International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Research Paper Volume-10, Issue-4 ,2023 Regular Edition E-ISSN: 2349-7084

Digital Railway Ticketing Using Ethereum and Smart contracts

D.Bhanu Sravanthi [1], P. Venkata Krishna [2]

[1] *Research Scholar,Dept of computer science & engineering,SPMVV,Tirupati*
[2] *BOS Chairman (CSE), Dept of computer science & engineering,SPMVV,Tirupati*

e-mail: dsravanthi.bs@gmail.com . pvk@spmvv.ac.in

**Corresponding Author: D.Bhanu Sravanthi*

https://doi.org/10.22362/ijcert/2023/v10/i04/v10i0404

Received: 11/03/2023, Revised:04/04/2023, Accepted: 11/04/2023 Published:28/04/2023

Abstract:-Blockchain is a technology that allows for the secure exchange of values. It is made up of a "chain" of data packets that cannot be changed later. With blockchain technology, transactions between two parties may be efficiently and authentically recorded in an open distributed digital ledger. It uses a secure peer-to-peer technique in which verification and validation are carried out by the dispersed network's nodes rather than depending on a third trusted entity, such as a bank. This technology decreases the additional transaction costs that Third Parties suffer in addition to doing away with the need for them altogether. Blockchain based digital ticketing makes it possible to quickly create refundable, transferable, and traceable tickets. It might be used to the rail sector for intelligent ticketing and open, effective supply networks. It also improves security, ensures ticket validity, and gives you more power over the secondary market. This article describes an innovative blockchain-based digital ticketing network. We employ ether and smartcontracts after considering numerous factors such as ticket issuing platforms and earlier attempts at digital rail ticketing. Passengers can purchase tickets using an Ethereum wallet, and each passenger's address is saved in the blockchain along with the ticket price.

Keywords: Distributed ledger, Ethereum, Smartcontracts,Peer-to-peer

---

1. Introduction

This report discusses the potential of blockchain technology as a digital rail ticketing system. Background information on blockchain technology and train ticketing is given in Section I. The existing platform's requirements are discussed in Section II. The new platform design and functions are discussed in section III.Section IV provides the smartcontract-based train ticketing architecture. Part V talks about the conclusion and future work.

1.1 Background Information on Blockchain Technology and Train Ticketing:

Blockchain: Blockchain is a decentralized database that maintains an ever-growing collection of sequentially organised documents called blocks that are connected together via encryption. Each block contains the date, an encryption hash of the previous block, and transaction data. A blockchain is a decentralized, distributed, and open digital log that is used to track activities across many computers using a way that the record cannot be changed retrospectively without changing all valid transactions and receiving network consent.

Train Ticketing:

The Passenger Experience: There are two distinct ways for passengers to buy tickets when using the railways: either at any station on the network using cash or a credit card (henceforth referred to as station purchase), or online (henceforth referred to as online purchase). In contrast to online purchase, which avoids the need to use station amenities and enables the passenger to buy a ticket via a browser or a customised phone application, station purchase allows passengers to buy from a machine or (where accessible) at the ticket office from a member of staff. Depending on how they were purchased, the passenger then gets their passes. If a customer selects station purchase, a paper ticket is printed at the point of sale by the machine (or a staff member at the ticket office). Passengers can print tickets online using a personal printer at home, at a terminal machine or employee, or in specific circumstances, downloaded as an m-Ticket. While riding a train, passengers validate their tickets with a conductor as they approach or exit stations. A staff member verifies the ticket by looking up the person's information and the specific PNR number.

2. Existing System

Ethereum smart contracts are utilized in digital railway ticketing to handle challenges such as detecting the legitimacy of tickets acquired online (which can be fake or copies of real tickets), the broad price variance of tickets sold again in the resale market, and cumbersome return procedures. Although ticket prices are normally determined by organizers, each reseller is free to set their own.

Tickets purchased on the primary market are traded on the secondary market for a different price, based on demand. Brokers and dishonest dealers will sometimes charge exorbitant prices for their tickets, particularly when it comes to famous railway ticketing. These deals greatly help secondary market sites, which occasionally participate in the "black market." Secondary market inventory sales, in which tickets are frequently purchased by automatic algorithms and rapidly resold at a higher price using a strategy known as scalping, are beyond the control of the organizers.

