Study of Blockchain with Bitcoin based Fund Raise Use case using Laravel Framework

Aparna Ramalingaiah and Thaniya Sulthana
Department of CSE, Ramaiah Institute of Technology,
Bangalore, India
Email: aparna@msrit.edu, thaniyasulthana999@gmail.com

***Abstract*—Blockchain is a deliberately spreading set of data called as Blocks, which are associated and assured by the use of Cryptography. Each Block of this Blockchain consists of cryptographic hash of the preceding block, a timestamp and transaction information. Modification of Data by fraudsters is highly challenging in Blockchain by its design. It is an accessible shared register that can store activities between two internet users securely. Such a technology is an easy way for one person using internet to send fragment of digital property to other person who is also using internet, such that transfer of data or communication will be very secure and none of the sensitive details would be leaked. With the usage of Blockchain technology, several people can write the data into the Record and also sector of users can manage how the Record should be added with new entries. This technology is now being employed in a variety of applications like digital currency, supply chain management, medical information systems etc. In this paper, we have studied the technology behind Blockchain and the application of the same in several use cases. We have also implemented fund raise use case using Laravel PHP Framework to illustrate the steps of using Blockchain to assure secure transactions**

Keywords—Blockchain, Distributed ledger, cryptographic hash

I. INTRODUCTION

Blockchain technology involves a chain of blocks which contain information of interest. Most important problem that was solved using Blockchain was to remove the requirement of a trusted third party for doing any secure transaction and hence it is decentralized in nature. To elaborate, this technology aids in recording transactional data very efficiently and in a trusted way. A distributed ledger is maintained to record these vast transactional data over a secure peer-to-peer network. This kind of a shared form of record-keeping eliminates delays of third-party verification for transactions – and produces a complete, auditable and indisputable system of record that each authorized member of the network can access. Each block contains data, Hash value of the block and hash of previous block. Data that is stored inside the block depends on type of Blockchain. Blocks will also have hash value which is always unique. Once the block is created, its hash is also created. Changing something inside a block causes its hash value that is stored in the next block to change and hence becomes invalid. Because of this, Blockchain is secured. Storage of Hash of previous block in its next neighboring block effectively creates a chain of blocks.

For instance, consider a chain of 3 blocks. Each block has hash of its own and hash of the previous block. First block is called as Genesis block. Suppose consider that the data is tampered in the second block. Hence hash value of this block changes and in turn that will make immediate next block and all following blocks to be invalid. Because it no longer stores the valid value of previous block. So, changing a single block makes all following blocks to become invalid. [7]

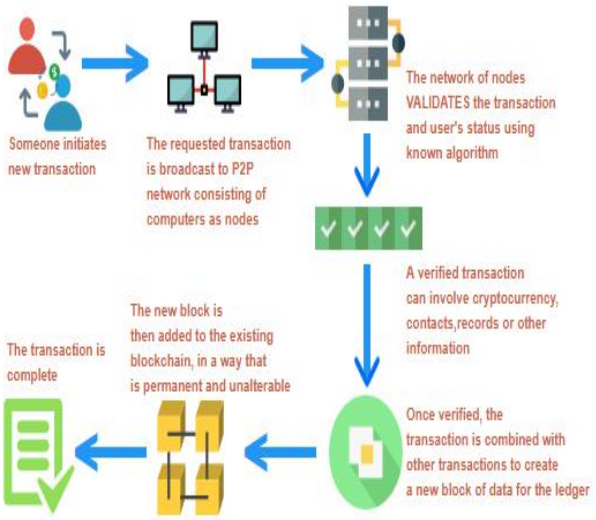

Figure 1. Overview of Blockchain technology

Figure 1 gives an overview of the steps involved in Blockchain technology. When a user initiates a transaction in a peer to peer network, the user's status and the transaction is validated by his peers by using known Blockchain validation protocols. Once the transaction is verified, it is combined with other transactions to create a new block and added to the existing Blockchain. This marks the end of transaction.

As per the literature, blockchain networks are available in three varieties based on the way they are governed - public blockchains, private blockchains and consortium blockchains.[8]

Public blockchains pose no access restrictions. Anyone with an internet connection can send transactions, provided that these validators possess some internal or external resources as their security deposit. A single validator cannot take the complete control of recording network's history unless a consensus is exhibited by all the nodes in the network.[8] These blockchains assure security by using some type of a Proof of Stake or Proof of Work algorithm and these networks offer economic incentives for those who secure them. Examples of such practically implemented public blockchains available today are Bitcoin and Ethereum.

Private blockchains are maintained by network administrators. Participants and validators can join the network only by receiving an invitation from the administrators. Such private blockchains could be used by companies for logging records and accounting purposes and who need a stricter level of access control when compared to public networks so that the risk of publishing company

ISBN: 978-1-5386-6078-2 © 2018 IEEE

specific sensitive data to the public can be entirely eliminated.

Consortium blockchains are also permissioned like a private Blockchain but instead of a single organization owning and controlling it, a number of companies operate as nodes on such a network. The administrators of a consortium chain grant access to a limited set of trusted nodes and restrict users' reading rights as they are applicable.

II. VARIOUS USE CASES OF BLOCKCHAIN TECHNOLOGY

A. *Protecting Medical data using Hash Blockchain technology [1]*

Most of the data or information is presented in the digital format these days. This digital image of data travels across the internet and between several Electronic Devices. Medical data is composed of sensitive and personal information specific to one's human body. In this case, it is very important to protect this personal data from modification or alteration by attackers and also from stealing of this Data. If any of these Personal Medical Data is altered, it will lead to wrong data presented to doctors for treatment which will end up to be a disaster to the concerned patient. Therefore, such data is very critical and sensitive and there arises a need to protect it in all ways. During the time, this data is transmitted over the Internet, it is prone to attack. To protect the data from the attackers and for authenticity of this data, Hash Blockchain technology is used.

B. *Authentication with Blockchain algorithm in Social Networking [2]*

Identification of the community is very significant for interpreting the Social network. Various procedures exist for identifying the community. One among them is to identify community by interpreting human hobbies and their personal properties. But these basic details are not enough to interpret the communities. So, we tend to utilize the details of user connections, user associations and their communications. These Social networks mimic the personal details to the outside world which is not safe. Once this information is retrieved by the other users who are not friends, they will make use of these data to pretend to be like other known users or attackers will get to know the interaction between the other two legitimate users in Social network. In order to protect these types of personal and crucial data about users and to avoid this risk, we should verify the identity of users in the procedure of developing Social networks. In this process public key cryptography is used. But this technology will fail in condition such as when other person pretends the identity and key matches and person cannot be identified which will lead to leak of personal data. So Blockchain Technology is utilized here to secure the identity of users and securing their particular keys to block the attackers and semi honest users from misusing sensitive personal information of users.

C. *Secure Storage of Agricultural products tracking details using Blockchain [3]*

Agricultural products go through the entire process of Planting, Processing and Transporting the products to finally sell them to the customers. It tends to serious food safety issues if it is falsified in any phase of the production to selling to customer. Internet of Technology has been a boon in tracking the entire process of planting to Sales of Agricultural products to guarantee that no food safety issue occurs. Once we get the complete details of entire process it should be stored securely. If we use the simple storage techniques to store these Agricultural products tracking details then attackers can easily modify the data and it will be very difficult to remove this modification made by attacker. To avoid all these kind of safety issues, we make use of Blockchain technology. To protect the data storage, a scheme is developed which is based on Blockchain technology for tracking the agricultural products. These products are tied with sensors, so that these sensors can get the data of Agricultural Products and store in the server. Here the server makes use of double-chain structure to automatically share the data in the Blockchain, at the same time, this system is able to request the required data and present it to the higher application. Hence we can make best use of Blockchain technology to store the Tracking details of Agricultural Products securely.

D. *Multi-Level Demand Response Mechanism using the Blockchain [6]*

Besides the development of the entire society, high consumption of electricity has also increased. To stabilize the demand and supply of electricity and decrease the economic cost of power system function, research on power systems at the user level is being carried out immensely since demand response plays a very important role in such scenarios. Demand response defines the number of power users with respect to the market price to react to change the usual usage level of electricity. The expense of developing a dedicated service transmission network is quite high. So, for deploying the Demand Response in the power communication network, a strong communication structure is required.

