Applied Information Technology And Computer Science Vol. 2 No. 2 (2021) 236-248

AITCS

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/aitcs
e-ISSN :2773-5141

Decentralized Application for Charity Organization Crowdfunding using Smart Contract and Blockchain

Winson Lee Hong Yee, Nordiana Rahim*

Faculty of Computer Science and Information Technology,
Universiti Tun Hussein Onn Malaysia (UTHM), Parit Raja, 86400 MALAYSIA

DOI: https://doi.org/10.30880/aitcs.2021.02.02.016
Received 13 June 2021; Accepted 09 September 2021; Available online 30 November 2021

Abstract: Online crowdfunding platforms have become places where people donate funds to support lifelong missions, such as donating funds to support local art sales or supporting underprivilege people to gain access to an education. However, with the rise of cybercrime and data breaches, important information and transaction records in crowdfunding have become the targets of cybercriminals. In this project, Blockchain technology is implemented to protect the information in crowdfunding such as the transactional of donation. This study demonstrates the role of Blockchain in storing information on the Ethereum network. Subsequently, a decentralized Blockchain web application, FundDapp, is proposed, which aims to design a decentralized crowdfunding web application that provides peer-to-peer transfers, develop a Blockchain website for crowdfunding purposes, and to test the application on the Ethereum network This application is developed using an Object-Oriented Software Development Model, and the main functions are developed with the use of Python Flask framework and Web3.js library. Meanwhile, results show that the web applications can initiate point-to-point between two parties through the smart contract mechanism. It is expected that the results of this research are expected to significantly influence and increase the use of cryptocurrency in our daily lives, and the use of Blockchain technology in enterprise data protection.

Keywords: Blockchain, Crowdfunding , Data Protection. Ethereum, Smart Contract

1. Introduction

According to U.K Financial Conduct, Crowdfunding is defined as a way in which people and businesses (including start-ups) can try to raise money from the public to support a business, project, campaign or individual [1]. An online crowdfunding has made raising capitals easier as this allows capital seekers to raise funds from the crowd for specific purposes from a large number of capital givers through online platforms that served as intermediaries. On the other hand, traditional crowdfunding organizes physical talks and people are invited to witness the crowdfunding ceremony [1]. The main concern of online crowdfunding system is the issue of trust and security [2]. The designed system must be able to handle transaction through a protected and secured channel. This is especially true when the

*Corresponding author: nordiana@uthm.edu.my

crowdfunding platform needs to handle a large monetary funds. Some of the security requirements are fraud prevalent, secured paywall and privacy [2].

Blockchain is a technology that will produce a public electronic ledger as its end goal. It is built around a peer-to-peer network system that can be openly seen by everyone on the network. Each time a transaction happens, the data contains the transaction together with the timestamp are added as another block connected to the previous block. As a result, a public ledger is formed [3]. When one of the blocks is tampered or changed, this will also affect the parent block since the present block contains the address of its parent block. Therefore, it is difficult to tamper a present block while it has many other blocks before it. This is what makes blockchain trustworthy and immutable [4].

This study aims to use the Blockchain technology extensively to secure the important information such as the transactional records of donation. The Blockchain solution solves and preserves the integrity of information and resolves unauthorized modification issue [5]. The solution also allows public to trace the donation records of the crowdfunding platform and benefit from real-time transaction assurance [6]. Lastly, the solution erases the need for intermediaries. Hence, charitable organizations can streamline the processes and reduce costs [6].

The objective of this study is to design, develop and test the decentralized crowdfunding web application, FundDapp, in facilitating the donation process on Ethereum network. It should be noted that this web application requires to install the Metamask wallet extension before getting the full experience in using this application.

This paper is organized into the following sections: Section 2 provides the review of Blockchain related work that includes Blockchain and Ethereum Smart Contract. Section 3 describes the design and development of FundDapp web application. Section 4 presents findings and discussion. Lastly, section 5 concludes the study.

2. Related Work

In this section, the literature review of the relevant terms revolve on the proposed system such as Blockchain architecture, Blockchain characteristics, Ethereum network, and comparative study of the existing systems with or without Blockchain technology.

2.1 Blockchain Architecture

Figure 1 shows the explanation of the Blockchain through its block header and block body. Block header as mentioned in the table has six fundamental information about the block data which is the block version, Merkle tree root hash or current block hash, timestamp, nBits, nonce and previous block hash. The lower part of the block contains how many transactional records can be hold within a block. This depends on the size of the block and the size of the transactional records [7][8][9].

Furthermore, the block consists of block header and block body. The block version shows what kind of validation rules to follow for the architecture. The timestamp in the Blockchain shows the current time measured in seconds using UNIX timestamp. While the nonce represents the random value that can be changed according to the likes of the owner. Lastly, the Blockchain contains the parent block hash which is the previous block hash with 256-bit hash value [10].

