The Knowledge Engineering Review, Vol. 35, e12, 1 of 9.
doi:10.1017/S0269888920000181

A loyalty program based on Waves blockchain and mobile phone interactions

LUIS J. DOMINGUEZ PEREZ[1], LUIS IBARRA[2], GARCÍA-FERNÁNDEZ ALEJANDRO[2], AGUSTÍN RUMAYOR[2], and CARLOS LARA-ALVAREZ[3]

[1]*ITESO, Universidad Jesuita de Guadalajara, Periferico Sur Manuel Gomez Morin 8585, C.P. 45604, Tlaquepaque, Jalisco, Mexico;*
e-mail: luisjdominguezp@iteso.mx
[2]*Mathematics Research Center (CIMAT), Parque Tecnologico Quantum, C.P. 98160, Zacatecas, Mexico;*
e-mails: antonio.ibarra.g46@gmail.com, agarciafdz@gmail.com, agustin.rumayor@gmail.com
[3]*Center for Research and Advanced Studies, Unidad Tamaulipas, Parque Cientifico y Tecnologico Tecnotam Km, 5.5 carretera Cd. Victoria - Soto La Marina, C.P. 87130, Cd. Victoria, Tamaulipas, Mexico*
e-mail: calara@cinvestav.mx

Abstract

Loyalty cards programs have been used by retailers to increase customer retention. Loyality cards provide means to identify a particular customer and to collect customer-specific data, thus enabling individualized marketing; however, operating a loyalty program is complicated for retailers since they require to manage balances, collections, and transfers of customers. This is exactly the same problem the retailers were facing before credit cards were readily available. A new problem is that customers now have too many cards, customers may forget, or even deliberately decide to carry only a selection of their cards. This paper proposes a loyalty program based on a blockchain that does not require a physical card for identifying customers as it associates customers to their phone numbers, since nowadays people always carry their phone. In this perspective, companies can reduce overhead costs associated to managing the loyalty program. This paper reviews the technology required and describes the implementation of a loyalty program based on blockchains. Finally, it also enumerates the reasons for choosing the blockchain technology for this application.

1 Introduction

Rewards programs, also known as loyalty programs, are a mechanism used by businesses and a variety of industries to collect information, retain, and create customer loyalty (Stathopoulou & Balabanis, 2016). Rewards programs can be categorized as point- or level-based. Point-based programs grant points redeemable for products or services; for example, a coffee shop can give a reward for a free coffee if the customer has already bought three in the last week. Level-based programs assign a level according to the behavior of the client; for example, when accumulating purchases, the client can receive additional benefits.

Usually, a single company offers rewards to its customers; however, two or more partner companies can offer rewards; for example, a customer of restaurant ‘A’ can receive rewards in restaurant ‘B’. This strategy can provide substantial benefits to the partner companies: retain customers, mutually publicize their products, and increase their market.

The clients’ participation is fundamental for any rewards program; having a large number of members is not a guarantee for the success of the program. The 2017 Colloquy Loyalty Census shows that, despite that 3.8 billion members of loyalty programs have been identified, more than 50% of members are not

actively participating in them and about 28% of consumers leave a program without having charged his rewards (Fruend, 2017).

The three main reasons why members actively participate in rewards programs are as follows: the program is easy to use, easy to understand, or offers useful rewards (Fruend, 2017). The first factor is associated with the usability of a system. Rewards programs with high usability have a positive effect on customer satisfaction (Lee *et al*., 2015). If a loyalty program is difficult to use, clients will decide to abandon it (Stauss *et al*., 2005), and a high-usability system usually induces high customer satisfaction (Dowling & Uncles, 1997).

This paper describes the implementation of a loyalty program based on blockchain technology and mobile phone interactions. Blockchain technology reduces the investment required and improves the security and reliability of the program. The program directly interacts with users (members and partners) by using their mobile phone which improves the usability. The user can still receive benefits if she left her phone at other location or the phone ran out of battery.

The rest of this article is organized as follows. Section 2 presents the related work. Section 3 describes some concepts about blockchain technology that will help to clarify the implementation. Section 4 describes the implementation. Section 5 discusses why the blockchain is required for the proposed loyalty program and presents the concluding remarks.

