Journal of Engineering and Technological Advances (JETA)
https://jeta.segi.edu.my/index.php/segi
2021 Vol. 6 No. 2

E-DONATION BY CLOUD BASED ETHEREUM PUBLIC BLOCKCHAIN

Rakib, H. *, Rashid, A.M.A.

Faculty of Engineering, Built Environment and Information Technology, SEGi University, 47810 Petaling Jaya, Selangor, Malaysia.

*Corresponding Author: rakibpt2016@gmail.com TEL: +6016 5815400

Abstract: E-Donation cloud funding system is an indispensable part of the society. It is a feasible method to assist any donors in any part of the world. Donors require fully secured system where there all information will not be hacked by hackers. As Web 3.0 is the third generation of internet services that can make the system fully secured which is distributed decentralized and semantic. It means with the Artificial Intelligence (AI); it does not have a centralized control node. Public Blockchain- a decentralized, distributed ledger technology - is the implementation of Web 3.0 that technology will be used to develop this system which would be an open source. This paper will look into Ethereum Blockchain technology and recognize the fundamental support it provides for Web 3.0 framework.

Keywords: E-donation; Web 3.0; Public Blockchain; Distributed decentralized; Semantic; Cryptocurrency; Security; Ethereum.

1. Introduction

E-donation is a new way of social assistance which has a great impact to decline discrimination between rich and poor. An increasing number of individuals are able to get humanitarian assistance because of this new channel of assistance. An irony of fate that, this emerging system shows downward trend to achieve donor’s satisfaction (Li, 2017). Under the outbreak of many disasters - Covid-19 pandemic, drought, flood, global warming and so on, the information of E-donation is asymmetric. With the purpose of preventing this situation, the goal of the research is to study the use of E-Donation service system, where system is guaranteed by the Ethereum Public Block chain-based technology.

2. Background

Public welfare crisis over the world has a long history, and there are frequent events involved in E-donation that are not enough to tackle the world biggest issues. Promoting public participation in E-Donation has become an urgent social problem for many reasons. Fundraising for the help seekers has a long history in the world. For example, in 1938, the March of Dimes Foundation was established to improve the health of mothers and babies as a charity firm where anyone could donate by following traditional way (Liu et al., 2017).

Like this E-donation platform and at the early stage of E-donation system till now, there are some lacking available which could not create satisfaction in donor's mentality for fundraising. When donors think about cloud funding, "trust" is the biggest issues among them. Their trustworthiness could be broken for the insecure E-Donation site where they may concern about their personal data, choosing right platform to donate (Floship, 2016).

In previous, E-donation sites were developed depending on Web 2.0 Technology (Rajamohan & Sajib, 2019) which databases were owned by any charity organisation, government or private associations which are hackable as it depends on web servers, and hackers could hack the system and steal money from the system that create a negative impact on not only donors but also authorities (Floship, 2016).

In addition, most previous and running system could take a long time for processing as donors and destitute people could not contact directly where donors and in need person cooperate with third party to send and receive donation. In this period, third parties cut huge amount of money from the donation as their platform fees which figures depend on platform basis.

Fundly is an E-Donation site who charges a straightforward 4.9% platform fee, with payment processing fees of 3% per transaction. Other platforms like Donorbox, Snowball Fundraising, Qgiv, Razoo, @pay, Network for goods donate now, PayPal Donation. FirstGiving charges a certain amount of money as their platform fees which would be totally cut in the proposed system where donors and needy person or group of people could contact directly (Small, 2017).

Moreover, many E-donation platforms do not show contributors list which is also another negative effect for increasing fund. If there is a donors list, others could get inspiration to donate (Killoran, 2021). After encountering all the issues with E-Donation site, where this helping site suffer a lot to adopt with the users and failure to achieve actual output.

3. Literature Review

3.1 Blockchain Technology

Blockchain, which is the foundation of Bitcoin (Nakamoto, 2008) is a decentralized, non-tamper able, anonymous, and traceable technology with enormous potential for revolutionizing established businesses (Zheng et al., 2017). A distributed database system with numerous independent nodes is known as a Blockchain.

The database is kept up to date by nodes all around the network. All transaction information can be recorded on the Blockchain, which has an efficient and transparent method and extremely secure data (Hu & Li, 2020).

A Blockchain is made up of a sequence of blocks, each of which has a block header and a block body. The block header includes metadata, and the block body contains the transaction data. The header (Hu & Li, 2020) contains the previous block's hash value (PrevBlockHash), timestamp (Timestamp), random number (Nonce), and Merkle Root. In the structure of a Merkle Tree, the block body stores numerous transactions from the preceding block. The hash value of the transaction information is stored in the Merkle Tree's leaf node, while the hash value of all the leaf nodes below it is stored in the non-leaf node.