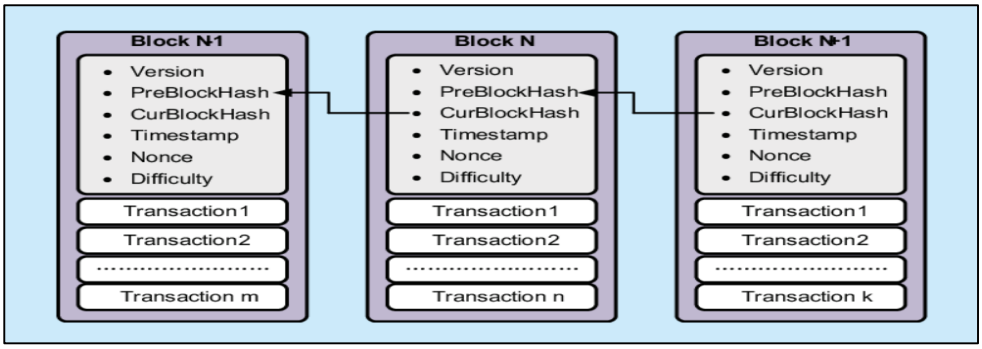

Figure 1: Blockchain Architecture[8]

2.2 Key Characteristics of Blockchain

Blockchain has four facets or four main characteristics [11].The first characteristic of Blockchain is that it is distributed and synchronized. It encourages data stored in blockchain to be distributed as a public ledger across all network nodes. This allows the trust to be established between different unknown network nodes. Hence, all nodes are responsible to maintain the blockchain information whereby there is no single entity to take full control of it. This reduce the risk of single failure and data integrity [12].

The second characteristic of blockchain is that it contains smart contract. Smart contract is a digital agreement that binds every user on the blockchain application. The smart contract is stored in the blockchain and it is a computer protocol to facilitate digitally, verify and enforce the conditions as agreed among the users in the Blockchain application[13][14].

The third characteristic of blockchain is that it is built on peer-to-peer network. This means every user on the blockchain represents a node, and the nodes are responsible to validate whether a block added in to the existing blockchain is valid or not. When blockchain is built on a peer-to-peer network, it can prevent inaccurate and fraudulent transactional data out of database. Lastly, Blockchain is immutable. Hence, immutability will give blockchain to preserve the integrity of a data and avoid alteration by any person. This will provide provenance of assets, as the assets can be traced as where is it is and what has happened to the assets in the Blockchain structure [12].

2.3 Ethereum network

Ethereum is a platform that was first mentioned by Vitalik Buterin, the Ethereum platform's inventor. Apart from Bitcoin, it is a platform for developing applications. Compared to the traditional Bitcoin design, Ethereum provides a number of advantages. It improves the Blockchain structure and adds smart contracts to the mix. The adoption of smart contracts has far-reaching implications, as it can successfully eliminate reliance on third parties [15]. The Ethereum Foundation is responsible for the upkeep of Ethereum. The Ethereum Foundation is the governing organization in charge of Ethereum's and its tools' future development. Ethereum has its own official information sources. The technical information regarding the protocols involved is contained in the Ethereum White Paper and Ethereum Yellow Paper [16].

With Ethereum, it has full-Turing completeness. It supports all types of computation and it uses its programming language, Solidity. It can run software code written for the blockchain environment. Such software is considered to take the advantages of the blockchain in order to implement constraints that two parties can agree on when signing the contract. The software is named Smart Contract. Solidity in Ethereum can be used to write smart contract scripting that allows users to create their own rules of ownership and determining the format of transactions [17].

2.4 Smart Contract and Solidity

A smart contract contains executable code that aims to implements rules according to different constrains. It consisted of three main parts [17]：

- The code of the program that contains logical steps
- The inputs that the smart contract receives and what triggers the event of smart contract
- The set of methods that are activated by the code

When the smart contract is finished, it is uploaded to the blockchain platform. The smart contract used is immutable, meaning it can't be changed in any way. The smart contract's terms will serve as a legal instrument that binds the parties involved together. Many blockchain platforms, such as Hyperledger Fabric [18] , Qtun [19], and Achain platform can host the deployment of smart contracts. The process to deploy the smart contract is separated into three parts. Firstly, the code is written in Solidity. Then, the code compiling process happens, whereby the code in Solidity is compiled into Ethereum virtual machine bytecode which only can execute on the local environment. Lastly, transaction that served as inputs can then trigger the smart contract. At the moment of deployment, an address is assigned. The assigned address can be accessed to visualize the data of the smart contract such as its address and balances [17].

2.5 Existing Solutions and Systems for Crowdfunding Application

Many companies have developed crowdfunding applications because of the potential of crowdsourcing to provide as a platform for individuals to support philanthropic initiatives while also reducing the challenges caused by centralized systems. Existing crowdfunding applications include the Entrepreneurship Crowdfunding Website and the Funding Community Project using Smart Contract on Blockchain.