2 Related work

Contemporary loyalty programs are structured marketing strategies that encourage customers to continue to shop at or use the services of businesses associated with each program, for instance, United Airlines and the Marriot Hotels exchange points (‘miles’) for products and services (Berry, 2015). Bijmolt and Verhoef (2017) note that there are still difficulties in the companies to create real customer loyalty, but whenever there are better tools to achieve it (i.e., digitalization), the loyalty programs also foster the total customer experience.

Creating and maintaining a loyalty program is a considerable investment (Dowling & Uncles, 1997; Stauss *et al*., 2005); the expenses of running a loyalty program include extra marketing work, finances, training the associates, technology, and the rewards themselves (Lee *et al*., 2014); furthermore, before starting a rewards program, companies do not have the certainty that it will be successful. Many factors must be considered; for instance, consumers are increasingly careful to choose the program that is most compatible with their life stages, their lifestyle, and their needs (Fruend, 2017). According to the ‘Framework for blockchain adoption’ (Iansiti & Lakhani, 2017), the proposal in this document falls into the replacement quadrant: it is not a very novel application, but it needs a lot of coordination and possibly changes the way reward programs work.

Small shops can offer rewards by using cards and stamps addable to them; but, this system has some disadvantages as cards cannot be tracked and profiled—for example, a customer can transfer her stamps to someone else. Cuennet *et al*. (2015) study the problem of implementing the functionality of paper-based loyalty cards as a mobile app. They define security requirements for such a system (as unforgeability of points, no double-spending of points, customer anonymity, customer privacy, etc.); then, they suggest a simple protocol that satisfies these requirements. In the implementation presented in this paper, the phone number is used as identifier and a simple authentication protocol via SMS is performed.

According to the self-determination theory, blockchain loyalty programs could have positive effects on users’ participation because they cover four needs: economy, autonomy, competence, and relationship (Wang *et al*., 2018).

There are several commercial efforts to implement loyalty programs based on blockchain (LoyaltyCoin, 2018). Even, some models have been proposed in the literature (Wang *et al*., 2018; Choi, 2018); for instance, Choi (2018) proposes an integrated program model that uses credit cards. But, as far as the authors know, this is the first paper that shows a complete implementation of a rewards program.

A local Ethereum node can be used for the transactions (Ibarra González *et al*., 2018); alternatively, a public node can reduce the footprint in a local system. The advantages of using a public node are introduced in the following section.

3 Blockchain technology

A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made (Crosby *et al*., 2016).

Cryptocurrencies are digital currencies supported by a blockchain, to simulate the registration of transactions of a physical currency between users and encourage the consensus of the canonical version of the transaction history, avoiding altered transactions. Another advantage of using the blockchain is that no third parties are needed to make a transaction. At present, there are stores that accept payments with this type of currency, as well as exchanges that can exchange cryptocurrencies with other types of assets (US dollar, USD). A virtual wallet is an application that facilitates interaction with a blockchain. A wallet allows exchanging cryptocurrencies between accounts (among other things) (Dannen, 2017).

Smart contracts are computer programs that can be correctly executed by a network of mutually distrusting nodes, without the need of an external trusted authority (Atzei *et al*., 2017). Everyone can make (deploy) a smart contract inside the Ethereum's blockchain, but you can also create new cryptocurrencies or tokens by using smart contracts (Dannen, 2017). The ERC20 standard specifies an API that tokens contracts must implement to integrate with exchange libraries and user interfaces (Vogelsteller & Buterin, 2018).

3.1 Reasons to use the blockchain technology

You might ask, 'why to use the blockchain technology?' The easiest way to answer this question is to observe the five key points on blockchain usage: (a) multiple writers, (b) absence of trust, (c) central party, (d) data size, and (e) throughput and scalability. The following paragraphs describe these points and their relationship with the proposed rewards system.

Multiple writers. Blockchain technology is specially designed to have multiple writers—for example, if a system needs more than one entity to write to the database, then it may need the use of blockchain technology. In principle, in a small *Software as a Service* (SaaS) scenario, there is a single instance—in the form of a central webpage— accessing the database, also managed by the same service provider. There is no doubt who is accessing the database; hence, who is accessing or altering the information may depend on the user authentication rules specific to the application.

