ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE ENGINEERING AND TECHNOLOGY

# A BLOCKCHAIN-BASED FRAMEWORK FOR CUSTOMER LOYALTY PROGRAMS

**M.Sc. THESIS**

**Şeref BÜLBÜL**

**Department of Computer Engineering**

**Computer Engineering Programme**

**DECEMBER 2018**

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL OF SCIENCE

ENGINEERING AND TECHNOLOGY

# A BLOCKCHAIN-BASED FRAMEWORK FOR CUSTOMER LOYALTY PROGRAMS

M.Sc. THESIS

Şeref BÜLBÜL
(504161550)

Department of Computer Engineering

Computer Engineering Programme

Thesis Advisor: Asst. Prof. Dr. Gökhan İNCE

DECEMBER 2018

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

# MÜŞTERİ SADAKAT PROGRAMLARI İÇİN BLOKZİNCİR TABANLI BİR ÇERÇEVE

**YÜKSEK LİSANS TEZİ**

**Şeref BÜLBÜL**
**(504161550)**

**Bilgisayar Mühendisliği Anabilim Dalı**

**Bilgisayar Mühendisliği Programı**

**Tez Danışmanı: Dr. Öğr. Üyesi Gökhan İNCE**

**ARALIK 2018**

Şeref BÜLBÜL, a M.Sc. student of ITU Graduate School of Science Engineering and Technology student ID 504161550, successfully defended the thesis entitled “A BLOCKCHAIN-BASED FRAMEWORK FOR CUSTOMER LOYALTY PROGRAMS”, which he prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

**Thesis Advisor :** **Asst. Prof. Dr. Gökhan İNCE** ..............................
Istanbul Technical University

**Jury Members :** **Asst. Prof. Dr. Şerif BAHTİYAR** ..............................
Istanbul Technical University

**Dr. Mahmut Şamil SAĞIROĞLU** ..............................
Erlab Technology

**Date of Submission :** **16 November 2018**
**Date of Defense :** **12 December 2018**

***To my family,***

## FOREWORD

This thesis is made as a master project, as part of the requirements for the awarding of a degree in Master of Science in Engineering at the department of Computer Engineering at the Istanbul Technical University. I wish to thank colleagues at adesso Turkey who were more than generous with their expertise and precious time. A special thanks to Asst. Prof. Dr. Gökhan İNCE, my advisor for his countless hours of reflecting, reading, encouraging, and most of all patience throughout the entire process. I also would like to thank adesso Turkey for financial support. Finally, I would thank to my family and my lovely fiancee for always supporting me.

December 2018

Şeref BÜLBÜL
Mobile Team Lead

## TABLE OF CONTENTS

**Page**

## ABBREVIATIONS

| | |
|---|---|
| **AML** | : Anti Money Laundering |
| **API** | : Application Programming Interface |
| **DAO** | : Decentralized Autonomous Organization |
| **DBFT** | : Delegated Byzantine Fault Tolerance |
| **DLT** | : Distributed Ledger Technology |
| **DPoS** | : Delegated Proof-of-Stake |
| **ETH** | : Ethereum |
| **EVM** | : Ethereum Virtual Machine |
| **FinTech** | : Financial Technology |
| **FMCG** | : Fast-moving Consumer Goods |
| **GAS** | : NeoGas |
| **ICO** | : Initial Coin Offerings |
| **IoT** | : Internet of Things |
| **KYC** | : Know Your Customer |
| **PAX** | : Promotion Asset Exchange |
| **PoS** | : Proof-of-Stake |
| **PoW** | : Proof-of-Work |

## SYMBOLS

| | | |
|---|---|---|
| A | : | User of blockchain system |
| B | : | User of blockchain system |
| C | : | User of blockchain system |
| X | : | Node of blockchain system |
| Y | : | Node of blockchain system |
| Z | : | Node of blockchain system |

## LIST OF TABLES

**Page**

## LIST OF FIGURES

**Page**

# A BLOCKCHAIN-BASED FRAMEWORK FOR CUSTOMER LOYALTY PROGRAMS

## SUMMARY

Loyalty programs have grown in travel, retail, financial services and other economic sectors. Therefore, Loyal customers are one of the primary driving forces of any profit-making business. By creating loyalty rewards programs, companies aim to increase customer experience. Customer loyalty and engagement play an important role in the growth of companies and reward programs therefore represent strategic investments for all types of organizations. However, while customer loyalty programs are growing rapidly, some bottlenecks arise which lead to inefficiencies.

In the Fast-Moving Consumer Goods (FMCG) industry, manufacturing companies put promotion cards to their products. Their aim is gaining customers' loyalty and directing them to buy company products more frequently. Therefore, customers who bring promotion cards to merchants, are allowed to get promotion products.

Traditional customer loyalty programs have several bottlenecks especially in the FMCG industry such as lost coupons and payback process complications. Customers earn promotion cards by buying snacks and chips. They need to bring promotion cards back to merchants for promotion products. However, since these cards are small and oily due to exposure to products, users generally ignore or sometimes forget bringing them back. Lost coupons decrease the participation ratio of the loyalty program which also means manufacturers cannot get customers' loyalty. In addition, merchants collect thousands of promotion cards from customers and they need to give them back to manufacturers for payback. Manufacturers get those promotion cards from merchants and make payback to them according to the quantity of promotion cards. Counting thousands of promotion cards is a challenging issue thus some of the manufacturers prefer weighing cards to find an approximate number instead of counting which can cause unreliability in the process. Moreover, manufacturers have to cooperate with third-party companies to maintain customer loyalty programs. Collaboration with third parties requires integration with third-party services, including data sharing.

Blockchain creates a shared registration system between network members and eliminates the need to reconcile different stakeholders. Benefits of using blockchain technology are intrinsically related to its technical features. This distributed technology allows reduction of costs and bureaucracy as well as the improvement in trust and efficiency in systems. Logic of block chaining also guarantees that the data not to be altered and together with the temporality feature it allows the traceability up to the very first data generated.

This thesis presents the design of a blockchain-based customer loyalty program, Promotion Asset Exchange (PAX) framework, to solve bottlenecks in the traditional customer loyalty programs thanks to replacing promotion cards with virtual tokens. PAX framework adopts the smart contracts of blockchain technology by using PAX

tokens to digitalize transaction processes. It provides better usability for customers and more information from manufacturing companies' perspective.

# MÜŞTERİ SADAKAT PROGRAMLARI İÇİN BLOKZİNCİR TABANLI BİR ÇERÇEVE

## ÖZET

Müşteri sadakat programları seyahat, perakende, finansal hizmetler ve diğer ekonomik sektörler arasında giderek artmaktadır. Şirketler, sadakat programları oluşturarak müşterilerinin deneyimini artırmayı hedefliyor. Müşteri sadakati ve katılımı şirketlerin büyümesinde önemli bir rol oynamaktadır ve ödül programları bu nedenle her tür organizasyon için stratejik yatırımlar arasındadır. Ancak, müşteri sadakat programları hızlı bir şekilde büyüdükleri için, verimsizliklere yol açan bazı problemlerle karşılaşmaktadırlar.

Hızlı tüketim ürünleri sektöründe, üreticiler ürünlerine promosyon kartları koymaktadır. Amaçları, müşterilerinin sadakatini kazanmak ve onları şirket ürünlerini daha sık almak için yönlendirmektir. Böylece promosyon kartlarını marketlere getiren müşteriler promosyon ürünleri alabilirler.

Özellikle hızlı tüketim ürünleri sektöründe, geleneksel müşteri sadakat programlarının iyileştirmeye ihtiyaç duyan, kayıp kuponlar ve geri ödeme sürecindeki karışıklıklar gibi bazı süreçleri vardır. Müşteriler, cips ve aperatifler satın alarak promosyon kartları kazanırlar ve bu promosyon kartlarıyla promosyon ürünleri alabilmek için kartları tekrar marketlere götürmeleri gerekir. Ancak, bu küçük kartlar ürünlere maruz kaldıklarından dolayı genellikle yağlı olduğundan, kullanıcılar çoğunlukla onları geri götürmeyi ihmal eder veya unutur. Kaybedilen kuponlar, sadakat programının katılım oranını azaltır ve bu da üreticilerin müşteri sadakatini kazanamamasına ayrıca veri kaybı yaşamasına sebep olur. Buna ek olarak, marketler binlerce promosyon kartını müşterilerden toplayarak geri ödeme için üreticilere tekrar vermeleri gerekir. Üreticiler bu promosyon kartlarını satıcılardan alır ve promosyon kartlarının sayısına göre onlara geri ödeme yaparlar. Binlerce promosyon kartının sayılması zorlu bir süreçtir, bu yüzden üreticilerin bazıları kartları saymak yerine tartarak yaklaşık bir sayı bulmayı tercih edebiliyorlar. Ancak bu da kesin sayılarla çalışabilmenin önüne geçmekte ve süreçte güven sorunu ortaya çıkarmaktadır. Ayrıca, müşteri sadakat programlarını sürdürmek için üreticiler üçüncü taraf şirketlerle işbirliği yapmak zorunda. Üçüncü taraflarla yapılan işbirliği, veri paylaşımı da dahil olmak üzere üçüncü taraf hizmetleriyle entegrasyon gerektirir.

Blokzincir teknolojisinden söz edilmeye ilk kez Satoshi Nakamoto lakaplı gizli bir yazarın 2008 yılında önerdiği Bitcoin dijital parası ile birlikte başlandı. Blokzincir teknolojisi ağ üyeleri arasında paylaşılan bir dağıtık kayıt sistemi oluşturur ve farklı otoritelerin mutabakatının gerekliliğini ortadan kaldırır. Bu dağıtılmış teknoloji, maliyetlerin ve bürokrasinin azaltılmasına ve sistemlerde güven ve verimliliğin artmasına olanak sağlar. Blokları zincir şeklinde birbirine bağlama mantığı, verilerin değiştirilmemiş olduğunu garanti eder ve zaman tabanlı tutulan kayıtlar sayesinde üretilen ilk verilere kadar takip edilebilirliği sağlar. Blokzincir teknolojisi nesnelerin

interneti, akıllı ev sistemleri, tedarik zinciri ve finansal teknolojiler gibi birçok endüstride kullanılmaya başlanmıştır.

Blokzinciri blokların birbirini takip ederek sıralanmasıyla oluşturulur. Blok kendinden önceki bloğun özet değerini tutarak sıralı bir liste oluştururlar. Her bir blok, blok başlığında bir önceki bloğun özet değeri, zaman damgası, nonce değeri ve Merkle kök değeri ile blok gövdesinde işlem listesini tutar. Her bir işlem eşsiz kimlik numarasını, gönderenin adresini, alıcının adresini ve gönderilen varlığın miktarını içerir. Blokzincir ağında 2 çeşit düğüm vardır. Sade düğümler sadece blok başlıklarını tutarak işlemlerin kimlerini doğrulamaktan sorumluyken, tam düğümler tüm blokzincirini başlangıçtan itibaren tutarlar ve sisteme eklenecek yeni blokların mütabakat protokolleri ile doğrulanmasından sorumludurlar.

Bu tez müşteri sadakat programlarındaki promosyon kartlarını sanal jetonlarla değiştirerek sistemdeki tıkanıklıkları çözmek için blokzincir tabanlı müşteri sadakat programı, Promosyon Varlık Değişimi (PAX) çerçevesinin tasarımını ve uygulamasını sunmaktadır. PAX çerçevesi, işlem süreçlerini dijital hale getirmek için PAX jetonunu kullanarak blokzincir teknolojisinin akıllı kontraktlarını kullanır. PAX jetonu sayesinde müşteriler, marketler ve üreticiler arasındaki bütün işlemler kayıt altında tutulur. Tüm müşteri sadakat sistemi işlemleri dijital ortamda tutulduğu için marketler ve üreticiler arasındaki geri ödeme sürecinde yaşanan kurtulmuş olunur. Buna ek olarak, müşteriler için daha iyi kullanılabilirlik ve üretim şirketlerinin bakış açısından daha fazla müşteri verisi sağlanır.

NEO ve Ethereum çerçeveleri blokzincir teknolojisinin avantajlarından yararlanmayı olanak veren altyapılar sağlar. NEO, 2015 yılında Çin'in ilk blokzincir çerçevesi olarak sunulmuştur. Ethereum ise 2013 yılının sonlarında Vitalik Buterin isimli bir geliştirici tarafından sunulup, 2015 yılında kullanılmaya başlanmıştır. İki çerçeve de akıllı kontraktların kullanımını desteklese de çerçeveler kullanışlılık, işlem kapasitesi ve ölçeklenebilirlik yönünden karşılaştırılmıştır. Ethereum'da teorik olarak saniyede en fazla 30 işlem yapılabilirken NEO'da bu miktar 10000'dir. Bunun en büyük sebeplerinden birisi Ethereum mütabakat protokolü olarak Emek Kanıtı (Proof-of-Work) kullanırken NEO Delege Edilen Bizans Hata Toleransı (Delegated Byzantine Fault Tolerant) kullanıyor olmasıdır. Ayrıca, akıllı kontrakt geliştirirken Ethereum çerçevesinde Solidity dili kullanılırken NEO çerçevesinde çok daha yaygın kullanım alanı olan Python dili kullanılmaktadır. Bu sebeplerden dolayı NEO çerçevesi daha avantajlı bulunmuştur ve PAX çerçevesi için NEO altyapısı kullanılmıştır.

