Bulletin of Electrical Engineering and Informatics
Vol. 14, No. 4, August 2025, pp. 3110~3120
ISSN: 2302-9285, DOI: 10.11591/eei.v14i4.8806

A single-user electronic ticketing system using ERC-721 protocol for smart contracts

Kennedy Okokpujie[1,2], Oghenetega Owivri[1], Olamide Olusanya[2], Samuel Daramola[1], Morayo E. Awomoyi[4]
[1]Department of Electrical and Information Engineering, College of Engineering, Covenant University, Ota, Nigeria
[2]Africa Centre of Excellence for Innovative & Transformative STEM Education, Lagos State University, Lagos, Nigeria
[3]Department of Computer Engineering, College of Engineering, Bells University of Technology, Ota, Nigeria
[4]School of International Service, American University, Washington D.C, United States

Article Info

Article history:

Received Jul 17, 2024
Revised Feb 24, 2025
Accepted Mar 9, 2024

Keywords:

Blockchain technology
ERC-721
Ethereum virtual machine
E-tickets
Smart contracts

ABSTRACT

Single-user electronic ticketing systems face significant security challenges, including fraud and counterfeiting. While blockchain has been explored for electronic ticketing, existing solutions often remain centralized or focus solely on event-based scenarios, not single-user tickets such as flight, train, bus, big transport schemes, movie tickets, and vouchers. This paper presents a decentralized single-user ticketing system to address this gap by utilizing Ethereum's ERC-721 standard for smart contracts (SC). Transparency and privacy are ensured through asymmetric encryption. Digital signatures validate ticket authenticity, and an innovative ERC-721-based verification process is applied. Leveraging Ethereum's ERC-721 Protocols, digital signatures, and the interplanetary file system (IPFS) for decentralized metadata storage, this paper addresses centralization, security, traceability, and transparency concerns. The SC is integrated into a web application, and empirical analysis based on blockchain metrics demonstrates its performance. Results indicate that the system exhibits an efficient ticket transaction completion time of 19.64 seconds and a mean ticket verification time of 3.17 seconds. The outcome illustrates the efficiency of the system in mitigating fraud, counterfeiting, and security risks in single-user electronic ticketing systems.

Corresponding Author:

Kennedy Okokpujie
Department of Electrical and Information Engineering, College of Engineering, Covenant University
KM 10 Idoroko road, Ota, Ogun State, Nigeria
Email: kennedy.okokpujie@covenantuniversity.edu.ng

1. INTRODUCTION

Ticketing helps certain businesses manage and keep track of purchase requests, as tickets serve as substantial proof that a purchase was requested and act as a binding agreement ensuring that a vendor will provide the goods or service requested. Without it, the requested service would not be provided [1]. A major drawback of the traditional ticketing architecture is its high dependency on paper for its functionality [2]. With the evolution of the internet, the computer, and web technologies, the traditional system of obtaining conventional paper tickets is being replaced and gradually eliminated by an electronic approach. Electronic tickets replace conventional paper tickets by allowing customers to purchase services over an electronic device such as a telephone, personal computer (PC), or mobile device, eliminating the need to visit a ticket counter to obtain a ticket [3]. The use of electronic tickets has increased rapidly over the years, significantly enhancing ticketing management's effectiveness, and decreasing the cost of storing ticketing data compared to paper

tickets [4], [5]. With the increasing popularity of online ticketing, there is a growing need for secure and transparent systems that can handle a large number of transactions. A major drawback of current electronic ticketing systems that have been proposed and implemented is only the fact that they operate on a centralized architecture. In centralized ticketing systems, a central entity responsible for storing, an intermediary that is trusted, typically supplies processing and providing service; this makes centralized ticketing systems have many challenges, such as lack of transparency, data security, privacy, and an auditable registry [6], [7].

Blockchain technology offers a solution by allowing for decentralized and autonomous systems that eliminate the need for intermediaries [8]. Liu [4] expressed that a ticketing system should consider various problems such as the authenticity of tickets, the traceability of tickets, privacy protection, system transparency, and verification against ticket reuse. Blockchain is employed to address these challenges while providing a decentralized architecture for ticketing. Blockchain is a distributed ledger with a decentralized architecture that tracks the history of a digital asset; it utilizes a peer-to-peer linked structure to maintain an immutable order of transactions, thereby mitigating the problem of double-spending [9]. The sole aim of blockchain is to provide a secure and reliable system that utilizes cryptography to achieve proof of trust, thereby eliminating the need for an intermediary and third party, such as payment gateways and financial institutions, for its operation [10]. By inherent design, it is impossible to modify the data on the blockchain [11]. Transactions are grouped in a constrained-sized structure called *blocks*; these blocks have the same timestamp and are linked to each other chronologically by nodes of the network known as *miners; thus*, a blockchain is created, each block holding the hash of the one before it; thus, the blockchain network contains an auditable and profound registry of every transaction [12], [13].

Another emerging technology in the field of blockchain technology is intelligent contracts, also known as smart contracts (SC), which work by automating contractual terms and clauses through triggers created and configured in software [14]. SC work on a blockchain network, which enables contract transactions to be permanently recorded in an immutable and transparent ecosystem [15]. Once an SC is deployed onto the blockchain, its code is immutable due to its computational nature, as with the execution of any software program, and the conditions stipulated by the contract's parties must be followed [16]. SC can be created, deployed, maintained, and stored on a blockchain.