There are, of course, cases where it is preferable to have multiple copies of the server in order to have a better performance, which is one of the main ideas of using a (elastic) cloud provider; however, they are all essentially the same entity, just different copies or instances accessing the same database, or a copy, which is quickly replicated between each other.

Absence of trust. We have a lack of trust between the parties since the idea is to have the system accessible to many partners. The technology would provide certainty to the system and that the information is valid, *despite coming from different sources* that are not trusted among everybody in the network, including competitors.

Central party. Since there are multiple parties that may not be trusted between each other, having no central authority provides with certainty that no one may attempt to abuse the system without this attempt being seen by the other participants. Such an attempt would need the approval of a majority or consensus of the other participants, according to whatever rules for approval are used to add data to the distributed ledger, for it to succeed in updating the ledger.

Data size. A disadvantage of the blockchain technology is that it was not intended to be a storage space for a large amount of data.

In our system, the idea is to only store the number of reward points into the chain, and this will keep it lean. As a matter of fact, reward points are valid up to a period of time since the idea is to create *active* client loyalty; hence, partners may want a way to expire unclaimed points every few months. For instance, we can create a new reward point chain every year.

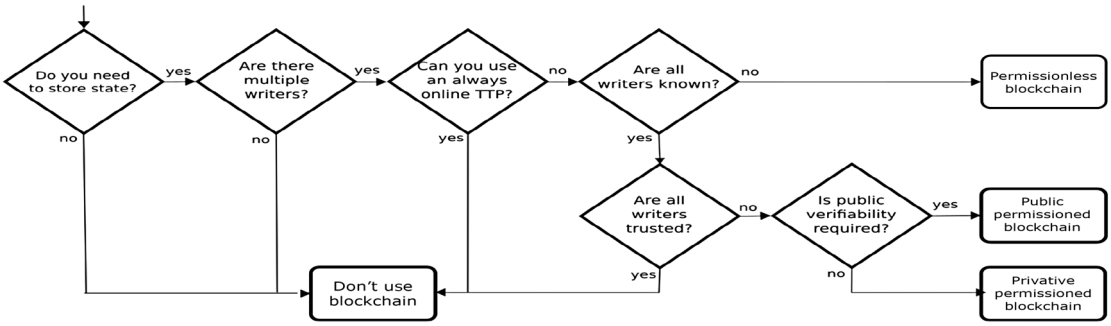

Figure 1 Decisional model for blockchain usage (Wüst & Gervais, 2017)

Throughput and scalability. Finally, the key indicator to not use this technology is that despite the technology was designed to be robust, and a heavy framework for multiple transactions, the ever increasing number of transactions would make it a slow solution in a future if the system is heavily used.

Another way to decide if a blockchain fits the requirement is with the use of a *decisional model*; several such models have been proposed in the literature, but some of them are sponsored by companies in order to attract sponsors. The model proposed by Wüst & Gervais (2017) was selected because it is simple and probably independent—as it comes from the academy.

As shown in Figure 1, one of the key stages where the system proposed here may seem that does not need a blockchain is where it asks for if we need or want a trusted third party (TTP) to control the information.

3.2 Reasons to use the Waves blockchain

There are two different algorithms that help on choosing the node that will validate the next block in a blockchain, *Proof of Work* (PoW) and *Proof of Stake* (PoS). The former selects the first node that solves a *challenge*, known as a 'puzzle'; for example, in Bitcoin, the challenge is to calculate a hash with a specific format, consuming a very large amount of resources (O'Dwyer & Malone, 2014). In the latter, the node is selected by its amount of stake, the more stake you have, the more likely is to be selected as the generator of the next block.

The 'puzzle' in the PoW strategy is a hard mathematical problem that usually does not have a known solution in subexponential time; then, the problem is solved by random guessing. The main issue with PoW is that it requires a large amount of real-world resources, such as electricity and computing power. Since the number of possible solutions is gigantic, a professional miner would invest in computer infrastructure to calculate a larger amount of possible answers than a casual participant. This leads to a large energy cost, which in turn presents a sensible ecological footprint.

