Anonymous Ticketing using Blockchain

Chinmay Dabke- Supervised by: Kostas Markantonakis, Raja Naeem Akram
Information Security Group, Smart Card and IoT Security Centre

ROYAL HOLLOWAY UNIVERSITY OF LONDON

The Smart Card and Internet of Things Security Centre

Objectives

Anonymous ticketing, whether deployed in a high throughput and low latency environments like transport networks is an enormous challenge. As per requirements of such a system, for example TfL requires the ticket processing within 300-500 milliseconds, any anonymous ticketing solution has to be efficient and does not require internet connection (in most cases. In this project, we explore the potential of deploying an efficient ticketing framework that utilise blockchain (smart-contracts) technology to provide anonymity but within the strict requirements of the transport systems. To research methods of implementing an anonymous ticketing system using blockchain technology.

- Evaluating the found methods and selecting the best option.
- Designing a solution based on the method and implementing the solution by creating a software system/application that is usable and sustainable.
- Designed solution should be efficient, reliable and secure.

Introduction to blockchain

Blockchain as a concept describes a ledger or a distributed database. This makes the records in the database decentralised and immutable and allows for a peer-to-peer verification system which makes the information trustworthy and unchangeable once it's added to the ledger.

The blockchain contains numerous blocks of data that are linked and secured using cryptography. For each block of data that is to be added, it needs to go though a verification process. In this process, all other nodes of the network validate the block and add it to the chain if majority of the nodes approve the block.

Making use of blockchain to create an anonymous ticketing system is the main objective of this project.
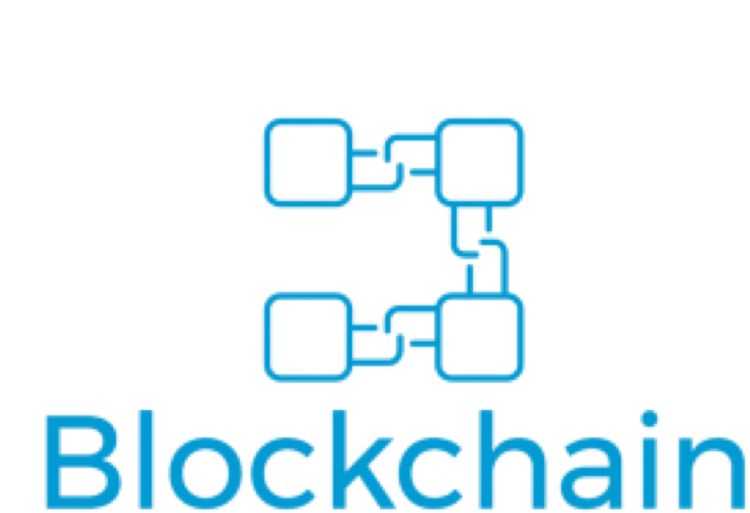
Figure 1: Blockchain icon

Figure 2: Ethereum logo

Early explorations of the methods that can be used to implement such a system are carried out on the Ethereum platform. The Ethereum platform allows for development of smart contracts on both private and public blockchains.

The programming language called Solidity will be used to write smart contracts to be deployed on the Ethereum bloackchain.

Description of project

The main application of this system is its usage in public transport system. The system will store information about ticket purchases in blocks in the blockchain. When a user uses their ticket i.e. scans their e-ticket at the machine, the system will verify its validity by referring to the blocks on the blockchain.
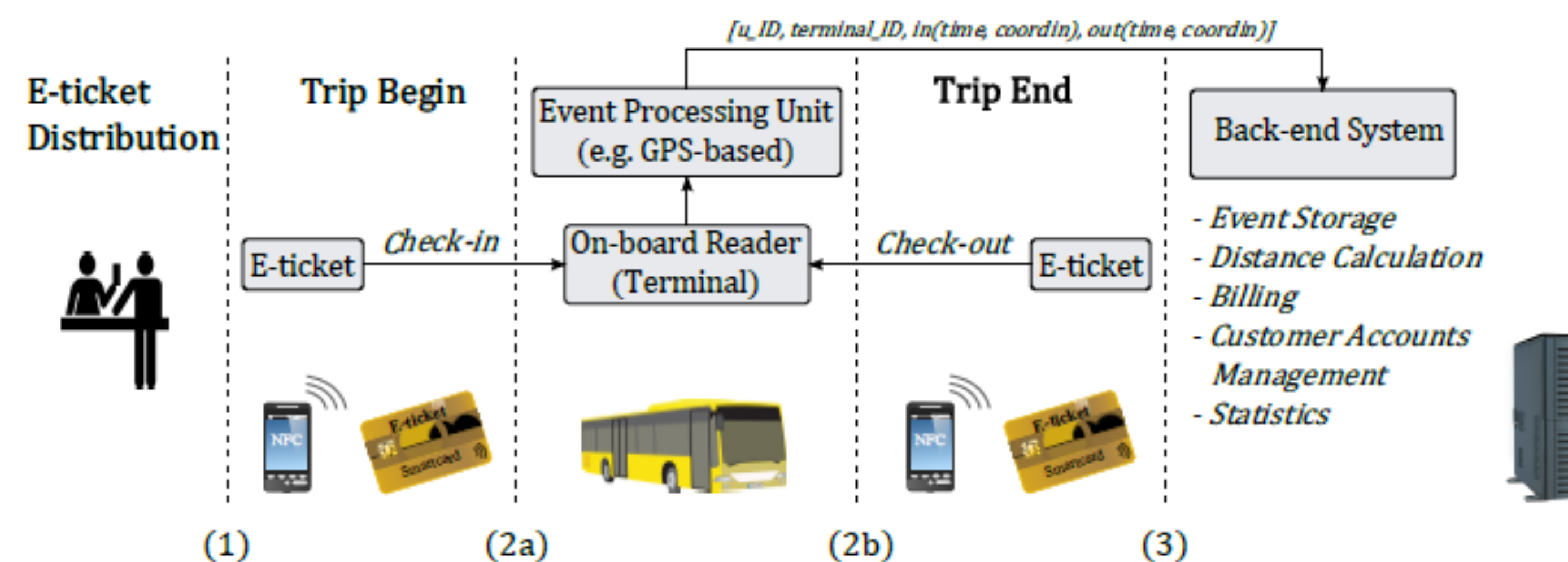

Figure 3 : Traditional e-ticketing

References

Firgure 1 : [online] https://www.kinesense-vca.com/wp-content/uploads/2018/03/Blockchain-Icon-300x214.png
Figure 2: [online]
https://ih1.redbubble.net/image.358612536.1165/flat,55 0x550,075,f.jpg
Figure 3: [online]
https://mistscholars.files.wordpress.com/2014/08/t.png

Additional Information

This project is related to the EPSRC funded project "Data to Improve Customer Experience (DICE)". The project is particularly interested in personal data, and is using rail passengers as a specific focus of interest. The overall aims of the project are:
• Understand the role that personal data plays in enhancing the user experience of rail passengers
• To develop technical solutions to data privacy
• To develop an evaluation framework that can be implemented so passengers can understand how their data is used and how they can control and verify its use.
The project started in October 2016, and runs for three years to September 2019. For more information about the project, please visit http://www.dice-project.org.

Acknowledgements

Contact Information

- Web: https://scc.rhul.ac.uk/
- Email: Chinmay.Dabke.2017@live.rhul.ac.uk
- Phone: +44 (0)1784 414409