The Blockchain system is based on a peer-to-peer network and does not require credit endorsement from a centralized body. Following the transaction, a consensus process allows each node to compete for accounting rights. The winning node will package all transactions that occurred within a specified time frame. The block will be broadcast to the whole network and will be verified by all nodes.

The block will be added to the chain after the majority of nodes have properly authenticated. One transaction is open and transparent from start to finish, and there is no way for nodes to deceive each other. Anonymous transactions are possible thanks to asymmetric encryption, and transaction traceability is ensured thanks to the chain structure. The Blockchain's structure is depicted in **Figure 1**.

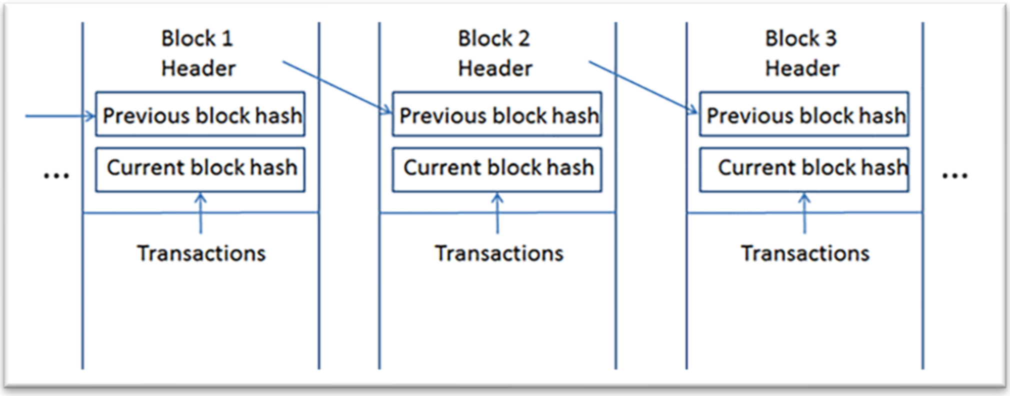

Figure 1. Blockchain technology (Pan et al., 2018)

3.2 Public Blockchain

The technology of Blockchain is divided into public and private where the main difference between both is related to who get the access in this network, execute the consensus protocol, and maintain the shared ledger (Jayachandran, 2017).

A public Blockchain is an open-source network where anybody could join and participate. This network has an incentivizing mechanism to inspire more users to join the network. For instance, Bitcoin and Ethereum are the largest public Blockchain networks in production today. Substantial amount of computational power is necessary to manage a distributed ledger at a large scale which is one of the drawbacks of a public Blockchain (Kim & Kang, 2018).

3.3 Ethereum

Ethereum is an open-source Blockchain framework that allows anyone to use it. This platform has a high degree of protection against various types of attacks. On the Ethereum Blockchain, users could create and deploy smart contracts as well as develop decentralized applications. The network is operated by peers who run Ethereum nodes and is not owned or managed by a single entity.

3.4 Ethereum Virtual Machine (EVM)

The Ethereum Virtual Machine (EVM) is the Ethereum smart contract runtime environment. The EVM is run by the Ethereum network's nodes. The EVM acts as a sandbox, allowing for a separate execution environment. Since all nodes in the Blockchain network perform the same computations, smart contracts could be executed with redundancy. Although this level of redundancy is inefficient in terms of execution, it is essential to preserve network consensus in the absence of a centralized authority or a trusted third-party (Bahga & Madisetti, 2016).

3.5 Smart Contract

A smart contract is a piece of code that lives on the Blockchain and has its own address. A smart contract is made up of a series of functions that could be executed and state variables that could be modified. When transactions are made to these functions, the functions are executed. The transactions contain input parameters that the contract's functions require. The state variables in the contract shift when a function is executed, depending on the logic applied in the function. Contracts could be written in a number of high-level programming languages such as Solidity or Python (Bahga & Madisetti, 2016).

Smart contracts are compiled into byte code using language-specific compilers (such as Solidity or Serpent). The contracts are then uploaded to the Blockchain network, where they are assigned unique addresses. By sending transactions to the contract, any user on the Blockchain network may activate the contract's functions. As part of the verification of new blocks, the contract code is executed on each node in the network. **Figure 2** depicts the framework of a smart contract (Macrinici et al., 2018).