PoS requires that a miner places a stake, locking up that amount of their own coins in order to be allowed to verify a block of transactions. The miner only needs to prove that it owns a certain percentage of all coins available in a given currency in order to mine. For example, if you own 2% of all Ether (ETH), you would be limited to mine up to 2% of all transactions across the Ethereum blockchain. This way, PoS would be a more fair system than PoW, since anyone could become a miner. PoW allows winning miners to continuously get more computer power to continue mining. PoS limits the blocks a miner could confirm, since it is based on that persons stake in the cryptocurrency.

In principle, Ethereum is the most known Smart Contracts Platform and may switch in a future to the PoS paradigm, but there are some other technologies that let us run smart contracts with different characteristics; for instance, Waves exposes an API in which we can perform requests, and it uses a small variant of PoS algorithm called *leased PoS*, which was unique at the time of writing this article. Additionally, the Waves platform permits the customization of tokens since 2017, while providing extensive documentation.

In Ibarra González *et al*. (2018), we proposed a scenario in which each partner is writing directly to the blockchain. This was needed in order to avoid using a central database, described previously, that keeps

Table 1 User stories for the rewards points system

US_{01}	As a partner, I assign rewards points to members to encourage their loyalty as clients
US_{02}	As a member, I pay with the accumulated points to save money and enjoy the program benefits
US_{03}	As a member, I see the balance of my points to know how many I have
US_{04}	As a member, I see a report of transactions
US_{05}	As a member, I approve the points charges, to be sure that other people do not spend them
US_{06}	As administrator, I manage partners data (registrations, cancellations, and changes) in the system and I see all the members

Table 2 Test cases for the rewards points system. Where $\mathcal{M}_1$ and $\mathcal{M}_2$ are the members, $\not{\mathcal{M}}$ is a false member, and $\mathcal{P}_1$ and $\mathcal{P}_2$ are the partners

	Given	**When**	**Then**
TC_{01}	$\mathcal{M}_1$ has 1 point and $\mathcal{P}_1$ has 9999 points	$\mathcal{P}_1$ rewards $\mathcal{M}_1$	$\mathcal{M}_1$ has 2 points and $\mathcal{P}_1$ has 9998 points
TC_{02}	$\not{\mathcal{M}}$ has 0 points and $\mathcal{P}_1$ has 9999 points	$\mathcal{P}_1$ rewards $\not{\mathcal{M}}$	$\not{\mathcal{M}}$ has 0 points and $\mathcal{P}_1$ has 9999 points
TC_{03}	$\mathcal{M}_1$ has 1 point and $\mathcal{P}_1$ has 0 points	$\mathcal{P}_1$ rewards $\mathcal{M}_1$	$\mathcal{M}_1$ has 1 point and $\mathcal{P}_1$ has 0 points and receives a message warning that it does not have enough points
TC_{04}	$\mathcal{M}_1$ has 10 points and $\mathcal{P}_1$ has 0 points	$\mathcal{M}_1$ pays one point to $\mathcal{P}_1$	$\mathcal{M}_1$ has 9 points and $\mathcal{P}_1$ has 1 point
TC_{05}	$\mathcal{M}_1$ has 0 points and $\mathcal{P}_1$ has 0 points	$\mathcal{M}_1$ pays 1 point to $\mathcal{P}_1$	$\mathcal{M}_1$ has 0 points and $\mathcal{P}_1$ has 0 point, and receives a message warning that it does not have enough points
TC_{06}	$\mathcal{M}_1$ has 10 points	$\mathcal{M}_1$ asks for his balance	$\mathcal{M}_1$ is notified that he has 10 points
TC_{07}:	$\mathcal{M}_1$ has 10 points and $\mathcal{P}_1$ has 10 points, and receives a message warning that it is collecting from a wrong member	$\mathcal{P}_1$ collects rewards given to $\mathcal{M}_2$	$\mathcal{M}_1$ has 10 points and $\mathcal{P}_1$ has 10 points
TC_{08}	$\mathcal{M}_1$ has 10 points and $\mathcal{P}_1$ has 10 points	$\mathcal{P}_1$ collects one point given to $\mathcal{M}_1$ and $\mathcal{M}_1$ provides his PIN	$\mathcal{M}_1$ has 9 points and $\mathcal{P}_1$ has 11 points
TC_{09}	There are three partners	Administrator inserts partner X with the number '1234567890'	There are four partners
TC_{10}	There are three partners	Administrator inserts partner X with the number '12345'	There are three partners

