JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

BLOCK CHAIN-BASED SECURE E-COUPON SERVICE

J.Sahaya Jeniba[1], Gladrene Sheena Basil[2]
Ashwin P[3,] Esakkimuthu T[4,] Nava Nishanth N[5]
[1] Assistant Professor, [2] Professor
[1] Computer Science and Engineering
[1] Loyola Institute of Technology and Science, Nagercoil, Tamilnadu

Abstract : Electronic coupons, sometimes known as "e-coupons," are frequently employed, as the use of online shopping increased. The majority of e-coupon systems manage the information of e-coupons on a single server. However, due to their centralized nature, e-coupon systems frequently face security risks. It becomes difficult to match the user and the e-coupon's owner, for instance, and an expired e-coupon can be used repeatedly (i.e., double-spent), when the e-coupon information that is maintained in a centralized e-coupon server is forged. By utilizing a block chain technology to increase the service's security, we suggest a new e-coupon service to address this problem. In order to accomplish this, we must first create a server that can both enable the e-coupon service and communicate with the block chain system. In addition, we create a smart contract on the block chain system to guarantee the facts and business logic of an e-coupon are accurate. On a block chain system built on Ethereum, we implemented the suggested service. The experimental findings indicate that, when compared to an existing e-coupon service, our suggested service increases security while just slightly affecting performance.

IndexTerms – **Block Chain, e-coupons, Bit Coin, E-Commerce.**

1. INTRODUCTION

Our research seeks to create a novel e-coupon service that forbids unauthorized e-coupon forgery and information manipulation on the e-coupon server. In order to do this, we design an e-coupon service based on a block chain technology.

Electronic coupons, or e-coupons, are becoming a common marketing strategy as the electronic commerce industry expands. E-coupons' electronic form makes them convenient for users as well as an effective management tool for coupon suppliers like merchants and marketers. Since an e-coupon is offered by a digital code, for instance, e-coupon providers can quickly disseminate the e-coupon to the clients online and get statistics about e-coupon usage and downloads. Additionally, users can simply manage their e-coupons on their computers or mobile devices. E-coupons provide these benefits, and according to Global Mobile Coupons Market 2016-2020 [3], the market will expand at a compound annual growth rate (CAGR) of 73.14% from 2016 to 2020.

In order to increase the security of the service, we suggest an e-coupon service based on a block chain system in this article. To accomplish this, we first create a server that can interface with the block chain system and enable e-coupon service. Second, to ensure the integrity of the operations, we create an e-coupon smart contract in the block chain system. We also immediately deploy an e-coupon smart contract on the block chain for customer convenience.

For the security of e-coupon data and business logic code i.e., downloading, giving, and utilizing an e-coupon, we apply and implement the suggested service on the Quorum block chain system. Experimental findings show that the proposed service has a relatively low performance overhead when compared to existing services while also enhancing security. Our work has made the following contributions:

- In terms of security and e-coupon trade, we look into the current e-coupon processing mechanism.
- We suggest a brand-new service that automatically builds an e-coupon smart contract on a block chain system to enable secure e-coupon trade.
- We show that the proposed e-coupon service is safer than the already available ones.

The rest of this paper is organized as follows. Section 2 describes the background and motivation. Section 3 presents the proposed design. Section 4 shows implementation of the proposed service and the experimental results. Section 5 concludes this paper.

2 RELATED WORKS

In this section we discuss some of the literature about the block chain technologies used for digital transformation. In 2018, According to Naskamoto, Using a peer-to-peer network, he suggested a solution to the double-spending conundrum. In order to create a record that cannot be changed without repeating the proof-of-work, the network timestamps transactions by hashing them into a continuous chain of proof-of-work based on hashes. The network's unstructured simplicity makes it robust[17]. The issue is that the payee is unable to confirm that one of the owners did not double-spend the coin. Also there is an issue of determining representation in majority decision-making is similarly resolved by the proof-of-work.