NEO kar amacı gütmeyen topluluk tabanlı bir blokzincir projesidir. NEO ile amaçlanan, blokzincir teknolojisi ve dijital kimlikler ile varlıkların dijitalize edilmesi, akıllı sözleşmelerin kullanımı ile dijital varlıkların yönetimini otomatize etmek ve dağıtık bir ağ ile akıllı ekonomi gerçekleştirmektir.

Akıllı sözleşmeler, taraflar arasında kabul edilmiş şartları yerine getirmek için kendi protokolleri olan yazılım parçalarıdır. Blokzinciri teknolojisi ile akıllı sözleşmeler merkezsiz, bozulmaya/değiştirilmeye dayalıklı ve güvenilir bir sistemde çalışabilmektedir. NEO geliştirme önerilerinin beşincisi (NEP-5) NEO blokzinciri için jeton standartlarını belirtmektedir. Bu standartlar diğer sistemlere genel bir etkileşim mekanizması sunmaktadır. NEO blokzincirinde geliştirilen bir akıllı sözleşme NEP-5 standartlarını sağlıyorsa, sözleşmenin sağladığı jetonlar geçerli bir varlık olarak takas edilebilir, borsalarda alım satımı yapılabilir.

İlk Dijital Para Arzı (Initial Coin Offering, ICO), kitle fonunun kripto para versiyonudur ve görünüşe göre kripto para dünyasında kullanılmaya devam edecektir. Şirketlerin ve bireylerin projelerine sermaye bulmasının ve sıradan kullanıcıların değerli olduğunu düşündükleri projelere yatırım yapmalarının en kolay ve en etkili yollarından biridir. ICO'lar genellikle bir hafta veya daha fazla süren ve insanların zaten bilinen kripto paralar (Bitcoin vb.) karşılığında piyasaya yeni çıkmış jetonlardan alabildiği bir etkinliktir. ICO'larda bir projenin desteklenmesinin belli bir limiti veya amacı olabilir, yani her token'ın önceden tasarlanmış belli bir ücreti vardır ve ICO periyodu boyunca değişmez. Bunun sonuçlarından biri olarak da, sabit sayıda token tedarik edilir.

Müşteriler, aldıkları cips, bisküvi gibi atıştırmalık ürünlerin içerisinden çıkan karekodları telefonlarındaki mobil uygulama ile okutarak süreci başlatırlar. Okuttuları karekoda karşılık gelen promosyon tutarı, müşterilerin cüzdanlarına PAX jetonu olarak gönderilir. Müşteriler tek kullanımlık kartlardaki karekodlarını okuttuktan sonra, artık kartlara ihtiyaç duymadıkları için yağlı kartları saklamak zorunda kalmazlar. Böylece kayıp olan promosyon kartı sorunu da ortadan kalkmış olur. Müşteriler yeterli miktarda PAX jetonu topladıklarında bu jetonları kullanarak promosyon ürünleri almak için marketlere gidebilirler. Satın alma işlemi için, müşteriler satıcıların mobil uygulamasındaki karekodunu okutarak onların cüzdanlarına gereken miktarda PAX jetonu gönderirler ve istedikleri promosyon ürününü alırlar. Satıcılar gelen müşterilerden topladıkları PAX jetonları ile üreticilerden geri ödeme talep edebilirler. Üreticiler de geri ödemeyi satıcıların biriktirdiği PAX miktarına göre yaparak promosyon kartı saymakla ya da tartmakla uğraşmazlar. Böylece geri ödeme sürecindeki belirsizliklerden de kurtulmuş olurlar.

# 1. INTRODUCTION

Customer loyalty programs aim to gain customers' loyalty to become their everyday routine. Therefore, customers are rewarded in accord with their purchases. Manufacturers are able to know their customers through customer loyalty programs. In the Fast-Moving Consumer Goods (FMCG) industry, manufacturers generally put promotion product coupons into product packages. Customers collect these coupons after purchasing the products and bring them to merchants so that they can get their rewards. On the other side of the program, merchants collect those coupons to receive a payback from manufacturers.

Customer loyalty programs include many asset transactions between subjects like customers to merchants and merchants to manufacturers. However, there are some bottlenecks which block or slow down the loyalty program's flow, such as lost coupons, counting thousands of coupons for payback to merchants and so on. These bottlenecks cause customer data to get lost and complications in the system for payback process. In addition, manufacturers have to cooperate with third-party companies in order to maintain customer loyalty programs. Collaboration with third-parties requires integration with third party services including data sharing. In this thesis, to overcome these deficits and eliminate third parties a blockchain-based customer loyalty program is proposed.

Blockchain technology is first mentioned by Satoshi Nakamoto in [4]. Although this paper describes blockchain technology in details, it was never published officially in a scientific journal. In addition, Satoshi Nakamoto is still considered to be anonymous [5]. Blockchain system is designed to provide a single source of truth without the need of third-party systems. It distributes the data on the network and keeps the data consistent, thanks to consensus protocols [6]. Therefore, it can be used in the error-prone systems to decrease the amount of incoherent data.

In this thesis, we propose a blockchain-based customer loyalty program called *Promotion Asset Exchange (PAX)* framework . Regular promotion coupon is replaced with PAX token in the loyalty program. We aim to keep track of all transactions in the blockchain system to provide consistency of the data. In addition, manufacturers can track all transactions in the system which will increase the amount of information about the customer from company's perspective.

The remainder of this thesis is organized as follows. Chapter 2 gives information about related work and literature review. In chapter 3, we propose the design and implementation of the blockchain-based customer loyalty program, define the PAX system technically and give information about PAX token. Chapter 4 describes the experiments and results for effects of number of nodes in the blockchain system in terms of confirmation time. Chapter 5 concludes the thesis by summarizing the whole thesis and presenting the future plans.

# 2. LITERATURE REVIEW

In this chapter, we review the literature with respect to customer loyalty programs and blockchain systems. First, we explain importance of the customer loyalty programs and their bottlenecks. Then, we describe the blockchain systems with technical details and application fields.

## 2.1 Customer Loyalty Programs

Business success depends entirely on establishing a good relationship with customers. The fact is that attracting a new customer is more expensive than retaining an old one, so companies cannot afford to lose customer loyalty. There is a phenomenon where customer loyalty leads to improved profitability of institutions [7].

Customer loyalty is an asset that can be gained by companies through different type of programs. These programs should attract customers to buy brand products frequently, encourage to spend more for the companies' products and attract new customers [8]. Customers who join customer loyalty programs can get discounts and promotion products. On the other hand, companies have the opportunity to know their customers' shopping habits and they accomplish advantage compared to their competitors since customers will prefer their products [9].

In the FMCG industry, customer loyalty programs usually utilize promotion product coupons. Programs have three main subjects. Customers, the first subject, buy FMCG products such as chips, cookies and collect coupons from product packages. Then they bring these coupons to the merchants which constitute the second subject of the program, to get the promotion products. Finally, manufacturing companies which are the third subject, collect coupons from the merchants to make a payback.

There are some problems with the transactions among subjects. Firstly, customers usually lose or forget coupons which are small and oily cards mostly due to their exposure to the product directly. It strongly affects the participation of the customers in the program negatively because lost or forgotten coupons cannot make the customer to join the system anymore. Secondly, customers cannot access their purchase or promotion history in the system. Once they give promotion coupons to merchants, they do not have any records about their purchase history. Thirdly, payback between merchants and manufacturing companies is a problematic operation because generally, merchants need to collect thousands of coupons to give back to manufacturing companies. Therefore, manufacturing companies should count all cards otherwise they need an alternative solution. With the traditional customer loyalty programs, the alternative solution is weighing all cards using a scale and finding an approximate count to make the payback. In addition, if manufacturer want to arrange targeted promotions such as age specific or gender specific promotions, they do not have technical infrastructure with the traditional customer loyalty programs. Moreover, manufacturers have to collaborate with third-party companies in order to manage customer loyalty programs. Cooperation with third-parties requires integration with third party services including data sharing.

### 2.2 Blockchain Systems

Blockchain is a database that keeps a digital ledger and distributes it with the participants of blockchain network. It allows keeping data safely without requiring any central authority.

Blockchain consists of blocks by including former block's hash value. It provides immutable data in a consistent manner. Therefore, transactions between subjects can be kept regularly without errors.

While keeping immutable and distributed data on the network, participants of the network which are called nodes do not need to trust each other. There are certain rules for the validations of the transactions, which are called consensus protocol. Nodes apply consensus protocol for the transaction to decide the validity of the transaction. It provides a trustless environment so trust is gained as a feature that emanates from the interaction of different participants in the system [10].

When the system finds the appropriate block and appends to the chain, it shares the last block with the network. Therefore, nodes can start to find the next appropriate block with new transactions.

Assume that A, B and C are the users of the Blockchain system and X, Y and Z are the nodes of the Blockchain system as shown in the Figure 2.1. User A wants to send 100 coins to user C and user B wants to send 10 coins to user C. These requests are received by nodes of the system which are X, Y and Z. Duty of the nodes is finding the next block which will be added to blockchain. There are different methodologies called consensus protocols, for finding process such as Proof-of-Work and Proof-of-Stake. If X in the system finds the next block, Y and Z should validate that block and its transactions. If any of the nodes try to convince the system, other nodes realize the inconsistency in the block and reject the proposed block. Therefore, fraud is prevented in the system. Once, other nodes validate the proposed next block, it is added to blockchain and user C receives coins from user A and B successfully.

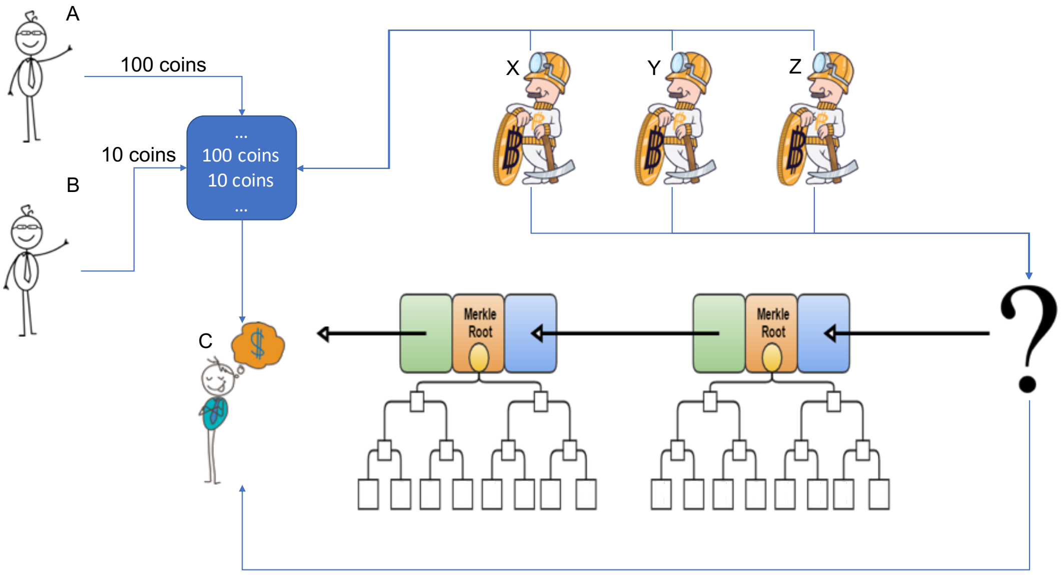


**Figure 2.1** : Flow of the blockchain.

### 2.2.1 Structure of blockchain

Blockchain basically consists of blocks and transactions. Genesis block is the first block of the blockchain which does not have parent block [11]. Every block includes a hash of the previous block, timestamp, nonce value, root hash in the header and transactions in the body which is shown in Figure 2.2.

Hash of the previous block is included in the block header to keep blocks in a linked order. In addition, holding the previous block's hash in the block header provides immutability of the data since changing one of the blocks in the chain will cause changes on all the following blocks.

Timestamp is a digital record which holds the current time of occurrence of a particular event. Timestamps are essential for synchronization of blocks since they refer to the creation time of the blocks. Nonce is a counter which is used to make sure each transaction can only be processed once [12].

