CEng 491 -- Project KickOff Document

“TCOIN” KickOff Document

Description

There is no unified transportation payment system among countries and cities. Some cities even lack a unified payment method between different transportation means. We aim to solve this problem by creating a blockchain system. In addition to that it will allow offline secure transactions at payment gates but process them on online payment infrastructure in order to achieve transaction transparency. The usage of blockchain provides us to bring transaction generators and the auditors into a shared trusted platform and to offer transparency over recorded transactions and so ultimately to fulfill our aim. Our end-product will consist of a new crypto coin, *TCOIN*, to allow easy adaption of our proposed model to any city around the world and so ultimately to have interoperability between them. The expected users of our product are people who use transportation services that are available to the public.

Master feature list

1. It will utilize blockchain based transaction methods to verify transactions between any transport operators and end users.
2. It will construct a unified and decentralized payment system for public transport operators.
3. It will use a cryptocurrency as main payment good.
4. It will utilize near field RFID systems to information exchange between public transport operators and end users.
5. It will utilize NFC chips for the RFID
6. It will use smartphones and chip cards for NFC payments.
7. It will have its own unique protocol for payments using NFC chips.
8. It will provide offline contactless payment flow through blockchain based transaction flow using NFC.
9. It will provide a web application for end users to track their activities.
10. It will provide a web application for end users to reload their balances.
11. It will provide a mobile application for end users to track their activities.
12. It will provide a mobile application for end users to reload their balances.
13. It will provide web application for operators to monitor and manage their systems.
14. It will provide design of top-up machines for users to add our cryptocurrency to their accounts.
15. It will provide hardware for contactless payment verifiers to make transportation payments.
16. It will provide a permissioned blockchain for collaborators.

Workpackages

WP #	Term	WP title (this should be as short and as descriptive as possible)	Estimated number of person-months
1	491	Literature review regarding blockchain usage for payment and IoT, and finalization of software requirements	4
2	491	Identification of blockchain platforms and testing them based on the requirements to select the best one and deployment of basic demo codes	4
3	491	Blockchain platform development and implementation	6
4	492	Web development for web applications	4
5	492	Payment reader server side development	4
6	492	Mobile app development	4
7	492	Data integrity and security tests and implementation refinement	4
		Total:	30

Detailed Descriptions of High-Level Workpackages

WP1 - Literature review regarding blockchain usage for payment and IoT, and finalization of software requirements

1. Research on which blockchain platform to use (whether Ethereum or Hyperledger)
2. Research which bytecode compiling language should we use
3. Developing sample application in these languages
4. Reviewing literature in terms of offline contactless payments
5. Developing the list of software and hardware requirements (for example licenses and equipment)
6. Producing project development plan in accordance with Master Feature List.
7. Design the overall and generalized architecture of the project.

WP2 - Identification of blockchain platforms and testing them based on the requirements to select the best one and deployment of basic demo codes

1. Deciding which blockchain platform to use (whether Ethereum or Hyperledger)
2. Developing prototype and sample applications on two selected bytecode comping languages
3. Deciding which bytecode compiling language should we use in terms of security, resilience, speed, and efficiency
4. Developing sample applications on offline contactless payments
5. Deciding which backend and frontend frameworks that can be used in implementation phase
6. If needed, developing sample applications with these frameworks

WP3 - Blockchain platform development and implementation

1. Creating the coin, implementation of the blockchain
2. Design and implementation of the consensus algorithm
3. Implementation of the smart contracts
4. Writing tests to the smart contracts to ensure security

WP4 - Web development for web applications

1. Deciding which front end framework to use (React, Vue.js, Angular, Ionic etc.)
2. Designing front end site routes
3. Implementation and design of user layouts and pages
4. Integration of blockchain into the application
5. Implementation of reliable and secure authorization and authentication mechanisms between frontend and backend
6. If possible, ensuring scalability and resilience at the frontend

WP5 - Payment reader server side development

1. Providing a secure and reliable information exchange - retrieval protocol between end user and payment terminal (if needed a custom designed protocol or industrial standard protocol)
2. Method of storing information in passive tags for people without any online device
3. Developing a near field RFID communication sub-system with RFID transceivers and provided embedded software development libraries
4. Providing communication between our backbone (and also backend) in terms of supplied endpoints through IP.
5. Realization of these endpoints at the backend side.