Michael Crosby et al. 2016, [4] block chain enables security, anonymity, and data integrity without the need for an intermediary organization, so increased interest in block chain research. A distributed ledger of all transactions in a bitcoin mining operation is called a block chain which has the potential to play a crucial role in the Internet of Things' architecture. But Bitcoins have a scaling problem (at the moment, it processes 7 transactions per second). In the late 1990s, internet credit card processing was not all that secure. The sixth innovation focuses on the scaling issues with block chains.

According to Jani, and Shailak in 2020 [8], Building Blocks for Digital TransformationConcentrated on the most popular ones, including Ethereum, Hyper Ledger Fabric, Corda, Rootstock (RSK), EOS, and Stellar. Decentralization, Distributed Ledger Technology, Hyper Ledger Fabric, Ethereum, EOS, Corda, Crypto currency, Challenges in Smart Contracts, and Lifecycle of Smart Contracts are all concepts that are related to block chain technology. But smart contracts are computer programs that can be reliably carried out by an interconnected system of nodes that have no trust in one another, incorporating block chain technology.Because they are built into block chains, smart contracts allow for the automatic enforcement of contract terms without the involvement of a reliable third party.

Garg et al. 2002 [9], explained an Architecture for Secure Generation and Verification of Electronic CouponsIn this work, they provide a system for the safe production and validation of electronic manufacturer and retailer coupons. The suggested remedy is based on a 30-party centralised coupon mint that performs double-spending checks, comparable to an online electronic cash system.For electronic coupons, security concerns including coupon manipulation, exchange, duplication, and double spending b ecome highly important.The important distinctions that necessitate the creation of distinct protocols in order to carry out secure coupon transactions

Hsu et al. 2020 [10], demonstrated that Hashing algorithms and asymmetric encryption are just a couple of the encryption methods that block chain technology combines the best features of. In order to further safeguard the data integrity and identity verification, a digital signature is also used. Paper-based vouchers are susceptible to forgery, duplication, low operational efficiency, and other security issues.

According to Buterin in 2014 [21], If the contractor-1 is submitting the registration certificates, it is advantageous to use the block chain since the registration authority can access them. The key benefit over traditional business is that it is quicker, more effective, and more dependable for clients and partners. All transactions are secure and readily visible. Negatives: The primary drawback of the conventional method is the ease with which documents can be falsified. The quotation can still be altered with the help of internal authorities even after the paper has been submitted. Data is easily accessible to hackers.

Summary

In terms of security and e-coupon trade, we look into the current e-coupon processing mechanism. However, due of its centralization, e-coupon services are frequently susceptible to security problems. For instance, it can be challenging to match the user and the e-coupon's owner when the information that is maintained in a centralized e-coupon server is falsified. As a result, an expired e-coupon may be used repeatedly. The most crucial task is to verify an e-coupon because counterfeit or altered e-coupons caused by hostile assaults result in a financial issue.

We suggest a brand-new service that automatically builds an e-coupon smart contract on a block chain system to enable secure e-coupon trade. To enable the e-coupon service and connect to the block chain system, we first create a server. To ensure the integrity of the e-coupon business logic and its information, we secondly create a smart contract on the block chain system. On a block chain system built on Ethereum, we put the suggested service into practice. The experimental findings demonstrate that, when compared to an existing e-coupon service, our proposed service offers stronger security with a relatively low performance overhead. The advantages of the proposed system are

1. Users of PCs or mobile devices can simply manage their e-coupons.
2. The majority of e-coupon providers maintain e-coupon data in a decentralised way to facilitate management.
3. An administrator can quickly change the information.

3 PROPOSED SYSTEM

3.1 Introduction to Block chain

Several businesses or financial organizations are experimenting with the distributed ledger system as a reliable means to track the ownership of the assets without any central authority in light of the introduction of digital money (also known as crypto currency).

Block chain technology is the primary system that underpins the new monetary system. Below is a breakdown of the fundamental Block chain technology building blocks.

In essence, a block chain is a sequence of blocks. To create the signature of the data attached to a block, the SHA-256 hashing technique is used.

Imagine a block chain as a linked list with the following properties at each node:

1. Block number is a sequential number that is assigned to a block and increases monotonically.
2. Nonce is a random number that is used to create a hash value (as in #5) that begins with four zeros (0000). Mining is the term for the process of creating this Nonce.
3. Data: The real user information connected to the block.
4. Prev - holds the hash of the preceding block, such as the current block number minus 1. The value for the first block in the chain is 64 zeroes (0000000000000000000000000000000000000000000000000000000000000000).