The Ethereum network is a blockchain network, a programmable ledger, and a comprehensive virtual machine that can execute blockchain-specific software programs and, specifically, SC [17]. The Ethereum blockchain has a Turing-complete computer integrated with it; this enables software programs to be uploaded to the blockchain and run on the nodes that make up the peer-to-peer network [18]. SC can theoretically carry out any computational and logical task that can be carried out by standard programs, but because of the decentralized nature of the blockchain and the consensus protocol and standards employed by Ethereum, certain specifications must be followed, which leads to SCs displaying unique features and characteristics that are not seen in conventional software development [19].

This work employs blockchain technology to develop a system that can track and automate the sales and verification of electronic tickets without a trusted intermediary, making it function in a decentralized manner. The Ethereum virtual machine (EVM) will be used to deploy the SC that will govern the issuance of tokens and tickets and the verification of the tickets on the blockchain network. ERC-721 protocol is employed to issue electronic tickets as non-fungible tokens on the blockchain network, which ensures that the tickets issued by the system are secure, unforgeable, and unalterable. The interplanetary file system (IPFS) [20] is used as a decentralized storage solution for storing ticket information that would be queried during verification. By utilizing blockchain technology, a fully decentralized electronic ticketing system that is secure, transparent, and immutable is realized.

2. RELATED WORKS

Several research works have been undertaken on using blockchain technology as a solution to decentralized payments and a few focused on ticketing systems. Garcia-Alfaro *et al.* [21] developed a secure event ticketing system using a permissioned blockchain framework to address double selling, counterfeit tickets, unauthorized resales, and trust issues among organizers. Event planners controlled the network nodes, and all transactions were recorded and processed using Hyperledger Fabric, ensuring data transparency. This system allowed all nodes to observe and monitor the financial distribution process for events.

According to Elsden e*t al.* [22], the Aventus team presented a white paper in 2018, introducing a platform that offers ticketing services at the protocol level on the public blockchain. Similarly, in 2017, the GUTS team introduced a comparable approach. Both systems utilized Ethereum's public blockchain to store and handle ticketing data and transactions, ensuring transparency within the system. Both the Aventus and GUTS solutions share several similarities. To protect the privacy of data stored on the public blockchain, both solutions employed asymmetric encryption techniques. This involved generating a key pair and using the public key to encrypt the private information, ensuring the confidentiality of sensitive data.

Cha *et al.* [23] introduced an event ticketing system using a public blockchain with a focus on data privacy, employing the non-interactive zero-knowledge proof (NIZK) technique. This method verifies consumer identities without compromising privacy or enabling surveillance. Consumers use unique key pairs with public keys for identity establishment. Instead of directly submitting public keys, consumers generate parameters based on their public keys for validation. These parameters vary each time, ensuring privacy and preventing the system from tracing past ticket purchases.

Preece and Easton [3] proposed a ticketing model using Hyperledger Fabric for decentralized data sharing among organizations. This private blockchain framework features a governing organization with administrative privileges, a certificate authority for assigning digital identities, and a node for ordering transactions. Sub-networks, or channels, are created for participating sub-organizations, each with its own ledgers and SC. Passengers receive digital identities via SC and can only purchase tickets with these identities. Ticket purchases are initiated through a user interface, verified by SC, and recorded on the vendor's ledger. A SC-based application validates tickets at admission.

Lin *et al.* [24] introduced a mobile ticketing system using SC and multi-signature functionality for secure payments and ticket verification. Tickets are generated as QR codes displayed in a mobile app, with each QR code signed digitally twice: first by the event organizer for authenticity and second by the customer at entry to prevent theft. A SC with digital signatures from both the event host and ticketing company ensures the integrity of the sales process. The system utilizes the EOSIO permissioned blockchain to execute ticketing SC.

A blockchain-based ticketing system using a private Hyperledger Fabric blockchain was introduced by [25] to create a direct contractual framework between event organizers and consumers, preventing agents from using macros to buy large quantities of tickets. This system restricts access to authorized users and conducts all transactions within the network, ensuring strict transaction control and minimizing the risk of excessive ticket orders. Liu [4] proposed a hybrid event ticketing solution using a public blockchain and private blockchain to implement his model. Thus, it focused on event tickets and did not consider single-user type tickets. The ticketing model was designed to mitigate the problem of inefficiency, security and privacy of data, transparency, and ticket scalping.

Niya *et al.* [26] proposed a decentralized ticketing management platform called DeTi using blockchain technology through SC to offer a dedicated service management functionality for event tickets and regulating the aftermarket. DeTi was implemented on the EVM using a SC to automate and validate the ticket life cycle from purchase to usage. Aldweesh [27] proposed a blockchain system that focuses on verifying E-ticket transmission between parties, with each entity having an Ethereum address and interacting with the blockchain, SC, and sometimes IPFS for storing large data. Initially, all parties sign an agreement stored on IPFS, while the blockchain stores only metadata to save space and cost. The process involves ticket issuers notifying advertisers of events, advertisers announcing events and terms via SC, and buyers requesting tickets and providing deposits. SC generate digital currencies for secure ticket downloads from advertisers, and buyers confirm downloads to complete transactions and release payments. In case of disputes, auditors verify transactions and decide on refunds. This system, using SC developed in Solidity and tested on Remix IDE, ensures secure and transparent ticket transactions, maintaining trust among all parties.

These studies offer insights into various methodological approaches for designing decentralized electronic ticketing systems using blockchain technology, each addressing specific system concerns. However, existing technologies like [4] which employ a private blockchain, present drawbacks due to their semi-decentralized architecture. This configuration risks compromising data integrity and consumer trust, as certain participants lack visibility into the private blockchain's operations. While [26] the DeTi platform focuses on decentralized ticket management on a public blockchain, it is limited to event tickets and not suitable for single-user ticket types. Research by Liu [4] offers a decentralized solution but still stores some data on a private blockchain, leading to some degree of centralization and limited throughput.