Entrepreneurship Crowdfunding Website is researched and planned by both Mr. Chen Dan Hong and Mr. Yi Tian Yu. Under their system, the target users are students who reside and currently study in college. The crowdfunding website is designed and made to support students who are active in entrepreneur and hoping that more funds are made available for students who wish to start a business. As stated in the paper, the main objective of establishing a crowdfunding website specifically for students is to design a exchange network platform that can better provide entrepreneurial resources and fund support for college students entrepreneurs. The platform will provide project sponsors or investors outstanding numbers of students' projects and also allowing students to obtain funds to continue their project's mission, which then link both parties together for raising funds [20]

Funding Community Projects with Smart Contracts on Blockchain is a decentralized crowdfunding application made using Ethereum platform and using smart contract as well. Blockchain technology is used to protect data from tampering and the data protected in this case [21]. The transaction carried out is using cryptocurrency, Ether, a cryptographically secured asset to serve as a medium of exchange on this website. Smart contract is used to facilitate the process in the website which includes the transactional exchange and prevent third party dependency [21].

Table 1: Comparisons of Existing Systems

Attributes	FundDapp	Entrepreneurship Crowdfunding Website	Funding Community Projects with Smart Contract
Public Permissioned Blockchain	Yes	No	Yes
Point-to-Point Transfer	Yes	No	Yes
Using Cryptocurrency	Yes	No	Yes
Using Smart Contract	Yes	No	Yes
Using OTP before transferring	Yes	No	Yes
Hashing using PBKDF2	Yes	No	No
Ethereum Blockchain	Yes	No	No

According to the table above, the suggested system can do the majority of the functions that none of the existing systems can. The suggested system can perform one-time password (OTP) authentication prior to payment, and the smart contract is housed on the Ethereum network. Both systems are incapable of doing these tasks.

3. System Development: Methodology and System Analysis

This project has adopted object-oriented analysis and design (OOAD) as the methodology for developing the project. This methodology and its flow are separated into object-oriented requirement analysis, object-oriented design, object-oriented implementation and testing.

Table 2: System Development Activity and Outcomes

Phase	Activity	Outcome
Object-Oriented Requirement Analysis	• Proposed Project's objectives • Determine project's requirements • Determine functional and non-functional requirements	• Problem statements and objectives of projects • Literature review and project scope
Object-Oriented Design	• Design architecture diagram • Design UML diagrams • Design ERD diagrams • Design class diagrams	• Interface design • Entity relationship diagram • Activity diagram • Sequence diagram • Use case diagram
Object-Oriented Implementation	• Frontend using HTML, CSS, and JavaScript • Create MySQL database scheme • Backend using Python Flask framework • Blockchain using Solidity	• Decentralized web application
Testing	• Positive testing and negative testing • Test plan and user acceptance test	• Application is tested by users

Figure 2 shows the use-case diagrams for both donators and organizations. It outlines what core functions can both the users perform in the proposed system. Donators can perform registration and

login module by filling in the required user's information. The donator is also able to create comments, transfer fund, manage profile, view transactional records, and lastly receive refund if the project has expired and the targeted fund needed is not reached.

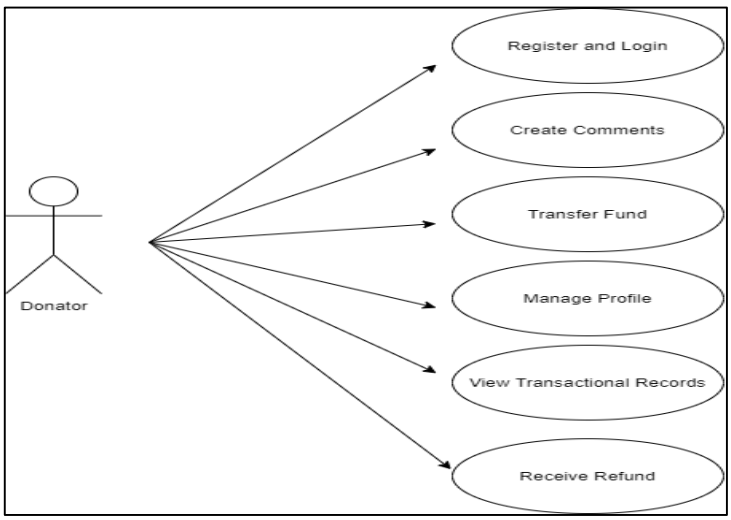

Figure 2: Use Case Diagram for Donator

Figure 3 shows the use case diagram for organizations. The core functions of what an organization can perform are linked to the modules as shown below. The organizations are able to perform registration and login module. Besides, the organization can create comments, create crowdfunding projects. Manage profile, view transactional records and also receive cryptocurrencies for the target crowdfunding projects.