5. Hash - the SHA-256-generated hash value for the current block. The hash of this block is calculated using all of the following qualities, with the exception of Hash, such as Block #, Nonce, data, and Prev.

[#=1, Nonce=3409, Data=x, Prev=00..0, Hash=0000ffgr5rg67j] <- [#=2, Nonce=4986, Data=x,

Prev=0000ffgr5rg67j, Hash=000045tggr5rg..77yh] <-……and the chain goes on…

For instance, the value for Hash=0000ffgr5rg67j in block #1 above is produced using the variables 1,3409,x,00..0. The Hash value of this block will change if the value for any one of these 4 characteristics changes. The next Block (#2) will become unusable once the Hash value of this Block changes (for example, from 0000ffgr5rg67j to 34sdffgr5rg67j), as its Prev field will then point to an incorrect Hash (0000ffgr5rg67j no longer exists). This has a knock-on effect that renders the entire chain invalid or tampered with.

One option to correct it is to restart mining and recalculate Block #1's hash value, which will essentially provide a new value for Nonce and produce a legitimate hash value that begins with 4 zeros. Adding a copy of this to Block #2's Prev field these 2 Blocks will be fixed. But in order to fix the entire block chain, we must continue with this process for every block on the chain, making sure that every block points to fresh and legitimate hash codes for its preceding blocks.

As stated in the method above, the cost of correcting the tampered Block chain is very significant. Because we need to go fix the chain that runs from the first block to the last. If the Chain is vast, the procedure gets expensive. Repairing the Blocks becomes an even more expensive task in the case of Distributed Block chain, when multiple Peers are involved in the process and maintain a copy of the Block chain.

Finding the compensating data and adding this Block to the end of the Chain is a different and more effective method. E.g. If the Data field of each Block in your Chain contains a financial transaction (the movement of money), rather than correcting each Block's Data with a corrected financial transaction, come up with an adjusted financial transaction (also known as a compensating transaction) and create a Block (with Data=adjusted transaction record), adding it to the Block chain (adding to the end of the Chain).

3.2 Scope of the proposed work

By ensuring the accuracy of e-coupon data, we put our attention on raising the security bar. The current e-coupon service, for instance, makes use of a database system. In this system, an administrator can simply get the necessary power, which makes malicious data modification by the administrator very simple. While this is the case, the administrator of our offered service, which makes use of a block chain system, finds it difficult to acquire authority because it must be agreed upon by all users. As a result, it is challenging to seize power, and we can stop malicious modification. This indicates that the security level is raised by our suggested system. We go into more detail in section IV-C. Also take note of the numerous studies being conducted to enhance the functionality of the block chain. As a result, block chain performance issues will be reduced in the future, and we will leave work to increase block chain performance for another time.