Root hashes are created according to Merkle tree protocol [13]. A Merkle tree is a type of binary tree, composed of a set of nodes with a large number of leaf nodes at the bottom of the tree containing the underlying data, a set of intermediate nodes where each node is the hash of its two children, and finally a single root node, also formed from the hash of its two children, representing the "top" of the tree [12]. In the figure 2.2, only four transactions which are Tx0, Tx1, Tx2 and Tx3, are included in the blocks for the illustration. Hash of the transactions referring to Hash0, Hash1, Hash2 and Hash3 respectively are calculated one by one. After that, hashes are combined in pairs and hashes of the pairs are calculated and named Hash01, Hash23 respectively. Finally, Hash01 and Hash23 are combined to calculate root hash.

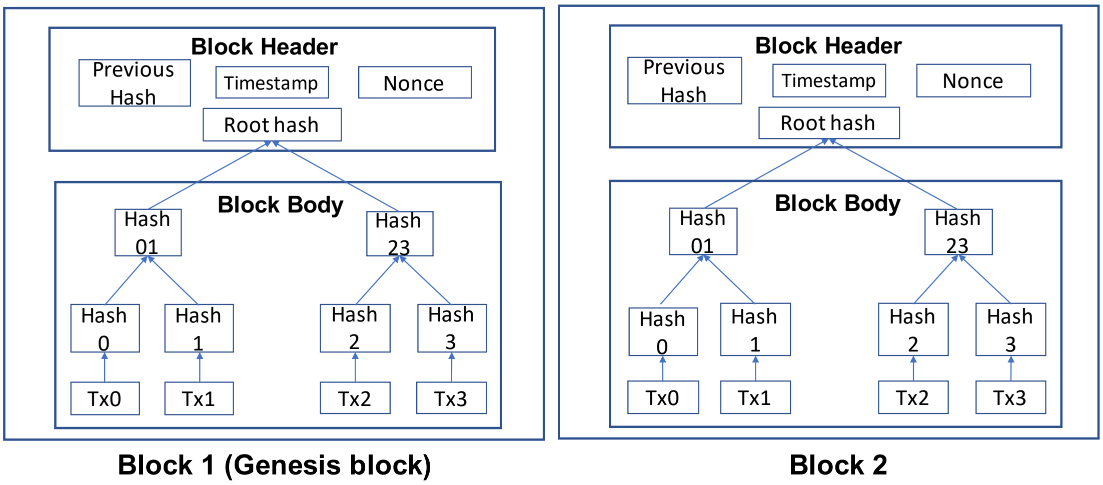


**Figure 2.2 :** Structure of the blocks in blockchain.

Values of the 549855th block of Bitcoin blockchain is shown in Table 2.1. Since Bitcoin is a public blockchain, all blocks and transactions can be examined.

**Table 2.1** : 549855th block of Bitcoin blockchain [1].

| Key | Value |
|---|---|
| Height | 549855 |
| Hash | 0000000000000000001db699ca85ecb4ee9d893beeb6aad26126bd43c96038ea |
| Previous Block | 0000000000000000001c4f2575f33139064f214a3b921b0c45225790ce712d00 |
| Time | Nov 13, 2018 2:00:04 AM |
| Number Of Transactions | 421 |
| Merkle Root | 6c7072675cef7396d68bbc06c775c0455f50068907d0a595ef6f6d127547a7cc |
| Nonce | 119137471 |

### 2.2.2 Transactions

Transactions are records in the blockchain system. The sender creates the transaction and shares it with the network. Once they are added to the blockchain, they cannot be changed. Asset transfer can be made easily with the transactions in the blockchain system. Every transaction has an id, sender's address, receiver's address and sent amount. Values of the one of the transaction from 549855th block of Bitcoin blockchain is shown in Table 2.2.

**Table 2.2** : A transaction from 549855th block of Bitcoin blockchain [2].

| Key | Value |
|---|---|
| Transaction id | dc8559f78f723abe4808fef57f12eee5921de861c9dc7e8106ce58fb9553ca98 |
| Sender address | 1GVbvEE1FfDpGVEmA41wZHswhfr5UV4j78 |
| Receiver address | 3QGp8gCcn8N24xdg51FEv4ASWHrcorBdo7 |
| Amount | 0.02602735 BTC |
| Time | Nov 13, 2018 2:00:04 AM |

### 2.2.3 Network

In this subsection, 3 types of blockchain network types which are public, permissioned and private, and blockchain network node types which are light and full node, will be described.

#### 2.2.3.1 Blockchain network types

There are 3 types of blockchain network types which are public, permissioned and private networks:

1. Public Blockchain: Public Blockchain enables a user to join and contribute to an open network. The network of public blockchain is entirely open so that anyone can join and work in different core activities. Also, anyone on a public blockchain can run a node without any conditions on the terms of admission into the network.

2. Permissioned Blockchain: A permissioned blockchain is operated by known entities such as stakeholders of a given industry. It is a mix of both private and public blockchain. In this type of blockchain network, a participant may not need permission to join the network, but needs permission to transact with another network participant.

3. Private Blockchain: In a private blockchain, it is enough to know who in the network attempted to play foul. Private blockchains are guided by business policies which can levy a fine for a participant who attempts to add an invalid or double spent transaction. If one needs to run a private blockchain that allows only selected entry of verified participants, like those for a private business, one can opt for a private blockchain implementation. A participant can join such a private network only through an authentic and verified invitation, and a validation is necessary either by the network operator(s) or by a clearly defined set protocol implemented by the network.

#### 2.2.3.2 Blockchain network node types

Blockchain network includes two types of nodes which are full nodes and light nodes [12].

1. Light Node: Light nodes keep only headers of the blocks. They use a method named Simplified Payment Verification (SPV) to validate the authenticity of the transactions [14]. They do not validate the rules of the consensus.

2. Full Node: Full nodes keep the whole blocks from the beginning. Full nodes download every block and transaction and check them against consensus rules [15]. If a transaction or block violates any of the rules, it is rejected.

When transactions are requested from nodes, they listed on the pending transactions list. Then some of the transactions from the list are included for the next block. Blockchain system has some consensus rules to approve and append the next block into the chain. Some of the consensus rules:

- Blocks must be in the correct data format.
- Block's transactions must not be used before.
- Block's hash values must be in the correct format e.g. leading seven zeros for the hash value of block

Top 5 countries with their respective number of reachable nodes in the Bitcoin blockchain are shown in the Table 2.3

**Table 2.3** : Top 5 countries with their respective number of reachable nodes in the Bitcoin blockchain [3].

| Rank | Country | Nodes |
|---|---|---|
| 1 | United States | 2388 (23.78%) |
| 2 | Germany | 1942 (19.34%) |
| 3 | France | 672 (6.69%) |
| 4 | China | 667 (6.64%) |
| 5 | Netherlands | 504 (5.02%) |

### 2.2.4 Consensus protocols

Blockchain systems can use different approaches for approving new blocks to the chain. Hash of the previous block guarantees the order of the blocks. It is possible on the blockchain that sometimes there can be two different chains. As shown in Figure 2.3, nodes accept the longest chain as a valid chain, then new blocks are appended to that valid chain in that situation [11].

There are many different consensus protocols such as Proof-of-Work, Proof-of-Stake, Delegated Proof-of-Stake, Delegated Byzantine Fault Tolerance, Practical Byzantine

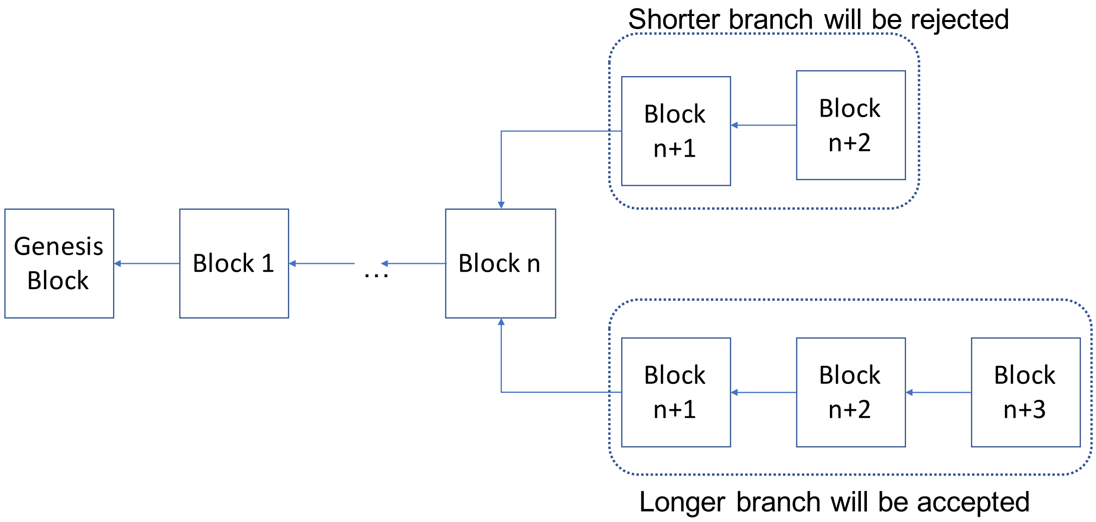


**Figure 2.3** : Longest chain acceptance on the blockchain.

Fault Tolerance, Tangaroa, Unique Node Lists [10]. In this section, we will only discuss the most commonly used three of them.

#### 2.2.4.1 Proof-of-work

In this consensus protocol, blockchain system rewards the user who finds the next block of the chain. Therefore, users who are called miners, perform computational calculations to find the next block. This provides a community which supports blockchain system continuously. The found block is shared with all nodes on the network which can then verify the correctness of the block by checking the hash calculation. If the found block is decided as a valid block, then nodes append the block into the chain. Bitcoin system depends on Proof-of-Work protocol to prevent misusages, attacks, and attacks on the network [16]. One of the biggest disadvantage of the proof-of-work is energy consumption. Since it requires excessively computational calculations to find the appropriate block, electricity usage is a crucial problem.

#### 2.2.4.2 Proof-of-stake

Blockchain systems that use proof-of-stake, make a randomized selection for the leader who will be responsible for the next block which will be appended to the chain. Similar to the proof-of-work protocol, the miner who found the next blockchain, is rewarded. Selection process is made among users who have an amount of cryptocurrency of the system. In addition, a user who has more amount of cryptocurrency is more likely to be selected. Although proof-of-stake partly resolves the energy consumption problem of the proof-of-work, new problems occur which do not exist in the proof-of-work protocol. For instance, malicious parties can try to influence the elective process in their selection process. This could allow them to earn more rewards than their actual rewards or they can double spend their money more easily [17].

#### 2.2.4.3 Delegated proof-of-stake

It is stated in [18] that, in Delegated Proof-of-Stake (dPOS), each node has right to vote, and the vote right is called token, which should be bought in public environment or be preassigned in private environment. Each token holder should choose several creators of blocks, which are responsible for writing information on blockchain in turn. If attackers want to make illegal changes, they must have 51% of the tokens, which must be costly to buy or steal from many accounts with tokens.

### 2.2.5 Hyperledger Fabric

Hyperledger Fabric is a blockchain framework implementation and one of the Hyperledger projects hosted by The Linux Foundation. Intended as a foundation for developing applications or solutions with a modular architecture. Hyperledger Fabric is an permissioned blockchain as shown in Table 2.4 that only authorized users are included in. It is difficult for external attackers to steal private data in Hyperledger Fabric because only authorized users can access the blockchain network [19]. Hyperledger Fabric was not designed for digital cash, and each transaction is directly recorded in a global ledger without verifying its legality. Therefore, for our specific use case it should be possible to use the framework publicly.

### 2.2.6 EOS

EOSIO platform was developed by the private company block.one and released as open-source software on June 1, 2018 [20]. EOS project addresses important aspects like creating peer-to-peer terms of service agreements, separating authentication from application. These aspects are very important if the aim is to create a decentralized peer-to-peer data marketplace. Similar to the authors' line of thinking, EOS Whitepaper [21] emphasizes that the piece of data to be stored in blockchain should be relevant to the application.

Recently, benchmarking firm Whiteblock concluded that the EOS token is essentially a cloud service for computation and is built on an entirely centralized premise. As such, it lacks some of blockchain's most fundamental aspects, like immutability. EOS is not a blockchain, rather a distributed homogeneous database management system, a clear distinction in that their transactions are not cryptographically validated. EOS block producers are highly centralized and users can only access the network using block producers as intermediaries. Block producers are a single point of failure for the entire system. The report indicates since EOS uses dPoS as a consensus protocol as shown in Table 2.4, it suffers from consensus failures with no Byzantine Fault Tolerance (BFT), leaving the network open to being controlled by rogue, colluding members [22]. Because of the all these suspicions about EOS blockchain, we thought it is not suitable for our framework.