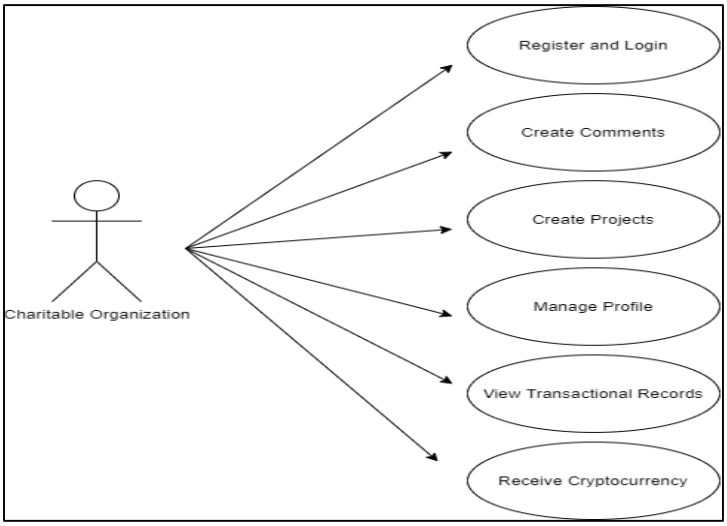

Figure 3: Use Case Diagram for Organization

Figure 4 below shows the general system architecture for the crowdfunding system. Firstly, the user is needed to sign up for an account, either to become a donator or registering for an organization account. The information is then stored into the database provided by the hosting service.

The user who signed in as a donator has several functionalities that can be performed. Functionalities such as managing the user profile, viewing ongoing campaigns, joining ongoing campaigns and creating comments are linked to the database of the system. Besides, functionalities such as donating the funds in Eth, getting refund after a failed project and viewing and verifying the Blockchain data are then connected to the Ethereum Blockchain. User who signed in as an organization

has several functionalities as well. The organization can manage the profile, creating campaigns and creating comments. These functionalities are linked to the database and are stored within it. On the contrary, the functionalities of claiming funds and viewing the transactional activities are then linked to the Ethereum Blockchain network which preserves the integrity of the information.