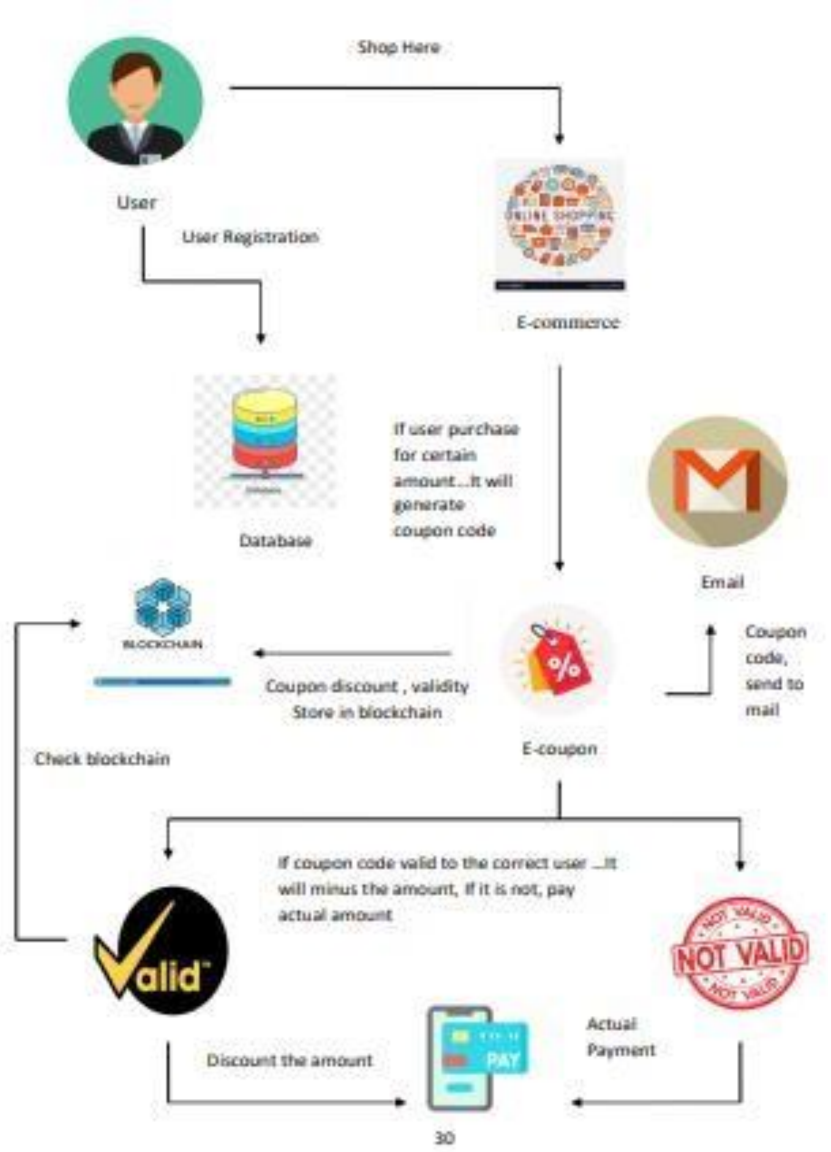

Shop Here
User
User Registration
E-commerce
Database
If user purchase for certain amount...It will generate coupon code
Email
BLOCKCHAIN
Coupon discount , validity Store in blockchain
Coupon code, send to mail
E-coupon
Check blockchain
If coupon code valid to the correct user ...It will minus the amount, If it is not, pay actual amount
Valid
NOT VALID
Discount the amount
PAY
Actual Payment
30

FIGURE 3.1: Architecture Diagram

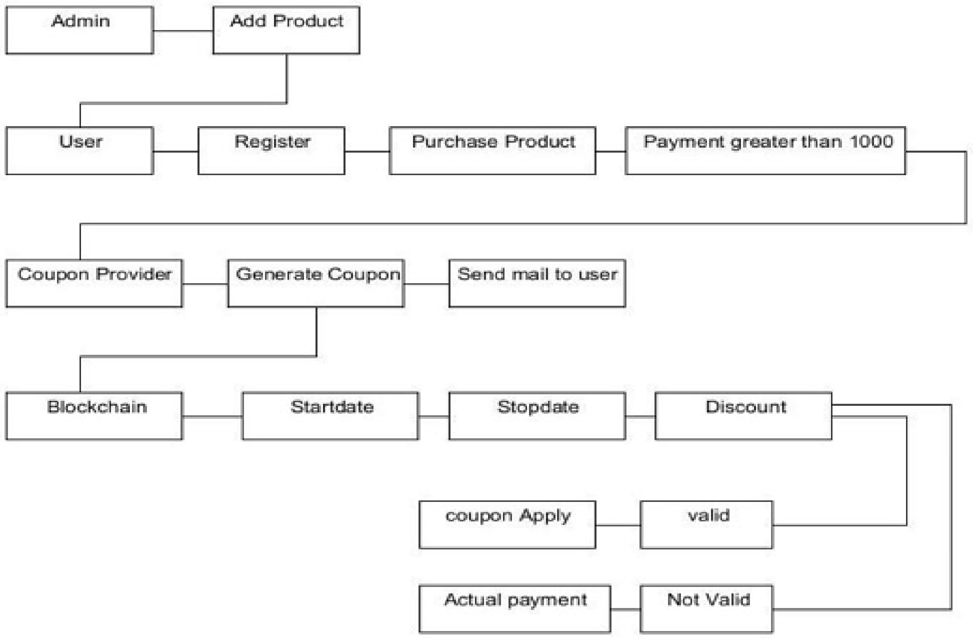


FIGURE 3.2: The work flow of the proposed system

4 IMPLEMENTATION AND RESULTS

The implementation of the proposed work deals with the Admin Configuration, Coupon generation and the Block chain

