International Conference on Recent Innovations in Science, Engineering & Management
R.R. INSTITUTE OF TECHNOLOGY, Bengaluru (India)
10th - 11th May 2019 www.conferenceworld.in ISBN : 978-93-87793-87-3

Decentralized Distress Relief Using Blockchain

Adithi Hande T[1], Apoorva V[2], Nikhil Meduri[3], Kumar K[4]

[1,2,3]*Student, Computer Science and Engineering,*
K.S. Institute of Technology, Bengaluru, India
[4]*Assistant Professor, Computer Science and Engineering,*
K.S. Institute of Technology, Bengaluru, India

Abstract

A universally applicable disaster relief system is difficult to implement, as different kinds of response and aid might be required for different disasters. Introducing blockchain into traditional payment methods can offer a more secure and streamlined means of fund transfer. This could prevent fraudulent activity by making the details of all transactions available on a public ledger. The blockchain can contain verified transactions and make it immutable. Smart contracts can provide a medium for non-monetary donations by managing supply and demand. Implementing such a system would offer decentralized control as no single entity owns it. This allows any individual to be a node in the network and does not require a lot of resources for maintenance. Such a platform would be easily accessible by first responders and volunteers all over the world and not limit disaster relief to a particular area or government agency.

Keywords- *blockchain, decentralized, distress relief, funding, ledger*

1. Introduction

Blockchain gained popularity with the advent of bitcoin. This has opened up new avenues for a multitude of other use cases for blockchain technology. In the event of a disaster, it is important to have the provision of a distributed means of providing relief to the affected parties. By nature, blockchain does not require an intermediary to facilitate the transferring of data or other transactions, hence providing a seamless platform between the distressed party and the individual or organization assisting them. In a traditional scenario, the intermediate authority would be responsible for any kind of security breach or failures that may occur during a financial transaction. Blockchain replaces the need for a central authority with a public distributed ledger which does not allow any party to corrupt the transaction data on it. This ledger is shared among all the participating nodes within the network [1]. Such a system can reduce fraudulent operations by increasing transparency and user accountability. This would also be more resilient to failures as it is not dependent on a single server or node to operate.

2. Literature Review

Blockchain technology is often believed to be the de facto medium forillegal transactions. Blockchain is being viewed in a different light as more and more socially beneficial applications and concepts are realized. Kewell et al. have discussed several applications and use cases of blockchain for achieving targets for global sustainability. Blockchain can be used to address several requirements in a sustainable ecosystem by gaining an ethical understanding of how technologies work [2].

Using the Blockchain for monetary aid certainly has many benefits. Jayasinghe et al. Have enumerated a few of them, such as, the auditability and transparency of financial trails, low international transaction fees, speed of transactions and the ability to bypass banking systems in war zones. This model allows the donor to query whether the donated funds are being used. It illustrates how blockchain token donations can be performed over SMS in an offline mode [3].

The use of a distributed file system such as IPFS may enhance the applications of smart contracts in a blockchain network. This can also allow nodes to share intelligence and make informed decisions. IPFS has file sharing capabilities similar to BitTorrent and this might be able to bring in new insights for artificial intelligence use cases in blockchain [4].

Nor et al. have proposed a system for crowd funding for disaster aid as well as have compared the various attributes of commonly used blockchain platforms. This highlights issues in traditional systems such as, a middle man regulating and administering funds may be able to commit fraud. This is attributed to the lack of transparency and accountability in such a system and how blockchain can overcome these issues [5].

3. Methodology

Blockchain allows two or more entities to perform a transaction without having to establish trust between them. This is done by ensuring certain conditions are satisfied before a transaction is written into the blockchain. These conditions have to be agreed upon by all the nodes or participating entities in the network.

3.1 Analyze needs

To implement a decentralized distress relief system, the needs of the distressed party are to be known. This may be predicted by analyzing past data for similar disasters using simple machine learning algorithms or allowing an organization to explicitly specify the requirement. This can include both monetary and non-monetary funding. Non-monetary funds typically include items such as clothing, non-perishable food, clean drinking water and other necessities based on the kind of disaster. This can assist in speedy recovery to normal life for the residents of the affected area. Once the requirements are determined, the details should be made available across the system.