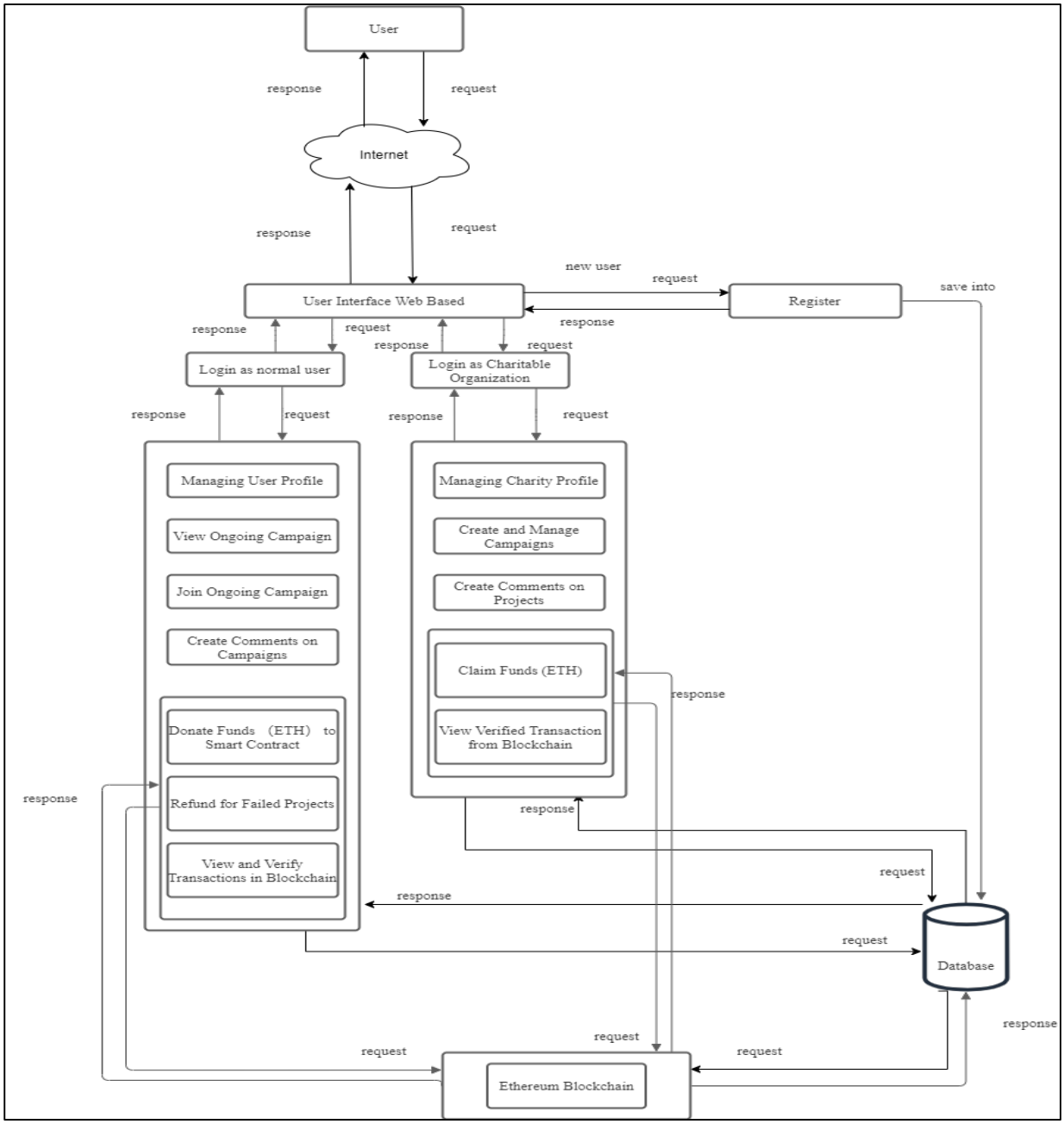

Figure 4: General System Architecture for Crowdfunding FundDapp

Figure 5 shows that the user register to become a donator and then when successfully authenticated, the user is given the access to the system. After login, the user can perform functions such as viewing transaction records, manage profile, donate cryptocurrency to the crowdfunding projects as well as posting comments. Lastly. The user's session is destroyed when the user is logged out from the system.

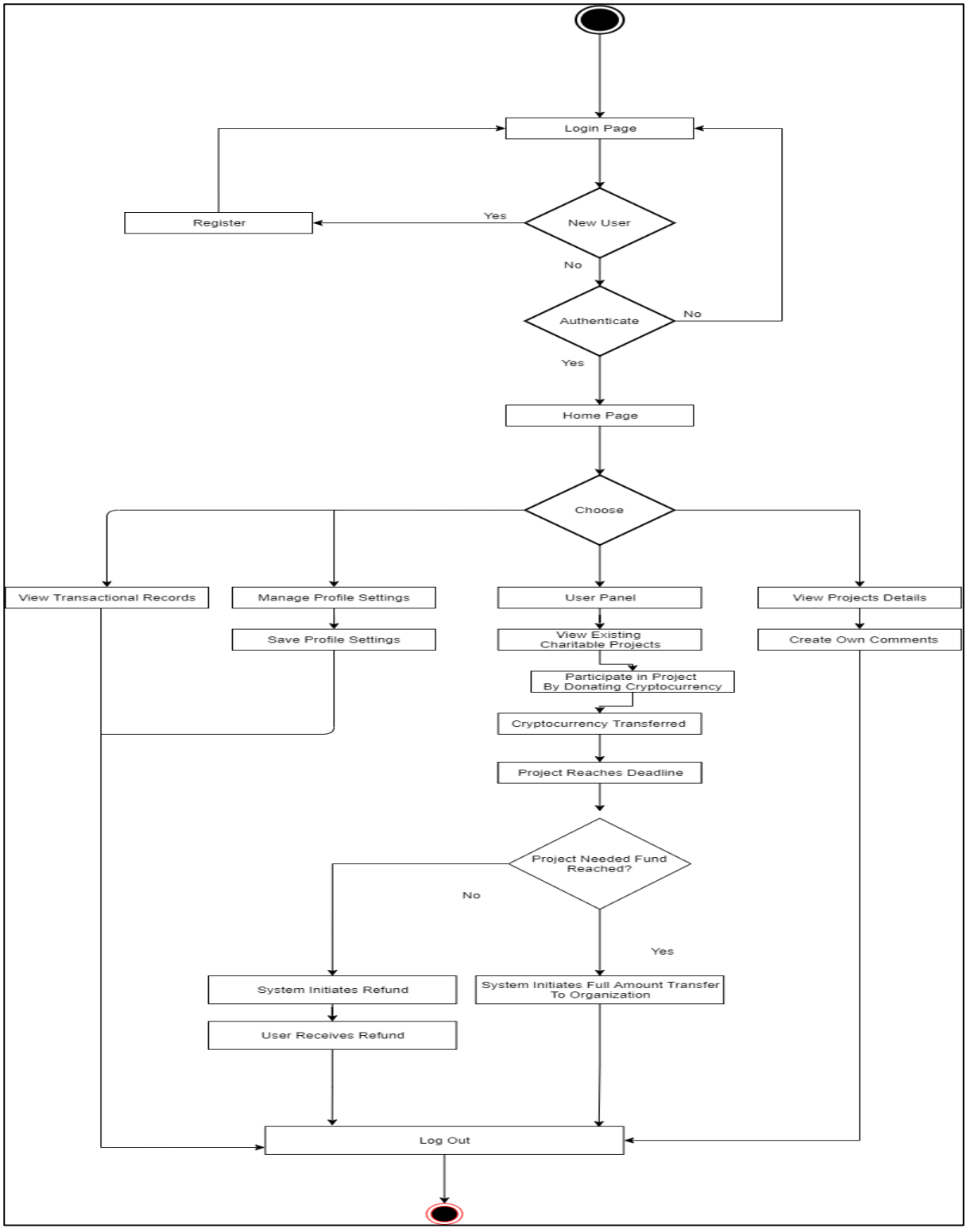

Figure 5: Activity Diagram for User as Donator

Figure 6 shows that the charitable organization registers to become a charitable organization and then when successfully authenticated, the organization is given the access to the system. After login, the organization can perform functions such as viewing transaction records, manage profile, receive cryptocurrency from the particular crowdfunding projects as well as posting comments. Lastly. The organization's session is destroyed when the user is logged out from the system.