3. METHOD

The proposed system in this paper is fully decentralized and does not require a trusted intermediary for the issuance, securing, storing, and verification of tickets. Figure 1 illustrates the overall framework of the proposed model. It consists of the consumer client, the ticketing SC deployed on the EVM, the IPFS utilized for storing metadata, the ticket verification system, and an administrative back-end user interface designed for data management and analysis. The consumer client is a decentralized web application with a responsive interface that would enable participants to interact the Ethereum blockchain network, track their token balance, request ticket purchases while maintaining ticket authenticity, and also track the history of purchased tickets. The consumer client will not store any data but act as an interface for participants to interact and exchange data with the SC uploaded to the EVM.

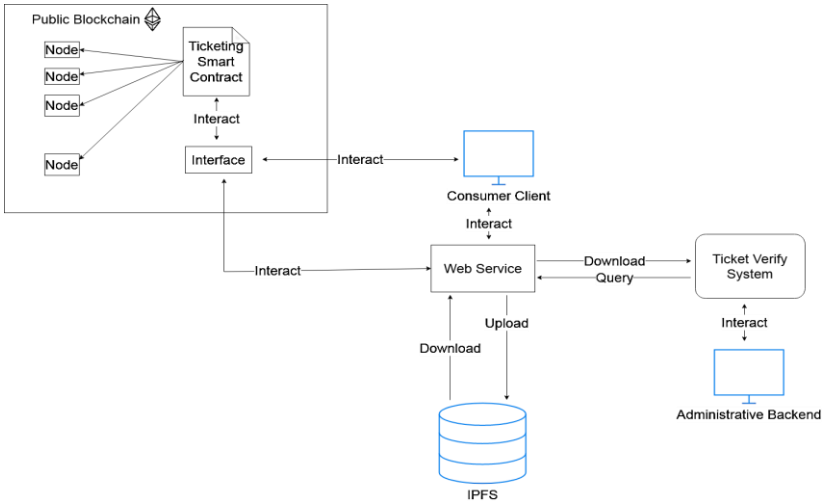


Figure 1. Overall architecture of the proposed system

The ticketing system's Web Service is intended to serve as an interface for processing communications between its many parts. Private data won't be processed by the Web Service directly. Before any data is uploaded to the Web Service, it will be encrypted as a ciphertext. The SC will be deployed on the EVM, which would make up the ticketing system. The ticketing SC would accept digital tokens and issue a non-fungible instance of the electronic ticket using asymmetric encryption, SHA-256 encryption, and ERC-721 techniques.

To address the privacy concern and data protection, the IPFS will be used in this work as a decentralized storage solution, thereby making the system fully decentralized. The ticket verification system is designed to scan the QR code presented at the point of admittance and decode the encrypted data which will be used to verify the authenticity of the ticket. The ticket verification system will be able to interact with the ticketing SC to validate a ticket by verifying if the encrypted SHA-256 data decoded from the QR code presented at the point of admittance was generated by the ticketing contract since the blockchain network is a distributed ledger that contains an immutable record of all ticket transactions. The function of the verification system is to check if the decoded information was generated by the ticketing contract on the basis that all transactions signed to the SC are recorded on the blockchain network since the most reliable way to verify if a transaction is absent is to be aware of every transaction. An administrative user interface would be designed that would be able to give an error message if the decoded transaction information is not recorded on the blockchain network and a success message if the transaction is a valid one.

The SC would have to implement the ERC-721 standard, which allows for creating multiple classes of tokens within the same SC. It would have a function that accepts ether tokens as payment and encrypts the transaction hash to the customers' public key resulting to a unique hash digest that represents a non-fungible instance of the ticket. This non-fungible token is indexed on the SC which represents the token ID.

The SC deployment can be summarized in the highlighted sequence:

a. Create an ERC-721 SC on the Ethereum blockchain that manages ticket sales and distribution. ERC-721 SC standard allows for unique and non-fungible tokens, which is perfect for single-user type tickets.
b. Ticket information, such as ticket type, validity period, amount, and the owner of the ticket, which makes up the identity proof, will be uploaded to the IPFS.
c. To purchase a ticket, the user interacts with the SC, transfers ERC-20 tokens to the contract address, and specifies the type of ticket they want to purchase.
d. The SC mints a unique token that represents the ticket, assigns the token to the user's Ethereum address and also stores the ticket information on IPFS, and associates it with the unique token ID.
e. The SC returns a QR code, which encodes the IPFS hash and the unique token ID, to the user.
f. When the user wants to access the service or product, they present the QR code to the service provider, who scans the code and retrieves the ticket information from IPFS.
g. Upon verification of the ticket's authenticity, validity is checked by the service provider, who can then grant the user access to the service or product.
h. Once the user has used the ticket, the SC will mark the token as "used" and it cannot be used again.

IPFS library is used to upload the encrypted hash to the IPFS network. The SC would have to keep the mapping of each minted token to the IPFS address where the ticket was uploaded. The SC would also implement a transfer function that allows transferring the ownership of the minted token.

From the sequence diagram, as shown in Figure 2, the ticketing organization represents the ticket issuer and is a major participant in the system. The ticket issuer deploys the SC on the EVM. With the help of suitable web technologies, the SC is integrated with the consumer client. The user sends a purchase request via the consumer client; the purchase request contains the ticket type, amount, and validity period encrypted as cypher text to ensure data privacy and security. The request triggers the SC, the ticket is generated and the ticket ID is encrypted to the public key of the buyer as the owner. The corresponding ticket evidence information is uploaded to the IPFS, and the consumer client displays a QR string containing the corresponding hash of the metadata. The ticket owner has to authorize the ticket to be able to be spent before it can be marked as used by the back-end administrative client. At the point of admittance, the administrative back end decrypts the ticket evidence information and checks if the ticket ID is valid, has not expired, and has been authorized to be spent by the owner. The administrator can go ahead and mark the ticket as used if these three conditions are met. The administrative back end is also called a read function that listens to all events that occur on the SC and can be used for audit purposes.