**Table 2.4** : Blockchain development environment comparison.

| Environment | Network Type | Development Language | Transactions per second | Consensus Protocol |
|---|---|---|---|---|
| Hyperledger Fabric | Permissioned, Private | Go, JavaScript | 3,500 | BFT |
| EOS | Public, Private | C++ | 3,000 | dPoS |
| Ethereum | Public, Permissioned, Private | Solidity, Serpent | 15 | PoW |
| NEO | Public, Private | C#, Python | 1,000 | dBFT |

### 2.2.7 Ethereum

Ethereum was proposed in late 2013 by Vitalik Buterin and launch of Ethereum took place in July 2015 [23]. Ethereum blockchain is an public, open-source, distributed platform enables the verification of data integrity without relying on any third party. The distributed nature assures its service continuity however the use of blockchain also has drawbacks. Scalability of Ethereum remains an open issue, leaving doubts regarding its suitability for large scale systems [24]. Solidity is a programming language which is design for smart contract development in Ethereum framework [25].

Solidity was influenced by C++, Python and JavaScript and is designed to compile for the Ethereum Virtual Machine (EVM) [12]. Since, Solidity is a new programming language, we do not want to base all our work on it and Ethereum provides 15.6 transactions per seconds [26] which is not high enough for our use case, we did not prefer Ethereum for our framework.

### 2.2.8 NEO

NEO which was launched in 2015 as China's first public blockchain [27], is the use of blockchain technology and digital identity to digitize assets, and the use of smart contracts for digital assets to be self–managed. This establihes, what is called, a Smart Economy with a distributed network. Hence, it's a smart contracts ecosystem, similar to Ethereum [12]. NEP5 tokens are tokens that are managed by smart contracts on the NEO blockchain. Most existing NEO projects use a NEP5 token which describes the protocol that these tokens conform to, as the PAX token does as well.

NEO has two native tokens, NEO and NeoGas (GAS) [27]. NEO represents the right to manage the network with a total of 100 million tokens. Management rights include voting for bookkeeping, NEO network parameter changes, and so on. The minimum NEO unit is 1 and the tokens cannot be subdivided.

GAS is the fuel indicator for performing the NEO network resource control with a maximum total limit of over 100 million. NEO charges the network for the operation and storage of markers and smart contracts, thus creating economic incentives for accountants and preventing misuse of resources. The minimum GAS unit is 0.00000001.

#### 2.2.8.1 Delegated Byzantine Fault Tolerant

Delegated Byzantine Fault Tolerant (dBFT) is a Byzantine Fault Tolerant (BFT) consensus mechanism that allows extensive participation in proxy voting. The owner of the cryptocurrency can vote by voting on the accountant he supports. The selected group of accountants reach consensus through the BFT algorithm and generate new blocks [27]. NEO Framework which is used to develop PAX token uses dBFT protocol for the consensus mechanism [27]. Improved BFT algorithm which is adapted to be used in the NEO blockchain system, is described in [28] in detail.

#### 2.2.8.2 Smart contracts

Smart contracts which was first proposed in [29], are self-running scripts on the blockchain system. They allow making general purpose computations on the blockchain [30]. For instance, it is not possible to make a monthly automatic payment from your customer with standard blockchain system. However, companies can make monthly automatic payment with cryptocurrencies to their customer using smart contracts. Smart contracts are executed by a computer network which uses consensus protocols to ensure the order of actions that result from the contract's code. For a shared database that runs a blockchain protocol, the smart contracts are executed automatically and all parties immediately validate the result without the need for a third-party intermediary [31]. In addition, PAX Token is also smart contract that is used to define promotion amounts of the customers and merchants on the system.

In the NEO Frameworks, smart contracts are able to insert, query, and delete data in the persistent store. Such property is defined in the system as a *storage*. In addition, smart contracts can interact with each other which is named *dynamic invoke* property. While importing smart contracts into the blockchain system, it should be specified that whether smart contract needs storage and dynamic invoke. Although PAX token uses storage property to keep the amount of promotions in the customer loyalty program, it does not use dynamic invoke property since it does not interact with other smart contracts.

#### 2.2.8.3 NEP-5

The NEP-5 Proposal [32] outlines a token standard for the NEO blockchain that will provide systems with a generalized interaction mechanism for tokenized Smart Contracts. This mechanic, along with the justification for each feature is defined. A template and examples are also provided to enable the development community.

NEP-5 Standard requires some function implementations from smart contracts to work in NEO blockchain properly:

- totalSupply: Returns the total token supply deployed in the system
- name: Returns the name of the token
- symbol: Returns a short string symbol of the token managed in this contract
- decimals: Returns the number of decimals used by the token
- balanceOf(byte[] account): Returns the token balance of the account
- transfer(byte[] from, byte[] to, BigInteger amount): Transfers an amount of tokens from the from account to the to account

### 2.2.9 Comparison of NEO and Ethereum technologies

Each system design has trade-offs, thus we list three criteria for comparison below.

- Usability: In Ethereum (ETH), it is easy for a smart contract to interact with a user's balance of ETH, but difficult for a node to prove that a transaction has taken place without syncing the full chain and running the Ethereum Virtual Machine (EVM). In contrast, it is easy for third parties in NEO to verify that a transaction has taken place on the chain but more difficult for smart contracts to program interactions with a user's NEO or GAS balance.
- Transaction Throughput: Ethereum is still bound by Proof-of-Work, which limits the transactions to 10-30 transactions per second. While some solutions are currently in development to increase the throughput [33], most do require some trade-offs, and more importantly, none is still available. On the other hand, NEO does have fast transaction speeds, very cheap (current 0) gas costs, and high throughput, mainly derived from the use of Proof-of-Stake (PoS) [34] consensus implemented with the Delegated Byzantine Fault Tolerance (dBFT) [28] algorithm.
- Scalability: Transaction throughput scaling is a current problem in the blockchain space. Both options do propose future solutions, with Ethereum having Raiden [33] and others, and NEO also has its own proposals for future advances in scalability with the coming of sharding and state-channels.

### 2.2.10 Other application fields

In this section, application fields of the blockchain are covered according to different industries.

The Internet of Things involves collecting, processing and transmitting a wide variety of data to services and other devices. Business and engineering issues increase the both volume and detail of IoT data streams. Significant obvious confidentiality risks arise from IoT-connected devices while transmitting authenticated information, as this may reveal the activity of device users. When the bulk device data is available for analysis due to the identification or redefinition of users, and when linking to the helper data sets, there are more subtle risks [35]. It is stated in [36] that blockchain can solve some problems of the Internet of Things such as IoT node legal identity certification, data privacy and security issues, centralized databases are expensive and have limited computing and storage capabilities, IoT equipment maintenance and upgrading issues.

Recently, smart home appliances and wearable devices have been developed in many companies. Most devices can interact with various sensors, have a communication function to connect the Internet on their own. These devices will offer users a wide range of services through mutual exchange of information. However, because the nature of the IoT environment is likely to increase security threats and the impact of security threats is likely to expand, appropriate security functions should be applied extensively for safe and reliable smart home services [37]. In [38], they show that their proposed blockchain-based smart home framework is secure by thoroughly analyzing its security with respect to the fundamental security goals of confidentiality, integrity, and availability.

Supply chain usage cases are the most commonly used blockchain application to solve real business problems due to the lack of visibility of shipment data for product or component information when moving within the shipment supply chain. Each participant has visibility in the appropriate shipment data in the blockchain according to the participant's role. Logistics management systems are used by manufacturers to query the blockchain for shipping data and providing additional shipping information to the blockchain [39].

Financial technology (FinTech) sector has high potential value in cryptocurrency blockchain protocols or distributed ledger technology (DLT). The FinTech industry refers to this whole technology stack as distributed ledger technology; these layers represent two distinct opportunities: use the security and reliability of the underlying infrastructure and implement intelligent contract functionality [40].

It is stated in [41] that Blockchain Research Institute is beginning to look at a series of research reports and case studies on the potential impact of the blockchain on industries and the role and obstacles it faces in the health care industry. Because the blockchain for the cryptocurrency is an open or public blockchain that is universally transparent, everyone can look at the processes that have occurred. This may work for some applications, but is not suitable for medical information. As a result, the innovators have began to develop alternative blockchain protocols (e.g. Hyperledger [42]) to allow the transfer of value items in a more specific way. Therefore It is possible in the blockchain with alternative protocols that private health records can be saved and changed and people can vote.

The e-government system has greatly improved the efficiency and transparency of a government's daily operations. However, most of the existing e-government services are centrally provided and rely heavily on human individuals to control. The highly centralized infrastructure is more vulnerable to external attacks. Also, it is relatively easy to jeopardize data integrity by rogue users. In addition, relying on individuals to monitor and control some work flows makes the system vulnerable. To address these challenges, it is recommended in the [43] that using blockchain technology and decentralized autonomous organization (DAO) the e-government system can be improved. The Blockchain-based DAO system operates fully decentralized and is immune to both external and internal attacks. At the same time, the operations of such a system are controlled only by predefined rules. Thus, the uncertainty and errors caused by human processes are greatly reduced.

# 3. DESIGN AND IMPLEMENTATION OF THE PAX FRAMEWORK

In this chapter, we define the conceptual business model of PAX framework, describe the initial coin offering procedure and give information about development environment of PAX Framework and technical flow.

## 3.1 Conceptual Business Model of PAX Framework

In this section, the proposed PAX System including customer rewards, transactions between subjects is explained and business flow of the system is shown in the Figure 3.1.

Transaction data is preferred to be kept in blockchain system due to some problems with the traditional customer loyalty programs. Such a system provides persistent and consistent data for manufacturing companies. In addition, easy and useful programs are offered for users and merchants.

Promotion coupon is replaced with PAX token in the system. Customers do not need to keep physical coupon cards anymore. Instead of keeping cards, they just read the QR code on the card with their smartphone once and get the reward for their purchase. They keep and collect their rewards in their mobile wallet.

Blockchain-based customer loyalty program makes payback process between merchants and manufacturing companies easier. Since every transaction among subjects is kept in the blockchain system, manufacturing companies are able to keep the track of transactions for every merchant. In addition, merchants have certain amount of PAX tokens which comes from customers, in their corporate mobile wallets. Therefore, they make the payback for merchants based on the amount of PAX tokens in merchants' wallets instead of counting promotion cards.

Moreover, customers register to the customer loyalty program through their smartphones and customer loyalty program requests some information from customers such as age, gender, city and so on. Manufacturing companies can know and track customers better with this information because all of the promotion transactions between customers and merchants are kept in the blockchain system safely. Manufacturing companies can analyze these transactions to learn information such as the most preferred products in the cities, purchase volume of the cities, product preference according to gender and so on.

As shown in Figure 3.1, customers purchase a product (e.g. snack) which is kind of FMCG product and get the promotion card from the package. The transaction starts with the customers reading QR code on the promotion card by their mobile phone. Therefore, that promotion amount related to the corresponding QR code is sent to customers' wallets as a PAX token. After reading QR code from the disposable cards, they do not need the card anymore which eliminates the possibility of the lost coupons. If customers collect enough PAX tokens to get a gift, they can go to merchants to get promotion products with their PAX tokens. For the purchase processes, merchants show QR code which refers to merchants' wallet, for the customers and customers read that QR code to send required amount of PAX to merchants' wallet. In the end, merchants can request products with collected PAX tokens from manufacturing companies. They exchange PAX tokens with the products just like customers interacted with them. Using this procedure, manufacturing companies can make a payback to the merchants.

### 3.2 Initial Coin Offering

Initial Coin Offerings (ICO) are the public offerings of new cryptocurrency in return for existing ones, mostly aimed at financing projects in the blockchain development arena. [44]. Users who want to join ICO, need to register for ICO and then they need to make payment with required amount of NEO or GAS token according to requested PAX token. ICO is an optional feature of the PAX framework, manufacturing companies which uses PAX framework, can decide whether using or not using ICOs. Since ICO process public network usage from manufacturers' side, companies which use PAX framework with their own private network, cannot use ICO feature.