Creating a reliable structure between aggregator, Grids and users is very challenging. Blockchain technology is very much popular in building trust among strangers and it does not require reliable third party to verify. These benefits of Blockchain removes the complexity of centralized network and that is exactly what is required to solve this problem. i.e. Using the excellent characteristics of Blockchain, it is possible to protect the user's electricity usage details confidential and protect them from damage. The characteristics include *Decentralization:* The method of authentication, accessing, storage, maintenance and transfer of data are dependent on the reliable distributed system mechanism rather than centralized mechanism to develop reliability between other users; *Off Trust:* To join the whole process of data transaction, there is no requirement of trust because everything is visible to all users in that network; *Safe and trustworthy:* By hiding the data using cryptography, it becomes difficult for attackers to steal or tamper the data and hence data is safe. In this way, Blockchain technology is utilized to authenticate the users and give secure communication between aggregators, grids and users without employing an expensive and complex centralized network.

ISBN: 978-1-5386-6078-2 © 2018 IEEE

E. Skew Reduction in Reducer phase of MapReduce using Blockchain [5]

Big data is becoming very popular in this digital world. It mainly defines the huge amount of data stored and processed for the benefit of the users. In this current digital world, all the required data should be displayed to the user within few seconds as a real-time response. If the process takes more time to give required details to the user then the user will lose interest in the response. Users expect that the data has to be processed as fast as possible and results are displayed to the user in the blink of an eye. Processing Big data poses many challenges like different types of data, skewness, etc., The huge volumes of data that the Big data processes accept may be structured or unstructured. In such jobs, longest running task will decide the speed of the job. If a task inside the job takes longer duration to complete, then whole job will take longer to get executed. Skew in the data will occur when unequal amount of data is assigned to each task or unequal amount of effort to process the data is distributed amongst tasks. Skew gives much difficulty in processing the data. Various algorithms are designed to decrease the skew in the reducer phase but they are mainly specific to the application and not applicable to all. In MapReduce process, id is kept in the Master table, so time is displayed with the functional feature of the product at the search time as these ids are present in the master table. In Blockchain technology, ids of the particular items are stored on the Master or the slave data. If the id is found in the master then path of that id is kept in the master storage. If the id is not found in the master storage then id is searched in the slaves storage one by one. If the id is found in any of the slave, then that path is also stored in the master storage for faster access in the future. So, Blockchain method can be used effectively to reduce the skew in data is much efficient and faster than MapReduce method.

F. Blockchain technology in Bitcoin [4]

Bitcoin is the Digital coin which was invented by Satoshi Nakamoto in 2009 and the whole idea of Blockchain was his brain child. Blockchain technology enables moving digital assets from one individual to another individual. Each block contains data, hash value of the block and hash of previous block. Bitcoin Blockchain stores details about Transaction such as From details, To Details and Amount of transaction that happened between the two parties. Every block has its unique hash value. Once a block has been created, its hash value is also created. Changing the value of the block will internally causes hash value to be changed. Hash of previous block effectively creates chain of blocks. In Bitcoin, it takes 10 minutes to create a new block. Block will be sent to each and every person in the network so that all users are getting updated each time a transaction happens so it is transparent and secured.

III. BITCOIN BASED FUND RAISE USE CASE USING LARAVEL FRAMEWORK

The use case used for implementation demonstrates a proper FUND RAISE Example. Platform used for implementation is Laravel PHP Framework and MySQL is the database used to store the data. Laravel is a free, open-source PHP web framework used for the development of web applications that follows the model view controller (MVC) architectural pattern. Some of the highlighting features of Laravel Framework are built-in support for authentication, localization, models, views, sessions, routing mechanism.