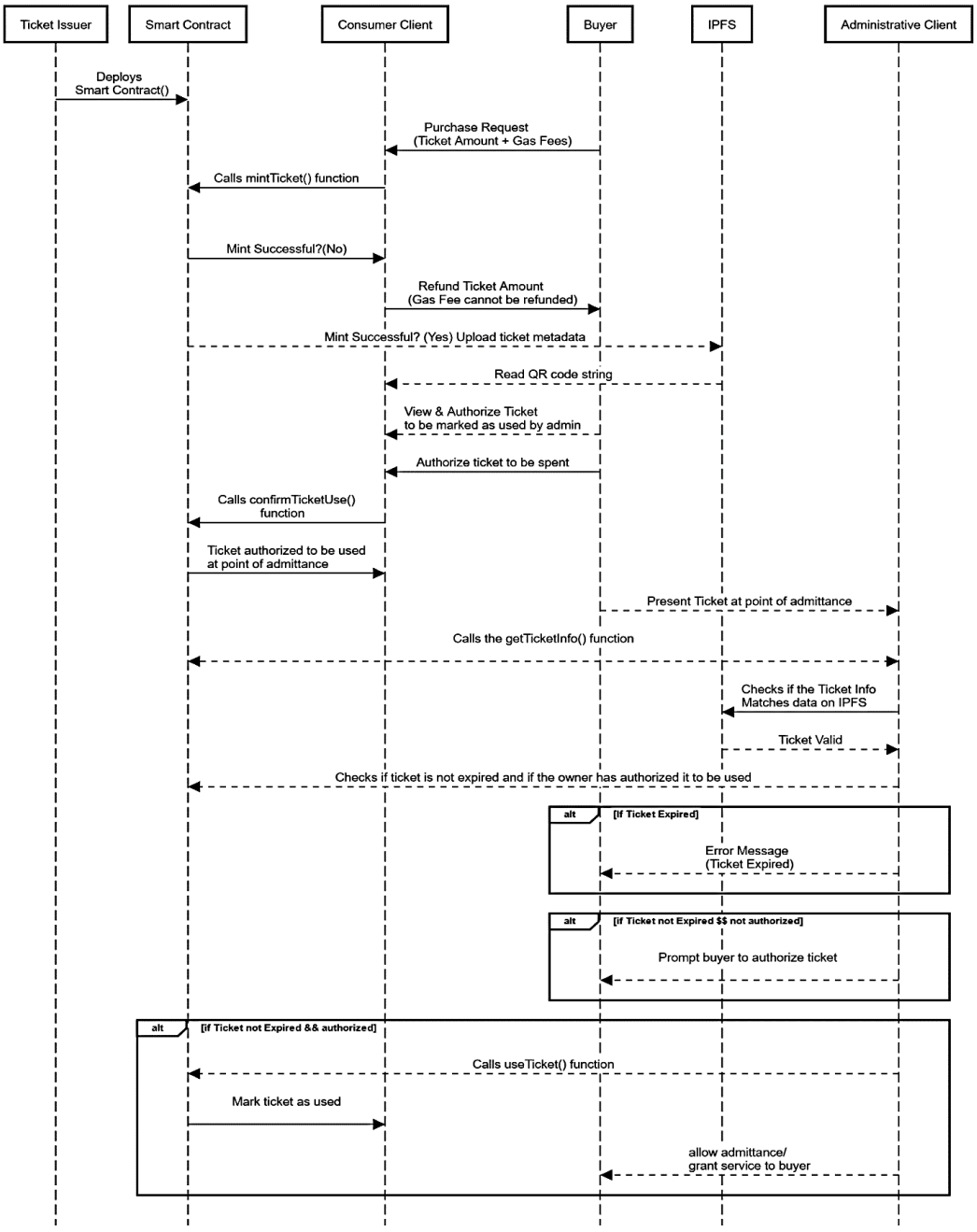


Figure 2. Sequence diagram of the proposed ticketing system

Various functions that make up the ticketing SC can be classified as either read or write functions [28]. Read functions are used to request or query data and information about certain variables based on the current state of the EVM write functions on the other hand are functions that can change the state of certain variables and parameters stored on a blockchain. For a participant on the blockchain to be able to send a transaction that alters the state of the EVM they have to satisfy certain cryptographic conditions and verification mechanisms based on elliptic curve cryptography (ECC). Table 1 shows the classification of all functions featured in the SC.

Table 1. Classification of SC functions

Function	Functionality	Read	Write
mint ( )	Used to create and mint new tickets		✓
confirmTicketUse ( )	Used by the ticket owner to authorize the use of the ticket by the administrative client		✓
useTicket ( )	Can only be called by the owner/deplorer of the contract and is used to mark the ticket as used at the point of admittance		✓
getUsedTickets ( )	Returns an array of ticket ids that have been marked as used by the system	✓	
getBalance ( )	Returns the balance of the contract	✓	
withdraw ( )	Used by the admin to withdraw to the balance of the SC.		✓
getTicket ( )	Used to get the details of a ticket by its ID	✓	

4. RESULTS AND DISCUSSION

The obtained results regarding the development of the ticketing system presented in this paper are discussed in this section. The approach presented in this paper clearly shows that the SC on the EVM is the spine of the ticketing system. A detailed empirical analysis of the entire framework is presented, providing insights into information regarding its effectiveness at tracking and automating ticket sales, security, reliability, and traceability of ticket information while ensuring consumer data is private and secure.