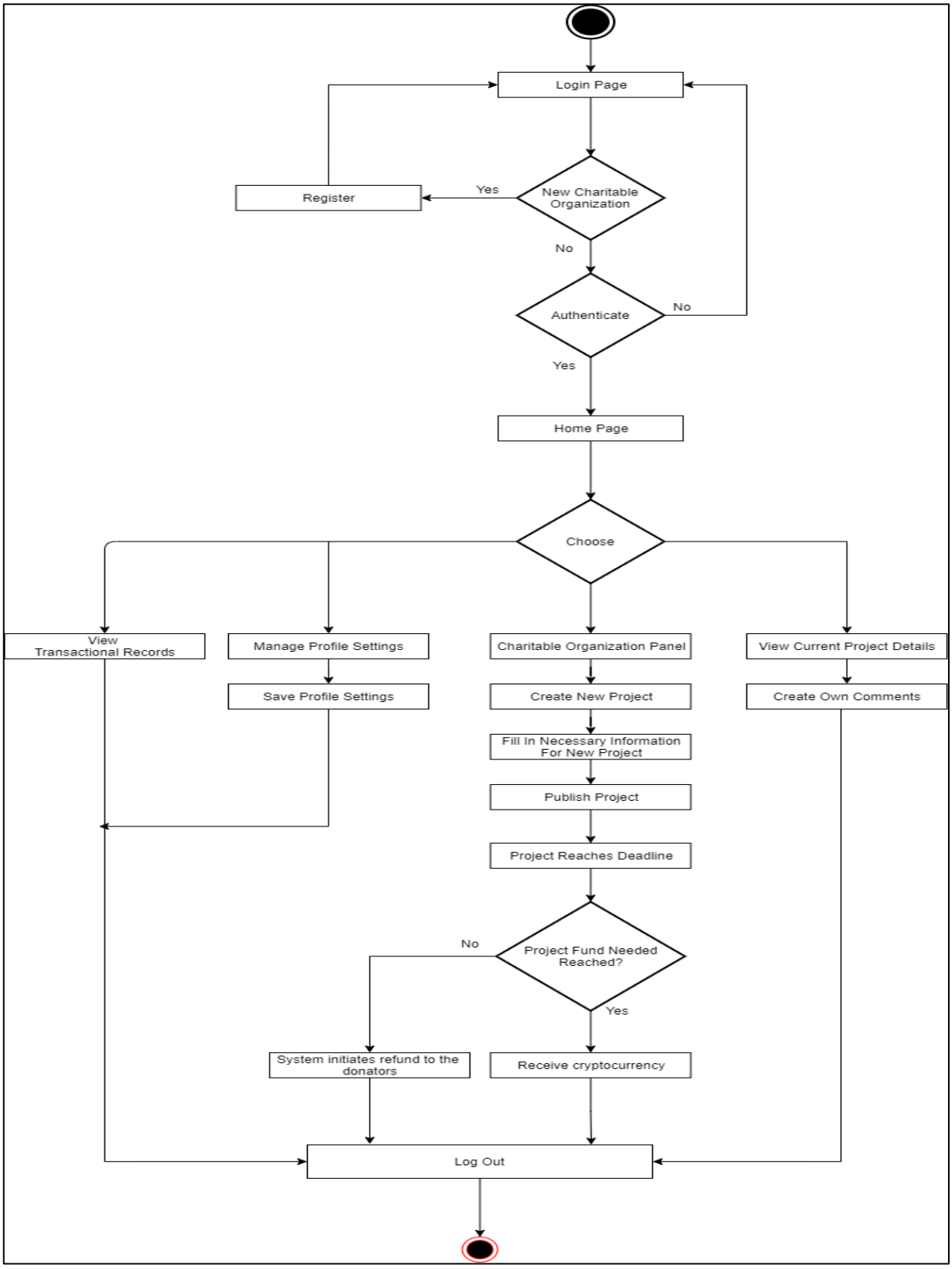

Figure 6: Activity Diagram for User as Organization

4. Result and Discussion

4.1 Implementation

The system begins with the design of the interfaces using HTML, CSS and JavaScript on the client side. The backend is developed using Python as a backend language with the aid of Python Flask framework. The smart contract for Ethereum Blockchain network is coded using Solidity programming language via the Remix IDE online browser. The smart contact is later deployed to the Ethereum Blockchain network. The deployed smart contract address and its ABI code is programmed into the backend of the proposed system. Figure 7 shows the Remix Online editor with some of the smart contract code.

