Security Issues and Integrity of e-Coupon Business Logic

Mr.G.Jeevanantham[1] , Dr.D.Satishkumar[2]
[1]Assistant Professor, [2] Associate Professor,
[1,2]Department of Computer Science and Engineering,
Hindusthan Institute of Technology (Autonomous), Coimbatore, Tamil Nadu- 641032
Nehru Instittue of Engineering and Technology , Coimbatore , Tamilnadu -641105
[1]jeevas1984@gmail.com,[2]satishcoimbatore@gmail.com

Abstract— As the popularity of e-commerce grows, an electronic coupon (e-coupon) is widely used due to its convenience and portability. In most e-coupon services, the information of e-coupons is managed on a centralized server. However, e-coupon services are often vulnerable to security issues because of centralization. For example, when the e-coupon information which is stored in a centralized e-coupon server is forged, it becomes difficult to match the user and the e-coupon's owner, and an expired ecoupon can be used repetitively (i.e., double-spending). To handle this issue, we propose a new e-coupon service by exploiting a blockchain system to improve the security of the service. To do this, we first design a server to enable the e-coupon service and communicate with the blockchain system. Second, we devise a smart contract on the blockchain system to provide integrity of the e-coupon business logic and the e-coupon's information. We implemented the proposed service on an Ethereum-based blockchain system. The experimental results show that our proposed service improves higher security with a minor performance overhead compared with an existing e-coupon service

Keywords— E-coupon, blockchain, smart contract, security.

I. Introduction

With the growth of the electronic commerce market, electronic coupons (e-coupons) are being adapted as an effective marketing tool The electronic nature of ecoupons not only provides coupon providers, such as sellers and marketers, with an efficient way of management but is also convenient for customers. For example, since an e-coupon is provided by digital code, ecoupon providers can distribute the e-coupon to the customers online and easily collect statistics such as downloading and using e-coupons. Also, customers can easily manage the e-coupons via their mobile devices or PCs. Because of these advantages of e-coupons, Global Mobile Coupons Market 2016-2020 reports that the global mobile coupon market will grow to a compound annual growth rate (CAGR) of 73.14% over 2016-2020.

Although the e-coupon market evolves and an e-coupon provides several benefits, there are some challenges. For easy management, most e-coupon services manage e-coupon information in a centralized system. When an e-coupon is used, the e-coupon is validated by using the information in the centralized database system. However, the information can be easily manipulated by an administrator due to the centralization nature so that there can be a forgery and fraudulent usage of an e-coupon. For example, an e-coupon may be redeemed multiple times (double spending), or a malicious attacker may manipulate the discount rate. In the United States, Penn Live estimates real e-coupon crime costs to be around $300-$600 million dollars per year. To enhance the security of e-coupons, Hsueh et al propose an e-coupon system using a hash chain which is combined with block chain technology. Our study is in line with the work in terms of providing the integrity of e-coupon information via block chain technology. In contrast, further- more, we provide the integrity of operations (e.g., managing e-coupons, etc.) as well as the integrity of ecoupon information by devising a secure smart contract. In this paper, we propose an e-coupon service based on a block chain system to improve the security of the service. To do this, we first design a server to enable e-coupon service and communicate with the block chain system. Second, we devise an e-coupon smart contract in the block chain system to provide the integrity of the operations (i.e., business logic code) and e-coupon information. In addition, we deploy an e-coupon smart contract to the block chain automatically for user convenience. We apply and implement the proposed service on the Quorum block chain system for the security of e-coupon information and business logic code (i.e., downloading, giving, and using an e-coupon). Experimental results demonstrate that the proposed service improves security and has a minor performance overhead compared with existing services. The contributions of our work are as follows V

_ We investigate the existing e-coupon processing mechanism in terms of security and e-coupon trading.

Mr.G.Jeevanantham, Assistant Professor, Department of Computer Science and Engineering, Hindusthan Institute of Technology (Autonomous), Coimbatore, Tamil Nadu- 641032. (Email id : jeevas1984@gmail.com,)
Dr.D.Satishkumar, Associate Porfessor, Department of Computer Science and Engineering,   Nehru Instittue of Engineering and Technology , Coimbatore , Tamilnadu -641105. (Email Id : satishcoimbatore@gmail.com)

_ We propose a new service that enables secure e-coupon trading via an e-coupon smart contract on a block chain system and deploys the e-coupon smart contract automatically.

