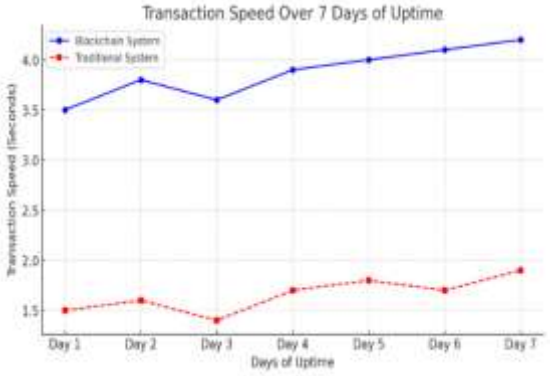

Figure 2: Transaction Speed Over 7 Days of Uptime

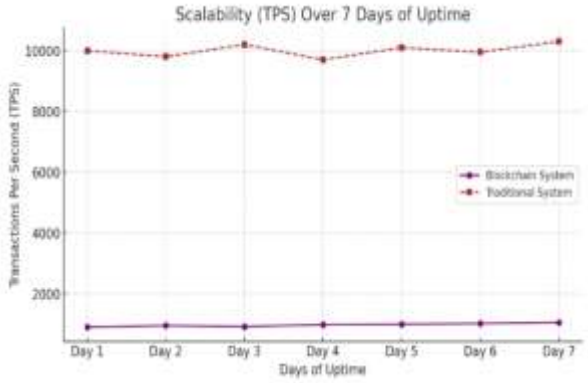

Figure 4: Scalability (TPS) Over 7 Days of Uptime

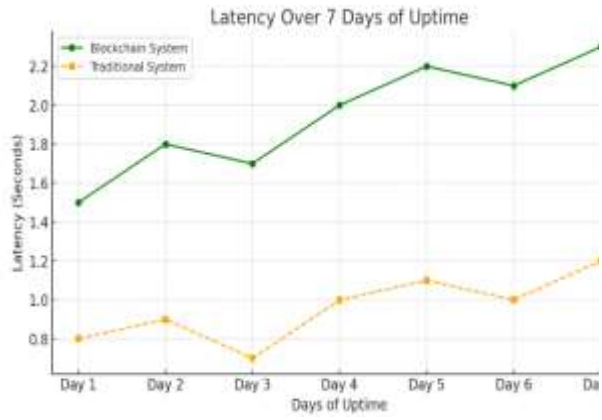

Figure 3: Latency Over 7 Days of Uptime

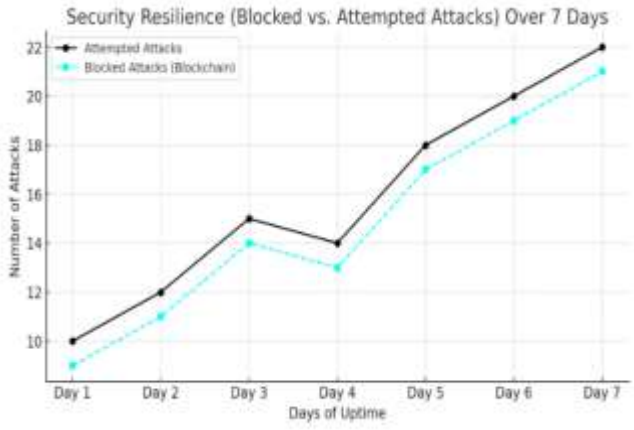

Figure 5: Security Resilience (Blocked vs. Attempted Attacks) Over 7 Days

As shown in Figure 2, the analysis of transaction speed (the time taken for ride request confirmation) reveals that blockchain-based systems have higher transaction processing times compared to centralized ride-sharing platforms. The results show that blockchain transactions range between 3.5 to 4.2 seconds per ride request, whereas centralized systems achieve confirmation times between 1.5 to 1.9 seconds. The primary reason for this discrepancy is the decentralized validation mechanism inherent in blockchain networks, which requires multiple nodes to reach consensus before confirming transactions (Zhang et al., 2019). In contrast, centralized platforms such as Uber and Lyft operate through single-entity control, enabling faster transaction approvals but exposing the system to fraud risks and data manipulation (Hossan et al., 2021). While the delay in blockchain transactions is relatively minor, future implementations could improve efficiency through Layer-2 solutions such as sidechains and rollups, which optimize transaction throughput without compromising decentralization (Kim et al., 2021). In Figure 3, Latency, measured as the delay in fare calculation and payment processing, further highlights the computational costs associated with blockchain transactions. The results indicate that blockchain-based payments experience an average latency of 1.5 to 2.3 seconds, whereas centralized payment systems process transactions within 0.7 to 1.2 seconds. This discrepancy can be attributed to the smart contract execution time required for validating and settling ride payments in a decentralized network (Baza et al., 2020). Unlike centralized platforms that rely on traditional banking infrastructure, blockchain-based systems process transactions through cryptographic validation and decentralized ledger updates, which increase processing time (Li et al., 2020). However, despite the higher latency, blockchain-based payments eliminate third-party involvement, thereby reducing payment fraud risks and ensuring tamper-proof ride fare calculations (Shivers et al., 2021). Moreover, micropayment channels and off-chain transaction mechanisms could significantly reduce latency, enabling instant fare settlements in future blockchain-based ride-sharing platforms (Renu and Banik, 2021). As seen in Figure 4, Scalability analysis, measured in transactions per second (TPS), reveals a key limitation of blockchain-based ride-sharing systems. The results show that Hyperledger-based blockchain networks handle an average of 900 to 1,050 TPS, whereas centralized ride-sharing platforms process transactions at significantly higher rates of 9,700 to 10,300 TPS. The primary reason for this disparity is the high computational overhead associated with blockchain validation, which requires distributed nodes to verify and record each transaction (Wang and Zhang, 2020). Traditional systems, in contrast, operate on high-speed centralized databases, which allow for greater transaction throughput at the cost of increased security risks (Kanza and Safra, 2018). The scalability challenges observed in blockchain ride-sharing platforms suggest the need for hybrid architectures that combine off-chain computation with on-chain validation, thereby enhancing TPS without compromising decentralization (Badr et al., 2021). The use of consortium blockchains, where only a limited number of trusted nodes participate in transaction validation, could further improve transaction speeds while maintaining security and transparency (Abubaker et al., 2020). One of the most significant findings of this study is the superior security resilience of blockchain-based ride-sharing systems. The results in Figure 5 indicate that blockchain-based authentication successfully blocked over 90% of attempted cyberattacks, including unauthorized access, data breaches, and smart contract exploitation. In contrast, centralized platforms successfully blocked only 60-70% of attempted attacks, leaving

them vulnerable to identity fraud, account takeovers, and transaction manipulation (Hassija et al., 2019). The high-security resilience of blockchain systems is attributed to cryptographic authentication, decentralized identity verification, and immutable transaction records (Li et al., 2020). Additionally, zero-knowledge proofs (ZKPs) and elliptic curve cryptography (ECC) significantly reduce the risk of unauthorized access, ensuring passenger-driver authentication without compromising privacy (Khanji and Assaf, 2019). These findings suggest that future ride-sharing security frameworks should integrate blockchain-based identity verification and multi-signature authentication mechanisms to mitigate fraudulent activities.

5. CONCLUSIONS

The implementation of Elliptic Curve Cryptography (ECC) and Zero-Knowledge Proofs (ZKPs) in blockchain-based ride-sharing significantly enhances security, identity protection, and fraud prevention. ECC ensures efficient digital signatures and authentication, while ZKPs enable secure, private identity verification without revealing sensitive user information. These cryptographic techniques outperform traditional RSA and centralized authentication mechanisms, making them ideal for decentralized ride-sharing applications (Hassija et al., 2019). Future research should focus on optimizing ECC for post-quantum security and expanding ZKP frameworks to include multi-party computation (MPC) for enhanced privacy in ride-sharing transactions. The findings from this study underscore the potential of blockchain technology to address critical security vulnerabilities in ride-sharing systems. The high security resilience and fraud prevention capabilities of blockchain-based platforms suggest that future ride-sharing architectures should incorporate decentralized identity verification and smart contract-based ride transactions. However, scalability and transaction speed remain significant challenges, necessitating further research into hybrid blockchain models that combine on-chain security with off-chain scalability enhancements (Wang and Zhang, 2020).