Figure 7: Smart Contract on Remix Editor

For donation function, the code is first coded into the smart contract and then the function is then initiated on the proposed system's backend. On the donation function, donator is required to donate a specific amount of ETH coins in Wei and then the system takes a minute or two to add the new data to the Ethereum blockchain network. The system also requires donator to use OTP authentication before authenticating the payment. Figure 8 shows the donation interface for the proposed system.

After pressing the confirm donate button, the donator is directed to a loader to wait for the Blockchain to process the transactions. The transaction data requires gas fees in order to be added into the Ethereum Blockchain. While the user waits for the data to be added, in the Blockchain network, the data is being mined by the nodes in the Ethereum network. If the miner has completed the mining, the transaction data is added to the block in the Blockchain with hash values. The crowdfunding system will return the hash values of the data as a proof showing that the data has been added into the Ethereum Blockchain network and the data integrity is preserved. At the same time, the data is also stored in the MySQL database.

Figure 8: Donating Interface

On claim fund function, when the project has expired and the fund collected is more than or equal to what is required, then the organization clicks on the claim fund button to retrieve the fund stored in the smart contract. While the organization waits for the fund to be claimed, on the Blockchain side, the

transactional activities are being mined in the Ethereum network. If the mining process is done, and the data is added to the Blockchain successfully, the system will return the current block hash value as a proof to show that the data integrity is preserved. Then, the funds stored in the smart contract is then released back to the organization.

4.2 Integrity and Auditability of Blockchain in Crowdfunding Application

Maintaining the integrity of information and providing auditability are the core functions of Blockchain technology. With the use of the Blockchain, transaction records such as donation and withdrawal of funds in the crowdfunding are stored in the Ethereum Blockchain ledger. Each record after the donation or claim is stored in a Blockchain block, which contains information such as the previous hash value and the current block hash value. Any change to the block information will also affect its block hash and the next block that contains the hash value of the previous block. Complete modification of crowdfunding records across all nodes on the network will take a long time and is impossible with today's computing power. Therefore, Blockchain is immutable and maintains the integrity of the crowdfunding records.

Furthermore, the Ethereum Blockchain also provides record auditability. In the function of the donations and claims fund, each transaction made by the users of both parties is stored in a smart contract and leaves a trace in the Metamask wallet. All the input status of the Eth coin is displayed on the record page, which also can be viewed on Etherscan. This prevents fraudulent crowdfunding as the amount of ETH transferred from any party is recorded in the Etherscan, a feature provided by Metamask. Hence, crowdfunding organization's spending can be tracked and if the organization forges a fake spending receipt, it can be tracked down and deemed illegal. Figure 9 shows the particular transactional activities that happened within a Metamask wallet address.

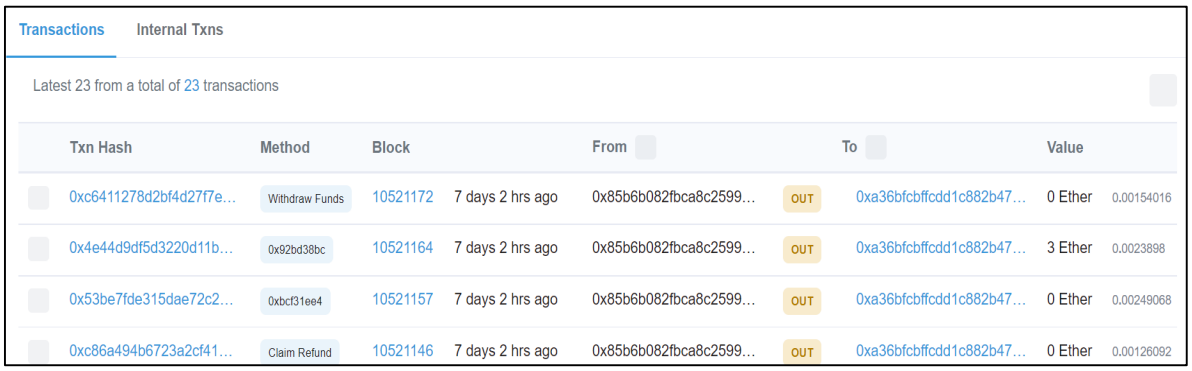

Figure 9: Auditing the Crowdfunding Funds on Etherscan

4.3 Testing

Once the application has been developed, a testing phase is commenced to examine the functionality of the application. Testing was conducted to identify any sorts of error that comes arise when using the FundDapp web application. Another purpose of testing is to find out whether the application able to achieve their objective and scope specified. Table 3 shows the summary of the functional testing results.