_ We demonstrate that the proposed e-coupon service is more secure compared with the existing services.

II. OBJECTIVES

An e-coupon service based on a blockchain system to improve the security of the service. To do this, we first design a server to enable e-coupon service and communicate with the blockchain system. Second, we devise an e-coupon smart contract in the blockchain system to provide the integrity of the operations (i.e., business logic code) and e-coupon information. In addition, we deploy an e-coupon smart contract to the blockchain automatically for user convenience. They apply and implement the proposed service on the Quorum blockchain system for the security of e-coupon information and business logic code (i.e., downloading, giving, and using an e-coupon).

a new e-coupon service by exploiting a blockchain system to improve the security of the service. To do this, the first design a server to enable the e-coupon service and communicate with the block chain system. Second, we devise a smart contract on the blockchain system to provide integrity of the e-coupon business logic and the e-coupon's information. We implemented the proposed service on an Ethereum-based blockchain system. The experimental results show that our proposed service improves higher security with a minor performance overhead compared with an existing e-coupon service.

- We investigate the existing e-coupon processing mechanism in terms of security and e-coupon trading.
- We propose a new service that enables secure e-coupon trading via an e-coupon smart contract on a blockchain system and deploys the e-coupon smart contract automatically.
- We demonstrate that the proposed e-coupon service is more secure compared with the existing services.

III. LITERATURE SURVEY

As the Internet is getting easier and faster to use, electronic coupon (e-coupon) distribution is becoming a more and more popular advertising technique. E-coupons are the digital analogue of paper coupons which are used to provide customers with discounts or gift in order to incentive the purchase of some products. Nowadays, the potential of digital coupons has not been fully exploited on the web. This is mostly due to the lack of “efficient” techniques to handle the generation and distribution of e-coupons. In this paper we discuss models and protocols for e-coupons satisfying a number of security requirements. Furthermore we present a lightweight implementation of our protocol, which preserves the privacy of the users, since it does not require any registration phase.

IV. EXISTING SYSTEM

Blundo et al. [2] propose new e-coupon models and e-coupon protocols using message authentication code (MAC) for e-coupon security. Agarwal et al. [12] propose a solution based on a third-party centralized coupon mint, which checks for double-spending. Hsueh et al. [13] sign the e-coupon with digital signatures (i.e., PKI) an use hash functions to check the consistency of the information and verify all digital signatures of the e-coupon. hang et al. [15] use one-way hash function and MAC, allowing e-coupon providers to prevent e-coupon from being double-redeemed by customers without any additional computation cost on mobile devices.

Hsueh et al. [5] provide a hash chain which is combined with the blockchain technology to verify the forgery of e-coupons. They guarantee the integrity of e-coupon information by using blockchain technology. Our study is in inline with the work [5] in terms of using blockchain technology for integrity of e-coupon. In contrast, we exploit a smart contract to provide the integrity of the e-coupon business logic such as downloading, using, and gifting an e-coupon.

Podda et al. [29] analyze and compare several blockchain-based coupon systems. It also proposes a general schema of digital coupons and points out the basic properties that a coupon system should guarantee. Hsu et al. [30] analyze to prove that the security requirements of the e-voucher system and explore how to apply blockchain technology and cryptography to build a secure e-voucher system. And, They pro- pose a feasible application model that integrates blockchain technology in the context of vouchers to support the field of the campus welfare meal voucher system.

1) Disadvantages

The security is very less since an existing system is not in E-COUPON SMART CONTRACT IN ETHEREUM-BASED BLOCKCHAIN.

In an existing system, in the process of e-coupon services, verifying an e-coupon is the most important task because the forged or manipulated e-coupons by malicious attacks lead to a financial problem.

V. PROPOSED SYSTEM

In this paper, we propose an e-coupon service based on a blockchain system to improve the security of the service. To do this, we first design a server to enable e-coupon service and communicate with the blockchain system. Second, we devise an e-coupon smart contract in the blockchain system to provide the integrity of the operations (i.e., business logic code [6]) and e-coupon information. In addition, we deploy an e-coupon smart contract to the blockchain automatically for user convenience.