Fund Raise example shows the recent transactions and where the money came from and the recipient who received the money. A Graph is designed to depict the Highest Transaction of a particular user. Assume Alex (Fund Raise Company) will be the user used in the implementation. New users have to register with the application. Registered users can then login with their credentials and view a dashboard that shows several components like Bitcoin Exchange, Total amount received, Highest transactions, Tables of address of Bitcoin Senders and Received. A pie chart depicting the highest transactions made by the user. Some of the snapshots of the implementation that explains the flow of logic are shown next.

Figure 2 shows two options for the user to Login and Register(in case of new users). New user registers as shown in Figure 3 whereas the existing users login as shown in Figure 4.

Figure 2. Welcome Page

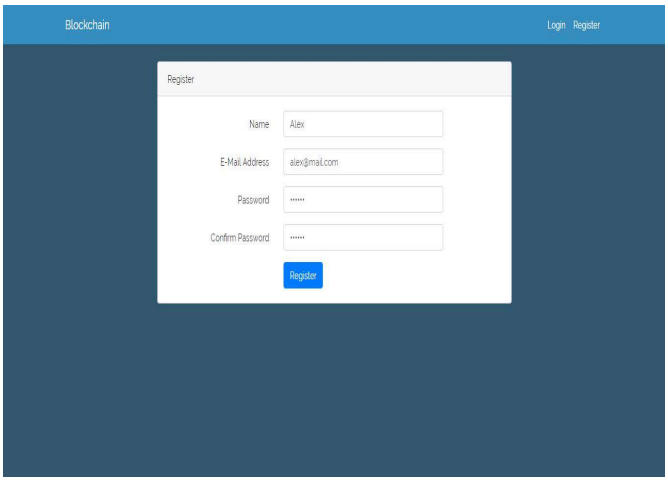

Figure 3. New User Registration

Successful login displays the Dashboard of Bitcoin, which consists of several components as shown Figure 5. Dashboard has the following components such as Bitcoin Exchange, Total amount received, Highest transactions, Tables of address of Bitcoin Senders and Received.

ISBN: 978-1-5386-6078-2 © 2018 IEEE

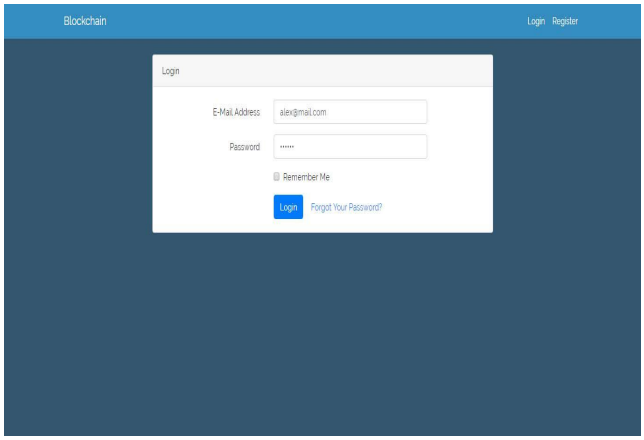

Figure 4. Existing User Registration

Successful login displays the Dashboard of Bitcoin, which consists of several components as shown Figure 5. Dashboard has the following components such as Bitcoin Exchange, Total amount received, Highest transactions, Tables of addresses of Bitcoin Senders and Received.

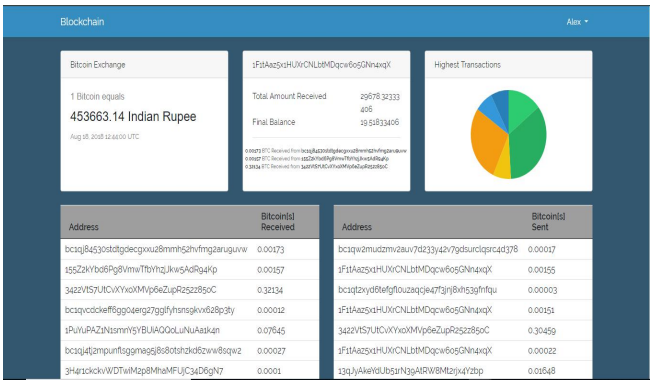

Figure 5. Components of Bitcoin Dashboard

Bitcoin Exchange, in this example uses satoshi unit normally and it is converted to INR. The satoshi is the smallest unit of the Bitcoin crypto currency. It is named after Satoshi Nakamoto. Global time is also displayed. Figure 6 shows the current Bitcoin Exchange rate in INR.

