Blockchain-based Framework for Customer Loyalty Program

Şeref Bülbül[1,2], Gökhan İnce[1]
[1]Faculty of Computer and Informatics Engineering
Istanbul Technical University
[2]Adesso Turkey Information Technologies Ltd. Şti
Istanbul, Turkey
{seref.bulbul, gokhan.ince}@itu.edu.tr

***Abstract*—Traditional customer loyalty programs in the Fast-Moving Consumer Goods industry have several bottlenecks such as lost paper-based coupons and payback process complications. This paper presents the design of a blockchain-based customer loyalty program called Promotion Asset Exchange (PAX) framework, to solve bottlenecks in the traditional customer loyalty programs. PAX framework adopts the smart contracts of blockchain technology by using PAX token to digitalize transaction processes. It provides improved usability for users and more detailed information to be gathered from manufacturing companies' perspective.**

***Keywords* —Customer Loyalty Program, Blockchain, Smart Contract, NEO.**

I. Introduction

Customer loyalty programs aim to gain customers loyalty to become their everyday routine. Therefore, customers are rewarded because of their purchases. Manufacturing companies can know their customers through customer loyalty programs. In the Fast-Moving Consumer Goods (FMCG) industry, manufacturing companies 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 get a payback from manufacturing companies.

Customer loyalty programs include many asset transactions between subjects like customers to merchants and merchants to manufacturing companies. 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 lost customer data and complications in the system for payback process. In this paper, to overcome these deficits a blockchain-based customer loyalty program is proposed.

Blockchain technology is first mentioned by Satoshi Nakamoto in [1]. 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 [2].

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 [3]. Therefore, it can be used in the error-prone systems to decrease the amount of incoherent data.

In this paper, we propose *Promotion Asset Exchange (PAX)* framework called a blockchain-based customer loyalty program. 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, manufacturing companies 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 paper is organized as follows. Section II describes the background about customer loyalty programs and blockchain technology. In section III, we propose the design of the blockchain-based customer loyalty program. In section IV, we define the system technically and give information about PAX token. Section V concludes the paper with the summary of the system.

II. Background

In this section, we overview literature with respect to the customer loyalty programs for FMCG industry and the blockchain technology.

A. Customer Loyalty Programs for FMCG Industry

Customer loyalty is an asset that should 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 [4]. Customers who join customer loyalty programs can get discounts and promotion products. On the other side, companies have the opportunity to know their customers shopping habits and they accomplish advantage according to competitors since customers will prefer their products [5].

In the FMCG industry, customer loyalty programs usually work with 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

978-1-5386-7893-0/18/$31.00 ©2018 IEEE

are the third subject, collect coupons from the merchants to make a payback.

There are some problems with the transactions among subjects. Customers usually lose or forget coupons which are small and mostly oily cards due to their exposure to the product directly. It strongly affects the participation in the program because lost or forgotten coupons cannot make the customer to join the system anymore. In addition, payback between merchants and manufacturing companies is a problematic operation because generally, merchants have thousands of coupons to give 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.

B. Blockchain Technology

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 blocks 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 [6].

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.

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 [7]. 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 1.

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 from the chain will cause changes on the all 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 [8].

Root hashes are created according to Merkle tree protocol. 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 [8]. In the figure 1, only four transactions which are Tx0, Tx1, Tx2 and Tx3, are included in the blocks for the illustration. Hash of the transactions are calculated one by one, refers to Hash0, Hash1, Hash2 and Hash3 respectively. 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.

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 asset's id.

3) Network: Blockchain network includes two types of nodes which are full nodes and light nodes [8].

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 [9]. 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 [10]. 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.
- Blocks transactions must not be used before.
- Blocks hash values must be in the correct format e.g. leading seven zeros for the hash value of block

4) Consensus Protocols: Blockchain systems can use different approaches for approving new blocks to the chain. Hash

