Enhancing retail business and customer experience using blockchain approach

B.P. Aniruddha Prabhu*

Cambridge Institute of Technology,
Bangalore, 560036, India
Email: aniprabhubp@gmail.com
*Corresponding author

Arup Das

JPMorgan Chase & Co.,
Bangalore, Karnataka 560071, India
Email: das12997@gmail.com

Abstract: The retailers of supermarkets today quite often use the transactional marketing strategy to entice their customers by issuing discount coupons. The proposed system aims at enhancing this reward-based system and automating customer shopping experience by building a 'pay as you choose the item' technology. Employing such a system would help in providing a faster, safer and more convenient means of transaction alongside improving the overall efficiency of the supermarkets achieving higher revenue with lesser manpower. The authors utilise the concept of blockchain to perform transactions using a cryptocurrency called value-coins. Such a digital system would be commonly available to all the outlets of the retailer.

Keywords: value-coins; proof of authority; PoA; digital signature; blockchain; consensus algorithms; layer pattern architecture.

Reference to this paper should be made as follows: Prabhu, B.P.A. and Das, A. (2020) 'Enhancing retail business and customer experience using blockchain approach', *Int. J. Blockchains and Cryptocurrencies*, Vol. 1, No. 3, pp.273–285.

Biographical notes: B.P. Aniruddha Prabhu is an Assistant Professor at Cambridge Institute of technology. He completed his BE and MTech from Visvesvaraya Technological University (VTU). His research area includes big data analytics, cloud computing, artificial intelligence, machine learning and blockchain.

Arup Das is a Software Engineer in JPMorgan Chase & Co. He completed BE from Siddaganga Institute of Technology, Tumkur (VTU). His research area includes big data analytics, machine learning and blockchain.

1 Introduction

The blockchain is a concept which was introduced back in 1991 but was left unnoticed until Satoshi Nakamoto developed the 'bitcoin' in October 2008. The blockchain is shorthand for an entire suite of distributed ledger technologies that can be programmed to contain a never-ending list of records referred to as 'blocks'. Each and every block is related to one another and is protected using various cryptographic techniques. Enterprises like Google, British Airways, AIA Group, Alibaba Group, JPMorgan Chase & Co., Prudential, Samsung and MetLife are working towards implementing blockchain to track anything of value ranging from data protection, transportation, data integrity, e-commerce, finance and healthcare, respectively. The notable advantage offered by blockchain is that it enables communication between two non-trusting parties without the involvement of an intermediary thus cutting down on time and money spent in recording any sort of activity requiring a ledger system (Nayak and Dutta, 2017). Essentially, the blockchain is categorised into two types: public blockchain also known as permissionless blockchain and private blockchain also known as permissioned blockchain (Dinh et al., 2018).

A public blockchain is openly available for reading and writing whereas on the contrary the participant in a private blockchain would require special permission to read or write access. It contains a greater number of network participants than in a private blockchain. The speed of transaction is much slower in a public blockchain (e.g., bitcoin) whereas in contradiction the transaction speed is considerably faster in a private blockchain. All this is attributed to the usage of the consensus algorithm used in a private blockchain that allows only pre-approved participants to be a part of the transaction validation mechanism. The identity of an individual remains pseudonymous in a public blockchain whereas on the contrary the identities of the entities involved in the transaction are always known (Chris Skinner's Blog, https://thefinanser.com/). A blockchain is used when there is a database which needs to be shared, presence of several writer nodes or there is a requirement to analyse the relation between the transactions (Gatteschi et al., 2018). The decentralised blockchain eliminates single point failure which could have potentially occurred in using a central record keeping, validation and verification authority. Also, it safely eliminates the cost and time incurred in maintaining such middle-man practices and charges only a minimal nominal fee required to complete the transactions between the parties involved and reward the miners on the network (Mirko Kickvic's Blog, https://medium.com/altcoin-magazine/blockchain-centralization-is-that-the-future-of-decentralized-network-5d95c6f89de6). The concern of data loss on compromising of the single copy of data is no longer a problem as the same data is available at several location. Hence, loss of data is never a matter of concern when a decentralised blockchain system is used. A decentralised system does have some limitations. Firstly, it possess low throughput as a decentralised system can process only a limited number of transactions. Second, it reduces the transaction speed. For, e.g., a new block is bitcoin is mined after every ten minutes where as in Ethereum it takes 14 minutes (BitRewards Blog, https://medium.com/@bitrewards). Third, the decentralised system comprises of overwhelming number of miners which leads to greater difficulty resulting in several useless highly intensive computations. A centralised blockchain platform collect all the data at one point through a private server or hub, this offers several advantages like higher throughput, data security, more customisation and control over the network as it can be decided in the initial stage itself who can get to

participate in the network (Swan, 2015). According to our problem statement, we want a system which can process the transaction in a faster manner and it can process any number of the transaction at the given time. It is also easy to update our business logic easily. For our problem statement, centralised blockchain would be a best option.