3.2 Transferring Tokens

The users of the system can use tokens as a means of fund transfer. To facilitate this, a standard currency to token conversion rate should be maintained in the system. This can enable simple global transactions by making equivalent token values for the corresponding currency value. The users can buy tokens which will be stored in

a wallet, which can be donated to their choice of a registered organization in the system. The organization can cash out the amount from their wallets as per requirement. Smart contracts can be used on blockchain networks which can enable the requirements to be automatically satisfied by managing supply and demand. This facilitates the use of reliable contracts that can be verified [5]. When users pledge a donation to an organization, it can be recorded and confirmed by the organization when the physical donation takes place. The use of smart contracts, coupled with an inventory management system, can be a useful tool in efficiently managing items in different locations. A user can initiate a transaction and the necessary number of tokens are sent over the system. A new block is created for each transaction which contains the data for the transaction block with the hash value of the previous block in the chain. The transaction block is open for scrutiny by all nodes in the network and if found satisfactory, it is added to the blockchain. This quality of blockchain makes it extremely difficult for an attacker to modify or tamper with transactions that have been already performed, as they would have to calculate and change the hash values of all the blocks until they can change the value of the intended block. This would require a very large amount of computing power and resources to attain. This can prevent fraud by allowing only legitimate and verified transactions on the blockchain along with writing data to a publicly accessible ledger to increase transparency.

3.3 Sharing Data

The data should be shared with all the nodes participating in the network. For this purpose, InterPlanetary File System (IPFS) is used. IPFS is a protocol that allows data to be stored as a distributed file system in a peer-to-peer network, which connects all the devices with the same file system. This overcomes the data size limitation of blockchain by storing a collection of hashed files on each node of the network. A client can access this data through an abstraction layer by fetching files available in a certain node by combing through all the nodes. The transfer of hash values through the network can be secured by asymmetric encryption.

3.4 Handling Requests

A request handler can be set up to manage any kind of transaction requests, be it fund transfers, managing smart contracts or deploying smart contracts. This should monitor the requests sent to the system to perform a suitable action that can output its result. The handler can determine a suitable action for a transaction such as writing to a database, retrieve private keys, etc. The request manager should be able to read requests, handle new requests, monitor and write transactions to a secure location, manage different keys required for operations, etc. Request operation flow with a request manager is illustrated in Fig. 1.

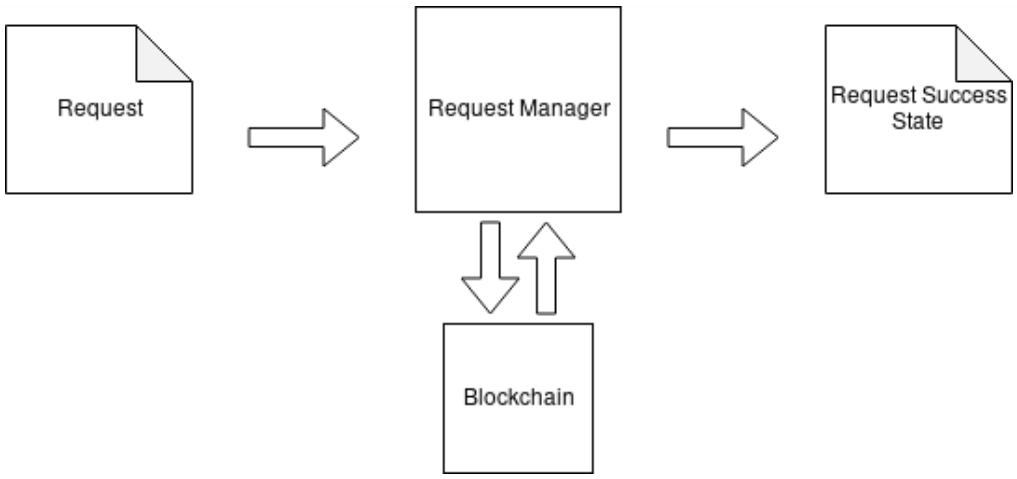

Fig. 1. Request manager design

4. Implementation

A decentralized distress relief system can be implemented using technologies such as Ethereum and BigchainDB. A user should be provided with the facilities to transfer ERC20 tokens or ethers from one wallet to another. Such a system will increase accountability for the users sending or accepting donations as a ledger records every transaction being made. The cryptographic addresses of each wallet can be publicly displayed on the platform for the donors to verify whom they are donating to. When a successful transaction is made, the details are saved in the blockchain database such as BigchainDB. In a decentralized blockchain network, as each node is owned by a different entity, there is no single point of failure for the network. This concept can be extended to a larger area, possibly globally scaling the system to welcome relief operations from all over the world. Other use cases such as startup funding, trading, etc. can be implemented using this system design. Having a diverse set of nodes can be beneficial to the network. However, if necessary, the system can be implemented within an area or an organization using a private blockchain. Since data is replicated over all nodes, it becomes quite impossible for an attacker to modify records in a large network as all the nodes have to be modified. To ensure the integrity of data, an external monitor such as a trusted third party such as a government agency or, in the case of distress relief donations, the general public can audit or scrutinize all the transaction data to find any irregularities.