Know Your Customer (KYC) is one of the Anti Money Laundering (AML) procedure which is also provided by PAX Framework. Manufacturing companies can choose to require participants to get verified before contributing to ICO. This works by

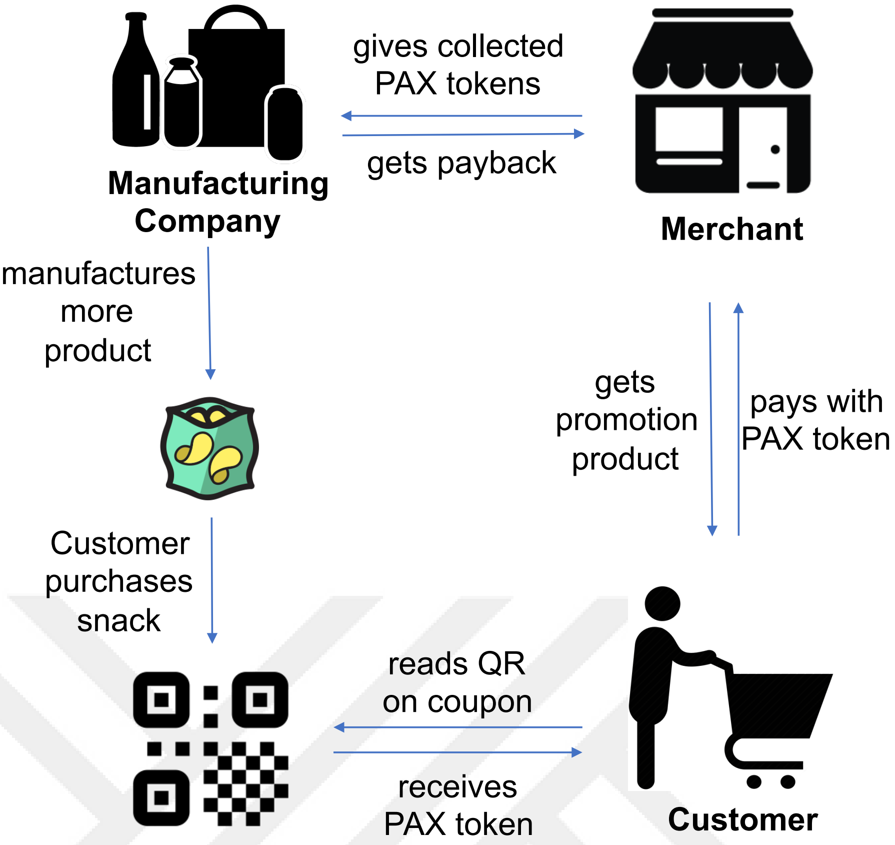


**Figure 3.1** : Business blow of the PAX token transactions.

whitelisting participant addresses before they can receive their PAX tokens. In addition, PAX framework provides simplified refund and rejection mechanism which includes several methods to avoid invalid ICO contributions and to automatically process refunds. For instance, when a participant is not yet whitelisted, or contributes outside the ICO window.

Definition of the PAX Token with its parameters are shown below:

```
TOKEN_NAME = ’Promotion Asset Exchange’
TOKEN_SYMBOL = ’PAX’
TOKEN_DECIMALS = 8
TOKEN_OWNER =
b’#\xba\’\x03\xc52c\xe8\xd6\xe5"\xdc2 39\xdc\xd8\xee\xe9’
TOKEN_TOTAL_SUPPLY = 10000000 ⋆ 100000000
TOKEN_INITIAL_AMOUNT = 2500000 ⋆ 100000000
TOKENS_PER_NEO = 40 ⋆ 100000000
TOKENS_PER_GAS = 20 ⋆ 100000000
```

```
MAX_EXCHANGE_LIMITED_ROUND = 500 * 40 * 100000000
BLOCK_SALE_START = 1
LIMITED_ROUND_END = 1 + 10000
KYC_KEY = b’kyc_ok’
```

- TOKEN_NAME: Name of the token in the blockchain
- TOKEN_SYMBOL: Symbol of the token in the blockchain
- TOKEN_DECIMALS: Decimals of the token in the blockchain. Decimals means how divisible a token can be referring to number of digits that come after the decimal place when displaying token values on-screen.
- TOKEN_OWNER: Address of the token’s owner wallet.
- TOKEN_TOTAL_SUPPLY: Total possible number of token that will be created.
- TOKEN_INITIAL_AMOUNT: Initial number of token that will be created. This amount will be transferred to owner’s wallet.
- TOKENS_PER_NEO: Value of 1 NEO in terms of PAX token which will be used during ICO.
- TOKENS_PER_GAS: Value of 1 GAS in terms of PAX token which will be used during ICO.
- MAX_EXCHANGE_LIMITED_ROUND: Maximum number of tokens can be exchanged during ICO.
- BLOCK_SALE_START: Number of the block that ICO will be available.
- LIMITED_ROUND_END: Number of the block that ICO will end.
- LIMITED_ROUND_END: Number of the block that ICO will end.
- KYC_KEY: Key indicator whether KYC will be activated or not.

As shown in Figure 3.2, *crowdsale_register [addr1, addr2, ...]* method provides an ICO operator which is manufacturer in our framework, with the ability to specify an address or list of addresses as eligible for the ICO. Then, users can check KYC status of their address with *crowdsale_status [addr]* method. Once an address is KYC registered, users can participate in the ICO by invoking the *mintTokens* method with some attached NEO / GAS.

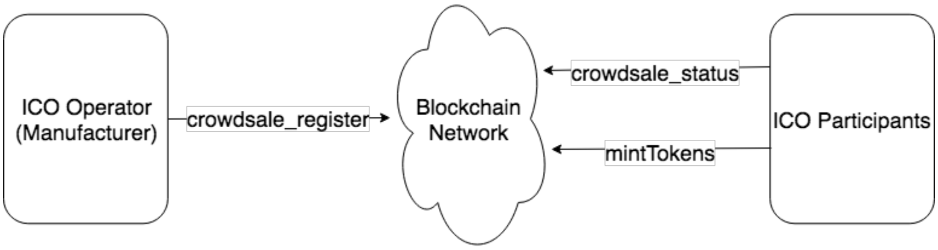


**Figure 3.2** : Initial coin offering with know your customer procedure.

### 3.3 Development Environment

Different tools which are provided by NEO Community, is used for this study.

- Neo-python: Neo-python [45] is Python Node and SDK for the NEO blockchain. This project aims to be a full port of the original C# NEO project [46].
- Neonjs: Neonjs [47] the JavaScript SDK for the NEO blockchain platform. This project aims to be a lightweight library focused on providing blockchain interactions in the browser.
- Neonscan: Neoscan [48] is blockchain explorer for NEO framework. It shows created wallets and transactions in the network.
- Private Network: For development environment Docker container [49] which is provided by NEO Community, is used. It works on a private network locally and has four NEO full nodes in its private network. PAX smart contract is deployed to this private network.

### 3.4 Technical Flow

As shown in the Figure 3.3, PAX Framework presents a mobile application for users. All users of the system which are customers, merchants, and manufacturing companies, notify the back-end server with that mobile application in their smartphone, through REST APIs. Back-end server communicates with blockchain system to store transactions between users. Communication between the back-end server and blockchain system provided by smart contract. Therefore, PAX token transactions between subjects are recorded on the blockchain system regularly.

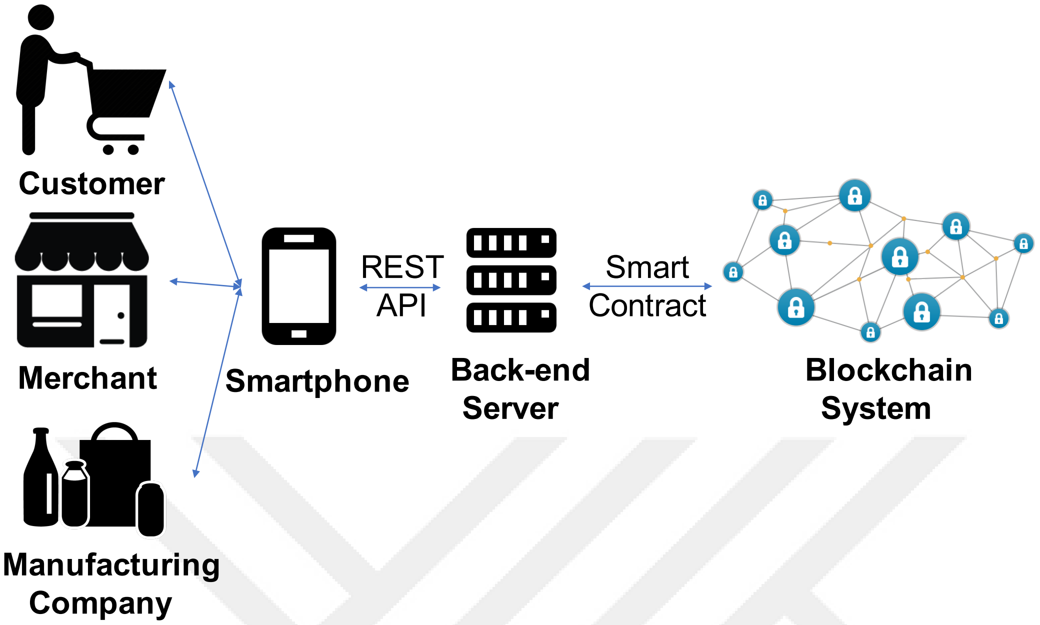


**Figure 3.3** : Technical design of blockchain-based customer loyalty program.

Mobile applications are native applications that are developed in iOS and Android platforms with Swift and Java languages respectively. They use REST APIs that are provided by the back-end server. Back-end server is developed using Sails [50]. It communicates with blockchain system through neon-js [47]. Neon-js provides an interface to interact with blockchain system and uses smart contracts. Blockchain system uses NEO framework [27].

PAX token is developed based on NEO Framework [27]. It is used on the private blockchain networks according to manufacturing companies. Neo-python environment [45] which is Python Node and SDK of the NEO framework is used for token development purposes. In addition, smart contracts are developed in Python language.

PAX token is defined in the system with its hash value. While communicating with the system, hash of the PAX token is used to make a transaction. Definition of the PAX token on the system is shown below:

```
{
    "version": 0,
    "code": {
        "hash": "0x8de01ed10f10319bd
                caa7993040c7a7b4dc39d74",
        "script": "0124c56b6a00527a...
                  561936a5752796c7566",
        "parameters": "0710",
        "returntype": 5
    },
    "name": "Promotion Asset Exchange (PAX)
            token",
    "code_version": "1",
    "author": "Seref Bulbul",
    "email": "seref.bulbul@itu.edu.tr",
    "description": "Blockchain-based
                    Customer Loyalty
                    Program with PAX
                    token",
    "properties": {
        "storage": true,
        "dynamic_invoke": false
    }
}
```

PAX token transactions are handled with smart contract functions. There are three main functions available get_promotion_pax, purchase_product, request_payback. These functions are not related to the user but back-end server calls these functions to make transactions.

- get_promotion_pax(qr_code): Customers read QR code with their smartphone and trigger this smart contract function through back-end server to get their PAX tokens.

- purchase_product(merchant_address, product_id): While customers get promotion product from merchants, they use this smart contract function to make a payment.
- request_payback(pax_amount): Payback between merchants and manufacturing companies is handled with this function. It gets requested amount of PAX token from merchant and notify the manufacturing company.

Thanks to PAX Framework, manufacturers does not need to cooperate with third party companies and share their data with them. Furthermore, they gather all the information about their loyalty program since transactions are kept in the blockchain system safely. Therefore, we discuss practicality and utility of PAX Framework in terms of the following:

- Customer engagement: Since customers participate in the program through their mobile application, number of the registered user indicates the engagement of the customers.
- Purchase frequency: Customers use their mobile wallets to get promotion products from merchants so repeated transactions can be tracked and measured through blockchain system.
- Tracking newcomer customers: Newly joined customers can be tracked with the PAX Framework.
- Measurability of the profit: Since all transactions and usage statistics can be reached from PAX Framework, it is quite easier to measure profit of the loyalty programs with the comparison of the data before and after loyalty programs.

# 4. EXPERIMENTS AND RESULTS

In this chapter, we illustrate the simulation of our proposed framework with different number of nodes and transactions to evaluate its scalability. Then, we prove the traceability of PAX framework and show its block and transaction data.

## 4.1 Experimental Conditions

Experiments were carried out on a NEO Docker container [49] which runs on the MacBook Pro (Retina, 15-inch, Mid 2015) with 2,2 GHz Intel Core i7 and 16 GB 1600 MHz DDR3 RAM.

## 4.2 Results

In this section, results of the scalability and traceability experiments are presented.

### 4.2.1 Results of scalability

It is aimed to examine effect of number of nodes in the blockchain for transaction confirmation times. NEO Docker container provides 4 default nodes on the blockchain network. We applied 1, 10 and 20 transactions per set on the working blockchain with 4, 8 and 16 nodes. Results visualized as Figure 4.1 depict the relation between the number of peers and the corresponding time taken for confirming N transactions. In the Figure 4.1, y axis refers to the confirmation time of the transactions in seconds and x axis refers to the number of transactions in terms of 4, 8 and 16 nodes.

It is clearly noticeable that more the number of nodes, more will be the confirmation time. This is caused by the requirement for more number of endorsements and more number of validations. Therefore, less number of nodes means that consensus is reached faster.

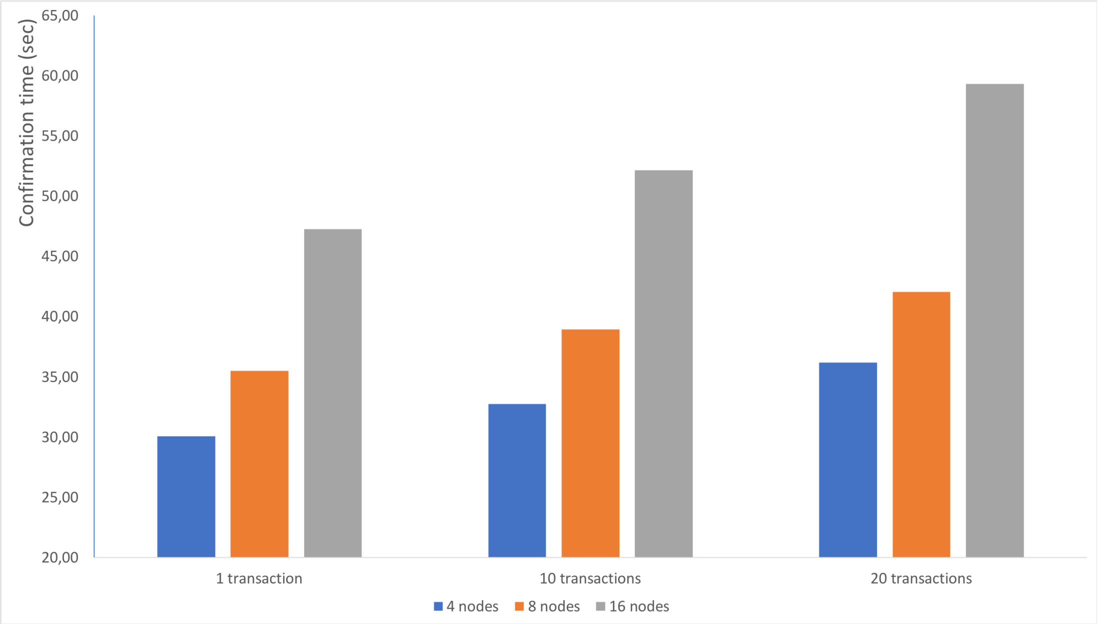


**Figure 4.1** : Confirmation times in terms of number of nodes.

### 4.2.2 Results of performance test

To test system performance under the load, 100 users created in the system and every user sends PAX token to another user at the same time. Therefore, 100 transactions created and this process is repeated 15 times. At the end, total 1500 transactions are created. Confirmation times of the every transaction set is shown in the Figure 4.2 and related CPU usage of the system during that period is shown in the Figure 4.3.

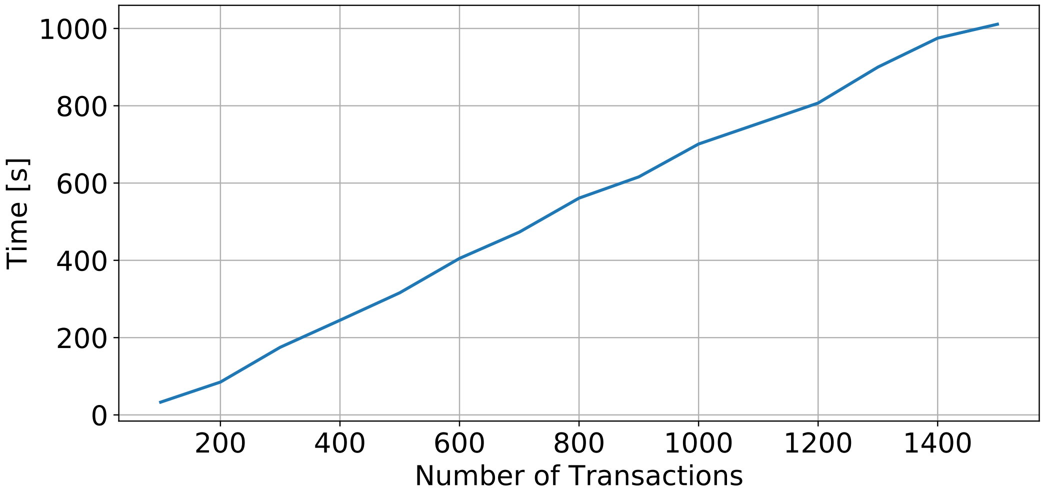


**Figure 4.2** : Transaction confirmation times for every set of 100 transactions.

In the Figure 4.2, y axis refers to the transaction confirmation times of the set of 100 transactions and x axis refers to the number of the transactions in an increasing order 100 to 1500.

In the Figure 4.3, y axis refers to the CPU usage of the NEO blockchain network Docker container and x axis refers to the time in seconds during transaction simulation. Peaks in the Figure 4.3 indicates that nodes in the blockchain network work to generate the next block which includes transactions.

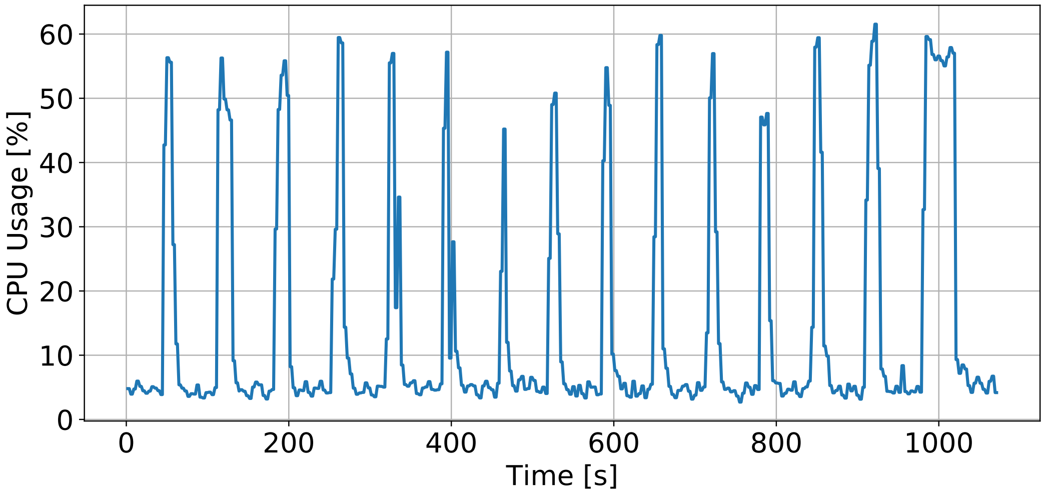


**Figure 4.3** : CPU usage during transaction simulation for every set of 100 transactions.

It can be examined from the Figures 4.2 and 4.3 that confirmation times and related CPU usages are consistent to each other.

To test system performance by forcing CPU, 1000 users created in the system and every user sends PAX token to another user consecutively in a short time. Therefore, 1000 transactions created and this process is repeated 10 times. At the end, total 10000 transactions are created. Confirmation times of the every transaction set is shown in the Figure 4.4 and related CPU usage of the system during that period is shown in the Figure 4.5. In the Figure 4.4, y axis refers to the transaction confirmation times of the set of 1000 transactions and x axis refers to the number of the transactions in an increasing order 1000 to 10000.

In the Figure 4.5, y axis refers to the CPU usage of the NEO blockchain network Docker container and x axis refers to the time in seconds during transaction simulation. Peaks in the Figure 4.5 indicates that nodes in the blockchain network work to generate

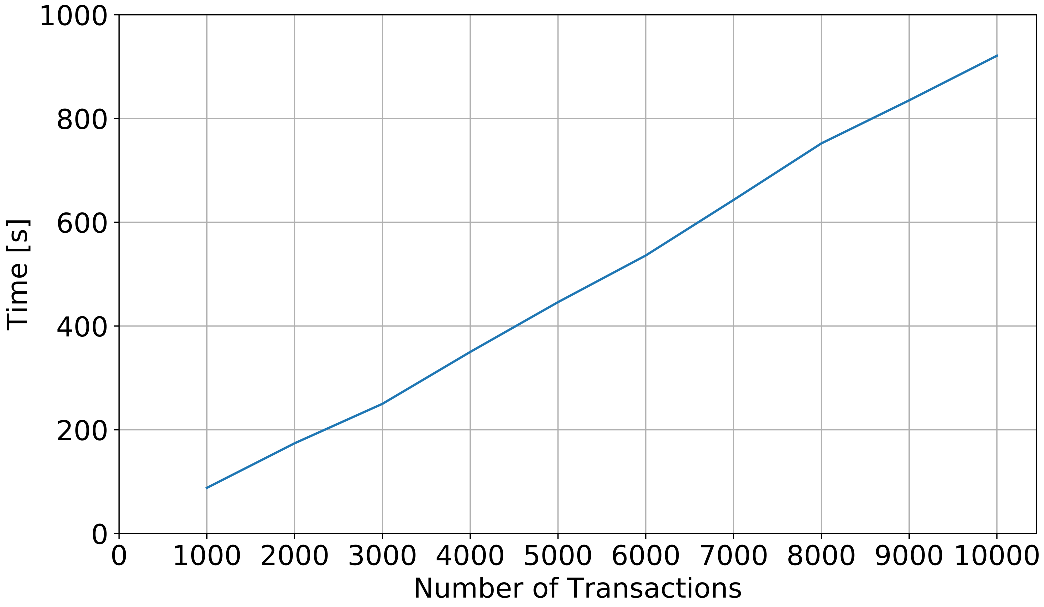


**Figure 4.4** : Transaction confirmation times for every set of 1000 transactions.

the next block which includes transactions. Since 1000 transactions are generated consecutively, transaction confirmations are completed in the 2 successive blocks. Therefore, 2 blocks are created in the blockchain for every confirmations of the 1000 transactions.

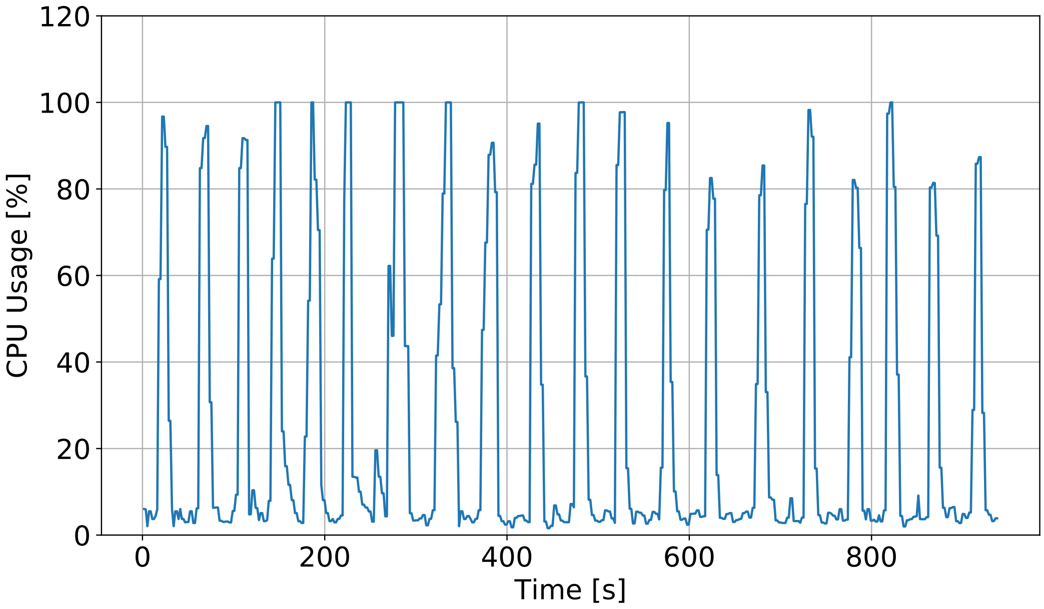


**Figure 4.5** : CPU usage during transaction simulation for every set of 1000 transactions.

It can be examined from the Figures 4.4 and 4.5 that confirmation times and related CPU usages are consistent to each other. It is obvious that CPU usage of the Docker container can go up to 100% for block creation with many transactions.

### 4.2.3 Results of traceability

It is aimed to verify blockchain system's traceability with simulation including a manufacturer company, a merchant and a customer. User wallets, created blocks and transactions are shown on Neoscan [48]. Defined subjects and related wallet addresses are shown in table 4.1.