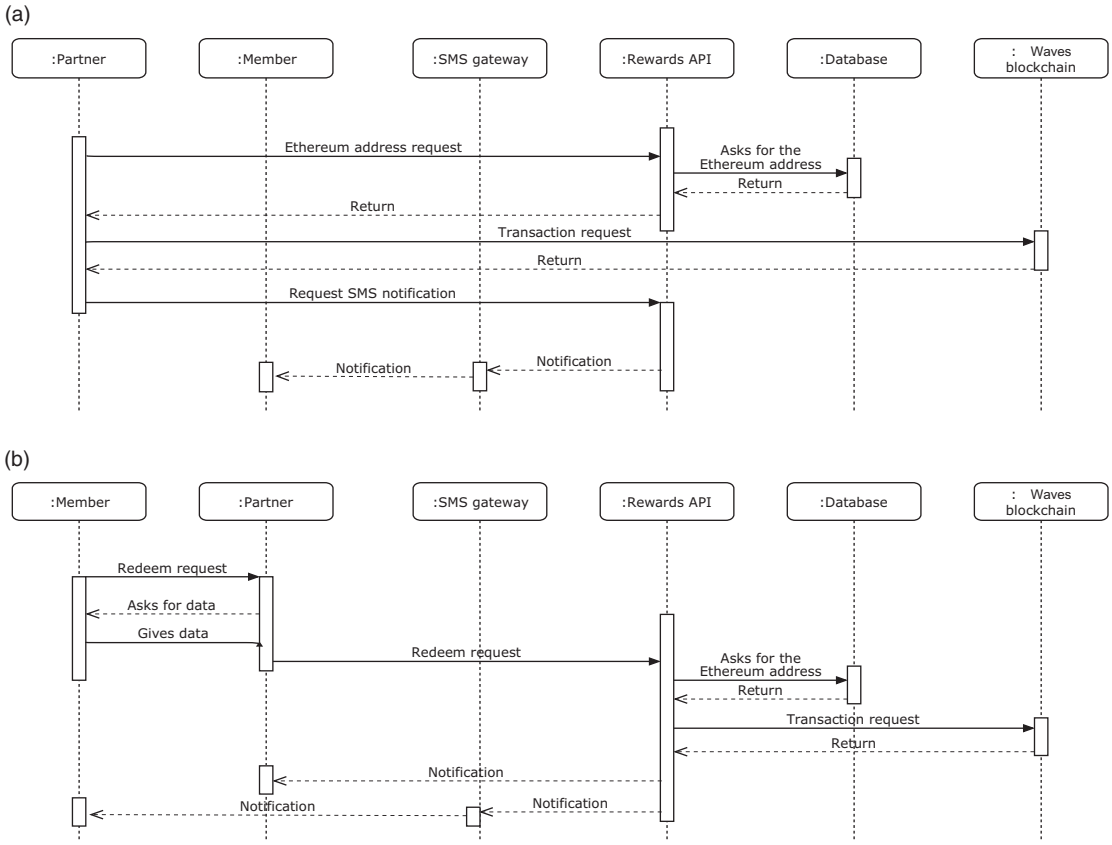

Figure 2 Flow for the first two user stories: (a) US_{01} and (b) US_{02}

track of all of the transactions and to only use an SMS for data exchange. This came with the privacy benefit, since only an interested partner would be able to keep track of the transaction in its premise.

The Ethereum requirements to run a local node are ever increasing in terms of storage and broadband use, making it expensive for today's simple PoS terminals to handle it. We propose using the Waves blockchain, and its public blockchain node services, as a light and fast alternative to Ethereum, since it uses the PoS technology, and a public node.

4 Loyalty program implementation

The following paragraphs describe the software development cycle phases (analysis, design, and implementation) performed to implement the reward system.

4.1 Analysis

User Stories (USs) are widely used for formulating requirements; they answer three basic questions: who? what? why? The USs selected for the rewards system (Table 1) involve three types of users: partners (associated companies that provide products or services), members (persons who could receive rewards by consuming products), and administrators (who control accounts). A set of *test cases* (TC) was constructed to test the USs (Table 2).