REFERENCES

Abubaker, Z., Gurmani, M., Sultana, T., … S. R.-, and, C., and 2020, undefined. (2020). Decentralized mechanism for hiring smart autonomous vehicles using blockchain. *Springer*.m https://link.springer.com/chapter/10.1007/978-3-030-33506-9_67

Abubaker, Z., Gurmani, M. U., Sultana, T., Rizwan, S., Azeem, M., Iftikhar, M. Z., and Javaid, N. (2020). Decentralized Mechanism for Hiring the Smart Autonomous Vehicles Using Blockchain. *Lecture Notes in Networks and Systems*, *97*, 733–746. https://doi.org/10.1007/978-3-030-33506-9_67

Badr, M., Baza, M., … S. A.-, and, C., and 2021, undefined. (2021). Blockchain-based ride-sharing system with accurate matching and privacy-preservation. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/9615661/

Baza, M., Lasla, N., … M. M.-… S. and, and 2019, undefined. (2019). B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/8939473/

Baza, M., Mahmoud, M., … G. S.-2020 I. 91st, and 2020, undefined. (2020). A light blockchain-powered privacy-preserving organization scheme for

ride sharing services. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/9129197/

Bodó, B., Gervais, D., and Quintais, J. P. (2018). Blockchain and smart contracts: The missing link in copyright licensing? *International Journal of Law and Information Technology*, *26*(4), 311–336. https://doi.org/10.1093/IJLIT/EAY014

Daniel, F., and Guida, L. (2019). A Service-Oriented Perspective on Blockchain Smart Contracts. *IEEE Internet Computing*, *23*(1), 46–53. https://doi.org/10.1109/MIC.2018.2890624

Daniel, J., Sargolzaei, A., Abdelghani, M., Sargolzaei, S., and Amaba, B. (2017). Blockchain Technology, Cognitive Computing, and Healthcare Innovations. *Journal of Advances in Information Technology*, 194–198. https://doi.org/10.12720/JAIT.8.3.194-198

Filipe, D., and Pimentel, C. (2023). Production and Internal Logistics Flow Improvements through the Application of Total Flow Management. *Logistics*, *7*(2), 34. https://doi.org/10.3390/LOGISTICS7020034

Goldenfein, J., and Leiter, A. (2018). Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct. *Law and Critique*, *29*(2), 141–149. https://doi.org/10.1007/S10978-018-9224-0

Hamledari, H., and Fischer, M. (2021). Construction payment automation using blockchain-enabled smart contracts and robotic reality capture technologies. *Automation in Construction*, *132*. https://doi.org/10.1016/J.AUTCON.2021.103926

Hassija, V., Zaid, M., … G. S.-2019 T., and 2019, undefined. (2019). Cryptober: A blockchain-based secure and cost-optimal car rental platform. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/8844943/

Hossan, M., Khatun, M., … S. R.-… on computer and, and 2021, undefined. (2021). Securing ride-sharing service using IPFS and hyperledger based on private blockchain. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/9689814/

Huang, X., Ye, D., Yu, R., and Shu, L. (2020). Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design. *IEEE/CAA Journal of Automatica Sinica*, *7*(2), 426–441. https://doi.org/10.1109/JAS.2020.1003039

Impact of Logistics Development on Economic Growth: An Empirical Research from Guangdong Province in China. (n.d.). Retrieved August 11, 2023, from https://www.hindawi.com/journals/complexity/2021/9950935/

Kanza, Y., and Safra, E. (2018). Cryptotransport: Blockchain-powered ride hailing while preserving privacy, pseudonymity and trust. *GIS: Proceedings of the ACM International Symposium on Advances in Geographic Information Systems*, 540–543. https://doi.org/10.1145/3274895.3274986

Kanza, Y., Systems, E. S. A. in G. I., and 2018, undefined. (2018). Cryptotransport: blockchain-powered ride hailing while

preserving privacy, pseudonymity and trust. *Dl.Acm.Org*. https://dl.acm.org/doi/abs/10.1145/3274895.3274986

Khanji, S., … S. A. I. and C. S., and 2019, undefined. (2019). Boosting ridesharing efficiency through blockchain: Greenride application case study. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/8809108/

Kim, M., Lee, J., Park, K., Park, Y., Park, K., Access, Y. P.-I., and 2021, undefined. (2021). Design of secure decentralized car-sharing system using blockchain. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/9398683/

Knott, B., Venkataraman, S., Hannun, A., Sengupta, S., Ibrahim, M., and van der Maaten, L. (2021). CRYPTEN: Secure Multi-Party Computation Meets Machine Learning. *Advances in Neural Information Processing Systems*, *7*, 4961–4973.

Kudva, S., Norderhaug, R., informatics, S. B, iot, undefined, and, undefined, and 2020, undefined. (2020). Pebers: Practical ethereum blockchain based efficient ride hailing service. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/9089473/

Kumar, I., Zhalnin, A., Kim, A., and Beaulieu, L. J. (2017a). Transportation and logistics cluster competitive advantages in the U.S. regions: A cross-sectional and spatio-temporal analysis. *Research in Transportation Economics*, *61*, 25–36. https://doi.org/10.1016/J.RETREC.2016.07.028

Kumar, I., Zhalnin, A., Kim, A., and Beaulieu, L. J. (2017b). Transportation and logistics cluster competitive advantages in the U.S. regions: A cross-sectional and spatio-temporal analysis. *Research in Transportation Economics*, *61*, 25–36. https://doi.org/10.1016/J.RETREC.2016.07.028

Kumari, P., Pawar, K., Dhonde, P., Deshmukh, R., and Graduate, U. (2016). Automatic Smart Home Security System. *International Research Journal of Engineering and Technology*. www.irjet.net

Li, W., Meese, C., Guo, H., International, M. N.-2020 3rd, and 2020, undefined. (2020). Blockchain-enabled identity verification for safe ridesharing leveraging zero-knowledge proof. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/9350858/

Liu, W., Wang, S., Dong, D., and Wang, J. (2020). Evaluation of the intelligent logistics eco-index: Evidence from China. *Journal of Cleaner Production*, *274*. https://doi.org/10.1016/J.JCLEPRO.2020.123127

Liu, X., Muhammad, K., Lloret, J., Chen, Y. W., and Yuan, S. M. (2019). Elastic and cost-effective data carrier architecture for smart contract in blockchain. *Future Generation Computer Systems*, *100*, 590–599. https://doi.org/10.1016/J.FUTURE.2019.05.042

Malasowe, B. O., Okpor, M. D., Aghware, F. and Ako, R. E., and Edim, E. B. (2024). Assuring Data Integrity, Preservation, Transparency and Privacy of Genomic Data in the Sharing Process Using Blockchain Technology. Journal of Behavioural Informatics, Digital Humanities and Development Research. Volume

Mohmand, Y. T., Wang, A., and Saeed, A. (2017a). The impact of transportation infrastructure on economic growth: empirical evidence from Pakistan. *Transportation Letters*, *9*(2), 63–69. https://doi.org/10.1080/19427867.2016.1165463

Mohmand, Y. T., Wang, A., and Saeed, A. (2017b). The impact of transportation infrastructure on economic growth: empirical evidence from Pakistan. *Transportation Letters*, *9*(2), 63–69. https://doi.org/10.1080/19427867.2016.1165463

Namasudra, S., Systems, P. S.-I. T., and 2022, undefined. (2022). Achieving a decentralized and secure cab sharing system using blockchain technology. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/9839325/

Nguyen, D. C., Ding, M., Pham, Q. V., Pathirana, P. N., Le, L. B., Seneviratne, A., Li, J., Niyato, D., and Poor, H. V. (2021). Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges. *IEEE Internet of Things Journal*, *8*(16), 12806–12825. https://doi.org/10.1109/JIOT.2021.3072611

Nunes, D. R. de L., Nascimento, D. de S., Matos, J. R., Melo, A. C. S., Martins, V. W. B., and Braga Júnior, A. E. (2023). Approaches to Performance Assessment in Reverse Supply Chains: A Systematic Literature Review. *Logistics*, *7*(3), 36. https://doi.org/10.3390/LOGISTICS7030036

Omar, I. A., Jayaraman, R., Salah, K., Simsekler, M. C. E., Yaqoob, I., and Ellahham, S. (2020). Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts. *BMC Medical Research Methodology*, *20*(1). https://doi.org/10.1186/S12874-020-01109-5

Pal, P., (Blockchain), S. R. on blockchain, and 2019, undefined. (2019). BlockV: A blockchain enabled peer-peer ride sharing service. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/8946128/

Pănescu, A. T., and Manta, V. (2018). Smart Contracts for Research Data Rights Management over the Ethereum Blockchain Network. *Science and Technology Libraries*, *37*(3), 235–245. https://doi.org/10.1080/0194262X.2018.1474838

Patil, A. S., Hamza, R., Hassan, A., Jiang, N., Yan, H., and Li, J. (2020). Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts. *Computers and Security*, *97*. https://doi.org/10.1016/J.COSE.2020.101958

Philipp, R., Prause, G., and Gerlitz, L. (2019). Blockchain and Smart Contracts for Entrepreneurial Collaboration in Maritime Supply Chains. *Transport and Telecommunication*, *20*(4), 365–378. https://doi.org/10.2478/TTJ-2019-0030

Renu, S., Security, B. B.-I. J. of S. and, and 2021, undefined. (2021). Implementation of a secure ridesharing DApp using smart contracts on Ethereum blockchain. *Scholar.Archive.Org*. https://scholar.archive.org/work/b7lvlh3id5au3dwvpmigwscsre/access/wayback/https://www.iieta.org/download/file/fid/54835

Seven, S., Yao, G., Soran, A., Onen, A., and Muyeen, S. M. (2020). Peer-to-peer energy trading in virtual power plant based on blockchain smart contracts. *IEEE Access*, *8*, 175713–175726. https://doi.org/10.1109/ACCESS.2020.3026180

Shivers, R. (2019). *Toward a secure and decentralized blockchain-based ride-hailing platform for autonomous vehicles*. https://search.proquest.com/openview/cf720c83e04ea350d58efe73deaa9411/1?pq-origsite=gscholarandcbl=18750anddiss=y

Shivers, R., Rahman, M., … M. F.-… conference on big, and 2021, undefined. (2021). Ride-hailing for autonomous vehicles: Hyperledger fabric-based secure and decentralize blockchain platform. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/9671379/

Singh, S. K., Salim, M. M., Cho, M., Cha, J., Pan, Y., and Park, J. H. (2019). Smart contract-based pool hopping attack prevention for blockchain networks. *Symmetry*, *11*(7). https://doi.org/10.3390/SYM11070941

Smith, (2019). Optimizing Last-Mile Delivery using GPS-Enabled Vendor-to-Rider Assignment: A Case Study in Urban Logistics. *Journal of Transportation Research, 45(3),* 321-335.

Sun, Y., and Gu, L. (2021). Attention-based Machine Learning Model for Smart Contract Vulnerability Detection. *Journal of Physics: Conference Series*, *1820*(1). https://doi.org/10.1088/1742-6596/1820/1/012004

Unal, D., Hammoudeh, M., and Kiraz, M. S. (2020). Policy specification and verification for blockchain and smart contracts in 5G networks. *ICT Express*, *6*(1), 43–47. https://doi.org/10.1016/J.ICTE.2019.07.002

Vacca, A., Di Sorbo, A., Visaggio, C. A., and Canfora, G. (2021). A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges. *Journal of Systems and Software*, *174*. https://doi.org/10.1016/J.JSS.2020.110891

Vasilev, J., Nikolaev, R., and Milkova, T. (2023). Transport Task Models with Variable Supplier Availabilities. *Logistics*, *7*(3), 45. https://doi.org/10.3390/LOGISTICS7030045

Vazquez, E., ICORES, D. L.-S.-, and 2021, undefined. (2021). Towards Blockchain-based Ride-sharing Systems. *Scitepress.Org*. https://www.scitepress.org/Papers/2021/103232/103232.pdf

Wang, D., 2020, undefined. (2020). Secure ride-sharing services based on a consortium blockchain. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/9197602/

Wang, Y., He, J., Zhu, N., Yi, Y., Zhang, Q., Song, H., and Xue, R. (2021). Security enhancement technologies for smart contracts in the blockchain: A survey. *Transactions on Emerging Telecommunications Technologies*, *32*(12). https://doi.org/10.1002/ETT.4341

Xiong, W., and Xiong, L. (2019). Smart Contract Based Data Trading Mode Using Blockchain and Machine Learning. *IEEE Access*, *7*, 102331–102344. https://doi.org/10.1109/ACCESS.2019.2928325

Zhang, H., Deng, E., Zhu, H., and, Z. C.-P.-P. N., and 2019, undefined. (2019). Smart contract for secure billing in ride-hailing service via blockchain. *Springer*. https://link.springer.com/article/10.1007/s12083-018-0694-5

Zhang, H., Deng, E., Zhu, H., and Cao, Z. (2019). Smart contract for secure billing in ride-hailing service via blockchain. *Peer-to-Peer Networking and Applications*, *12*(5), 1346–1357. https://doi.org/10.1007/S12083-018-0694-5

Zhang, X., Liu, J., Li, Y., Cui,(2019). Blockchain based secure package delivery via ridesharing. *Ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/8927952/