Digital tickets are easy to copy, and there is no safe way to check a ticket's authenticity prior to purchase. Tickets is occasionally purchased by unlicensed resellers, who then list them on different websites. If a ticket is not removed from the other sites after it has been sold, it may be offered again.

The smart contracts built and executed on top of Ethereum 2.0 serve as the foundation for code execution. Ethereum is version 2.0 of Bitcoin, which was intended in version 1.0 for peer-to-peer wealth exchange. Smartcontracts enable decentralised apps to do more than just transfer cash. Contracts are carried out when certain requirements are satisfied, and the outcomes are traceable and irreversible. They can be seen as "protocols" that transactions' internal messages use to start them. overcomes issues with fake tickets, ticket scalpers and bots, security and data, as well as digital train ticketing.

3. Proposed System

Today, the structure of ticketing data is primarily viewed as ticketing protocol. With a digital system, you can track tickets outside of the scope of a single provider and exchange customer information, providing you a crucial tool for managing the market.

Detailed Documents:

Knowledge really is strength when it comes to digital tickets. Ticket issuing portals can identify ticket buyers, view all previous transactions, and determine whether a ticket has been resold and at what price by giving the complete history of ticket transactions. This lowers operational and fraud expenses.

Regulation of the Secondary Market:

Globally, governments are closely examining the resale ticket market. The solution is digital passes. By issuing digital tickets, the transfer of tickets is controlled, the right price is established, and resale restrictions are imposed. It also aids in limiting the influence of scalpers.

Managing the Ticket Flow:

You will be able to track the sale of seats using digital tickets, whether they are blockchain-based or not. The origin of a ticket can be tracked and verified, providing a foundation for compliance and dispute settlement.

Fraud Avoidance: Every ticket that passes through the blockchain is given a unique "identity," and if customers want to resell or move the ticket, they must do so once more.

4. Smart contract-Based Train Ticketing Architecture

We need an open enrollment step to govern the resale market, which means ensuring that our system is only utilised by legitimate user and not, for example, bots. It only has to be done occasionally, by a centralized computer, which must check the legality of any identification given by the user (such as a passport scan) as well as the holding of the Ethereum account. Upon initial authentication, the verified Ethereum account is added to the smartcontract Validated Addresses; it should be mentioned that, for security reasons, user true identities are never never broadcast in the blockchain platform.

Once authenticated, an EthereumAddress may be used to purchase and trade tickets, as demonstrated in Figure 1. The two jobs are handled by smartcontracts. This design choice ensures that the system is accessible and that anybody can verify the legitimacy of the tickets, which is a core requirement that more traditional approaches do not fulfil; in practise, fraudsters regularly provide phoney tickets. Any

registered address holder can buy or sell tickets without the need for a middleman.

The secondary market for each train ticketing is under the management of its promoters, who have the authority to set price restrictions on reselling tickets. Additionally, because tickets are available to the general public, purchasers are free to select the vendor with the best deal.

If a person has to trade his or her ticket & the railway ticketing organiser agrees to accept the transaction in advance, a private sale is conceivable using a same process. The user promoting the tickets must specify the booking fee within the allowed range and publicise the bargain. When a ticket is sold, the buyer is given a new one, rendering the old one invalid.

The lower part of Figure 1 describes how to utilise a train ticketing system. Before the train ticketing process starts, ticket data is mirrored in a database that gatekeeper devices can view simultaneously. Because requiring continuous internet connectivity can be problematic in some venues, this allows an offline validation.