Users can be incentivized to use the system by implementing reward systems where individuals receive monetary compensation for their effort. This could influence the choices people make and encourage more people to donate for a cause. In Ethereum, the Proof of Work (PoW) consensus rewards miners with tokens. Mining is defined as the process where complex mathematical equations which require a lot of computing power have to be solved to ensure the validity of the transactions. This incentivizes users to offer computing power in the decentralized network in exchange for rewards. The Proof of Stake (PoS) consensus allows the nodes with the highest stake (i.e, money) higher authority to establish the validity of the transactions. This is

based on the idea that, if a node has a higher value in the network, faulty transactions would result in a higher loss to this node than the other nodes.

Decentralizing a distress relief system can provide a unified platform to reach out for aid all over the world. Organizations can specify their needs, and the donors can choose which organization they want to donate to. Monetary donations and other resources can be handled in a similar manner. Users will be able to view how the donations are being utilized, offering transparency and satisfaction. An overview of the operations of the proposed distress relief system is shown in Fig. 2.

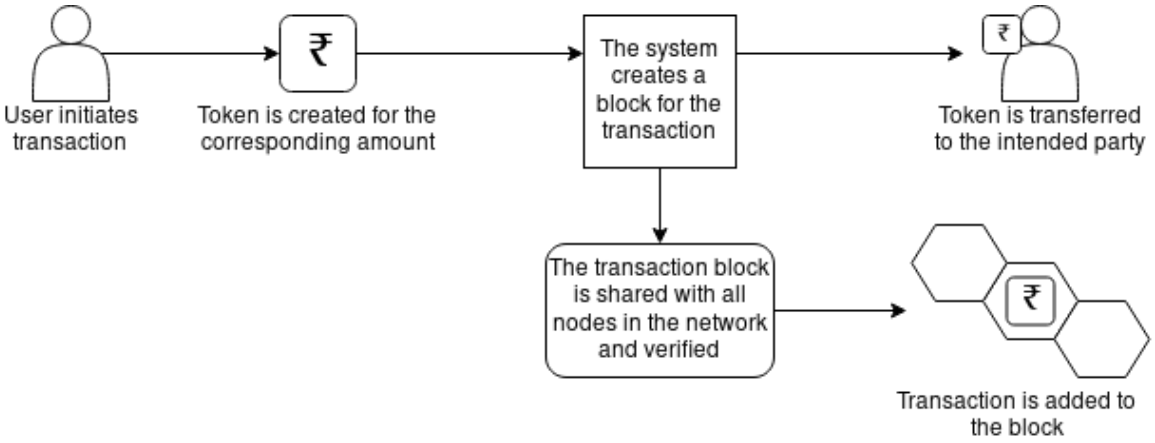

Fig. 2. Overview of the system

Only the verified legitimate transaction data will create a block, which also contains the hash value of the block before it. If any transaction is erroneous or could not be completed, it will not be linked to the blockchain. This can be a faster and safer method for fund transfer as it also protects the identity of the user, preventing possible identity theft. Providing a blockchain based system for distress relief donations is key to provide anonymity for the donor if they do not want to disclose their identity. Hence, this improves the integrity of the system.

5. Conclusion

Blockchain based payment systems can prove to be advantageous over traditional payment systems in several ways. A central authority is unnecessaryfor verification and validation of transactions as everynode is held accountable for their actions. The users can be suitably compensated. A high budget need not be set to employ special security precautions as data is automatically protected from tampering as soon as it is in the blockchain. Implementation is cheaper as there are no intermediate parties requiring commission or operational and maintenance fees to provide services. Tokens can be cashed out without delay whenever it is required, thus providing a faster alternative for global transactions. Strong peer-to-peer infrastructure not relying on any central node drastically improves transaction speed and recovery from any failure. Hence, blockchain can prove to be a useful technology to provide community based applications.

REFERENCES

[1]Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The Blockchain as a Decentralized Security Framework [Future Directions]. IEEE Consumer Electronics Magazine, 7(2), 18–21.

[2] Kewell, B., Adams, R., & Parry, G. (2017). Blockchain for good?. Strategic Change, 26(5), 429-437.

[3] Jayasinghe, D., Cobourne, S., Markantonakis, K., Akram, R. N., & Mayes, K. (2017, September). Philanthropy on the blockchain. IFIP International Conference on Information Security Theory and Practice (pp. 25-38). Springer, Cham.

[4] Swan, M. (2015, March). Blockchain thinking: The brain as a dac (decentralized autonomous organization). In Texas Bitcoin Conference (pp. 27-29). Chicago.

[5] Nor, R. M., Rahman, M. H., Rahman, T., & Abdullah, A. (2017). Blockchain Sadaqa Mechanism For Disaster Aid Crowd Funding. In Proceedings of the 6 th International Conference on Computing and Informatics (pp. 400-405).

[6] Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. J. (2015). Blockchain contract: A complete consensus using blockchain. 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE).