Towards STUB 2.0

Preece, Joseph; Morris, Chris; Easton, John

DOI:
10.1109/BigData55660.2022.10020309

Towards a Graph-Based World State on a Blockchain Platform to Facilitate Distributed Transport Ticketing

J. D. Preece
BCRRE
University of Birmingham
Birmingham, United Kingdom
j.d.preece@bham.ac.uk

J. M. Easton
BCRRE
University of Birmingham
Birmingham, United Kingdom
j.m.easton@bham.ac.uk

C. Morris
BCRRE
University of Birmingham
Birmingham, United Kingdom
c.morris.1@bham.ac.uk

***Abstract*—The System for Ticketing Ubiquity with Blockchains (STUB) is a novel solution to multi-modal transport ticketing. STUB utilises the distributed mechanics of blockchain technology right at the core of its architecture, allowing stakeholders from different transport modes to vend and validate tickets on a shared ledger. This open approach to ticketing data will benefit transport governing bodies, transport operators, and passengers alike by ensuring cross-party cooperation and presenting a fresh holistic approach to the ticketing sector.**

***Index Terms*—component, formatting, style, styling, insert**

I. Introduction

The market size of Mobility-as-a-Service (MaaS) is expected to grow to $451 billion by 2030, from just $25 billion in 2017 [1]. This increase in market size implies that new and existing Transport Service Providers (TSPs) will seek to operate within a multi-modal transport sector, with various services offered on differing modes of transport. As additional TSPs enter the space, demands for a unified Transport Ticket Interface (TTI) and Revenue Allocation System (RAS) will increase.

A. Ticket System Definitions

1) Transport Ticket Interfaces: A TTI is a method of dispensing, storing, and validating tickets for use within a transport infrastructure. A TTI may belong solely to one TSP (such as the Oyster Card for Transport for London (TfL)), or may cover a group of TSPs (such as the Trainline).

2) Revenue Allocation Systems: A RAS is a system that collects ticket data from multiple TSP that operate within a single TTI, and computes the revenue earned by each TSP. Latest Earnings Networked Nationally Over Night (LENNON) is an example of a RAS, and is used within the United Kingdom (UK) to allocate revenue generated on the railway network. It ensures that TSPs receive their fair share of revenue, even if they do not sell a ticket to a passenger directly.

The authors would like to thank the Trusted Content on Future Blockchains (TruBlo) consortium for funding this research.

B. Project Drivers

The simplistic traditional approach to defines agreements on a one-to-one basis between companies will become infeasible. If there are n organisations, and each must agree to use a bespoke system between one another, then the total number of systems N can be calculated as

$$N = \frac{n^2 - n}{2}. \tag{1}$$

Even for 10 organisations, this results in 45 separate systems. For an infrastructure that has 100 organisations, this becomes $4,950$. As each system must be separately developed and maintained, this is a costly process in both time and finance, for all stakeholders involved. As such, there is a clear business case to reducing the number of systems required, to provide the maximum impact for minimal expenditure.

This formula is never exact; high-level agreements by governing organisations exist to provide a shared legal agreement between stakeholders, reducing the number of systems required. However, these systems, known as closed-systems (where a central operator has full control of the network, such as the OV-chipkaart in the Netherlands) will become increasingly harder to build and maintain, especially as multi-modal journeys come to the forefront of the passenger experience.

Nonetheless, business will wish to retain the market competition which allows them to thrive in the industry. As such, fully central systems are not a complete solution to the problem, as they would eradicate the possibility of competition between Ticket Vending Organisations (TVOs). Moreover, many business cases are now focus on decarbonisation and their environmental impact. A new system would need to be enhanced not only in a financial sense, but an environmental sense too.

To summarise, the business drivers for STUB are as follows.

- Simplify the Information Technology (IT) infrastructure of transport ticketing to reduce development and maintenance costs, by reducing the number of systems to one single distributed system

- Design a platform that retains market competition to ensure competition amongst TSPs and TVOs, by enabling a trustless decentralised marketplace
- Improve sustainability and reduce negative environmental impact for the ticketing industry by providing a cross-transit, cross-continental multi-modal solution to incentivise use of public transport away from cars and planes
- Reduce the need for single-use ticketing (paper tickets)
- Allow for quick and dynamic updates to the system, without the requirement for a trusted third party

Along with the business case of simplifying the IT infrastructure of transport ticketing, there are multiple cases for passengers too. Due to the sheer number of differing ticket systems, fare structures, and TSPs operating, travelling even a simple journey can prove to be a minefield. There is increasing demand amongst passengers to simplify ticketing, to achieve a unified system that hides the complex industry relationships and IT infrastructure behind a user-friendly interface. Enable a single ticket process for travellers and businesses making it easier for both thus making public transport networks very attractive. This will enable travellers to consider using public transport modes in preference to their cars.