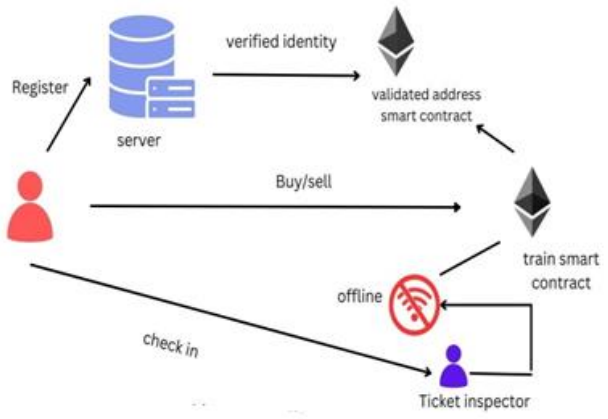

Figure 1. System Architecture

A. Registration:

Users must, as expected, register on a central server before using our technology. Only this aspect of digital railway tickets is centralised; the rest is spread across Ethereum via smartcontracts. The registration process is critical for validating Ethereum Addresses because it confirms that each user corresponds to a real individual and that no user can register more than one EthereumAddress. Every person is the owner of the specified EthereumAddress. The third condition acts as a "sanity check" to make sure that the location that has been confirmed can actually be used. The first two conditions must be satisfied in order to prevent train ticket scalping.

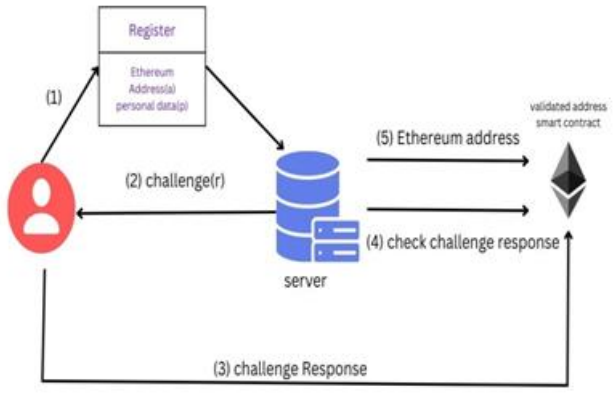

Figure 2. Successful Registration

The procedure to create a new user/address pair with a server is shown in Figure 2:

(1) User 'u' makes a validation request, including an Ethereum Address, some personal info, and identification documentation (such as a passport ID). If a subject to the following used the same real-world name during this phase of the procedure, the request would be refused immediately.

(2) The server checks 'p' in some way before sending a challenge to user with a random integer'r'. This is a simple technique to certify that you genuinely possess 'a';

(3) You have a limited amount of time to transfer r to the smartcontract. using a list of verified locations;

(4) After validating that the challenge answer was received successfully, 'S' can add a to the smartcontract's Validated Addresses and the link (a,p) to its own private database.

(5)A private database must be used to protect the privacy of authorised users while permitting the registration of the same real-world identity at numerous locations.

Only the system owner has the power to add or remove addresses from the Validated Addresses contract. To ensure this, their EthereumAddress is saved in the ValidatedAddresses function and is compared to the senders' addresses prior to any action being taken.

B. Purchase of tickets

The ingenious design Users can engage with train purchasing through a variety of apps, websites, and even straight from their Ethereum wallet. Railway ticketings is the business in charge of offering tickets to users. Although the contract covers both the main and secondary markets, we will only address the primary market here. Much like the administration of smartcontract Validated Addresses, the creating of new train tickets is limited to the address that created a contract.

The attributes kept in the smartcontract-specified objects explain how train tickets are allocated. These properties should include the identifier, title, and summary of the train ticketing, the various ticket types and prices, the start and stop times of the selling process, the maximum number of

locations at which a single user may purchase tickets, and an array of buyers identified by their Ethereum network addresses.