1.1 Literature review

This section briefly describes the kind of work that has been previously done in incorporating blockchain to improve the current status quo in cloud security and services, market settlement transactions and the algorithms developed to scale out blockchain to handle the conflicting situations that may arise while handling concurrent transactions. The integration of these developments as a whole has played a significant role in developing a unique market technology and leveraging the solution as proposed in this paper.

With the number of users of cloud-based services exponentially increasing the concern regarding security is also increasing. The most general and the safest approach is to use a Cloud Security Alliance which can be used to encrypt the data before sending it to the cloud. BoxCrypt, ARX and CryptDB are some of the tools which provide such encryption. Majority of the functions are exercised on the client side as the exchange of data occurs in a private manner. Merit of using the access control system is that it encompasses the capability to alter the accessing policy for the encrypted information without replicating it. The remnant functions are performed by the Ethereum virtual machine (Sukhodolskiy and Zapechnikov, 2018).

The development in the domain of blockchain has facilitated to ease the critical functions in clearance and business in the wholesale markets. The monopoly of banking establishments acting as trusted third party authorities for validating and enabling purchase and settling customer bills can be reduced from days to minutes. This has been possible to achieve by using a distributed data storage, peer to peer network and cryptography (Brainard, 2016).

There are numerous advantages to applying blockchain to market investments. The efficient transfer and administration of transaction details between the seller and the buyer are quite simple and safe with the blockchain technology. However, there are issues related to reliability and isolated utilisation of blockchain technology. Some major concerns pertaining to blockchain are 51% attack and the latency of the network bandwidth. The solutions corresponding to such problems have been effectively discovered and enlisted (Halpin and Piekarska, 2017).

The struggle to achieve scale-out throughput maintaining an equivalent level of decentralisation and security is actively going on. Namely, there are three conditions to be met for any consensus protocol to work effectively. They are correctness, consistency and liveness. These concepts explain the features of value-transfers in the blockchain. The solution comprises of key concepts like communication cost per transaction and spontaneous sharding. A blockchain is partitioned into various shards on the basis of the domain. Sharding is of two types: local and global shards. A transaction that can be completed in a single shard is referred to as a local shard and the transaction that is completed using two shards is known as a global shard. There are two types of consensus algorithms, Nakamoto consensus algorithms and Byzantine fault tolerance (BFT). The practical Byzantine fault tolerance (PBFT) algorithm is implemented with a message

complexity of $O(n^2)$. Each transaction pattern is divided into shards so as to reduce the size of proof in every transaction (Ren et al., 2018).

Blockchain can lay the foundation of a smart city. Effectively, blockchain can be categorised into three classes: Blockchain 1.0, Blockchain 2.0 and Blockchain 3.0. Blockchain 1.0 involves cryptocurrencies like bitcoin. Blockchain 2.0 involves financial settlements like equities, debt, insurance, smart contracts, etc. Blockchain 3.0 is involved with the creation of a decentralised cooperative in fields of health, science, culture and arts. Big data would form the heart for such a smart city implementation where blockchain would be required to provide security and maintain the privacy of information (Li, 2018).

Considering such significant factors this paper proposes a digitised, secure, scalable and conveniently deployable solution. The authors propose the usage of value-coin, a digital coin designed to enable instantaneous payments using blockchain technology. One value-coin is given the value equal to one INR. The customer needs to have the requisite number of value-coins purchased from the retailer before making the payment. The genesis block represents the retailer. Every other block represents a customer block which is chained together. When a customer enters the outlet of a supermarket, the local database of items present in the outlet is loaded into his mobile device via the application. The customer can then pick the items that he desires to purchase and scan the bar code of the product with help of the mobile device which will enable the application to virtually add items to the cart and keep track of the items that are going to be purchased by the customer. When the customer has completed shopping, he can then go ahead with the transaction. The transaction is validated by the transaction administrators in the proof of authority (PoA) network who play a crucial role in the completion and validation of a secure and non-fraudulent transaction. Each transaction enters the processing queue from which the transaction is taken by the transaction administrators. The transaction is validated by checking the customer's current balance status and then if the transaction is legitimate it is digitally signed by the authority and sent to the retailer. Now, if there are any discount schemes and coupons which are to be issued then the retailer issues a certain number of value-coins as per the scheme for the customer.