The system applies and implement the proposed service on the Quorum blockchain system for the security of e-coupon information and business logic code (i.e., downloading, giving, and using an e-coupon). Experimental results demonstrate that the proposed service improves security and has a minor performance overhead compared with existing services. The contributions of our work are as follows

The system investigates the existing e-coupon processing mechanism in terms of security and e-coupon trading.

The system proposes a new service that enables secure e-coupon trading via an e-coupon smart contract on a blockchain system and deploys the e-coupon smart contract automatically.

The system demonstrates that the proposed e-coupon service is more secure compared with the existing services.

Advantages

Ø By exploiting the feature of the smart contract, the proposed system guarantees the integrity of the e-coupon business logic.

In the proposed system,Ethereum is a one of popular blockchain-based platform that provides smart contracts. A smart contract is a set of promises in a digital form which users perform.

VI. MODULES IMPLEMENTATION

A. Issuer

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as Register and Login, View All Users And Authorize, View All Stores And Authorize, Add Category And Sub-Category, View All Products By Block chain, View All E Coupons By Block chain, View All E coupon Requested, View All Products Details, View All Users Search Transaction Categorized By Search Type, View All Users Search History, View All User Purchased Products, View All Keyword Facet, View Product's Rank In Chart.

B. CUSTOMER

In this module, there are n numbers of users are present. User should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like Register and Login, My Profile, Manage Accounts, Query Search By Keyword, All My Purchased Products Details, View All Search Transaction, View All My Search History, View Top K Searched Keyword Facets.

C. STORE

In this module, there are n numbers of users are present. Transport Company user should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like Login, My Profile, Add Products, All My Product Details, All My Purchased Products With Total Bill, View All Keyword Facet By Rank.

D.SYSTEM STUDY

E. FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

1) ECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

2) TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

3) SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

4) PRELIMINARY INVESTIGATION

The first and foremost strategy for development of a project starts from the thought of designing a mail enabled platform for a small firm in which it is easy and convenient of sending and receiving messages, there is a search engine ,address book and also including some entertaining games. When it is approved by the organization and our project guide the first activity, ie. preliminary investigation begins. The activity has three parts:

- Request Clarification
- Feasibility Study
- Request Approval

a) REQUEST CLARIFICATION

After the approval of the request to the organization and project guide, with an investigation being considered, the project request must be examined to determine precisely what the system requires.

Here our project is basically meant for users within the company whose systems can be interconnected by the Local Area Network(LAN). In today's busy schedule man need everything should be provided in a readymade manner. So taking into consideration of the vastly use of the net in day to day life, the corresponding development of the portal came into existence.

b) FEASIBILITY ANALYSIS

An important outcome of preliminary investigation is the determination that the system request is feasible. This is possible only if it is feasible within limited resource and time. The different feasibilities that have to be analysed.

c) Operational Feasibility

Operational Feasibility deals with the study of prospects of the system to be developed. This system operationally eliminates all the tensions of the Admin and helps him in effectively tracking the project progress. This kind of automation will surely reduce the time and energy, which previously consumed in manual work. Based on the study, the system is proved to be operationally feasible.

d) Economic Feasibility

Economic Feasibility or Cost-benefit is an assessment of the economic justification for a computer based project. As hardware was installed from the beginning & for lots of purposes thus the cost on project of hardware is low. Since the system is a network based, any number of employees connected to the LAN within that organization can use this tool from at anytime. The Virtual Private Network is to be developed using the existing resources of the organization. So the project is economically feasible.

e) Technical Feasibility

According to Roger S. Pressman, Technical Feasibility is the assessment of the technical resources of the organization. The organization needs IBM compatible machines with a graphical web browser connected to the Internet and Intranet. The system is developed for platform Independent environment. Java Server Pages, JavaScript, HTML, SQL server and WebLogic Server are used to develop the system. The technical feasibility has been carried out. The system is technically feasible for development and can be developed with the existing facility.

f) REQUEST APPROVAL

Not all request projects are desirable or feasible. Some organization receives so many project requests from client users that only few of them are pursued. However, those projects that are both feasible and desirable should be put into schedule. After a project request is approved, it cost, priority, completion time and personnel requirement is estimated and used to determine where to add it to any project list. Truly speaking, the approval of those above factors, development works can be launched.