**Table 4.1** : Wallet addresses of the subjects on the blockchain system.

| Wallet Owner | Wallet Address |
|---|---|
| Manufacturer Company | AK2nJJpJr6o664CWJKi1QRXjqeic2zRp8y |
| Merchant 1 | AJe24NjpjCDPkpKgYdGtg7Jy5CXNosn371 |
| Customer 1 | AZDbKdqH9V9mAYsiXVCujs4q1MeHiUPbaw |

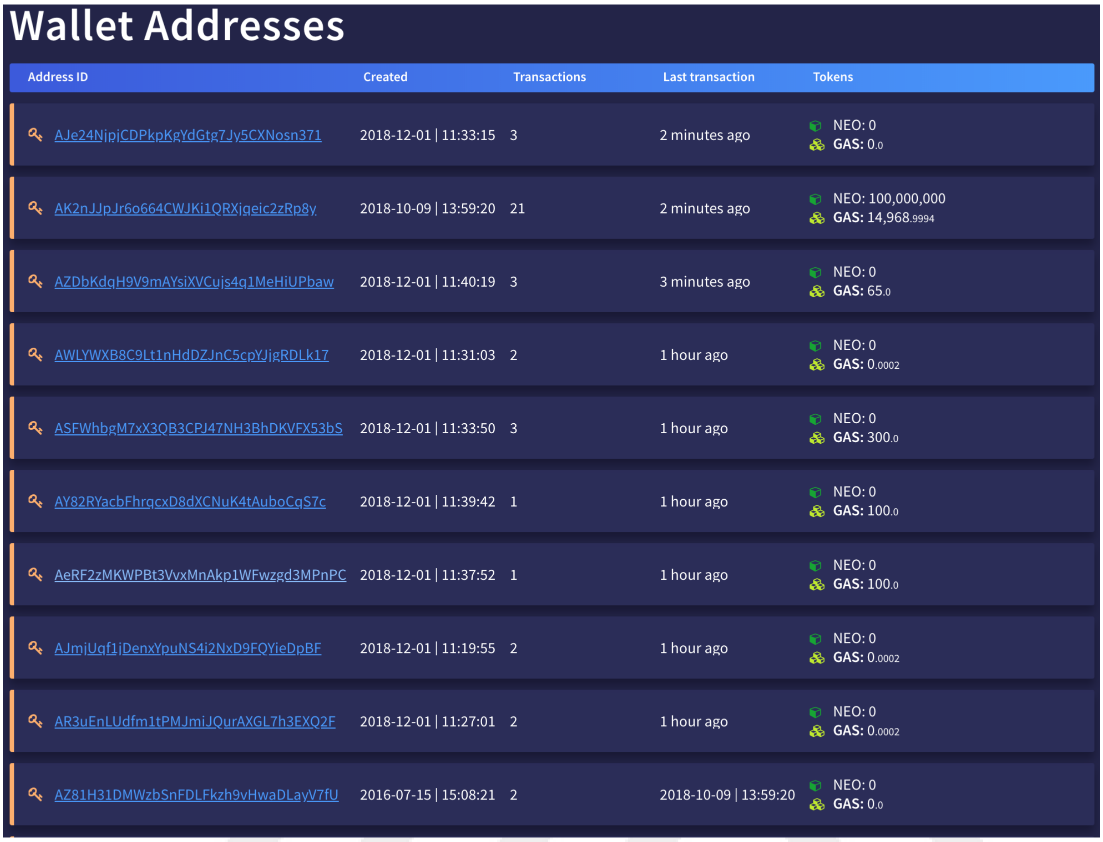
Generated user wallets can be listed on the Neoscan as shown in the Figure 4.6. In addition, creation time of the wallets, transaction counts, last transaction dates and owned token amounts in terms of NEO and GAS can be followed.

When Customer 1 buy snack and read its QR code, he gains 15 PAX token which is transferred from manufacturer's wallet as shown in the Figure 4.7.

If Customer 1 gains enough PAX tokens, he can go to Merchant 1 and get its promotion product. When he gets the promotion product, he sends 50 PAX to the merchant as shown in the Figure 4.8.

When manufacturer wants to payback for Merchant 1, it gets all PAX tokens from Merchant 1 and makes the payback according to its procedure. Related payback transaction from Merchant 1 to manufacturer's wallet is shown in the Figure 4.9.

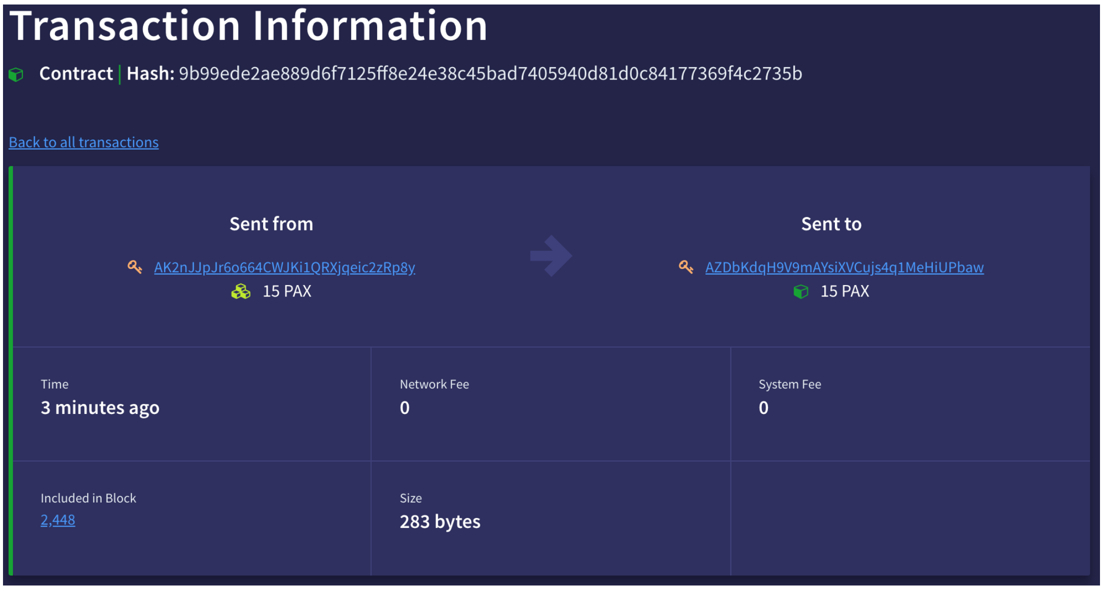
Obviously, transactions between subjects on the blockchain system can be observed and traced in a visualized manner thanks to Neoscan.



## Wallet Addresses

| Address ID | Created | Transactions | Last transaction | Tokens |
|---|---|---|---|---|
| AJe24NjpjCDPkpKgYdGtg7Jy5CXNosn371 | 2018-12-01 \| 11:33:15 | 3 | 2 minutes ago | NEO: 0<br>GAS: 0.0 |
| AK2nJJpJr6o664CWJKi1QRXjqeic2zRp8y | 2018-10-09 \| 13:59:20 | 21 | 2 minutes ago | NEO: 100,000,000<br>GAS: 14,968.9994 |
| AZDbKdqH9V9mAYsiXVCujs4q1MeHiUPbaw | 2018-12-01 \| 11:40:19 | 3 | 3 minutes ago | NEO: 0<br>GAS: 65.0 |
| AWLYWXB8C9Lt1nHdDZJnC5cpYJjgRDLk17 | 2018-12-01 \| 11:31:03 | 2 | 1 hour ago | NEO: 0<br>GAS: 0.0002 |
| ASFWhbgM7xX3QB3CPJ47NH3BhDKVFX53bS | 2018-12-01 \| 11:33:50 | 3 | 1 hour ago | NEO: 0<br>GAS: 300.0 |
| AY82RYacbFhrqcxD8dXCNuK4tAuboCqS7c | 2018-12-01 \| 11:39:42 | 1 | 1 hour ago | NEO: 0<br>GAS: 100.0 |
| AeRF2zMKWPBt3VvxMnAkp1WFwzgd3MPnPC | 2018-12-01 \| 11:37:52 | 1 | 1 hour ago | NEO: 0<br>GAS: 100.0 |
| AJmjUqf1jDenxYpuNS4i2NxD9FQYieDpBF | 2018-12-01 \| 11:19:55 | 2 | 1 hour ago | NEO: 0<br>GAS: 0.0002 |
| AR3uEnLUdfm1tPMJmiJQurAXGL7h3EXQ2F | 2018-12-01 \| 11:27:01 | 2 | 1 hour ago | NEO: 0<br>GAS: 0.0002 |
| AZ81H31DMWzbSnFDLFkzh9vHwaDLayV7fU | 2016-07-15 \| 15:08:21 | 2 | 2018-10-09 \| 13:59:20 | NEO: 0<br>GAS: 0.0 |

**Figure 4.6** : Wallets on Neoscan.



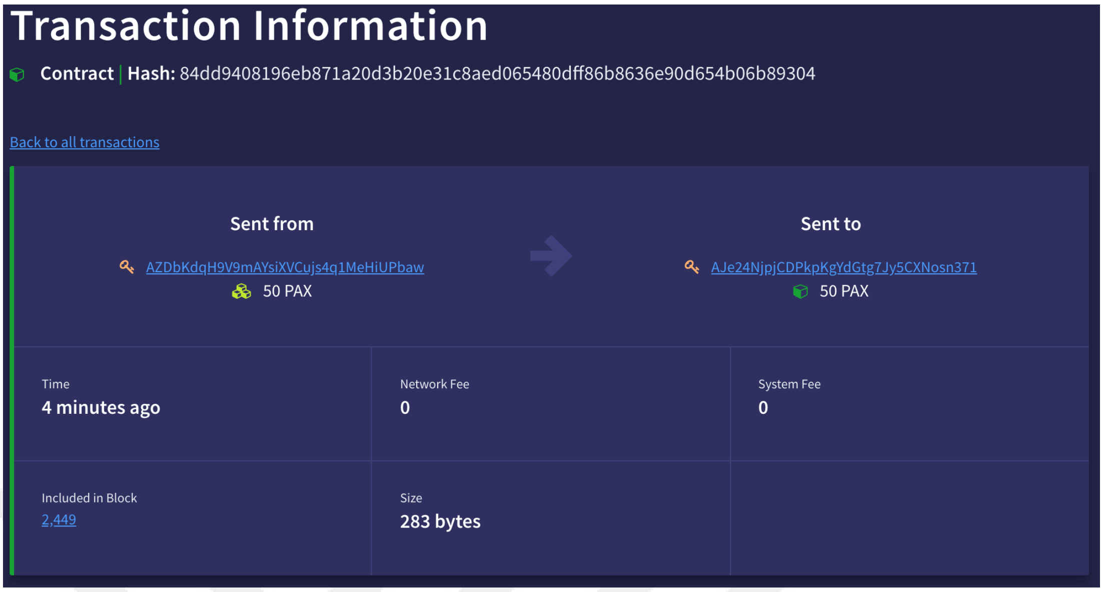
## Transaction Information

**Contract** | **Hash:** 9b99ede2ae889d6f7125ff8e24e38c45bad7405940d81d0c84177369f4c2735b

Back to all transactions

| Sent from | | Sent to |
|---|---|---|
| AK2nJJpJr6o664CWJKi1QRXjqeic2zRp8y<br>15 PAX | ➔ | AZDbKdqH9V9mAYsiXVCujs4q1MeHiUPbaw<br>15 PAX |
| Time<br>3 minutes ago | Network Fee<br>0 | System Fee<br>0 |
| Included in Block<br>2,448 | Size<br>283 bytes | |

**Figure 4.7** : Customer 1's QR code reading transaction on Neoscan.



Transaction Information

Contract | Hash: 84dd9408196eb871a20d3b20e31c8aed065480dff86b8636e90d654b06b89304

