iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** III **Month of publication:** March 2022

DOI: https://doi.org/10.22214/ijraset.2022.41021

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

Blockchain based Transparent and Genuine Charity Application

Omkar Sunil Naiknavare[1], Mr. Mandar Pravin Patil[2], Miss. Riya Chandrakant Chawate.[3], Miss. Amisha Bharat Borana[4], Prof. Sunil Sonawane Sir[5]
[1, 2, 3, 4]*Student,* [5]*HOD, Department of Information Technology, AISSMS's Polytechnic, Pune, Maharashtra, India*

Abstract: ***Non-governmental organizations (NGOs) in under-developed countries are receiving funds from donor agencies for various purposes, including relief from natural disasters and other emergencies, promoting education, women empowerment, economic development, and many more. Some donor agencies have lost their trust in NGOs in under-developed countries, as some NGOs have been involved in the misuse of funds. This is evident from irregularities in the records. For instance, in education funds, on some occasions, the same student has appeared in the records of multiple NGOs as a beneficiary, when in fact, a maximum of one NGO could be paying for a particular beneficiary. Therefore, the number of actual beneficiaries would be smaller than the number of claimed beneficiaries. This research proposes a blockchain-based solution to ensure trust between donor agencies from all over the world, and NGOs in under-developed countries. The list of National IDs along with other keys would be available publicly on a blockchain. The distributed software would ensure that the same set of keys are not entered twice in this blockchain, preventing the problem highlighted above. The details of the fund provided to the student would also be available on the blockchain and would be encrypted and digitally signed by the NGOs. In the case that a record inserted into this blockchain is discovered to be fake, this research provides a way to cancel that record. A cancellation record is inserted, only if it is digitally signed by the relevant donor agency.***

Keywords: blockchain; ensuring trust; NGOs; encryption.

I. INTRODUCTION

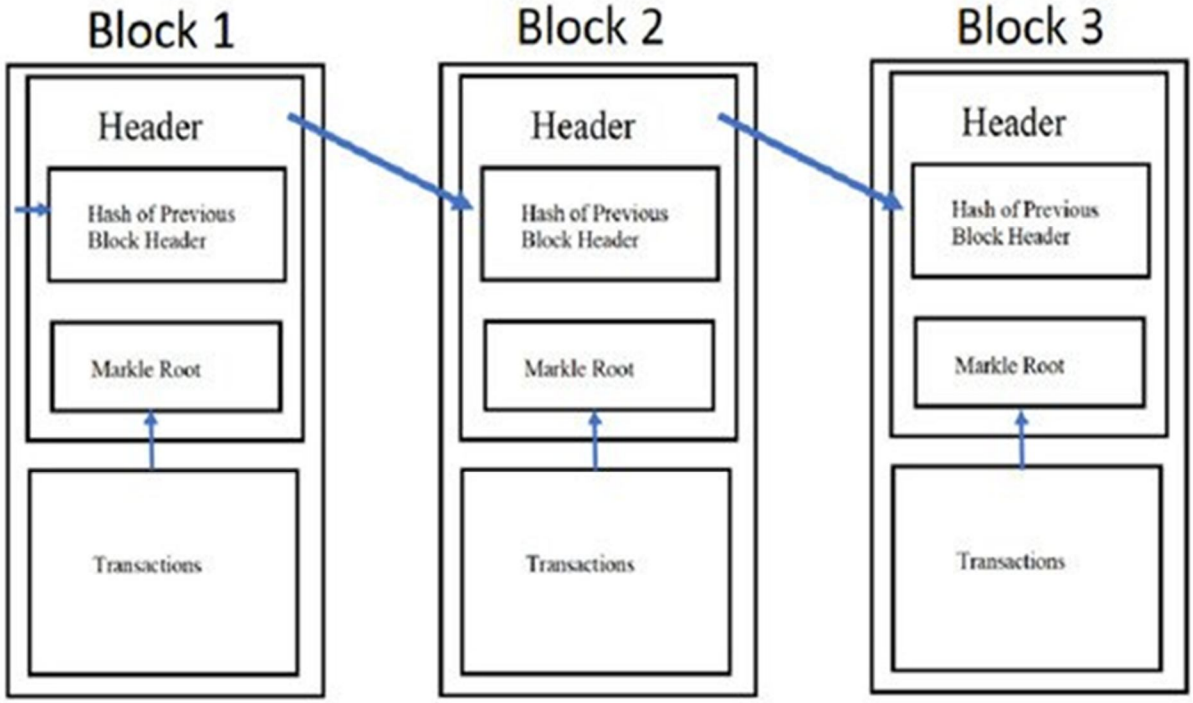
Blockchain is not a new technology. Digital signatures were introduced in 1991 to secure the integrity of the documents which are mostly considered the foundation of blockchain [1]. Satoshi Nakamoto proposed one of the important applications of blockchain by introducing Bitcoins in 2008 [2]. Within the last few years, after the exploration of the benefits of blockchain, governments and industries have been using it in various domains such as supply chain, identity management, recordkeeping [3], and education [4].

Blockchain is a decentralized technology that allows different stakeholders to access and replicate a database. The database can only be updated using predetermined rules, and once changed, it is shared with all parties. Each transaction in the blockchain is connected in a chain to make sure that everybody has the most up-to-date version of the ledger. On a blockchain network, a distributed ledger is a method for replicating and storing transactional data. The distributed ledger expands on this idea by replicating data across several nodes [5].