4.2 Design and implementation

Our system has three key components: (a) a token creator in the Waves testnet, (b) a web API that provides services over the Hypertext Transfer Protocol (HTTP) and (c) a database that stores accounts and PINs. The most important *US*s are shown in Figure 2.

Table 3 Endpoints

	Id	Verb	Endpoint	Description
Partners	EP_{01}	POST	/partners/{partner_cellphone}/reward/{cellphone}	Rewards customers through the phone number
	EP_{02}	POST	/partners/{partner_cellphone}/redeem/{cellphone}	Pays customer rewards through the cell phone number
	EP_{03}	GET	/partners/transactions	View transactions
	EP_{04}	GET	/partners/transactions/{transaction_id}	View details of a transaction
	EP_{05}	PUT	/partners/transactions/{transaction_id}	Validates a transaction
Members	EP_{06}	GET	/members/{cellphone}/balance/	Receives the balance of member account
	EP_{07}	GET	/members/{cellphone}/pin	Gets the PIN given by the platform
	EP_{08}	POST	/members/{cellphone}/pin	Sets a PIN for the first time
	EP_{09}	PUT	/members/{cellphone}/pin	Changes the PIN
	EP_{10}	POST	/members/{cellphone}/pay/{partner_id}	Pays with reward points
Admin	EP_{11}	POST	/admin/members	Sees all the members
	EP_{12}	POST	/admin/partners	Sees all the partners
	EP_{13}	POST	/admin/add_partner/{partner_id}/{cellphone}	Inserts a new partner

To reward points to members, a partner (that knows his own Waves address) requests the transaction by sending the number of reward points and the member's phone number. The system sends a query to the database; to get the member's address and if the query result is valid, it sends the transaction to the blockchain to the Waves public node. Finally, the transaction is notified to the API, the SMS gateway, and the user (Figure 2(a)).

To redeem points, partners and members agree the amount of points face-to-face. Then, the partner requests the transaction. As in previous cases, the system gets the member's address, performs the transaction, and sends notifications to both parties (Figure 2(b)).

To make transactions between members and partners, a token is created in the Waves platform—which are compatibles and interchangeables with other Waves tokens.

Table 3 shows the mapping of resource-related actions with the corresponding core module (partners, members, and administrators). These actions provide the required functionality, as shown in Table 4.

Some advantages of using the Waves blockchain are (a) a public node can be used, (b) it uses PoS, (c) it has a decentralized exchange, and (d) it has fixed transaction cost.

5 Discussion and conclusions

It would be a very valuable information for ads agencies to know which partners you are a loyal customer; however, one of our goals here would be privacy to the customer, and having no TTP to log the user would provide confidentiality to the information.

Table 4 Relationship between user stories and endpoints

		Endpoint													
		EP_{01}	EP_{02}	EP_{03}	EP_{04}	EP_{05}	EP_{06}	EP_{07}	EP_{08}	EP_{09}	EP_{10}	EP_{11}	EP_{12}	EP_{13}	Total
User story	US_{01}	×													1
	US_{02}		×								×				2
	US_{03}						×								1
	US_{04}			×	×										2
	US_{05}					×		×	×	×					4
	US_{06}											×	×	×	3

As a matter of fact, there is one central server that let users be part of the system, we could think this system is a *malicious* TTP, as it is shown in Table 1, there is some associated activity for this server, the idea is to fully unbalance the protocol to the partner, and to the Waves node, this way, the end customer should transparently use our system. This also has the benefit that any key management issues about the blockchain are obviated by the end customer.

Following the decisional model shown in Figure 1, now, the decision relies entirely on the fact that, as a partner, we do not know who else is part of the reward system (only the administration server knows for management purposes). Since we would like to let the end customer to verify the number of reward points available, we preferred a public blockchain, in which only the partners are able to log their transaction.

In this paper, we describe a loyalty program implementation that uses the Waves blockchain technology. Our working system does not require a physical card for identifying customers as it associates them to their phone numbers. All of the interaction between the user and the partner is done by SMS messages, and there is no need to have a physical reward card and even your phone present for some actions. By using the Waves blockchain, we reduce the complexity of the system since there is a public node, it uses PoS technology, and we will be able to exchange tokens between other partners, if required.