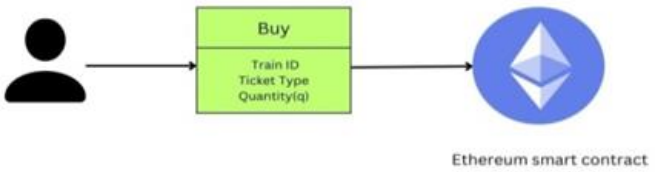

Figure 3. Ticket Purchase

Figure3 indicates that the buyer must activate the smartcontract function purchase. railway tickets with the following information: the requested train ticketing's key, the ticket class, the quantity 'q', and a list of 'k' hash values (t1,..., tk), where 1 k q. Each 'ti' is the unique identifier for the ith ticket, and it is generated by hashing the ith owner's name and a random value 'ri', as in 'ti' = h(ni +ri), where 'h' is a cryptographic hash function and the + stands for string concatenation. Furthermore, depending on whether k = q, each ticket may allow access for either a person or a group.The following checks are carried out when the smartcontract train ticketings gets the transaction calling the function buy

- Is the buyer's location accurate? Has it already been verified in the ValidatedAddresses contract, in other words?
- Does the present moment fall within the selling window for this specific train ticketing? Do there still be enough spots?
- Does this user still fit within the user limit for this specific train ticketing if q more places are added to him?
- Is there enough eth in the mixture?
- Are all t1,...,., tk IDs distinct and not used for railway ticketing? This check may appear useless because a collision in the hash ‘h’ should never be discovered if values ‘ri’ are genuinely chosen at random. But this verification ensures that none can erroneously "duplicate" a ticket that already exists.
- If every check is successful, the contract will record every aspect of this transaction in the train ticketing's data structure. If not, the contract reverts and returns the funds to the buyer's Ethereum account.

C. Access to the train ticketing

The following restrictions should be taken into consideration when defining the train ticketing access procedure:

• Because writing to the blockchain is sluggish, we are unable to invalidate used tickets using blockchain (by design)

In some settings, having constant Internet connectivity can be problematic.

• While most participants today bring their smartphones, occasionally they are not accessible or the batteries run out.

We therefore created a system that not only require Internet connectivity but also permits access to the train ticketings only through paper.

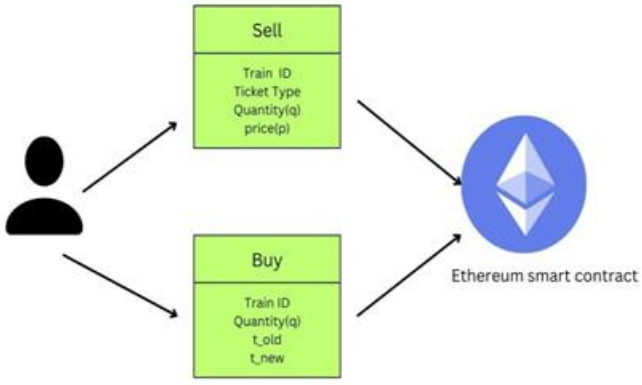

Figure 4. Secondary market

Figure 4 outlines the process for gaining entry to an train ticketing: Prior to the train ticketing (after the selling period), the blockchain dumps ticket data into a database server that gatekeeper devices can use to verify ticket validity and keep track of used tickets. The inability to offer last-minute tickets at the train ticketing's location is one disadvantage of this strategy.

D. The second-hand industry

The concept of a managed secondary market is advantageous to both train ticketing organisers and private purchasers who may need to sell their tickets for personal reasons as well as those looking to purchase seats at the last minute without running the risk of being taken advantage of.

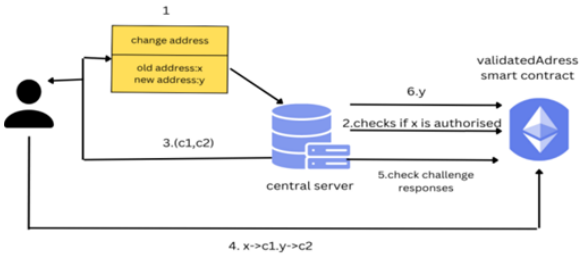

Figure 5 illustrates the sale process using a smartcontract.

describing the train ticketing identity, the number of tickets to be sold, the amount of tickets to be sold, and the ticket number ‘q’, all of which must be within the organiser-determined price limit to prevent train ticketing scalping.

A seller can cancel a sale at any moment, up until the ticket is transferred to another client, by calling cancel_Sale

and providing the ticket identifier. k. All previous purchases are immediately annulled prior to the issuance of railway tickets.By using the operation buySecondaryMarket and providing the following details:

The occurrence identifier is e.