Such a digitised approach of payment will make it easier for the retailer to enable greater customer retention, maintain an immutable list of transaction records and enhance the reward-based competition market by studying the customer purchasing pattern. From the customer's point of view, such a digitised system will enable the customer to maintain a digital bill which can be verified at their own ease and most importantly the common complaint of the customer regarding the time spent in the cash counter to pay their bills has also been tackled successfully.

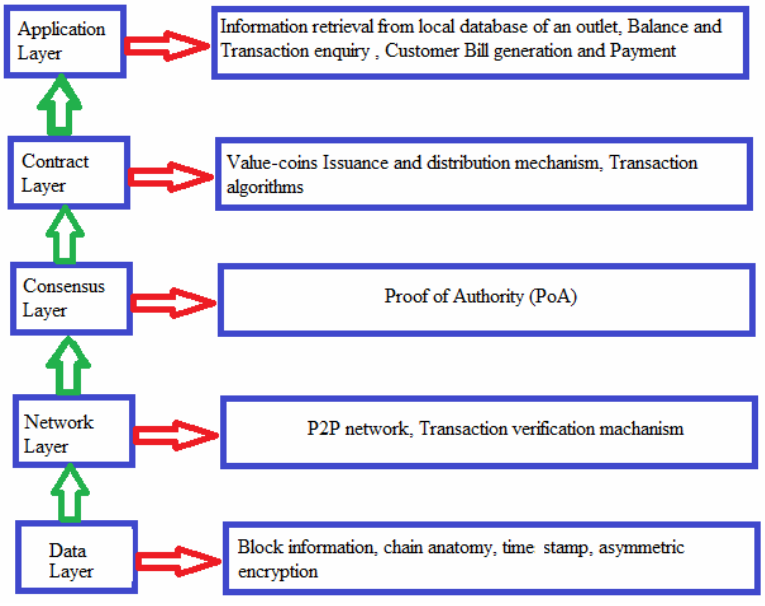
2 Design of the proposed system

There are three main software architecture patterns which are layer pattern, pipeline and filter pattern and blackboard pattern (Buschmann et al., 1996). Layer pattern architecture is the most suitable one and helps to structure applications that can be decoded into different subtask. The layers can be divided according to the OSI layers, different components (modules) and protocols. A large system needs decomposition. The

blockchain is a very vast system and its implementation has very different components which can be divided into different layers.

There are five conceptual layers of blockchain: data layer, network layer, consensus layer, contract layer and application layer as shown in Figure 1 (Marin, 2018).

Figure 1 Layers of blockchain technology architecture (see online version for colours)

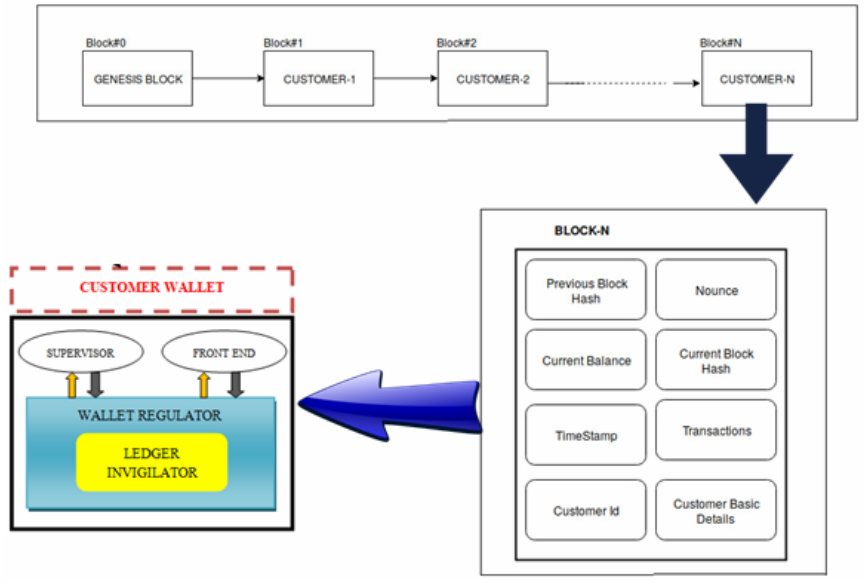


The data layer contains the block data, structure of the chain, customer address data, timestamp of block creation and details of asymmetric encryption. It is because of the data layer that transactions can happen transparently in a non-repudiated and authenticated manner. The networking layer makes sure that each node receives transactions. The consensus layer makes sure that each node agrees on the same transactions to modify their local state. The contract layer is responsible for checking the credit limit of the customer in order to make a successful transaction. It ensures a safe and secure transaction, issuance and distribution of value-coins by the genesis block. As for the application layer, it processes transactions. Given a transaction and a state, the application will return a new state. Each transaction abides by the norms of the contract layer and modifies the state according to the specific transaction rules.