Table 3: Test Case for Proposed System

No	Function Testing	Expected Result	Result
Login Function			
I	Users able to login to the system	Users able to login with right password and email	Pass
II	Users able to receive reactivate email	Reactivate email sent to registered email	Pass
III	Users able to reset password	Reset email sent to registered email	Pass
IV	Errors for invalid inputs	Error messages shown	Pass
Donate Function			
I	Users able to donate by typing in correct amount of value	Users able to donate with the right amount of value	Pass
II	Error messages for invalid fund inputs	Error messages for invalid amount	Pass
Claim Function			
I	Organizations are able to receive the fund after project has expired and fund needed has reached	Organizations able to receive fund	Pass
II	Transaction is stored in record	Transactional record is stored in database	Pass

5. Conclusion

The first objective has been achieved as this application provides point-to-point transfer from a donator to an organization without any central authority to facilitate the process of transactions. The next objective is also achieved as the Blockchain web application, FundDapp is developed as the result of this study. Lastly, the Blockchain web application is tested via user acceptance form and using the designed test plan which includes the functionalities tests and security tests.

The system contains some limitations such as the users need to install Metamask to use the transaction functions. Also, there is no search bar for users to search up a project. Users are also unable to edit the comment posted. Hence, there are some improvements to enhance the limitation stated. This application is suggested to design better UI/UX interface. A search bar should be introduced to search up projects easily. Also, the comment posted should be editable.

Acknowledgement

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia for its support and encouragement throughout the process of conducting this study.

References

[1] E. Kromidha, "A comparative analysis of online crowdfunding platforms in USA, Europe and Asia," 2015, Pp. 1–6, Doi: 10.1109/Echallenges.2015.7441070.

[2] I. Berenzhnoy, "Top 7 must have features of a crowdfunding website," 2018. Https://Justcoded.Com/Blog/Top-7-Must-Have-Features-Of-Crowdfunding-Website/.

[3] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," 2017, Doi: 10.1109/Bigdatacongress.2017.85.

[4] A. Lukman, J. Agajo, E. Adedokun, and Karngong Loveth, "Crypto hash algorithm-based blockchain technology for managing decentralized ledger database in oil and gas industry," 2019.

[5] J. Alois, "Crowdfunding site patreon gets hacked. Personal data accessed but no credit card info taken," 2015. Https://Www.Crowdfundinsider.Com/2015/10/75227-Crowdfunding-Site-Patreon-Gets-Hacked-Personal-Data-Accessed-But-No-Credit-Card-Info-Taken/.

[6] E&T, "Leading charities harness blockchain to prevent fraud," 2017. .

[7] Z. Ma, W. Huang, W. Bi, H. Gao, and Z. Wang, "A master-slave blockchain paradigm and application in digital rights management," China Commun., Vol. 15, No. August, Pp. 174–188, 2018.

[8] Vitalik Buterin, "A next generation of smart contract and decentralized application platform," P. 36, 2015.

[9] D. K. C. Lee, Handbook Of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. 2015.

[10] X. Yang, J. Liu, and X. Li, "Research and analysis of blockchain data," J. Phys. Conf. Ser., Vol. 1237, No. 2, P. 8, 2019, Doi: 10.1088/1742-6596/1237/2/022084.

[11] I. Patisson, "4 characteristics that set blockchain apart," 2017. Https://Www.Ibm.Com/Blogs/Cloud-Computing/2017/04/11/Characteristics-Blockchain/.

[12] M. Stevenson and J. Aitken, "Blockchain technology: implications for operations and supply chain management," Pp. 1–34, 2019, [Online]. Available: Http://Epubs.Surrey.Ac.Uk/850374/1/Manuscript-Text %281%29.Pdf.

[13] M. Pilkington, "Blockchain technology: principles and applications," P. 39, 2016, [Online]. Available: Https://Papers.Ssrn.Com/Sol3/Papers.Cfm?Abstract_Id=2662660#.

[14] W. Viriyasitavat and D. Hoonsopon, "Blockchain characteristics and consensus in modern business processes," J. Ind. Inf. Integr., Vol. 13, No. July 2018, Pp. 32–39, 2019, Doi: 10.1016/J.Jii.2018.07.004.

[15] D. Vujičić, D. Jagodić, and S. Randić, "Blockchain technology, bitcoin, and ethereum: a brief overview," 2018 17th Int. Symp. Infoteh-Jahorina, Infoteh 2018 - Proc., Vol. 2018-Janua, No. March, Pp. 1–6, 2018, Doi: 10.1109/Infoteh.2018.8345547.

[16] L. R. He, "E-cert Uthm using ethereum technology," 2020.

[17] P. Andrea, S. Ibba, G. Baralla, T. Roberto, and M. Michel, "A massive analysis of ethereum smart contracts. Empirical study and code metrics," P. 21, 2019.

[18] C. Cachin, "Architecture of the hyperledger blockchain fabric," P. 4, 2016.

[19] J. Earls and A. Nort, "Smart-contract value-transfer protocols on adistributed mobile application platform," P. 27, 2017.

[20] D. Chen and T. Yi, "Establishment and operation of college students entrepreneurship crowdfunding website based on the crowdfunding mode," P. 4, 2016.

[21] P. Chandra, A. Ranjan, L. R. Jaywardhan Sawale, G. Singh, and H. Wadki, "Funding community projects with smart contracts on blockchain," P. 4, 2017.