4.1 Admin Configuration:

The administrator will log in and add the e-commerce site's category and products. Additionally, he has access to the product and category lists. Additionally, the admin has the ability to edit or remove already-added categories and products.

4.2 Coupon Generation

The user will go through the initial registration process in this module, following registration. The MySQL database will be used to store these details. After logging in, the user can view and buy the product. Once the user has made a purchase in excess of $1,000, a promo code will be generated and sent to the user's email. The user must use the coupon before the expiration date after receiving the coupon code. If not, the promotional code will expire.

4.3 The Block chain:

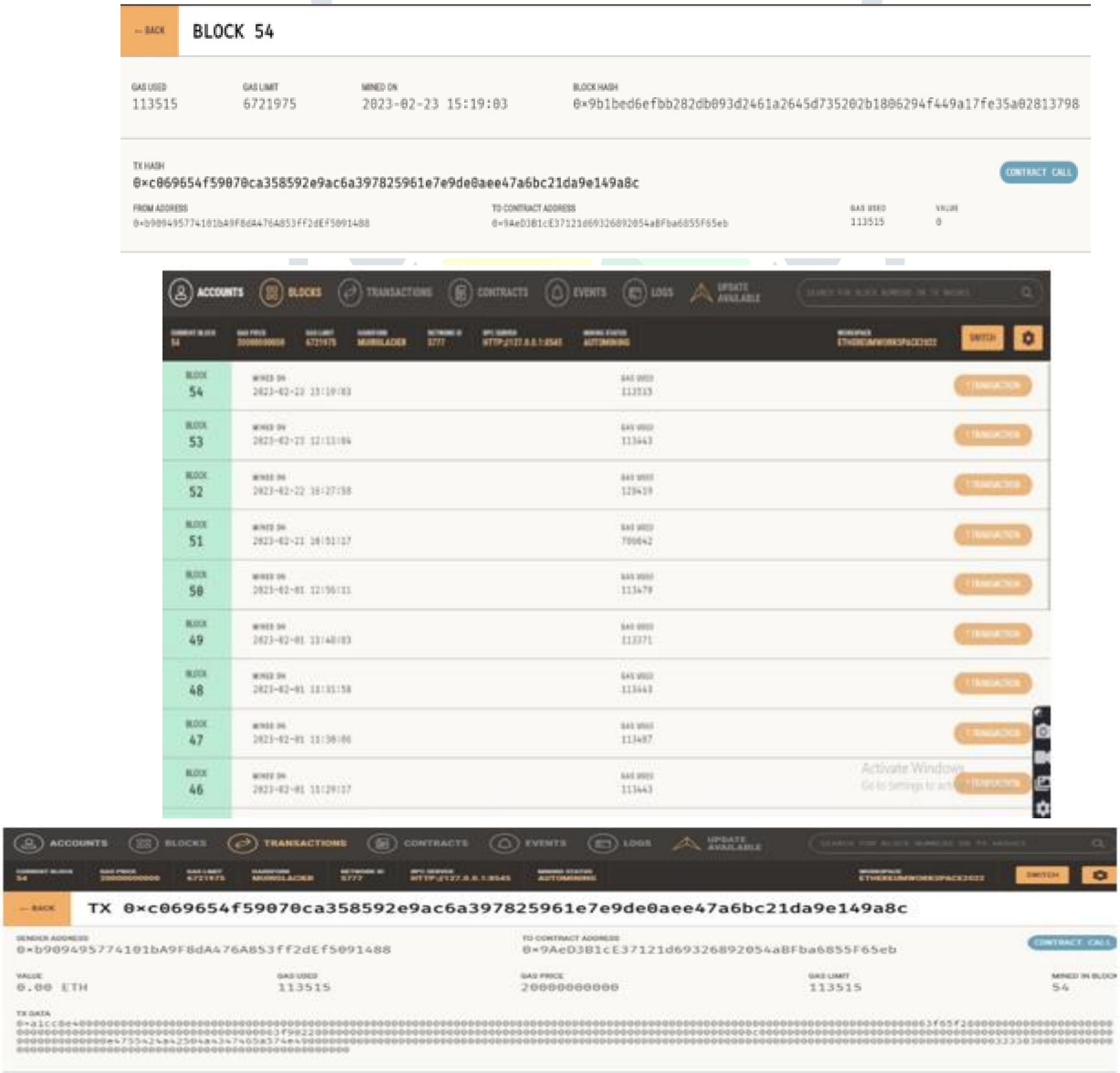
The e-coupon manager offers a user interface for deploying e-coupon smart contracts, getting e-coupon lists, downloading e-coupons, using them, and dispensing e-coupons to customers. The manager also interacts with the block chain to gather and store e-coupon data. For instance, an e-coupon provider may ask the e-coupon management to deploy an e-coupon smart contract while issuing an e-coupon. The e-coupon manager creates the transaction that launches the e-coupon smart contract on the block chain after that.