2.1 System architecture

Blockchain uses a linked list data structure to bind the data blocks together. As every block contains the previous hash of the other creating a chaining effect the blocks are chained together in a chronological order that is in the timestamp of the order of creation of the block (Nakamoto, 1998; Tabrizi, 2009). The overall system architecture is as shown in Figure 2.

Figure 2 System architecture (see online version for colours)



The genesis block represents the retailer and all the other blocks are the blocks of the customers (Dill and Smits, 2017). Each customer block contains the following elements:

1 Previous block hash: It contains the hash value of the previous block in the blockchain. It is used to make a connection between different blocks by using a linked list data structure.

2 Nonce: It is a 32-bit arbitrary random number that is typically used once. It is basically used for calculation of hash value of the current block.

3 Current balance: It indicates the amount of unspent value-coins present in the wallet.

4 Current block hash: It is calculated by hashing the value of nonce, previous block hash, timestamp value by applying SHA-256 algorithm.

5 Timestamp: Each block contains a Unix time timestamp. In addition to serving as a source of variation for the block hash, they also make it more difficult for an adversary to manipulate the blockchain.

6 Transactions: Inside each block, we store receipt of purchase as a JSON file.

7 Customer id: It is a unique identity for each customer in the blockchain.

8 Customer contact details: The basic contact details such as mobile number, name, address, etc. are stored.

The front-end of the customer wallet collaborates with the application layer to enable easy payments. The application will open with a login page and a sign-up page. The new user will have to login into our system and provide all the required details during the signing up. All the details asked will be useful for running our application successfully and reaching the expectation.

Once the sign-up procedure is completed, the user has to login again into the system via the application using their credentials. Customers can also change their credentials again afterwards according to their wish and comfort. Our application will be having the following options:

- Add value-coins (money) to the wallet: Since all payments are done using a digital currency, i.e., value-coins. We must add money to the digital wallet. Every value-coin will be equivalent to one INR.
- Add and delete items into the virtual cart: While in shops/marts customer can add some products into their cart by scanning the bar code on the product and keep it with them. And if they feel that some product are useless to them or not necessary, they can delete the item from their cart just using the re-move option available to every item present in the cart and the corresponding item will be removed.
- Check the list of items added in the cart: Customer can at anytime see the number of items available in their cart and can decide whether to shop more or not. They can even manage their checklist and it will also show the total cost of the cart helping them decide further.
- Make some transactions: After doing all the shopping the customer can just pay the amount, displayed below the cart. Payment will be made using the value-coins present in the wallet.
- Check account balance: After making all the payment or before shopping customer can check their balance.

Apart from this, the application would also provide prices of similar product and their corresponding discounts if any so that the customer could optimise their shopping experience economically and efficiently. The user interface could also contain a virtual map of the entire mall to guide the customer to their desired choices.

2.2 Consensus mechanism

The consensus algorithm evaluates the criteria's and circumstances that are to be reached in order to validate the blocks that are to be included in the blockchain. The consensus algorithm is an outcome of the Byzantine generals' problem which states that any two devices on the decentralised unreliable network cannot completely and indisputably ascertain that they are representing the same data. The BFT is an attribute which denotes the tough set of defective nodes that are associated with the Byzantine generals' problem (Chakroborty and Jayachandran, 2018). It can tolerate up to 33% defective nodes that is $3f + 1$ where f is the total number of faulty replicas present in the system (Bach et al., 2018). Significantly, there are four proofs used to implement the consensus algorithm: proof of work (PoW), proof of stake (PoS), delegated proof of stake (DPoS) and proof of authority (PoA).

Since the proposed system uses a private blockchain, it is favourable to implement PoA network for maintaining the consensus. PoA is a substitute for PoW in private blockchains which consists of authorities-nodes who are responsible for creations of a

block and secure operation and maintenance of blockchain. Two main algorithms used to implement PoA is AuRa and Clique. PoA consists of N trusted authorities wherein at least N / 2 + 1 authorities should produce the same result after conducting their operation to maintain consensus.