4.1. Performance evaluation

The performance of the SC was evaluated using two major metrics:

- The mean ticket purchase request completion time – which is the average time duration it takes to complete ticket evidence generation from the initiation of the purchase request and
- The mean ticket verification time – which is the average time it takes to verify a ticket presented at the point of admittance and mark it as used [4].

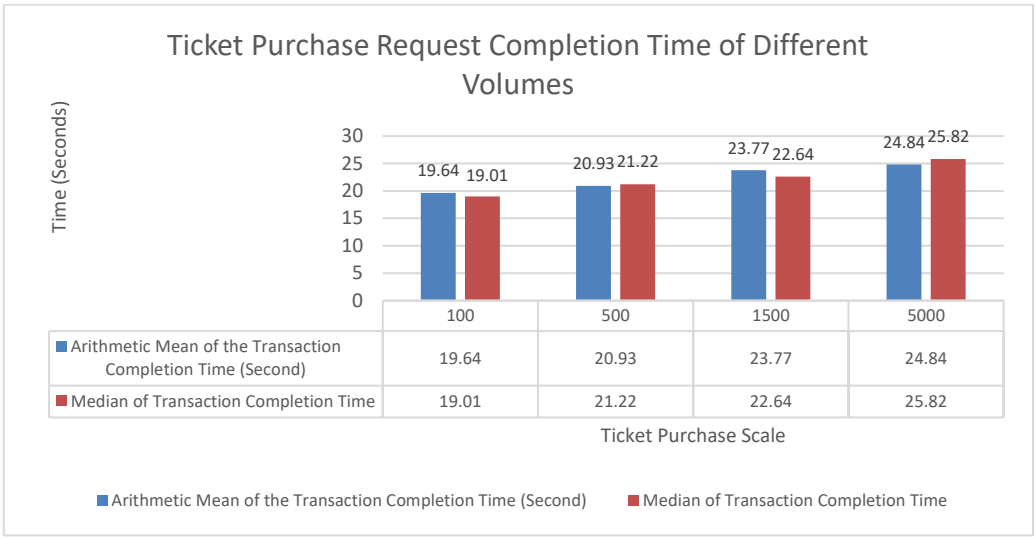
Figure 3 clearly shows the mean and median ticket purchase transaction completion time. A ticket purchase request completion time was mainly the benchmark for evaluation since it measures the speed and efficiency at which ticketing transactions may be executed. A series of ticket purchase requests were simulated on the SC to test the system's ability to handle large volumes of ticket purchases and transfers, as well as its resilience to network congestion and other common issues. As can be seen in Figure 3(a) the completion time of a purchase request increases with the scale of purchase requests. The mean and median completion time for ticket purchase for a volume of 5,000 tickets is 24.84 seconds and 25.82 seconds respectively.

The administrative client was also investigated to evaluate the performance and efficiency of ticket verification, validation, and admittance. The average verification completion and the average time it takes to authenticate ticket evidence information presented at the point of admittance were used as a metric for evaluating the administrative client. We experimented to determine the average transaction completion time of a ticket verification, a reduced timeframe for transaction completion would indicate a model with capabilities of processing a higher number of transactions. As clearly seen on Figure 3(b) the mean and median completion time for ticket verification for a volume of 5,000 tickets is 3.91 seconds and 3.66 seconds respectively.