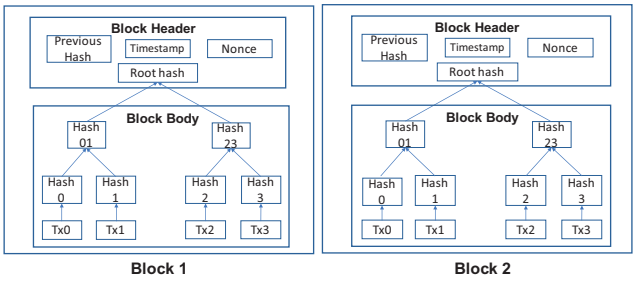

Fig. 1. Structure of the blockchain blocks

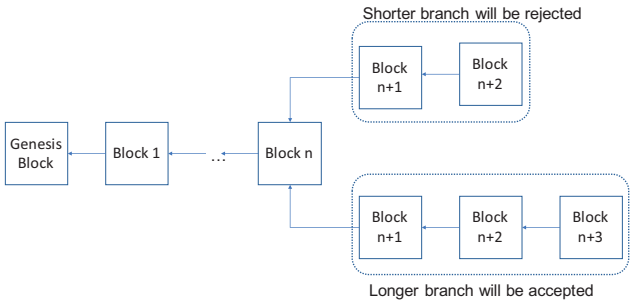

Fig. 2. Longest chain acceptance on the blockchain

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, nodes accept the longest chain as a valid chain, then new blocks are appended to that valid chain in that situation [7].

There are many different consensus protocols such as proof-of-work, proof-of-stake, Delegated Byzantine Fault Tolerance, Practical Byzantine Fault Tolerance, Tangaroa, Unique Node Lists [6]. In this section, we will only discuss the most commonly used two of them.

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 who can then verify their correctness 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 [11]. 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) 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 are not exist in the proof-of-work protocol. For instance, malicious parties can try to influence the electoral 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 [12].

III. Promotion Asset Exchange 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.

Transaction data is preferred to keep in blockchain system due to some problems with the traditional customer loyalty programs. Such system will provide 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 coupon cards anymore. Instead of keeping cards, they will just read the QR code on the card with their smartphone once and get the reward for their purchase. They will keep and collect their rewards on their mobile wallet.

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

Moreover, customers will register to the customer loyalty program through their smartphones and customer loyalty program will request 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 will be keep in the blockchain system safely. Manufacturing companies can analyze that transactions to learn such information like the most preferred products in the cities, purchase volume of the cities, product preference according to gender and so on.

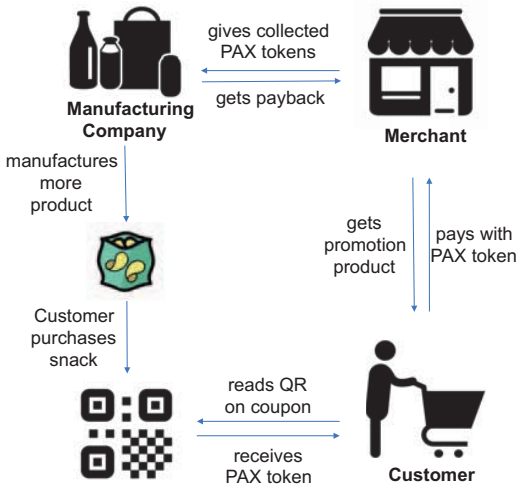

Fig. 3. Business flow of the PAX token transactions

As shown in Figure 3, customers purchase a 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 will be sent to customers wallets as a PAX token. After reading QR code from the disposable cards, they do not need cards 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 will show QR code which refers to merchants wallet, for the customers and customers will 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 will exchange PAX tokens with the products just like customers did with them. Therefore, manufacturing companies can make a payback to the merchants.

A. Delegated Byzantine Fault Tolerant

Delegated Byzantine Fault Tolerant (dBFT), 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 [13]. NEO Framework which is used to develop PAX token uses dBFT protocol for the consensus mechanism [13]. Improved BFT algorithm which is adapted to be used in the NEO blockchain system, is described in [14] in detail.

B. Smart Contracts

Smart contracts are self-running scripts on the blockchain system. They allow making general purpose computations on the blockchain [15]. 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 for their customer thanks to 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 [16]. 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 be 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 amount of promotions in the customer loyalty program, it does not use dynamic invoke property since it does not interact with other smart contracts.