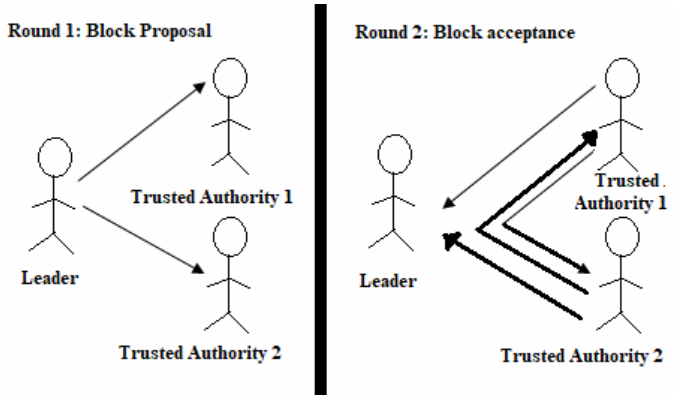
Table 1 Comparison of various consensus algorithms

	PoW	*PoS*	*DPoS*	*PoA*
Principle	The solution is complex to deduce but convenient to validate	Higher the stake of a validating node in the network, more chances and legitimacy it has to validate transactions	Panel of delegates elected by users of the network monitor the blockchain and propose changes to the protocol which must be approved by the users	Blocks are validated if signed by a specified quorum of signers
Node recognition and administration	Open	Open	Open	Permissioned
Energy saving	No	Partial	Partial	Yes
Tolerated power of adversary	< 25% computing power	< 51% stake	< 51% validators	< 33.33% validators
Throughput (TPS)	< 100	< 1,000	< 1,000	< 2,000
Scalability	Strong	Strong	Strong	Weak

AuRa is implemented in Kovan network. It comprises of three criteria's: count of nodes (n), aggregate of faulty nodes (f) and division of time duration (t) called steps in seconds. The time duration for every step is decided deterministically by the formula UNIX_TIME / t where t is some constant used to divide the time taken for each step in a discrete manner. In AuRa, every block is accepted in two rounds. In the beginning of the first round, the leader is elected by id mod n where id is a counter initialised to zero incremented by one each time there is a request for block creation. In the first round, the leader broadcasts the proposed block to all the other authorities. In the second round, the block is accepted only if N / 2 + 1 authorities claim to have received the same block. In this scheme, the leader is regarded as malicious when majority of the authorities do not have a trust on the leader. This situation arises when the leader does not propose a block or the leader proposes more blocks than expected (De Angelis et al., 2017; Shi, 2018). Figure 3 illustrates the above concept pictorially.

Clique is implemented in Geth. It takes only a single round to accept a block. Unlike AuRa, a block can be proposed by the current leader as well as other trusted authorities. But the block suggested by the current leader is assigned a score of 2 whereas the block suggested by any other legitimate authority is assigned a score of 1. This is done so that the block proposed by the leader has reached all the signing authorities first. A signing authority can propose a block after every N / 2 + 1 turn. This prevents a single block from proposing a majority of the blocks (Badretdinov, 2018).

Figure 3 Message exchanges in AuRa



2.3 Digital signature

There are different algorithms used for signing documents digitally. Some of the popular signing algorithms include: RSA algorithm, elliptic curve digital signature algorithm (ECDSA), ElGamal encryption system, Rabin cryptosystem and attribute-based encryption.

The ECDSA is a public-key encryption system which operates in a similar fashion to RSA algorithm but provides greater security with lesser key size compared to RSA. The disadvantage of this system is the possibility of error which makes it possible to select a private key value such that identical signatures for different documents can be obtained. However, enormous computational performance is required for this chance to materialise (Amara and Siad, 2011; Aimstone, 2018).

The ElGamal encryption system uses Diffie-Hellman encryption (Chew, 2016). It uses different keys for encryption and decryption. Suppose there are two users A and B, then A forms a mix of its private key and public key (A_{pub} + A_{pri}) and B forms a mix of its private key and public key (B_{pri} + B_{pub}). Then, these two exchanges their mixtures of the keys after the exchange of mixture the two add their private key to the exchanged mixture to obtain a secret key. This type of algorithm ensures encryption as well as digital signature. The shortcoming of this approach is that the encrypted text length is compared twice to the initial length. This causes longer computation time and tougher requirements for communication channel.

Rabin cryptosystem is an extension of RSA Algorithm which can be solved using Chinese remainder theorem (Quick Trixx, 2018). The algorithm begins with the selection of two prime numbers such that both the numbers on division with 4 gives a reminder as 3. Encryption is done using the formula $c = m^{2 \bmod N}$, therefore there is 4 possible output on decryption which is given as $mp = +\text{–}c^{((p+1)/n) \bmod p}$ and $mq = +\text{–}c^{((q+1)/n) \bmod q}$ which can be solved using Chinese remainder theorem and we have to select any one of the four outputs. Though this algorithm has higher operating speed vs. RSA, it is needed to select necessary message out of the four possible outcomes, hence increasing time of execution and decreasing efficiency.