The e-coupon details and the smart contract address are subsequently saved in the server's database. The e-coupon manager gives clients access to e-coupon information by leveraging the data from the database.

Keep in mind that the server only uses the e-coupon data that is saved there for the application to display. Data modification must be carried out through transaction processing using information from the block chain.

4.4 Results

The below figures denotes the representation of a single block and the block chain obtained for the shopping example



BLOCK 54

GAS USED 113515 | GAS LIMIT 6721975 | MINED ON 2023-02-23 15:19:03 | BLOCK HASH 0×9b1bed6efbb282db093d2461a2645d735202b1806294f449a17fe35a02813798

TX HASH 0×c069654f59070ca358592e9ac6a397825961e7e9de0aee47a6bc21da9e149a8c

FROM ADDRESS 0×b909495774101bA9F8dA476A853ff2dEf5091488 | TO CONTRACT ADDRESS 0×9AeD3B1cE37121d69326892054aBFba6855F65eb | GAS USED 113515 | VALUE 0

CURRENT BLOCK 54 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MUIRGLACIER | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:8545 | MINING STATUS AUTOMINING | WORKSPACE ETHEREUMWORKSPACE2022

BLOCK	MINED ON	GAS USED
54	2023-02-23 15:19:03	113515
53	2023-02-23 12:11:06	113443
52	2023-02-22 16:27:58	129419
51	2023-02-21 16:51:17	700642
50	2023-02-01 12:56:11	113479
49	2023-02-01 11:40:03	113371
48	2023-02-01 11:31:58	113443
47	2023-02-01 11:30:06	113487
46	2023-02-01 11:29:17	113443

TX 0×c069654f59070ca358592e9ac6a397825961e7e9de0aee47a6bc21da9e149a8c

SENDER ADDRESS 0×b909495774101bA9F8dA476A853ff2dEf5091488 | TO CONTRACT ADDRESS 0×9AeD3B1cE37121d69326892054aBFba6855F65eb

VALUE 0.00 ETH | GAS USED 113515 | GAS PRICE 20000000000 | GAS LIMIT 113515 | MINED IN BLOCK 54

TX DATA [illegible]

FIGURE 4.1: Representation of a single block and a block chain

5 CONCLUSION

We have looked into e-coupon systems that maintain e-coupon data on a single server. Our research revealed that the server-stored e-coupon data is susceptible to manipulation by a user or administrator. To solve this problem, we introduce a brand-new e-coupon service that boosts security by utilizing e-coupon smart contracts in a block chain system. On the Quorum block chain, we put the suggested service into practice, and we then used a fake benchmark to assess it. Our test results show that the suggested service effectively inhibits e-coupon information manipulation while imposing a little performance overhead. The performance of block chains will be improved in the future.