- **SYSTEM DESIGN AND DEVELOPMENT INPUT DESIGN**

Input Design plays a vital role in the life cycle of software development, it requires very careful attention of developers. The input design is to feed data to the application as accurate as possible. So inputs are supposed to be designed effectively so that the errors occurring while feeding are minimized. According to Software Engineering Concepts, the input forms or screens are designed to provide to have a validation control over the input limit, range and other related validations.

This system has input screens in almost all the modules. Error messages are developed to alert the user whenever he commits some mistakes and guides him in the right way so that invalid entries are not made. Let us see deeply about this under module design.

Input design is the process of converting the user created input into a computer-based format. The goal of the input design is to make the data entry logical and free from errors. The error is in the input are controlled by the input design. The application has been developed in user-friendly manner. The forms have been designed in such a way during the processing the cursor is placed in the position where must be entered. The user is also provided with in an option to select an appropriate input from various alternatives related to the field in certain cases.

Validations are required for each data entered. Whenever a user enters an erroneous data, error message is displayed and the user can move on to the subsequent pages after completing all the entries in the current page.

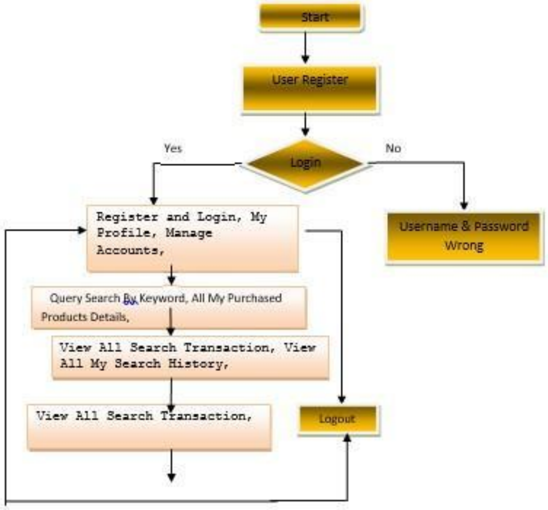
5) OUTPUT DESIGN

The Output from the computer is required to mainly create an efficient method of communication within the company primarily among the project leader and his team members, in other words, the administrator and the clients. The output of VPN is the system which allows the project leader to manage his clients in terms of creating new clients and assigning new projects to them, maintaining a record of the project validity and providing folder level access to each client on the user side depending on the projects allotted to him. After completion of a project, a new project may be assigned to the client. User authentication procedures are maintained at the initial stages itself. A new user may be created by the administrator himself or a user can himself register as a new user but the task of assigning projects and validating a new user rests with the administrator only.

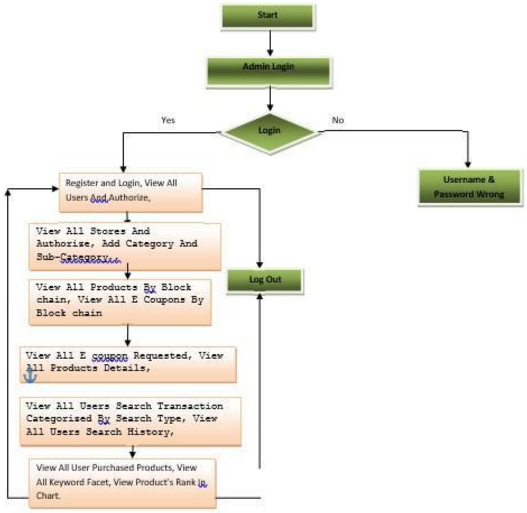
The application starts running when it is executed for the first time. The server has to be started and then the internet explorer in used as the browser. The project will run on the local area network so the server machine will serve as the administrator while the other connected systems can act as the clients. The developed system is highly user friendly and can be easily understood by anyone using it even for the first time.