• a collection of identifiers with the format told = t1,...,tn

• a listing of brand-new identifiers and transmission protocols.

The following conditions must be met for the proposition to be accepted:

• For train ticketing e, the ticket IDs t1,..., and tn are legitimate.

• P = Pn i=1 price(ti), where price(t) represents the price at which t is currently being sold.

• 1 |tnew| Pn i=1 *qi*, where *qi* = quantity(ti) identifies the number of seats made available on ticket ti.

• Each unique and underused identifier in tnew differs from the others.

E. Refund:

The offline process is typically drawn out and annoying when a train ticket purchase is cancelled by the organisers for any cause. Refunding is made simpler when purchases and payments are kept in the blockchain: When a train ticket is cancelled, a withdrawal feature may be engaged, which will automatically and almost instantly repay all ticket holders. It goes without saying that the event's organisers have the right to impose a fee to cover some of their expenses, and that only a portion of the ticket price would be refunded to customers. Depending on the kind of ticket and the consumer, different return policies may be used.

F. Change_Of_Address:

This strategy guarantees that none of the registered users' confidential information is ever made accessible to the public on the blockchain because we only keep their Ethereum IDs. Nothing, theoretically, links individual identities to Ethereum accounts. if particular user buys all of his tickets from the same location, it is feasible to identify his personal tastes by keeping track of the events for which he purchased tickets. In the bad case situation, their previous purchases and consequently personal interests would be made known if their EthereumAddress were to go public.

Our system gives users the option to modify their addresses in order to prevent scenarios like this:

(1) To begin, a user u can request a modification of address from the centralized server by submitting their old address 'x' and the new address 'y'.

(2) Second, by checking the smartcontract ValidatedAddress, the server certifies that 'x' is a valid address.

(3) if 'x' is correct, the server is going to provide you a pair two random challenges, 'c1' and 'c2'.

(4) The user 'u' must demonstrate access of those addresses by calling a Validated operation. (5) After confirming that both challenging replies were successfully received, the central server enters the new address 'y' and deletes the old address 'x'.

G. Authorized resellers

Train ticketings organisers have the option of selling tickets through licenced resellers who will also handle the marketing of the train ticketings through their specialised apps or websites in exchange for a fee. The task of adding a new reseller is left to the organisers in digital train ticketing: They accomplish this by creating a new smartcontract for the resale and adding the location of the contract on the set of known approved addresses. In truth, each train ticket comes with a list of authorised resellers.. Users who are interested in purchasing railway tickets through the Ethereum network can do so directly or by using the services of any reseller. Both times, the smart contract train ticketings function buy is called with the appropriate arguments and, in the event of a reseller purchase, a specified percentage.

V Conclusion and Future Work

We showed Digital railway ticketing, our idea for a ticketingsystem based on Ether smartcontracts, which deals with a number of problems with the present ticketing environment. The inability to confirm the validity of tickets purchased online (which may be counterfeit or copies of real tickets), the stark price differences between tickets bought and sold on the secondary market, and the lengthy refund processes are a few examples. We can stop railway ticket reselling by using smartcontracts in the following ways:

- allowing anyone to verify any ticket's authenticity;
- allowing users to register only in person to keep out bots;
- limiting the tickets a person can purchase for a train trip; managing price ranges on the secondary market.

References

[1] Aventus. 2018. A Blockchain-Based Event Ticketing Protocol. White paper, https://aventus.io/. [Online; accessed September 2018].

[2] Vitalik Buterin. 2013. Ethereum: A Next-Generation Smartcontract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/WhitePaper.

TickEth 2019 https://www.ticketh.io/

[3] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. White paper, http://bitcoin.org/bitcoin.pdf.

[4] Björn Tackmann. 2017. Secure Event Tickets on a Blockchain. In Data Privacy Management, Cryptocurrencies and Blockchain Technology, Joaquin Garcia-Alfaro, Guillermo Navarro-Arribas, Hannes Hartenstein, and Jordi Herrera-Joancomartí (Eds.). Springer International Publishing, Cham, 437–444.