Attribute-based encryption (Antonopoulos, 2014; Lewko and Waters, 2011) is a digital signature algorithm which can be used to sign the transaction message using the

unique customer id which in this case is the customer's mobile number. Since we are dealing with a private blockchain, the unique id of every block is known. So if a sender wants to send the data so that only an authorised person is able to access the data, the sender will encrypt the data with the unique id of the receiver. When the receiver decrypts the data, the receiver will initially compare the received id with the unique id of the receiver. On a successful match of the identities the receiver is granted the permission to view the data, i.e., if the receiver is not authorised then it will not be able to view the data even if the data has been received. The implementation of this also is very simple and works very well for a private blockchain.

Comparing all the different algorithms the authors conclude that attribute-based digital signature would be a better algorithm to be implemented as it does not need much high computation power and is better suited for the private blockchain authorisation under the proposed system architecture.

3 Discussion and analysis

To better understand the working of the proposed system, let us consider the example of a customer named Silvio who has entered one of the outlets of a supermarket. Silvio has logged into the mobile application and has purchased 1,500 value-coins from the retailer creating her block for shopping by invoking the sendFunds() method (Gulley, 2020). After adding the necessary items to her virtual cart, Silvio requests to make a payment of 1,500 value-coins to the retailer.

Figure 4 Illustration of working of the proposed system (see online version for colours)

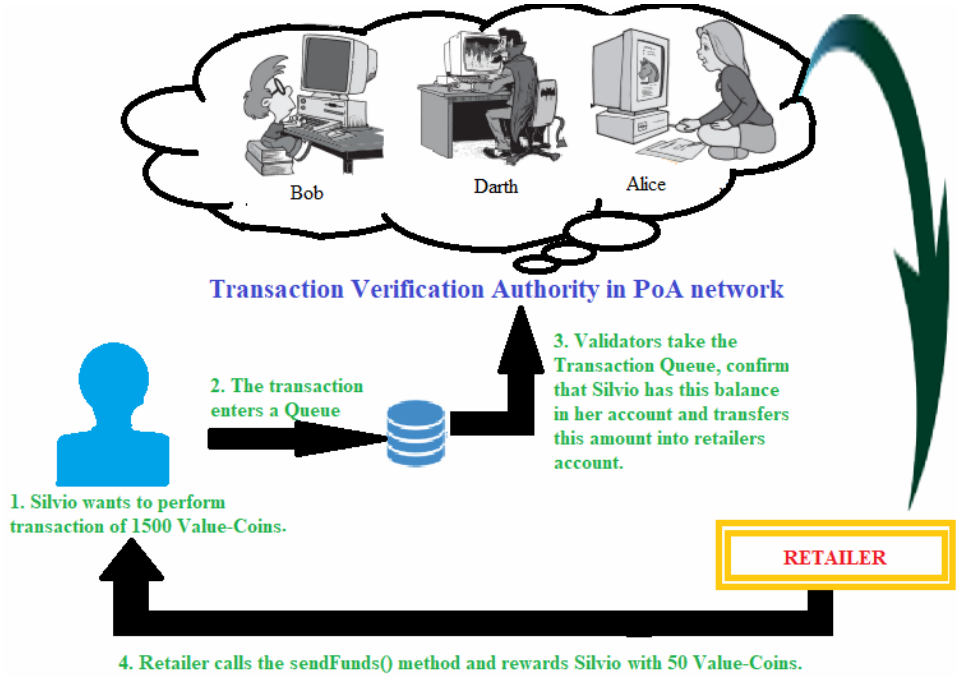


Figure 5 Block creation of Silvio and reward of 50 value-coins (see online version for colours)

```
Creating Genesis block...
Transaction Successfully added to Block
Block Mined!!! : 00003c364085d02447fc40090ea6dbe4a02f7c46b6ff85f8530540fd4acdd373

Value-Coins in circulation: 100.0
Enter the bill amount:1500
Transaction Successfully added to Block
Value-Coins sent to customer = 50
Block Mined!!! : 000f45b8af3d76ed39a415be0396da68779fc9141e9559d9af69078b6176446c
Blockchain is valid

Value-Coins in circulation:  4950
```

Figure 6 Automatic termination of offer (see online version for colours)