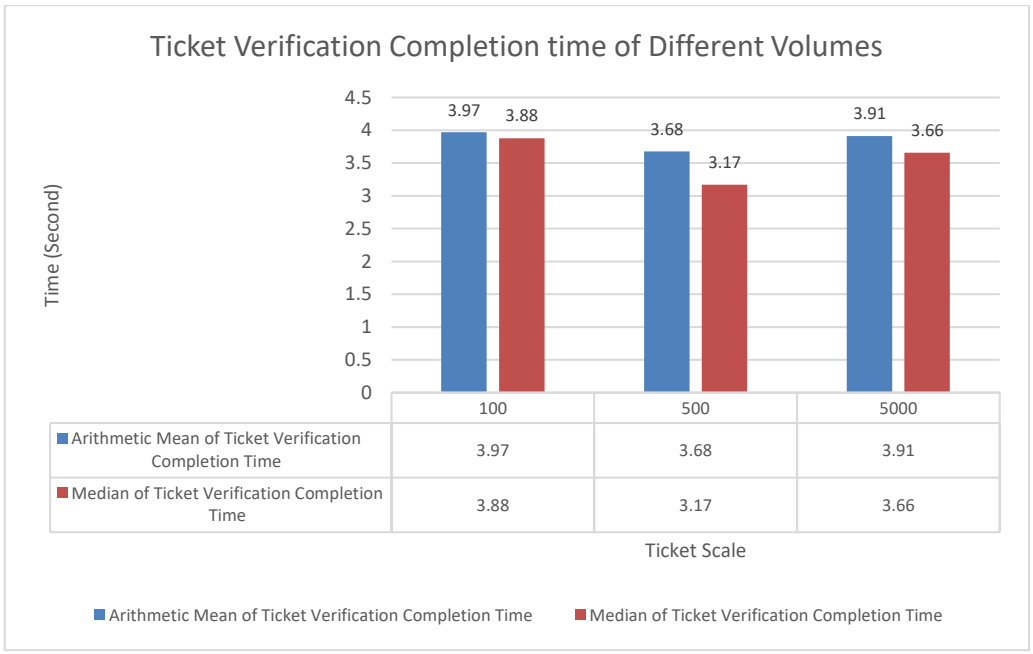
4.2. Security analysis

The EVM and the various cryptographic approaches utilized in this study contribute largely to the overall security of the model. Illegal transactions will not be appended to the blockchain network until at least 50% of all nodes respond honestly. Due to the ECDSA techniques and ERC721 standards for developing SCs', the model can operate as intended. Users are identified by their public/private key pair. Only a user's private key can be used to decrypt encrypted ticket information of that particular user and also authorize write operations (such as authorizing the ticket to be marked as used by the administrative client) using a digital signature algorithm (DSA). This means a malicious actor cannot access ticket data, or purchase tickets unless they gain access to the user's private key. The system incorporates cryptography to mitigate the risks of man-in-the-middle (MITM) attacks and replay attacks. Unauthorized individuals lacking the authorized private key are unable to forge a signature by substituting an alternative public key in place of

the authorized ticket owner's key. Hence, only the legal owner of a ticket can authorize the ticket to be marked as used by an administrator at the point of admittance.



(a)



(b)

Figure 3. Completion time for; (a) ticket purchase request and (b) ticket verification

4.3. Integrity and reliability

Due to the nature of SC, once an SC is deployed to the blockchain network its code is immutable and resides on the blockchain forever. Although a destruct function can be used to deactivate the SC and render its code inoperable. The code stays on the blockchain immutably. This ensures that the code cannot be altered by the deplorer thereby increasing the integrity of the model and customers can trust the system to always function as it should. Integrity is a vital component that ensures data is not altered. Immutable transaction logs give participants to trace and locate a particular event. The architecture of blockchain ensures the authenticity of every message exchanged between participants and the immutable log of events that are produced.

4.4. Trust

The need for trust is eliminated as the whole ticketing process is automated by lines of code that cannot be changed. The security measures that are blockchain built-in, apply to the system. Trust, transparency, immutability, traceability, integrity, and decentralization are all incorporated and apply to the system directly. Only authorized participants can interact with the model and call specific actions since the proposed model manages authentication and access control through cryptographically signed and time-stamped messages.

4.5. Privacy

The EVM public blockchain architecture ensures a consumer's true identity remains undisclosed to the public, which allows users to purchase tickets without revealing any personal data by utilizing a public/private key pair to authenticate transactions and prove ownership of data on the blockchain.

4.6. Benchmark with existing results

Although similar works utilize blockchain technology, albeit with different variations, to enhance security, transparency, and immutability. However, the main point of differentiation lies in the type of blockchain employed, which indicates that other related works are still in the conceptual or developmental phase. Additionally, only [26] provides a consumer client for evaluation, limiting the scope for direct comparison in terms of user experience.

The proposed ticketing model was evaluated against five similar works. Liu [4] utilized a public and private blockchain, while three employed a private blockchain. Although the systems utilized blockchain technology to address a targeted problem, they still function in a centralized manner. It is crucial to emphasize that only [26] deployed their system, and provided a consumer client for evaluating various key aspects, including transaction time, throughput, and overall efficiency, although their work did not highlight that. Out of the five similar works, only [26] successfully deployed their ticketing system. The proposed ticketing model in this research work boasts a mean transaction completion time of 19.64 seconds. This performance metric is considerably faster compared to the other works, which were not explicitly mentioned. The improved transaction time is likely attributed to various factors such as optimized SC execution, efficient consensus mechanisms, and the type of blockchain environment in which the model was deployed. In terms of throughput, the proposed ticketing model demonstrates superior performance with a throughput of 20,000 transactions per second (TPS). This outperforms [4], which reported a comparably lower throughput of 14 transactions per minute (TPM). The higher throughput of the proposed model can be attributed to its optimized system design, efficient block validation of the EVM, and potentially the DSA utilized in this research work.

Table 2 clearly illustrates a summary of the comparative analysis conducted in this section; We evaluated the proposed ticketing model against five similar works that function in a centralized manner. While two of the works used a public blockchain and three employed a private blockchain, all systems aimed to enhance security and transparency through the employment of blockchain technology. Notably, the proposed ticketing model demonstrated a significantly faster mean transaction time of 19.64 seconds and a higher throughput of 20,000 TPS compared to the reported 14 TPM by [4].

Table 2. Benchmark with existing results

Work done	Public block-chain	Private block-chain	Targeted problem	Consumer-application interface	Throughput	Mean transaction completion time	Mean ticket verification time
[23]	No	Yes	Ticket privacy preservation	No	No	No	No
[24]	No	Yes	Event ticketing	No	No	No	No
[25]	No	Yes	Macro event ticket booking	Yes	No	No	No
[4]	Yes	Yes	Event ticketing scalping	No	14 TPM	No	No
[26]	Yes	No	Event ticket scalping	No	No	No	No
Proposed system	Yes	No	Fully decentralized single-user ticketing (ticket traceability, security, privacy and authenticity)	Yes	20,000 TPS	19.64 seconds	3.17 seconds

5. CONCLUSION

This paper presented a fully decentralized software system for issuing and verifying single-user type tickets using blockchain technology. To mitigate the problem of trust, decentralization, traceability, and security, this paper introduces an electronic ticketing approach using cryptographic algorithms implemented with blockchain technology, the ERC721 standard for SC, and IPFS Technology. The sales, tracking, and

automating transactions are handled and governed by the SC on the EVM. The security and integrity of the system are ensured using ECC, SHA, and DSA to generate ticket evidence.