Having a local blockchain node for each PoS terminal was not practical since it requires a fast broadband access, and we prefer a solution that is suitable for both big and small partners. The use of the Waves blockchain provided us with a better flexibility than Ethereum in this scenario.

The system is practical, and we expect a larger use of blockchain technology in the future for this type of loyalty card programs and other virtual currency schemes. Visit our repository https://gitlab.com/Antoniio/rewards-codes.

References

Atzei, N., Bartoletti, M. & Cimoli, T. 2017. A survey of attacks on ethereum smart contracts (SoK). In *Principles of Security and Trust*, Maffei, M. & Ryan, M. (eds). Springer, 164–186.

Berry, J. 2015. *The 2015 Colloquy Loyalty Census. Big Numbers, Big Hurdles*. Colloquy.

Bijmolt, T. H. & Verhoef, P. C. 2017. Loyalty programs: current insights, research challenges, and emerging trends. In *Handbook of Marketing Decision Models*, Wierenga, B. & van der Lans, R. (eds). Springer, 143–165.

Choi, J. 2018. Modeling the intergrated customer loyalty program on blockchain technology by using credit card. *International Journal on Future Revolution in Computer Science and Communication Engineering* **4**(2), 388–391.

Crosby, M., Pattanayak, P., Verma, S. & Kalyanaraman, V. 2016. Blockchain technology: beyond bitcoin. *Applied Innovation* **2**, 6–10.

Cuennet, L., Pouly, M. & Radomirović, S. 2015. Guided specification and analysis of a loyalty card system. In *International Workshop on Graphical Models for Security*, 66–81. Springer.

Dannen, C. 2017. *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*, 1st edition. Apress. ISBN 1484225341, 9781484225349.

Dowling, G. R. & Uncles, M. 1997. Do customer loyalty programs really work? *Sloan Management Review* **38** (4), 71.

Fruend, M. 2017. *The 2017 Colloquy Loyalty Census*. https://www.the-cma.org/Contents/Item/Display/327325 (accessed February 18th, 2020).

Iansiti, M. & Lakhani, K. R. 2017. The truth about blockchain. *Harvard Business Review* **95** (1), 118–127.

Ibarra González, L. A., Dominguez Perez, L. J., Garcia Fernandez, A., Ruimayor, A. & Lara-Alvarez, C. 2018. A loyalty program based on blockchain and mobile phone interactions. In *The 3rd Symposium on Distributed Ledger Technology*. Griffith University.

Lee, D., Moon, J., Kim, Y. J. & Mun, Y. Y. 2015. Antecedents and consequences of mobile phone usability: linking simplicity and interactivity to satisfaction, trust, and brand loyalty. *Information & Management* **52** (3), 295–304.

Lee, J. J., Capella, M. L., Taylor, C. R., Luo, M. & Gabler, C. B. 2014. The financial impact of loyalty programs in the hotel industry: a social exchange theory perspective. *Journal of Business Research* **67** (10), 2139–2146.

LoyaltyCoin. 2018. Loyaltycoin. https://loyalcoin.io/ (accessed March 1st, 2018).

O'Dwyer, K. J. & Malone, D. 2014. Bitcoin mining and its energy footprint. In *25th IET Irish Signals Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*, 280–285. doi:10.1049/cp.2014.0699.

Stathopoulou, A. & Balabanis, G. 2016. The effects of loyalty programs on customer satisfaction, trust, and loyalty toward high-and low-end fashion retailers. *Journal of Business Research* **69** (12), 5801–5808.

Stauss, B., Schmidt, M. & Schoeler, A. 2005. Customer frustration in loyalty programs. *International Journal of Service Industry Management* **16** (3), 229–252.

Vogelsteller, F. & Buterin, V. 2018. ERC-20 token standard, 2015.

Wang, L., Luo, X. R. & Xue, B. 2018. Too good to be true? understanding how blockchain revolutionizes loyalty programs. In *24th Americas Conference on Information Systems, AMCIS 2018, New Orleans, LA, USA, August 16–18, 2018*. Association for Information Systems.

Wüst, K. & Gervais, A. 2017. Do you need a blockchain? *IACR Cryptology ePrint Archive* **2017**, 375.