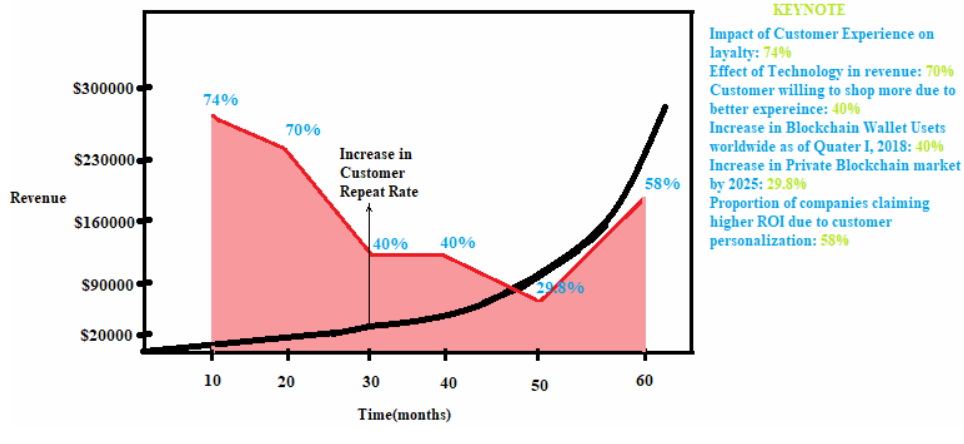
```
Value-Coins in circulation:  50
Enter the bill amount:1560
Transaction Successfully added to Block
Value-Coins sent to customer = 50
Block Mined!!! : 0009814829f5b9ea9e56ea9e49bb17efb8bf558800aaf0d3128f509d9669ebc4

OFFER ENDED!

Value-Coins in circulation: 0.0
```

The transaction verification authority in the PoA network performs a background check on the status of Silvio's digital wallet to ensure that Silvio has 1,500 unspent value-coins. On successful verification, the transaction is digitally signed and sent to the retailer. Say the retailer has an ongoing scheme of rewarding first hundred customers who perform a transaction of or above 1,500 value-coins using this proposed system with 50 value-coins with a validity period of next 30 days. As Silvio is eligible for the reward the retailer calls, the sendFunds() method to reward Silvio with 50 value-coins.

Figure 7 Customer retention with blockchain technology (see online version for colours)



Silvio's transaction is now complete without spending a single minute at the cash counter and she can conveniently walk out of the mall. This scenario is depicted in Figure 4. Figure 5 depicts the remaining 4,950 value-coins that are left for circulation by the retailer as per the given reward scheme. Figure 6 denotes the termination of offer as soon as the first hundredth customers have performed a transaction of 1,500 value-coins using the proposed system. The retailer rewards the customer with the remaining 50 value-coins and then the offer gets automatically terminated.

Figure 7 closely describes how investing on better customer experience and newer technology like blockchain can generate a higher rate of return and business gains.

4 Conclusions and future scope

By the implementation of the proposed system; the retailer would be free from employing people at the cash counter. Instead, the retailer can now employ more people for different roles like supermarket maintenance and theft prevention. Also by analysing customer's product purchasing pattern, several on the fly personalised schemes and advertisements can be developed to pave way for greater cross-selling opportunities.

The future enhancements to the proposed system could consider new emerging solutions introduced by start-ups like shopKick can be used to increase in-store customer traffic and gain better insights into customer purchasing patterns whether in physical retail stores or online. Also with the combination of artificial intelligence and augmented reality, it is possible to provide the best customer experience and services. Finally, with the installation of RFID tags and ink technology for expensive products and clothing and keen monitoring of the small-sized items with the introduction of video analytics, it is possible to achieve a theft-free environment at an affordable investment. Hence, the proposed system must be deployed in the real world to enjoy better profits by the retailer and simplify the customer shopping experience.

References

Aimstone (2018) *Math Behind Bitcoin and Elliptic Curve Cryptography (Explained Simply)*, 29 August [online] https://youtu.be/muIv8I6v1aE (accessed 24 January 2019).

Amara, M. and Siad, A. (2011) 'Elliptic curve cryptography and its applications', *7th International Workshop on Systems, Signal Processing and their Applications*, No. 978-1-4577-0690-5, pp.247–250.

Antonopoulos, A. (2014) *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, O'Reilly Media, Place of publication: Sebastopol, California, ISBN-13: 978-1449374044.

Bach, L.M., Mihaljevic, B. and Zagar, M. (2018) 'Comparative analysis of blockchain consensus algorithms', *MIPRO 2018*, Opatija, Croatia, 21–25 May, pp.1545–1551.

Badretdinov, T. (2018) 14 December [online] https://medium.com/@Destiner/clique-cross-client-proof-of-authority-algorithm-for-ethereum-8b2a135201d (accessed 20 December 2018).

BitRewards Blog [online] https://medium.com/@bitrewards (accessed 20 December 2018).