ACKNOWLEDGEMENTS

The authors acknowledge partial assistance from the Covenant University Centre for Research, Innovation, and Discovery (CUCRID), Ota, Ogun State, Nigeria.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Kennedy Okokpujie	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Oghenetega Owivri	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Olamide Olusanya	✓		✓	✓			✓			✓	✓		✓	✓
Samuel Daramola1	✓		✓	✓			✓			✓	✓		✓	✓
Morayo E. Awomoyi					✓		✓			✓		✓		✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

It is not applicable.

ETHICAL APPROVAL

It is not applicable.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] Y. Xu, H. Y. Chong, and M. Chi, "A Review of Smart Contracts Applications in Various Industries: A Procurement Perspective," *Advances in Civil Engineering*, no. 1, Jan. 2021, doi: 10.1155/2021/5530755.

[2] L. Finžgar and M. Trebar, "Use of NFC and QR code identification in an electronic ticket system for public transport," in *2011 International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2011*, 2011, pp. 81–86.

[3] J. D. Preece and J. M. Easton, "Blockchain Technology as a Mechanism for Digital Railway Ticketing," in *Proceedings - 2019 IEEE International Conference on Big Data, Big Data 2019*, IEEE, Dec. 2019, pp. 3599–3606, doi: 10.1109/BigData47090.2019.9006293.

[4] M. Liu, "A Hybrid Blockchain-Based Event Ticketing System," M.S. thesis, Department of Computer Science, University of Saskatchewan, Saskatoon, Canada, 2021.

[5] O. C. Owivri, K. O. Okokpujie, S. Daramola, and A. U. Adoghe, "A Decentralized Framework for Issuing Electronic Exam Pass Using Hyperledger Fabric," in *International Conference on Science, Engineering and Business for Driving Sustainable Development Goals, SEB4SDG 2024*, IEEE, Apr. 2024, pp. 1–6, doi: 10.1109/SEB4SDG60871.2024.10630342.

[6] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.
[7] P. Ewejobi, K. Okokpujie, E. Adetiba, and B. Alao, "Homomorphic Encryption for Genomics Data Storage on a Federated Cloud: A Mini Review," in *International Conference on Science, Engineering and Business for Driving Sustainable Development Goals, SEB4SDG 2024*, IEEE, Apr. 2024, pp. 1–13, doi: 10.1109/SEB4SDG60871.2024.10630232.
[8] M. Xu, X. Chen, and G. Kou, "A systematic review of blockchain," *Financial Innovation*, vol. 5, no. 1, pp. 1–14, Dec. 2019, doi: 10.1186/s40854-019-0147-z.
[9] J. Frizzo-Barker, P. A. Chow-White, P. R. Adams, J. Mentanko, D. Ha, and S. Green, "Blockchain as a disruptive technology for business: A systematic review," *International Journal of Information Management*, vol. 51, Apr. 2020, doi: 10.1016/j.ijinfomgt.2019.10.014.
[10] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, [Online]. Available: https://git.dhimmel.com/bitcoin-whitepaper/.
[11] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, IEEE, Jun. 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.
[12] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016, doi: 10.1109/COMST.2016.2535718.
[13] I. Simplice, O. Fidel, C. G. Kennedy, K. Okokpujie, and S. Gabriel, "Enhancing Information System Security: A Vulnerability Assessment of a Web Application Using OWASP Top 10 List," in *Lecture Notes in Networks and Systems*, vol. 914, pp. 385–397, 2024, doi: 10.1007/978-981-97-0573-3_31.
[14] D. Nadler Prata, H. X. de Araújo, and C. Santos, "A Literature Review about Smart Contracts Technology," *International Journal of Advanced Engineering Research and Science*, vol. 8, no. 2, pp. 001–004, 2021, doi: 10.22161/ijaers.82.1.
[15] A. Pinna, S. Ibba, G. Baralla, R. Tonelli, and M. Marchesi, "A Massive Analysis of Ethereum Smart Contracts Empirical Study and Code Metrics," *IEEE Access*, vol. 7, pp. 78194–78213, 2019, doi: 10.1109/ACCESS.2019.2921936.
[16] V. Y. Kemmoe, W. Stone, J. Kim, D. Kim, and J. Son, "Recent Advances in Smart Contracts: A Technical Overview and State of the Art," *IEEE Access*, vol. 8, pp. 117782–117801, 2020, doi: 10.1109/ACCESS.2020.3005020.
[17] V. Buterin, "Ethereum white paper". GitHub repository. 2013 Jan;1(22-23):5-7. Accessed October 10, 2024 https://static.peng37.com/ethereum_whitepaper_laptop_3.pdf
[18] S. V. Hoseini, "Mathematics and Data Structures in Blockchain and Ethereum," M.S. thesis, Department of Future Technologies, University of Turku, Turku, Finland, 2018.
[19] W. Zou *et al.*, "Smart Contract Development: Challenges and Opportunities," *IEEE Transactions on Software Engineering*, vol. 47, no. 10, pp. 2084–2106, Oct. 2021, doi: 10.1109/TSE.2019.2942301.
[20] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," *arXiv*, 2014, doi: 10.48550/arXiv.1407.3561.
[21] J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, and J. Herrera-Joancomartí, *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, in Lecture Notes in Computer Science, Cham: Springer International Publishing, 2017, vol. 10436, doi: 10.1007/978-3-319-67816-0.
[22] C. Elsden, A. Manohar, J. Briggs, M. Harding, C. Speed, J. Vines, "Making sense of blockchain applications: A typology for HCI," in *CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1-14, doi: 10.1145/3173574.317403.
[23] S. C. Cha, W. C. Peng, T. Y. Hsu, C. L. Chang, and S. W. Li, "A Blockchain-Based Privacy Preserving Ticketing Service," in *2018 IEEE 7th Global Conference on Consumer Electronics, GCCE 2018*, IEEE, Oct. 2018, pp. 585–587, doi: 10.1109/GCCE.2018.8574479.
[24] K. P. Lin, Y. W. Chang, Z. H. Wei, C. Y. Shen, and M. Y. Chang, "A smart contract-based mobile ticketing system with multi-signature and blockchain," in *2019 IEEE 8th Global Conference on Consumer Electronics, GCCE 2019*, IEEE, Oct. 2019, pp. 231–232, doi: 10.1109/GCCE46687.2019.9015425.
[25] D. H. Ko, H. K. Choi, and K. S. Kim, "A Design and Implementation of Macro Prevention Ticket Booking System Using Blockchain," in *ACM International Conference Proceeding Series*, New York, NY, USA: ACM, Feb. 2020, pp. 95–98, doi: 10.1145/3387263.3387277.
[26] S. R. Niya, S. Bachmann, C. Brasser, M. Bucher, N. Spielmann, and B. Stiller, "DeTi: A Decentralized Ticketing Management Platform," *Journal of Network and Systems Management*, vol. 30, no. 4, pp. 1–40, Oct. 2022, doi: 10.1007/s10922-022-09675-3.
[27] A. Aldweesh, "BlockTicket: A framework for electronic tickets based on smart contract," *PLoS ONE*, vol. 18, pp. 1–20, Apr. 2023, doi: 10.1371/journal.pone.0284166.
[28] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F. Y. Wang, "An Overview of Smart Contract: Architecture, Applications, and Future Trends," in *IEEE Intelligent Vehicles Symposium, Proceedings*, IEEE, Jun. 2018, pp. 108–113, doi: 10.1109/IVS.2018.8500488.