REFERENCES

[1] (2019). Wikipedia: E-coupon. [Online]. Available: https://en.wikipedia.org/wiki/E-coupon

[2] C. Blundo, S. Cimato, and A. De Bonis, ‘‘Secure E-coupons,’’ Electron.Commerce Res., vol. 5, no. 1, pp. 117–139, Jan. 2005. volume 10, 2022 21845

[3] (2016). World Mobile Coupons Market to Grow at 73.1% CAGR to 2020. [Online]. Available: https://www.prnewswire.com/newsreleases/world-mobile-coupons-market-to% -grow-at-7314-cagr-to-2020- 603320306.html

[4] Michael Crosby (Google), Nachiappan (Yahoo), Pradan Pattanayak (Yahoo), Sanjeev Verma (Samsung Research America), Vignesh Kalyanaraman (Fairchild Semiconductor), 2016, "BlockChain Technology: Beyond Bitcoin", Applied Innovation Review, Issue No. 2 June 2016,

[5] S.-C. Hsueh and J.-H. Zeng, ‘‘Mobile coupons using blockchain technology,’’ in Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. Springer, 2018, pp. 249–255.

[6] A. Knight and N. Dai, ‘‘Objects and the web,’’ IEEE Softw., vol. 19, no. 2, pp. 51–59, Mar. 2002.

[7] (2018). Quorum. [Online]. Available: https://github.com/jpmorganchase/ quorum

[8] Jani, Shailak. (2020). Smart Contracts: Building Blocks for Digital Transformation. 10.13140/RG.2.2.33316.83847.

[9] Garg, Rahul & Mittal, Parul & Agarwal, Vikas & Modani, Natwar. (2002). An Architecture for Secure Generation and Verification of Electronic Coupons.

[10] C.-S. Hsu, S.-F. Tu, and Z.-J. Huang, ‘‘Design of an E-voucher system for supporting social welfare using blockchain technology,’’ Sustainability, vol. 12, no. 8, p. 3362, Apr. 2020.

[11] (2017). The Coupon Insider: Digital vs. Paper Coupons. [Online]. Available: https://livingonthecheap.com/coupon-insider-digital-papercoupons//

[12] R. G.-P. M.-V. Agarwal and N. Modani, ‘‘An architecture for secure generation and verification of electronic coupons,’’ in Proc. USENIX Annu.Tech. Conf., Boston, MA, USA, Jun. 2001, p. 51.

[13] S.-C. Hsueh and J.-M. Chen, ‘‘Sharing secure m-coupons for peergenerated targeting via eWOM communications,’’ Electron. Commerce Res. Appl., vol. 9, no. 4, pp. 283–293, Jul. 2010.

[14] R. Rivest, ‘‘The MD5 message-digest algorithm,’’ Tech. Rep., 1992.

[15] C.-C. Chang, C.-C. Wu, and I.-C. Lin, ‘‘A secure e-coupon system for mobile users,’’ Int. J. Comput. Sci. Netw. Secur., vol. 6, no. 1, p. 273, 2006.

[16] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, ‘‘Blockchain technology: Beyond bitcoin,’’ Appl. Innov., vol. 2, nos. 6–10, p. 71, 2016.

[17] S. Nakamoto, ‘‘Bitcoin: A peer-to-peer electronic cash system,’’ Tech. Rep., 2008.

[18] M. Szydlo, ‘‘Merkle tree traversal in log space and time,’’ in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Springer, 2004, pp. 541–554.

[19] M. Castro and B. Liskov, ‘‘Practical Byzantine fault tolerance,’’ in Proc. OSDI, vol. 99, 1999, pp. 173–186.

[20] N. Szabo, ‘‘Smart contracts: Building blocks for digital markets,’’ Tech. Rep., 2018.

[21] V. Buterin, ‘‘A next-generation smart contract and decentralized application platform,’’ White Paper, vol. 3, p. 37, Jan. 2014.

[22] U. Maurer, ‘‘Modelling a public-key infrastructure,’’ in Proc. Eur. Symp. Res. Comput. Secur. Springer, 1996, pp. 325–350.