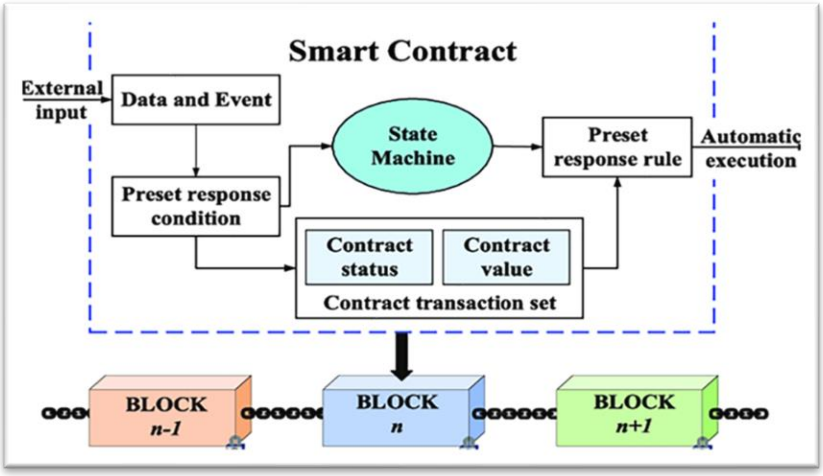

Figure 2. Smart contract (Chen & Zhang, 2019)

3.6 Transaction Process over Block Chain

Externally Owned Accounts (EOAs) send messages to other EOAs or contract accounts, which are known as transactions. The recipient's address, transaction data payload, and transaction value are all included in each transaction. The transaction value is passed to the receiver when a transaction is sent to an EOA.

The transaction data payload is used to provide input to the contract feature that would be performed when a transaction is sent to a contract account. The sender's private key is used to sign transactions. In the mining method, transactions are chosen and included in blocks. Only the transactions that are chosen for inclusion in the blocks alter the state of the network. Any of the network's participant nodes would read the transactions on a Blockchain network (Bahga & Madisetti, 2016b).

3.7 Cryptocurrency

Cryptocurrency refers to a system that employs cryptography to enable for the safe transfer and exchange of digital tokens in a distributed and decentralized manner. These tokens could be exchanged for fiat currencies at market rates. Bitcoin was the first cryptocurrency, and it began trading in January 2009 and Vitalik Buterin introduced the Ethereum platform to the public in 2013 (Whitepaper, 2021). Since then, a slew of new cryptocurrencies has emerged, each utilizing the same technologies as Bitcoin but tweaking some of the governing algorithms' unique parameters. Bitcoin's two main developments, which allowed cryptocurrencies, were solutions to two long-standing computer science problems: the double-spending problem and the Byzantine Generals Problem (Dourado & Brito, 2014).

3.8 KECCAK-256 (SHA-3) Hash Algorithm

The Ethereum platform relies on the Keccak256 hash algorithm (StackExchange, 2017). This algorithm allows the system more secure that would be hacked by hackers. The System would by design uses KECCAK-256 algorithm for hashing which is a modified SHA-3 256 algorithm. Keccak256 is a powerful and secure algorithm that is similar to Bitcoin's SHA256. The payment system and smart contract execution are both in the same layer, which gives Ethereum Classic its power. There will be no sidechains, trusted third parties, or merge mining. This gives developers access to programmable, sound money that is dependent on proof of work (Tsankov, 2019).

4. Analysing Similar Existing System

4.1 Donorbox

Donorbox is a popular donation site that uses cutting-edge technology to help charities boost donations. Their software is simple to set up and integrate into your organization's website. They assist charities in publicizing their fundraising activities and securing annual contributions from donors (Raj, 2020). It has some features which are totally against the proposed system. That features are given below:

- Donations can be made in more than 20 different currencies, including the US dollar, the British pound, the yen, the Australian dollar, and the Canadian dollar.
- Donorbox charges a 1.5 percent platform fee for the month's donations.
- 0.8 percent and $0.30 per transaction for ACH bank transfers (capped at $5 per transaction).

4.2 Fundly

Some features are given below:

- All contributions were subject to a 4.9 percent fee on this website.
- There is a 2.9 percent plus $0.30 per transaction credit card processing fee.
- Fundly's platform fee is higher than that of many of its rivals.

4.3 Snowball Fundraising

Snowball Fundraising is a great option for small non-profits on a tight budget. Non-profits could set up online donation sites using text giving and peer-to-peer giving(Raj, 2020).