- Provide a single cost to travellers for a journey no matter where it is from or to.
- Provide instant compensation to the travellers from the transport service providers should a portion of a journey suffer from problems or delays.
- Provide transparency for the consumer of their data, and giving ownership of personal data back to the consumer
- Increased ease of implementing social tariffs and fare structures
- Improving mobility by improving ease-of-access to transport

This platform will use the mechanics of blockchain technology to replace the legacy ticketing systems. The purpose of STUB is to create a true digital equivalent of the paper ticket: something that is recognised by all travellers across Great Britain, no matter where or how it was purchased, or from whom. From using and applying blockchain technology, this innovative research will address the need for travellers to have a multitude of various ticket types and technologies to hand enabling them to seamlessly access public transport services and modes using a single ticket. The innovative research will address the need for transport service providers to have disparate, varied ticketing strategies and systems and the associated costs of operating them. These drivers align with the core ideals of the TruBlo project; to provide trust in a whole system (transit network, ticket validity, fare distribution and passenger identity) to stakeholders

- Utilise the distributed mechanics of blockchain technology to share the ticketing data between multiple stakeholders, ensuring trust of asset and trust of the proof-of-validity of a ticket for all associated
- Use graph-based storage to represent a transit network graph and allow for the usage of transit patterns within a blockchain platform
- Design a blockchain network that is flexible to work on multiple devices with various computational capabilities, by designing suitable simulations

II. Legacy STUB Design

Figure 1 illustrates a rudimentary architecture for STUB, which may easily be extended. There are four organisations, here represented by different colours. Organisation A (red), Organisation B (yellow), and Organisation C (blue) represent TVOs. Organisation D (grey) represent a governing organisation, who set the policies for the other organisations on the network.

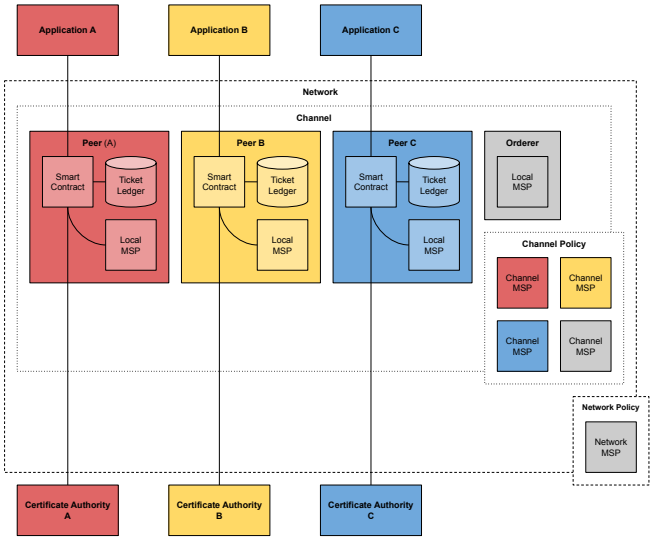

Fig. 1. Caption

At the highest level is the Network. The Network consists of a Network Policy and several Channels. The Network Policy defines who has access and specific rights within the entire network and defines high-level changes to the blockchain architecture. Channels exist to provide entirely desperate ledgers; this is particularly useful within the ticketing domain to separate geographical regions to improve latency and scalability. The Channel Policy defines the access rights within the Channel itself, potentially restricting other organisations from seeing transactions of certain ledgers.

In Figure 2 the Channel contains three Peer nodes (one per TVO) and one Orderer node (belonging to the governing organisation). The Peer nodes are responsible for holding copies of the ticket ledger and network graph within the world state, as well as copies of the chaincode to enable processing of the transactions. Outside of the network are a set of Applications (each belonging to an organisation) and Certificate Authorities. The Applications will be the interface between the ledger and the passengers, enabling both vending and validation via invocation of the smart contracts on the Peers, which they are connected to. The Certificate Authorities

dispenses the verifiable identities that the Membership Service Providers (MSPs) will use to determine access rights.

Figure 3 illustrates the process of vending and validating a ticket to a passenger. From this, we see that there will be two smart contract applications within the platform; one to generate tickets, and one to check the validity of the ticket. This is a simplified process, and we shall update this figure over the course of the project.

III. New STUB Design

As described in Section II, the original design of STUB used Hyperledger Fabric as the base platform. After careful consideration, we have decided to migrate to Hyperledger Besu. This is for several important reasons. First, Besu is an open-source Ethereum client. This enables us to develop upon refined Ethereum technologies (such as writing smart contracts in Solidity and testing on the existing test networks) and deploy the final application to the Ethereum main network, should that ever be required. Second, Besu supports the development of private permissioned networks too. This provides flexibility to the STUB project, as we envisage a private network whereby network peers are hosted by the ticket infrastructure stakeholders.

A. Network Considerations

Figure 4 demonstrates a simplified Besu architecture for STUB, with a three layer interaction system. Each colour represents a different stakeholder associated within the STUB network. The first layer are the passengers themselves, who interact with the second layer (for the applications) via function calls, as per traditional applications. The third layer is the Besu network itself, which the applications interact with via JavaScript Object Notation Remote Procedure Call (JSON-RPC) or Graph Query Language (GraphQL) calls. These calls control all interactions with the peers on the network; namely, smart contract invocations and world state querying. Figure 5 illustrates what a single STUB peer contains; a copy of the chain ledger, an instance of the Ethereum Virtual Machine (EVM) to execute the vending and validating smart contracts; a rocks DB to query the world state (and in the case of STUB, to store the graph-based world state), and an Orion Node to execute private transactions between peers within the STUB network.