Figure 6. Bitcoin Exchange

Recent 3 received transactions are shown for Alex in Figure 7 along with total BTC, Total amount received in BTC which is 29678.32333 BTC(BTC-> Bitcoin). Final balance after receiving and sending BTC to other users. 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX is the Bitcoin address of the Alex, which is used for transaction (For Example: Bank Account Number).

1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX is hashed to hash160, which is a block 99bc78ba577a95a11f1a344d4d2ae55f2f857b98. For each user there will be Bitcoin address and respective hash value. Once Alex receives or sends BTC to other user, new block will be created with hash value. The JSON_FORMAT of the Bitcoin gives us the full details of the Alex which will be shown in the further description.

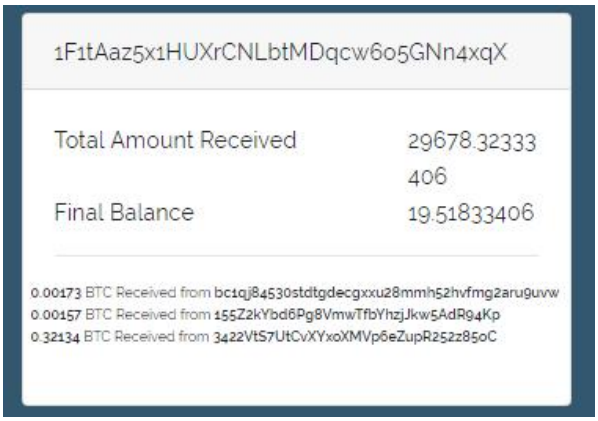

Figure 7. Recent 3 transactions received by Alex

Highest Transactions of a user with Bitcoin address 1AJbsFZ64pEfS5UAjAfcUG has given 36% of amount to the Alex as shown in Figure 8. Each color in the pie chart shows the address and percentage of amount given to Alex(Fund Raise).

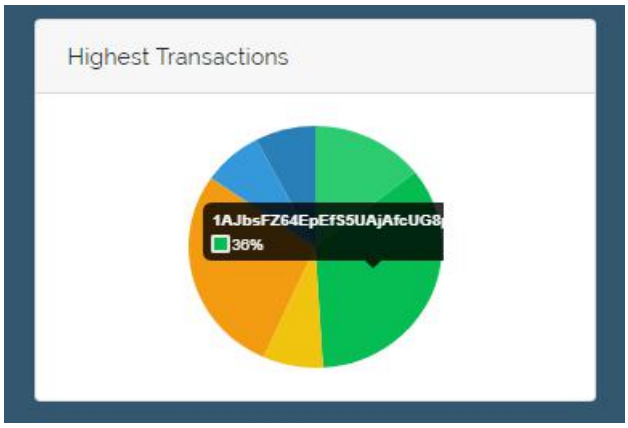

Figure 8. Pie chart - highest transaction by the particular user

Figure 9 shows table for address of the Bitcoin received by Alex.

For Example, Alex(Fund raise Company) has received 0.00173BTC from bc1qj84530stdtgdecgxxu28mmh52hvfmg2aru9uvw and so on.

Figure 10 shows the table of receivers to whom Alex has sent Bitcoin. For Example, Alex(Fund raise Company) has sent 0.00017 BTC to

bc1qw2mudzmv2auv7d233y42v79dsurclqsrc4d378 and so on.

ISBN: 978-1-5386-6078-2 © 2018 IEEE

IV. CONCLUSIONS

A decentralized, safe and trustworthy technology like Blockchain has several benefits of usage popularly called as 4Cs [9] namely Collaboration—enables interested parties to easily register themselves, organize and maintain transaction logging; Constraint—leverages "permissioned" designs that only allow verified participants to read, write or validate transactions; Consensus—utilizes agreement protocols for vetting, admitting and removing network members, and enforcing policies agreed upon by all members; Consistency—uses protocols to prevent temporary deviations or "forks" in Blockchain data that can lead expose participants to faulty or incorrect information. Hence, such a technology can be employed in various applications like supply chain auditing, governance, shared economy, File storage, smart contracts, crowd funding, Prediction markets, Protection of Intellectual property, Internet of Things etc.[7] We have surveyed different use cases where all these 4Cs are extensively applied. It gives the reader a wide perspective of the applications where Blockchain technology can be greatly employed.