6) FLOWCHART

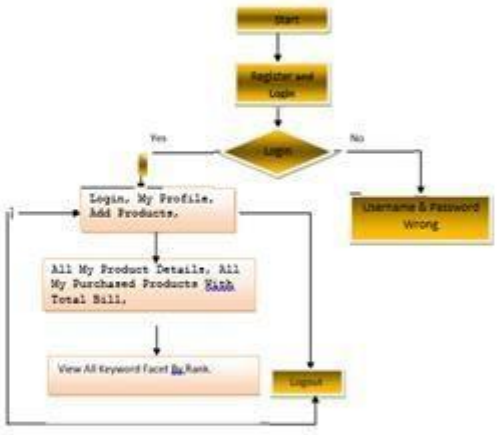
Flow Chart --- Customer


Start
User Register
Yes
Login
No
Register and Login, My Profile, Manage Accounts,
Username & Password Wrong
Query Search By Keyword, All My Purchased Products Details,
View All Search Transaction, View All My Search History,
View All Search Transaction,
Logout

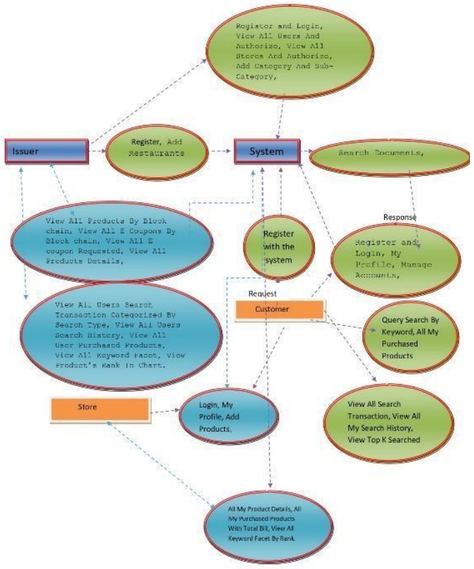
Flow Chart : Issuer


Start
Admin Login
Yes
Login
No
Register and Login, View All Users And Authorize,
Username & Password Wrong
View All Stores And Authorize, Add Category And Sub-Category,
Log Out
View All Products By Block chain, View All E Coupons By Block chain
View All E coupon Requested, View All Products Details,
View All Users Search Transaction Categorised By Search Type, View All Users Search History,
View All User Purchased Products, View All Keyword Facet, View Product's Rank in Chart.

Flow Chart :Store


Start
Register and Login
Yes
Login
No
Login, My Profile, Add Products,
Username & Password Wrong
All My Product Details, All My Purchased Products With Total Bill,
View All Keyword Facet By Rank.
Logout

DATAFLOW DIAGRAM


Register and Login, View All Users And Authorize, View All Stores And Authorize, Add Category And Sub-Category,
Issuer
Register, Add Restaurants
System
Search Documents,
Response
View All Products By Block chain, View All E Coupons By Block chain, View All E coupon Requested, View All Products Details,
Register with the system
Register and Login, My Profile, Manage Accounts,
Request
Customer
View All Users Search Transaction Categorized By Search Type, View All Users Search History, View All User Purchased Products, View All Keyword Facet, View Product's Rank in Chart.
Query Search By Keyword, All My Purchased Products
Store
Login, My Profile, Add Products,
View All Search Transaction, View All My Search History, View Top K Searched
All My Product Details, All My Purchased Products With Total Bill, View All Keyword Facet By Rank.

VII. FUTURE ENHANCEMENT

In the future, we will focus on improving blockchain performance In the era of the fourth industrial revolution, all aspects of the industrial domain are being affected by emerging technologies. Digitalization of every process is taking place or under process. One of the most important components common to every domain is the supply chain process. Organizations employ a digital supply chain to track the delivery of their products or materials. The digital supply chain is still suffering from a few issues such as no provenance, less transparency, and a trust issue. Blockchain technology, one of the emerging technologies, can be integrated with the supply chain to deal with the existing issues and to improve its performance. In this, a model is proposed to integrate blockchain technology with the supply chain to improve performance. The proposed model uses the combination of the Ethereumblockchain and the interplanetary file system to maintain the traceability, transparency, and trustworthiness of the supply chain.

VIII.CONCLUSION

We have investigated e-coupon services that store e-coupon information on a centralized server. We found that the e-coupon information stored in the server can be manipulated by a malicious attacker or administrator. To handle this issue, we present a new ecoupon service that improves security by exploiting ecoupon smart contracts in a block chain system. We have implemented the proposed service on the Quorum block chain and evaluated the service using a synthetic bench mark. According to our experimental results, the proposed service prevents the manipulation of e-coupon information with higher security and minor performance overhead. In the future, we will focus on improving block chain performance.