1) Peers: Each participating TVO shall host a single peer. The key responsibility of peers is to validate the transactions via the smart contract invocations, to maintain the latest correct state of the blockchain.

2) Accounts: Each passenger will have a STUB account in the form of a keypair: a public key and a private key. The public key will be used as the account address, whereas the private key will be used to sign transactions and validate the ownership of the account.

3) Consensus and Incentives: As each TVO will host a peer, there must be a competitive nature to validate transactions. Besu supports several consensus mechanisms, including proof-of-work and various flavours of proof-of-authority. At this stage, we envisage the private STUB network using Istanbul Byzantine Fault Tolerance (IBFT) 2.0, as the TVOs will be preapproved and this approach uses fewer computational resources, resulting in a more environmentally friendly approach. The private network will have its own currency, mapped one-to-one with a real-world currency to ensure stability. This currency will be issued as a reward for successfully creating new blocks and can be used as a form of 'gas' to ensure that smart contracts are run on the network.

4) Tickets: Tickets will be encoded as tokens on the blockchain network, with ownership determined by the associated public key of a passenger account. Tickets will store several details:

- Passenger Account Public Key
- Organisation ID
- Origin Station ID
- Destination Station ID
- Fare
- Restrictions
- Reservations

5) Transport Network Graph: The Transport Network Graph (TNG) is a graph $G = (V, E)$, where V are the stations on the network, and E are the forms of transport provided by TSPs between each station. This shall be stored as triples within the graph-based world state, in order to perform graphical queries and algorithmic processes with greater efficiency to enable proof-of-validity of a ticket and proof-of-route for a valid route.

B. Processes

For testing purposes, there will be three smart contracts on the blockchain platform: Update Transit Network, Vend, and Validate. Update Transit Network will be used by TVO to update/modify the state of the transit network, as stored within the graph storage. Vend and Validate will be used by passengers (via a TVO Application Programming Interface (API)) to purchase and validate tickets respectively.

1) Transport Network Graph Setting: The core area of novelty of STUB is the usage of graph-based storage to create and maintain a distributed graph of the transit network used. As additional TVOs opt-in to STUB, they will be required to add their section of network to vend tickets to their area. The Update Transit Network smart contract is the layer between the TVO and the TNG.

- Origin Station Information
  - Name
  - Global Positioning System (GPS) Coordinate
  - TSP ID
- Destination Station Information
  - Name
  - GPS Coordinate
  - TSP ID

The smart contract will perform the following tasks:

- Check whether the origin or destination already exist within the TNG.

- If a station does exist, retrieve it from the data store.
- If a station does not exist in the TNG, create a record of it.
- Add this section of route to the Transit Network Graph.

2) Ticket Vending: Assume a passenger intends to purchase a ticket to travel between two locations, Location A and Location B. The first decision the passenger must take is the method of how to purchase the ticket. There are currently several ways of doing so; from ticket offices, web applications, and mobile applications. STUB does not intend to become these applications directly; instead, an API shall be provided to enable the organisations in control of these various methods to access the blockchain and the smart contracts directly. As such, beyond the initial decisions by the passenger, the technical details of STUB will be identical across the various techniques. To begin, the passenger provides details of their desired journey. They also provide their public key, to inform the TVO of where they would like the ticket to be dispensed. The TVO dispatches this information (via the API) to the vending smart contract. Upon successful invocation and completion of this request, the passenger will receive a ticket to their provided account (from the public key). This ticket is encoded as a token within the blockchain and contains details of the passenger's journey. To summarise, the Vending smart contract is the mechanism for the platform to vend new tickets to passengers. This smart contract takes the following parameters:

- Passenger Public Key
- Vending Machine ID
- Origin Station
- Destination Station

3) Ticket Validation: Assume the passenger travelling between Location A and Location B is requested to validate their ticket. Just as with ticket vending, there are multiple ways this may be asked, such as at a ticket barrier or by an on-board conductor. Once again, it is not the responsibility of STUB to replace these mechanisms; rather, provide an API to interact with the data stored within the blockchain. Upon request, the passenger will provide their STUB credentials. In addition to the public key, the passenger must provide their private key, to prove that it is truly them. The private key is used with a digital signature scheme to obtain a digital signature. Once the passenger has verified their identity within the network, the ticket validation smart contract will query the ledger and the transit network state to check the validity of the journey. Upon approval or declination, the ticket token shall be updated to record the result. By storing this information on the blockchain, this will form a trusted proof-of-journey, accessible by all stakeholders on the network. To summarise, this smart contract takes two parameters:

- Passenger Public Key
- Passenger Digital Signature
- Validating Machine ID

REFERENCES

[1] Statista, "Global MaaS Market Size 2017-2025." [Online]. Available: https://www.statista.com/statistics/1180559/global-mobility-as-a-service-market-size/