Back to all transactions

Sent from

AZDbKdqH9V9mAYsiXVCujs4q1MeHiUPbaw
50 PAX

Sent to

AJe24NjpjCDPkpKgYdGtg7Jy5CXNosn371
50 PAX

Time
4 minutes ago

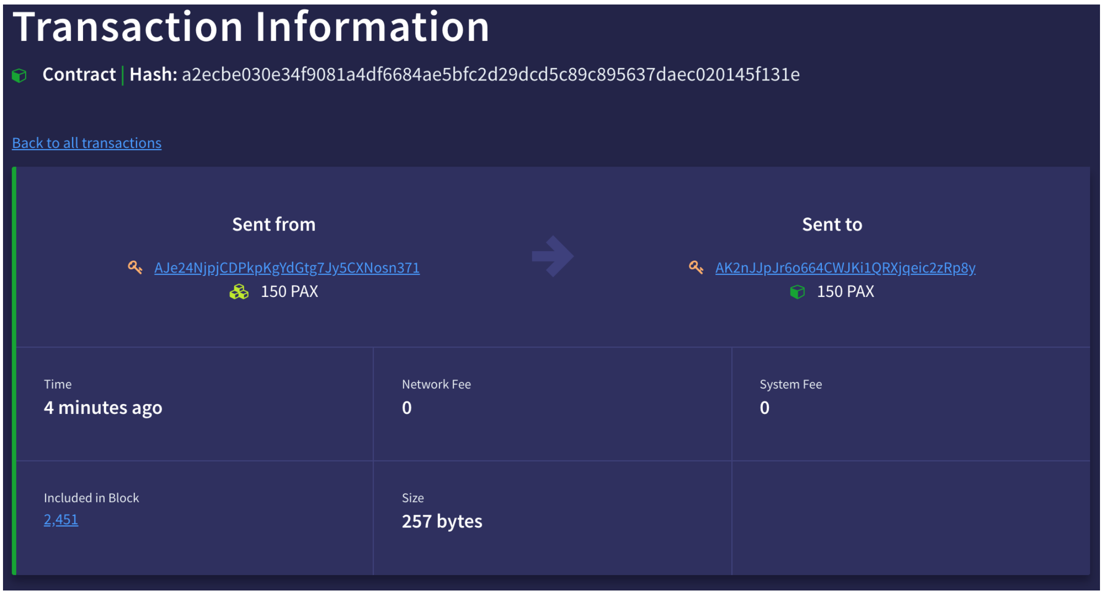
Network Fee
0

System Fee
0

Included in Block
2,449

Size
283 bytes

**Figure 4.8** : Customer 1's promotion buy transaction from Merchant 1 with PAX tokens on Neoscan.



Transaction Information

Contract | Hash: a2ecbe030e34f9081a4df6684ae5bfc2d29dcd5c89c895637daec020145f131e

Back to all transactions

Sent from

AJe24NjpjCDPkpKgYdGtg7Jy5CXNosn371
150 PAX

Sent to

AK2nJJpJr6o664CWJKi1QRXjqeic2zRp8y
150 PAX

Time
4 minutes ago

Network Fee
0

System Fee
0

Included in Block
2,451

Size
257 bytes

**Figure 4.9** : Merchant 1's payback transaction from Manufacturer 1 on Neoscan.

## 5. CONCLUSION AND FUTURE WORK

In this thesis, we investigated the bottlenecks of the traditional customer loyalty programs in FMCG industry. We propose Promotion Asset Exchange (PAX) Framework, a blockchain-based customer loyalty program. We prefer to use NEO for PAX framework implementation instead of Hyperledger Fabric, EOS and Ethereum. PAX Framework digitalizes the transaction process between subjects which are customers, merchants and manufacturing companies. It replaces regular promotion cards with mobile wallets and keeps all transactions in the blockchain system. Therefore, the usability of the system is increased, manufacturing companies can better know the customers and manufacturers also can use ICO to generalize their token usage between customers. Moreover, manufacturers do not need to collaborate with third-party companies so they do not share their data and spend effort for integration anymore.

As described in the Chapter 4, if number of nodes in the blockchain system increases, transaction confirmations times increase. In addition, blockchain system can responds to concurrent transactions similarly in different time periods and CPU usage of the system increases when nodes on the system try to generate the next block. Moreover, blockchain system keeps all transactions from the beginning which provides traceability of the system so manufacturers can observe their customer loyalty programs.

We plan to implement PAX Framework based on Hyperledger Fabric environment [42] for private network usages. Then we aim to compare the performance of the systems in terms of transaction confirmation time and transactions per second. According to results it is possible to use NEO for public solutions and Hyperledger Fabric for private solutions.

## REFERENCES

[1] Blockchain.com Bitcoin Block, `https://www.blockchain.com/en/btc/block-height/549855`, accessed: 2018-11-13.

[2] Blockchain.com Bitcoin Transaction, `https://blockexplorer.com/tx/dc8559f78f723abe4808fef57f12eee5921de861c9dc7e81-06ce58fb9553ca98`, accessed: 2018-11-13.

[3] Global Bitcoin Nodes Distribution, `https://bitnodes.earn.com/`, accessed: 2018-11-13.

[4] **Nakamoto, S.** (2008). Bitcoin: A peer-to-peer electronic cash system, `https://bitcoin.org/bitcoin.pdf`, accessed: 2018-05-03.

[5] **Di Pierro, M.** (2017). What Is the Blockchain?, *Computing in Science & Engineering*, *19*(5), 92–95.

[6] **Underwood, S.** (2016). Blockchain beyond bitcoin, *Communications of the ACM*, *59*(11), 15–17.

[7] **Yang, K.F.**, **Chiang, Y.C. and Lin, Y.S.** (2018). A Study on Service Quality, Customer Satisfaction, and Customer Loyalty: The Case of PChome, *Proceedings of the 2nd International Conference on E-Society, E-Education and E-Technology*, ACM, pp.88–93.

[8] **Dowling, G.R. and Uncles, M.** (1997). Do customer loyalty programs really work?, *Sloan management review*, *38*(4), 71.

[9] **Berman, B.** (2006). Developing an effective customer loyalty program, *California management review*, *49*(1), 123–148.

[10] **Christidis, K. and Devetsikiotis, M.** (2016). Blockchains and smart contracts for the internet of things, *IEEE Access*, *4*, 2292–2303.

[11] **Zheng, Z.**, **Xie, S.**, **Dai, H.**, **Chen, X. and Wang, H.** (2017). An overview of blockchain technology: Architecture, consensus, and future trends, *Big Data (BigData Congress), 2017 IEEE International Congress on*, IEEE, pp.557–564.

[12] **Ethereum**, ethereum/wiki, `https://github.com/ethereum/wiki/wiki/White-Paper`, accessed: 2018-05-23.

[13] **Szydlo, M.** (2004). Merkle tree traversal in log space and time, *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp.541–554.

[14] **Awasthi, D.** (2015). Barter to bitcoin: the changing visage of transactions, *Elk Asia Pacific Journal of Finance and Risk Management*, *6*(4).

[15] **Donet, J.A.D.**, **Pérez-Sola, C. and Herrera-Joancomartí, J.** (2014). The bitcoin P2P network, *International Conference on Financial Cryptography and Data Security*, Springer, pp.87–102.

[16] **Karame, G.** (2016). On the security and scalability of bitcoin's blockchain, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM, pp.1861–1862.

[17] **Siim, J.** (2017). Proof-of-Stake, *Research Seminar in Cryptography*.

[18] **Hu, Y.**, **Xiong, Y.**, **Huang, W. and Bao, X.** (2018). KeyChain: Blockchain-Based Key Distribution, *2018 4th International Conference on Big Data Computing and Communications (BIGCOM)*, IEEE, pp.126–131.

[19] **Gao, F.**, **Zhu, L.**, **Shen, M.**, **Sharif, K.**, **Wan, Z. and Ren, K.** (2018). A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks, *IEEE Network*.

[20] EOS An Introduction, `https://eos.io/documents/EOS_An_Introduction.pdf`, accessed: 2018-12-08.

[21] EOS Technical White Paper, `https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md`, accessed: 2018-12-08.

[22] Whiteblock completes industry's first EOS benchmark testing and blockchain investigation, `https://www.prnewswire.com/news-releases/whiteblock-completes-industrys-first-eos-benchmark-testing-and-blockchain-investigation-300742130.html`, accessed: 2018-12-08.

[23] **Juels, A.**, **Kosba, A. and Shi, E.** (2016). The ring of Gyges: Investigating the future of criminal smart contracts, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM, pp.283–295.

[24] **Chanson, M.**, **Bogner, A.**, **Wortmann, F. and Fleisch, E.** (2017). Blockchain as a privacy enabler: an odometer fraud prevention system, *Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers*, ACM, pp.13–16.

[25] **Rocha, H.**, **Ducasse, S.**, **Denker, M. and Lecerf, J.** (2017). Solidity parsing using smacc: Challenges and irregularities, *Proceedings of the 12th edition of the International Workshop on Smalltalk Technologies*, ACM, p. 2.

[26] **Özyilmaz, K.R.**, **Doğan, M. and Yurdakul, A.** (2018). IDMoB: IoT Data Marketplace on Blockchain, *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, IEEE, pp.11–19.

[27] **Zhang, E. and Hongfei, D.**, NEO White Paper, `http://docs.neo.org/en-us/whitepaper.html`, accessed: 2018-10-29.

[28] A Byzantine Fault Tolerance Algorithm for Blockchain, `http://docs.neo.org/en-us/basic/consensus/whitepaper.html`, accessed: 2018-05-12.

[29] **Szabo, N.** (1997). Formalizing and securing relationships on public networks, *First Monday*, *2*(9).

[30] **Luu, L.**, **Chu, D.H.**, **Olickel, H.**, **Saxena, P. and Hobor, A.** (2016). Making smart contracts smarter, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM, pp.254–269.

[31] Applications of Blockchain Technology to Banking and Financial Sector in India, `http://www.idrbt.ac.in/assets/publications/Best\%20Practices/BCT.pdf`, accessed: 2018-06-07.

[32] NEP-5 Token Standard, `https://github.com/neo-project/proposals/blob/master/nep-5.mediawiki`, accessed: 2018-10-29.

[33] Ethereum Raiden Network, `https://raiden.network/`, accessed: 2019-10-29.

[34] **Tosh, D.**, **Shetty, S.**, **Foytik, P.**, **Kamhoua, C. and Njilla, L.** (2018). CloudPoS: A Proof-of-Stake Consensus Design for Blockchain Integrated Cloud, *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, IEEE, pp.302–309.

[35] **Wilson, S.**, **Moustafa, N. and Sitnikova, E.** (2018). A digital identity stack to improve privacy in the IoT, *Internet of Things (WF-IoT), 2018 IEEE 4th World Forum on*, IEEE, pp.25–29.

[36] **Li, S.** (2018). Application of Blockchain Technology in Smart City Infrastructure, *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*, IEEE, pp.276–2766.

[37] **Han, J.H.**, **Jeon, Y. and Kim, J.** (2015). Security considerations for secure and trustworthy smart home system in the IoT environment, *Information and Communication Technology Convergence (ICTC), 2015 International Conference on*, IEEE, pp.1116–1118.

[38] **Dorri, A.**, **Kanhere, S.S.**, **Jurdak, R. and Gauravaram, P.** (2017). Blockchain for IoT security and privacy: The case study of a smart home, *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on*, IEEE, pp.618–623.

[39] **Miller, D.** (2018). Blockchain and the Internet of Things in the Industrial Sector, *IT Professional*, *20*(3), 15–18.

[40] **Eyal, I.** (2017). Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities, *Computer*, *50*(9), 38–49.

[41] **Mertz, L.** (2018). (Block) Chain Reaction: A Blockchain Revolution Sweeps into Health Care, Offering the Possibility for a Much-Needed Data Solution, *IEEE Pulse*, *9*(3), 4–7.

[42] Hyperledger, `https://www.hyperledger.org/`, accessed: 2018-10-28.

[43] **Diallo, N.**, **Shi, W.**, **Xu, L.**, **Gao, Z.**, **Chen, L.**, **Lu, Y.**, **Shah, N.**, **Carranco, L.**, **Le, T.C.**, **Surez, A.B.** *et al.* (2018). eGov-DAO: a Better Government using Blockchain based Decentralized Autonomous Organization, *eDemocracy & eGovernment (ICEDEG), 2018 International Conference on*, IEEE, pp.166–171.

[44] **Fenu, G.**, **Marchesi, L.**, **Marchesi, M. and Tonelli, R.** (2018). The ICO phenomenon and its relationships with ethereum smart contract environment, *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, pp.26–32.

[45] neo-python, `https://github.com/CityOfZion/neo-python`, accessed: 2018-05-15.

[46] NEO, `https://github.com/neo-project/neo`, accessed: 2018-10-29.

[47] neo-js, `http://cityofzion.io/neon-js/`, accessed: 2018-05-22.

[48] Neoscan, `https://github.com/CityOfZion/neo-scan/`, accessed: 2018-10-30.

[49] NEO Privatenet Docker Container, `https://hub.docker.com/r/cityofzion/neo-privatenet/`, accessed: 2018-10-29.

[50] Sailsjs, `https://sailsjs.com/`, accessed: 2018-05-29.

## CURRICULUM VITAE

**Name Surname:** Şeref Bülbül

**Place and Date of Birth:** K.maraş/TURKEY, 24.05.1993

**E-Mail:** seref.bulbul@itu.edu.tr

**M.Sc.:** Computer Engineering in Istanbul Technical University, December 2018

**B.Sc.:** Computer Engineering in Istanbul Technical University, July 2016

## PUBLICATIONS/PRESENTATIONS ON THE THESIS

- **Ş. Bülbül** and G. İnce, "Blockchain-based Framework for Customer Loyalty Program", *2018 3rd International Conference on Computer Science and Engineering (UBMK)*, Sarajevo, Bosnia and Herzegovina, 2018, pp. 342-346.