BIOGRAPHIES OF AUTHORS

Dr. Kennedy Okokpujie holds a Bachelor of Engineering (B.Eng.) in Electrical and Electronics Engineering, Master of Science (M.Sc.) in Electrical and Electronics Engineering, Master of Engineering (M.Eng.) in Electronics and Telecommunication Engineering and Master of Business Administration (MBA), Ph.D. in Information and Communication Engineering, besides several professional certificates and skills. He is currently lecturing in the Department of Electrical and Information Engineering at Covenant University, Ota, Ogun State, Nigeria. He is a member of the Nigeria Society of Engineers and the Institute of Electrical and Electronics Engineers (IEEE). His research areas of interest include biometrics, artificial intelligence, and digital signal processing. He can be contacted at email: kennedy.okokpujie@covenantuniversity.edu.ng and kenjie451@gmail.com.

Oghenetega Owivri holds a Bachelor of Engineering (B.Eng.) in Electrical and Electronics Engineering and a Master of Engineering (M.Eng.) in Computer Engineering, among other professional certifications. He is an Assistant lecturer and on his Ph.D. in the Department of Electrical and Information Engineering at Covenant University, Ota, Ogun State, Nigeria. His research areas of interest include blockchain, cryptography, software engineering, and cyber security. He can be contacted at email: oghenetega.owivri@covenantuniversity.edu.ng.

Olamide Olusanya holds a Bachelor's degree in Computer Engineering from Ladoke Akintola University of Technology, Ogbomoso, Nigeria, in 2008. Following this, she obtained a Master's degree in Computer Science from the University of Lagos in 2011, and a Ph.D. in Computer Science in 2017 from Ladoke Akintola University of Technology, Ogbomoso, where she researched the modeling of bank cash deposit transactions using Hierarchical Timed Colored Petri Nets. This research allowed her to explore the intricate dynamics of financial systems and their interactions with technology, equipping her with expertise in system modeling and simulation. Her main interest is in system modeling and simulation and her minor area includes embedded system design and information systems. She is currently lecturing in the Department of Computer Engineering at Bells University of Technology, Ota, Ogun State, Nigeria. He is a member of the Nigeria Society of Engineers and the Institute of Electrical and Electronics Engineers (IEEE). She can be contacted at email: ooolusanya@bellsuniversity.edu.ng and olamide4jc@yahoo.com.

Prof. Samuel Daramola is a Professor of Computer Engineering. He obtained Ph.D. from Covenant University in the year 2008. He obtained Master degree in Engineering (M.Eng.) and Bachelor degree in Engineering (B.Eng.) from University of Portharcourt in 2002 and Ondo State University in 1997 respectively. He is former Dean of Engineering, Director of Information Communication Technology (ICT) and Head of Computer Vision research group at Achievers University Owo. Currently. He is a lecturer at Department of Electrical and Information Engineering (EIE), College of Engineering, Covenant University Canaan Land, Ota, Nigeria. His research area is computer vision, web-application, biomedical image processing, and software development. He is a member of the Nigeria Society of Engineers (NSE) and the International Association of Engineers (IAENG). He can be contacted at email: samuel.daramola@elizadeuniversity.edu.ng

Morayo E. Awomoyi is a dedicated advocate for social transformation, holding a master's degree in International Peace and Conflict Resolution from American University in Washington, D.C. With a strong academic foundation and a passion for driving meaningful change, she focuses on the intersection of peacebuilding, social justice, and community empowerment. Throughout her career, she has explored innovative approaches to addressing systemic inequalities, fostering inclusive dialogue, and promoting sustainable peace in diverse contexts. She brings a global perspective to local challenges, drawing on both theory and practical engagement in the field of conflict resolution through statistical analyses. Guided by the belief that lasting peace is rooted in equity and social change, she collaborates with communities, organisations, and policy-makers to cultivate environments where justice and human dignity thrive. She can be contacted at email: ma8161b@american.edu.