Some features are available mentioned below:

- The Essential kit is the most affordable and does not require any upfront cost. A 2.9 percent fee plus $0.30 per transaction applies to all donations.
- The Premium bundle includes text giving, event and ticketing software, and fundraiser thermometers. The cost is $549 a year. A 2.2 percent fee plus $0.30 per transaction is added to all donations.

5. Conclusion

Blockchain is an evolving technology which will play an outstanding impact in every sectors. The standards are evolving to be a fully secure platform. While many tools and technology used in this secured software development process are still in their infancy and as time goes on, those tools would become more powerful and will make decentralized framework at most secured.

Ethereum Blockchain system would not be owned by any organizations, government or individual. This is to ensure personal information cannot be used for corporation gains. As web 3.0 is the nature of distributed decentralized and semantic, it could be controlled or censored by institution, or third party or individuals. The ongoing need for a cryptographic protocol that allows for global scale, decentralization, security, and fairness in the distribution of donations should be explored more with the use of Ethereum Blockchain technology.

Acknowledgement

We are grateful for the assistance from the referees in the evaluation of this paper submitted for publication. We would like to thank our colleagues, friends and family for continuously supported us with our passion in searching for new knowledge and exploring the world of block chain technology.

References

Bahga, A., and Madisetti, V. K. (2016). Blockchain platform for industrial Internet of Things. *Journal of Software Engineering and Applications*, 9 (10), pp. 533-546.

Chen, X., & Zhang, X. (2019). Secure electricity trading and incentive contract model for electric vehicle based on energy blockchain. *IEEE Access*, *7*, 178763-178778.

Dourado, E., and Brito, J. (2014). Cryptocurrency: The New Palgrave Dictionary of Economics, Online Edition.

Ethereum Whitepaper. (2021). *Ethereum Whitepaper, Use Ethereum*. https://ethereum.org/en/whitepaper/

Floship. (2016). *Problems With Crowdfunding: 7 Hazards to Watch Out For*. https://www.floship.com/7-potential-problems-with-crowdfunding/

Hu, B., and Li, H. (2020). Research on charity system based on blockchain. *IOP Conference Series: Materials Science and Engineering*, 768 (7). IOP Publishing.

Jayachandran, P. (2017). The difference between public and private blockchain. *Blockchain Unleashed: IBM Blockchain Blog*. https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/

Killoran, J. (2021). *Donation page mishaps: 4 common problems and solutions.* https://www.araize.com/donation-page-mishaps-4-common-problems-and-solutions/

Kim, N., and Kang, J. (2018). A case study for public blockchain and cryptocurrency technology focus on authentication system. *Journal of Engineering and Applied Sciences, 13*, 686-690.

Li, Q. (2017). Research on impact factors for online donation behaviour of bank customer. *The Journal of Finance and Data Science, 3*(1–4), pp. 13-19.

Liu, L., Suh, A., and Wagner, C. (2017). Donation behaviour in online micro charities: An investigation of charitable crowdfunding projects. In *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Macrinici, D., Cartofeanu, C., and Gao, S. (2018). Smart contract applications within blockchain technology: A systematic mapping study. *Telematics and Informatics, 35*(8), pp. 2337-2354.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*. https://bitcoin.org/bitcoin.pdf?

Pan, J., Liu, Y., Wang, J., and Hester, A. (2018). Key enabling technologies for secure and scalable future fog-IoT architecture: A survey. *https://arxiv.org/abs/1806.06188*

Raj. (2020). *Top 10 donation software that help nonprofits – Online donation tools*. https://donorbox.org/nonprofit-blog/top-donation-software/

Rajamohan, P., and Sajib, K. J. (2019). A neighbourhood centric approach to social networking based on WEB 3.0 technology. *Test Engineering & Management*, 81, pp. 1850-1857.

Small, N. (2017). 7 online donation tools to delight your donors. https://nonprofithub.org/nonprofit-technology/5-online-donation-tools-to-delight-your-donors/

StackExchange. (2017). How does the Keccak256 hash function work? https://ethereum.stackexchange.com/questions/11572/how-does-the-keccak256-hash-function-work

Tsankov, A. (2019). ECIP-1049: Why ethereum classic should adopt Keccak256 for its proof of work algorithm. https://antsankov.medium.com/ecip-1049-why-ethereum-classic-should-adopt-keccak256-for-its-proof-of-work-algorithm-e45aee32d8a9

Wu, H., & Zhu, X. (2020). Developing a reliable service system of charity donation during the covid-19 outbreak. *IEEE Access*, 8, pp. 154848-154860..

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557-564.