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 Ecoupons," Electron. Commerce Res., vol. 5, no. 1, pp. 117_139, Jan. 2005. [3]

[3] (2016). World Mobile Coupons Market to Grow at 73.1% CAGR to 2020. [Online]. Available: https://www.prnewswire.com/news- releases/world-mobile-coupons-market-to% -grow-at7314-cagr-to-2020-603320306.html (2017). Coupon Fraud is Crime, Even if it Feels

[4] Harmless: Coupon Coun- selor. [Online]. Available: https://goo.gl/2emab1. [5] S.-C. Hsueh and J.-H. Zeng, ``Mobile coupons using blockchaintechnol- ogy," in Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. Springer, 2018, pp. 249_255.

[5] A. Knight and N. Dai, ``Objects and the web," IEEE Softw., vol. 19, no. 2, pp. 51_59, Mar. 2002.

[6] (2018). Quorum. [Online]. Available: https://github.com/jpmorganchase/ quorum

[7] (2017). Coupon Statistics: The Ultimate Collection. m[Online]. Available: https://blog.accessdevelopment.com/ultimate-collectioncoupon- statistic%s

[8] (2017). emphDigital Coupon Marketing_Statistics and Trends. [Online]. Available: https://www.invespcro.com/blog/digitalcoupon-marketing

[9] (2019). Digital Coupons Continue to be the Fastest Growing Method of Redemption due to Shoppers' Increased Demand for Convenience. [Online]. Available: https://www.globenewswire.com/news-release/2019/ 02/13/1724510/0/en/Digi%tal-Coupons-Continue-to-bethe-Fastest-

[10] Growing-Method-of-Redemption-Due-t Sho%ppersIncreased- Demand-for-Convenience.html

[11] (2017). The Coupon Insider: Digital vs. Paper Coupons. [Online]. Available: https://livingonthecheap.com/coupon-insiderdigital-paper- coupons//

[12] R. G.-P. M.-V. Agarwal and N. Modani, ``An architecture for secure generation and veri_cation of electronic coupons," in Proc. USENIX Annu.

[13] Tech. Conf., Boston, MA, USA, Jun. 2001, p. 51. [13] S.-C. Hsueh and J.-M. Chen, ``Sharing secure mcoupons for peer- generated targeting via eWOMcommunications," Electron. Commerce Res. Appl., vol. 9, no. 4, pp. 283_293, Jul. 2010. [14] R. Rivest, ``The MD5 message-digest algorithm," Tech. Rep., 1992.

[14] C.-C. Chang, C.-C. Wu, and I.-C. Lin, ``A secure ecoupon system for mobile users," Int. J. Comput. Sci. Netw. Secur., vol. 6, no. 1, p. 273, 2006.

[15] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, ``Blockchain technology: Beyond bitcoin," Appl. Innov., vol. 2, nos. 6_10, p. 71, 2016.

[16] S. Nakamoto, ``Bitcoin: A peer-to-peer electronic cash system," Tech. Rep., 2008.

[17] M. Szydlo, ``Merkle tree traversal in log space and time," in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Springer, 2004, pp. 541_554.

[18] M. Castro and B. Liskov, ``Practical Byzantine fault tolerance," in Proc. mOSDI, vol. 99, 1999, pp. 173_186.

[19] N. Szabo, ``Smart contracts: Building blocks for digital markets," Tech. Rep., 2018.

[20] V. Buterin, ``A next-generation smart contract and decentralized applica- tion platform," Tech. Rep., 2014.

[21] V. Buterin, ``A next-generation smart contract and decentralized applica- tion platform," White Paper, vol. 3, p. 37, Jan. 2014. [23] U. Maurer, ``Modelling a public-key infrastructure," in Proc. Eur. Symp.

[22] Res. Comput. Secur. Springer, 1996, pp. 325_350. [24] D. Hankerson, A. J. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography. Springer, 2006.

[23] (2019). Apache JMeter_ApacheJMeterT. [Online]. Available: https;://jmeter.apache.org/