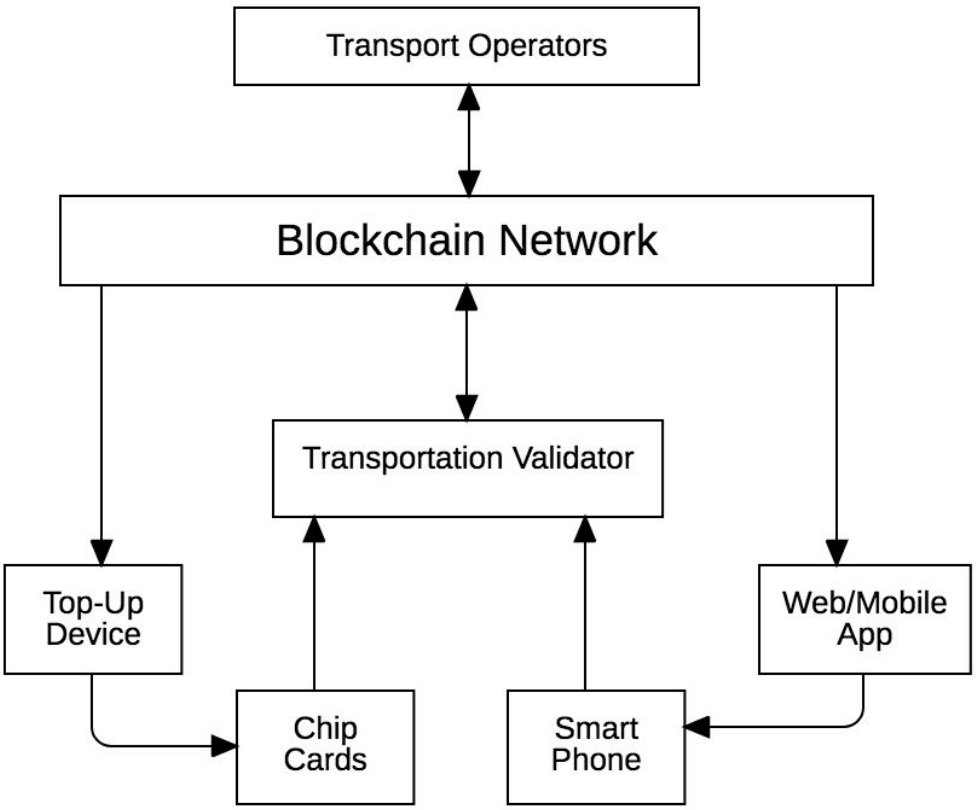
WP6 - Mobile app development

1. Deciding which mobile development technology to use for mobile application.
2. Developing a proof of concept application to see what problems may occur.
3. Integrating the mobile application into our blockchain.
4. Integrating authentication system and communication with readers to our mobile application.
5. Adding offline and online payment features to our application.
6. Testing the application for security and integrity.

WP7 - Data integrity and security tests and implementation refinement

1. Testing the system with an example IoT device and minimal number of mobile devices
2. Testing the system with for scalability using various cloud service providers.
3. Testing the system for online and offline verifications in real time.
4. Possible additional design and implementation into the system infrastructure.
5. Adding possible new payment methods(mobile, NFC, fingerprint authentication etc.)

Overall Systems Architecture



Our architecture consists of transport operators which are the private companies that are responsible for a way of transportation, transportation validators which are the devices that one interacts to use the services provided by a transport operator, top-up devices which are the devices one uses to deposit money into the system, web/mobile app which provides users with the ability to pay using their mobile device and also deposit money into their account without the help of top-up devices. Blockchain network will include multiple permissions, i.e. transport operator nodes and public users of the system will not have the same permission accessing the blockchain.

Timeline

Risk Assessment

In this section of the kick-off document, list (and briefly discuss) all foreseen risk items that (when realized) will be a major obstacle for successful completion of the project.

Risk #	Description	Possible Solution(s)
1	We may not be able to integrate our cryptocurrency in the given time.	We can work with a private Ethereum blockchain.
2	In order to provide a protected blockchain, we may actually need 2 blockchains, 1 as public and other as private.	We can go with just a private blockchain to ensure the security..
3	Because of scarcity of open source blockchain projects, blockchain development part can lock down the overall progress of the project	Using simple blockchain smart contract techniques (auction method etc.) to

		realize our project
4	If we fork the Ethereum and make our currency/blockchain, we may need to integrate current development tools to our currency/blockchain.	We may try to simulate the system in Ethereum during development and develop a continuous integration pipeline into our system