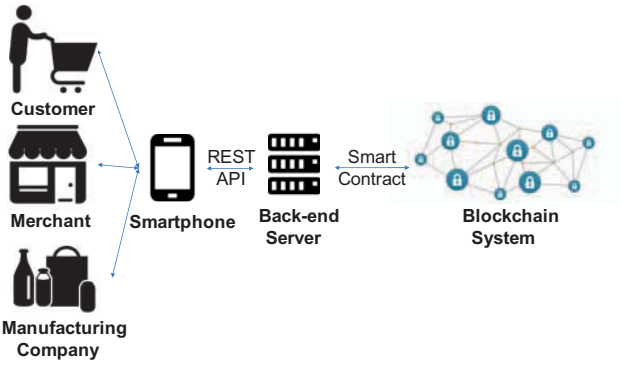

Fig. 4. Technical design of blockchain-based customer loyalty program

IV. Proof of Concept System

As shown in the Figure 4, PAX Framework presents a mobile application for users. All users of the system which are customers, merchants, and manufacturing companies, will notify the back-end server with that mobile application in their smartphone, through REST APIs. Back-end server will communicate with blockchain system to store transactions between users. Communication between the back-end server and blockchain system will be provided by smart contract. Therefore, PAX token transactions between subjects will be recorded on the blockchain system regularly.

Mobile applications will native applications that are developed in iOS and Android platforms with Swift and Java languages respectively. They will use REST APIs that are provided by the back-end server. Back-end server will be developed using Sails [17]. It communicates with blockchain system through neon-js [18]. Neon-js provides an interface to interact with blockchain system and uses smart contracts. Blockchain system will use NEO framework [13].

PAX token is developed based on NEO Framework [13]. It will be used on the private blockchain networks according to manufacturing companies. Neo-python environment [19] 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 will call these functions to make transactions.

- get_promotion_pax(qr_code): Customers will 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 will use this smart contract function to make a payment.
- request_payback(pax_amount) Payback between merchants and manufacturing companies will be handled with this function. It will get requested amount of PAX token from merchant and notify the manufacturing company.

Thanks to PAX Framework, manufacturing companies will gather the all information about their loyalty program since transactions are kept in the blockchain system safely. Therefore, we discuss practicality and utility of PAX Framework as follows:

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

V. Conclusion

In this paper, 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. 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 and manufacturing companies can better know the customers.

We plan to implement the proposed PAX Framework in a real environment. Then we aim to measure the performance of the system in terms of transaction confirmation time and transactions per second.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, accessed: 2018-05-03. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] M. Di Pierro, "What is the blockchain?" *Computing in Science & Engineering*, vol. 19, no. 5, pp. 92–95, 2017.

[3] S. Underwood, "Blockchain beyond bitcoin," *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[4] G. R. Dowling and M. Uncles, "Do customer loyalty programs really work?" *Sloan management review*, vol. 38, no. 4, p. 71, 1997.

[5] B. Berman, "Developing an effective customer loyalty program," *California management review*, vol. 49, no. 1, pp. 123–148, 2006.

[6] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

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

[8] Ethereum, "ethereum/wiki," accessed: 2018-05-23. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[9] D. Awasthi, "Barter to bitcoin: the changing visage of transactions," *Elk Asia Pacific Journal of Finance and Risk Management*, vol. 6, no. 4, 2015.

[10] J. A. D. Donet, C. Pérez-Sola, and J. Herrera-Joancomartí, "The bitcoin p2p network," in *International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 87–102.

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

[12] J. Siim, "Proof-of-stake," *Research Seminar in Cryptography*, 2017.

[13] "Neo white paper," accessed: 2018-05-12. [Online]. Available: http://docs.neo.org/en-us/

[14] "A byzantine fault tolerance algorithm for blockchain," accessed: 2018-05-12. [Online]. Available: http://docs.neo.org/en-us/basic/consensus/whitepaper.html

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

[16] "Applications of blockchain technology to banking and financial sector in india," accessed: 2018-06-07. [Online]. Available: http://www.idrbt.ac.in/assets/publications/Best%20Practices/BCT.pdf

[17] "Sailsjs," accessed: 2018-05-29. [Online]. Available: Link: https://sailsjs.com/

[18] "neo-js," accessed: 2018-05-22. [Online]. Available: Link: http://cityofzion.io/neon-js/

[19] "neo-python," accessed: 2018-05-15. [Online]. Available: Link: https://github.com/CityOfZion/neo-python