Brainard, L. (2016) *The Use of Distributed Ledger Technologies in Payment, Clearing and Settlement*, 14 April, Board of Governors of the Federal Reserve System at Institute of International Finance Blockchain Roundtable, Washington DC.

Buschmann, F., Meunier, R., Rohnert, H., Sommerlad, P. and Stal, M. (1996) *Pattern-oriented Software Architecture: A System of Patterns*, Vol. 1, Wiley Series, Hoboken, New Jersey, ISBN-10: 0471958697.

Chakroborty, S. and Jayachandran, P. (2018) *Blockchains: Architecture, Design and Use Cases*, Module 4, Lecture 17 [online] https://nptel.ac.in/courses/106105184/ (accessed 2 January 2019).

Chew, H. (2016) *ElGamal Encryption (Theory and Concepts)*, 17 August [online] https://youtu.be/mdxlFwRF4ek (accessed 24 January 2019).

Chris Skinner's Blog [online] https://thefinanser.com/ (accessed 18 December 2018).

De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A. and Sassone, V. (2017) *PBFT vs Proof-of-authority: Applying the CAP Theorem to Permissioned Blockchain*, Research Center of Cyber Intelligence and Information Security, Sapienza University of Rome.

Dill, B. and Smits, D. (2017) *Zero to Blockchain – An IBM Redbooks Course*, IBM [online] https://www.redbooks.ibm.com/Redbooks.nsf/RedbookAbstracts/crse0401.html (accessed 12 March 2020).

Dinh, T.T.A., Liu, R., Zhang, M., Chen, G., Ooi, B.C. and Wang, J. (2018) 'Untangling blockchain: a data processing view of blockchain systems', *IEEE Transactions on Knowledge and Data Engineering*, Vol. 30, No. 7, pp.1366–1385, 1 July, doi: 10.1109/TKDE.2017.2781227.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C. and Santamaría, V. (2018) *To Blockchain or Not to Blockchain: That is the Question*, March/April, IEEE Computer Society.

Gulley, A. (2020) *Retail Proof-of-concept Proves Viability of Blockchain for Serialized Data Exchange* [online] https://www.hyperledger.org/blog/2020/03/11/retail-proof-of-concept-proves-viability-of-blockchain-for-serialized-data-exchange (accessed 13 April 2020).

Halpin, H. and Piekarska, M. (2017) 'Introduction to security and privacy on the blockchain', *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*.

Lewko, A. and Waters, B. (2011) 'Decentralizing attribute-based encryption', *Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2011: Advances in Cryptology – EUROCRYPT 2011*, pp.568–588.

Li, S. (2018) 'Application of blockchain technology in smart city infrastructure', *IEEE International Conference on Smart Internet of Things*, No. 978-1-5386-8543-3.

Marin, G. (2018) [online] https://blog.cosmos.network/understanding-the-value-proposition-of-cosmos-ecaef63350d (accessed 13 February 2019).

Mirko Kickvic's Blog [online] https://medium.com/altcoin-magazine/blockchain-centralization-is-that-the-future-of-decentralized-network-5d95c6f89de6 (accessed 23 December 2018).

Nakamoto, S. (1998) *Bitcoin: A Peer-to-Peer Electronic Cash System* [online] http://www.bitcoin.org (accessed 12 December 2018).

Nayak, A. and Dutta, K. (2017) 'Blockchain: the perfect data protection tool', *International Conference on Intelligent Computing and Control (I2C2)*.

Quick Trixx (2018) *Rabin Cryptosystem Asymmetric Cryptographic Technique Cryptography & Network Security*, 29 November [online] https://youtu.be/iwCYey4im6Y (accessed 24 January 2019).

Ren, Z., Cong, K., Aerts, T.V., de Jonge, B.A.P., Morais, A.F. and Erkin, Z. (2018) *A Scale-out Blockchain for Value Transfer with Spontaneous Sharding*, No. 978-1-5386-7204-4/18, IEEE.

Shi, E. (2018) *Analysis of Deterministic Longest Chain Protocols*, 6 November, 122-12213, 10.1109/CSF.2019.00016.

Sukhodolskiy, I. and Zapechnikov, S. (2018) *A Blockchain-based Access Control System for Cloud Storage*, No. 978-1-5386-4340-2/18, IEEE Computer Society.

Swan, M. (2015) *Blockchain*, O'Reilly, USA, ISBN: 978-1-491-92049-7.

Tabrizi, S. (2009) *A Next-generation Smart Contract and Decentralized Application Platform* [online] https://github.com/ethereum/wiki/wiki/White-Paper (accessed 21 April 2020).