Address	Bitcoin[s] Received
bc1qj84530stdtgdecgxxu28mmh52hvfmg2aruguvw	0.00173
155Z2kYbd6Pg8VmwTfbYhzJkw5AdRg4Kp	0.00157
3422VtS7UtCvXYxoXMVp6eZupR252z850C	0.32134
bc1qvcdckeff6gg04erg27gglfyhsnsgkvx628p3ty	0.00012
1PuYuPAZ1N1smnY5YBUiAQQoLuNuAa1k4n	0.07645
bc1qj4tj2mpunflsgg9mag5j8s80tshzkd6zww8sqw2	0.00027
3H4r1ckckvWDTwiM2p8MhaMFUjC34D6gN7	0.0001
3H4r1ckckvWDTwiM2p8MhaMFUjC34D6gN7	0.0001
3H4r1ckckvWDTwiM2p8MhaMFUjC34D6gN7	0.00013
32bm4LJsuQjjdMekWGTFsvaWspUxbdR4vu	0.00004

Figure 9. Bitcoin Received Table

Address	Bitcoin[s] Sent
bc1qw2mudzmv2auv7d233y42v7gdsurclqsrc4d378	0.00017
1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX	0.00155
bc1qt2xyd6tefgfl0uzaqcje47f3jnj8xh539fnfqu	0.00003
1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX	0.00151
3422VtS7UtCvXYxoXMVp6eZupR252z850C	0.30459
1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX	0.00022
13qJyAkeYdUb51rN39AtRW8Mt2rjx4Yzbp	0.01648
bc1qcvr2qnp4lwt53nzq95agl8a8gnssh0nqrv5vec	0.00001
1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX	0.0001
1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX	0.00218

Previous 1 2 3 4 5 ... 22 Next

Figure 10. Bitcoin Sent Table

REFERENCES

[1] D. S. Prathiwi, W. Astuti, Adiwijaya and T. A. B. Wirayuda, "Watermarking scheme for authenticity and integrity control of digital medical image using Reed-Muller Codes and Hash Block Chaining," *2015 3rd International Conference on Information and Communication Technology (ICoICT)*, Nusa Dua, 2015, pp. 23-29.

[2] R. Yu *et al*., "Authentication With Block-Chain Algorithm and Text Encryption Protocol in Calculation of Social Network," in *IEEE Access*, vol. 5, pp. 24944-24951, 2017.

[3] C. Xie, Y. Sun and H. Luo, "Secured Data Storage Scheme Based on Block Chain for Agricultural Products Tracking," *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*, Chengdu, 2017, pp. 45-50.

[4] Wikipedia: Blockchain. [Online] https://en.wikipedia.org/wiki/Blockchain

[5] M. Jenifer and B. Bharathi, "A method of reducing the skew in reducer phase — Block chain algorithm," *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, Nagercoil, 2016, pp. 1-4.

[6] G. Cui, K. Shi, Y. Qin, L. Liu, B. Qi and B. Li, "Application of block chain in multi-level demand response reliable mechanism," *2017 3rd International Conference on Information Management (ICIM)*, Chengdu, 2017, pp. 337-341. doi: 10.1109/INFOMAN.2017.7950404

[7] Blockgeeks [Online]: https://blockgeeks.com/guides/what-is-blockchain-technology

[8] [Online]: https://perfectial.com/blog/leveraging-private-blockchains-improve-efficiency-streamline-business-processes/

[9] Charles King, Pund-IT, Inc, Ensuring Secure Enterprise Blockchain Networks A look at IBM Blockchain and LinuxONE.

[10] Laravel documentation[Online]: https://laravel.com