Blockchain removes the need for third-party providers to verify transactions because it is a peer-to-peer network that timestamps them. This type of recordkeeping is tamper-resistant as each peer has a copy of the complete ledger and new transactions can only be added with the consensus of the majority of peers or following the predetermined rules [3].

A typical blockchain consists of three parts: block, chain, and network. The block contains transactions that store information about some important activity, such as tracking goods or assets, sensitive medical information, or critical information generated by machines using IoT [6]. When a new blockchain network is formed then few rules are defined. These rules administer the working of the network and set the details, such as the size of the transaction in each block, the addition of transactions, etc. When the agreed number of transactions fills a block then that block is chained with the previous blocks using a hash value. A hash is a one-way algorithm that generates a fixed value that is unique for the transactions in that block, and the same hash can only be generated if the block contains the same transactions. The hash value would be different if a block of data is altered by someone during the transmission or modified by any peer. A different hash value shows that the data in the original block have been modified and data are not trustworthy anymore. Multiple hash values can be combined and hashed together to form a single hash or Merkle root. A Merkle tree is created by adding more hashes to the base. A simplified version of the blockchain is illustrated in Figure 1 below [3].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com



Blockchain platforms allow developers to develop blockchain applications. Many blockchain platforms with different features are available. The few common blockchain platforms are Bitcoin, Ethereum, Hyperledger, R3, Ripple, and Electro-Optical System (EOS) [7]. The selection of blockchain platform is highly dependent on various factors such as industry focus (financial services, digital asset management, cross-industry), ledger type (permissioned, permissionless), consensus algorithm (proof of work, pluggable framework, probabilistic voting, majority voting, chain-based Byzantine fault tolerant, Stellar consensus protocol), support of smart contracts and type of governance who managed the network. Bitcoin is the most famous blockchain platform. Bitcoin assumes that there is no trust between the parties, it facilitates a large number of decentralized nodes to ensure that the blockchain is not tampered with by cybercriminals. Miners, who are active users, manage the decentralized nodes. Miners are needed by cryptocurrency platforms to solve crypto puzzles as proof of work, which is then validated by other miners or nodes. Miners who solve and verify the puzzles are paid in cryptocurrency. Although miners are needed for cryptocurrency platforms, they are not required for other blockchain platforms [8].

Joe and Raafat [9] ranked the usage of blockchain in different domains based on recent peer-reviewed publications. The top ten areas of blockchain application based on their popularity in descending order are IoT, energy, health care, finance, resource management, government, exchange, transportation, BPM, and right management.

There is widespread consensus that education is critical for improving livelihoods and economic prosperity in developed countries [10]. Many developing countries are dependent on local and international donors due to scarcity of resources and other governance issues. Organizations, such as Association for Childhood Education International (ACEI), Education International, Save the Children, UNESCO, UNICEF, etc., work across continents and barriers to ensure that every child receives a high-quality education. Some donor agencies have lost their trust in the local NGOs in under-developed countries, as some NGOs have been involved in the misuse of funds.

This is evident from irregularities in the records. For instance, in education funds, on some occasions, the same student has appeared in the records of multiple NGOs as a beneficiary, when in fact, a maximum of one NGO could be paying for a particular beneficiary. Therefore, the number of actual beneficiaries would be smaller than the number of claimed beneficiaries as the same recipients are enjoying the benefits from the same/multiple NGO/s at the same time. This research proposes a blockchain-based solution to ensure that no beneficiary will receive the same benefit multiple times by the same NGO or by another NGO. The following sections provide a summary of the related work; the next section will explore research material and method of the proposed model; the next section discusses the structure and Maintenance of the Ledger, and finally paper concludes.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

II. LITERATURE SURVEY

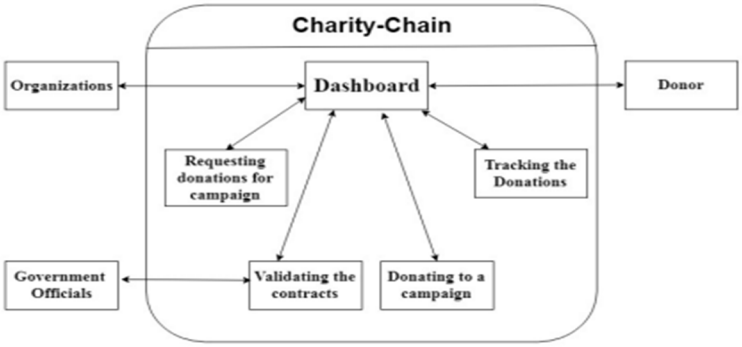
The blockchain provides a means to obtain a decentralized transaction ledger that can be used to generate, validate and send transactions to other nodes present in the same network. Various cryptographic hash functions of specific cryptocurrencies also increase the security that is needed during financial transactions. The blockchain can be applied to financial services, healthcare services and business and industry[1]. A charity application today needs a system that validates itself without depending on any other system or application. Blockchains are being used as they are not restricted to a particular system and because they can independently verify the integrity and consistency of transactions. Ethereum is chosen as a platform because it is a public platform and has better scalability. It can run 7-20 transactions per second[2]. Through blockchain, the charity system will no longer be monopolised and restricted to one authority. The public will have easy access to the transactions and can verify if their money is being used like they expected. A very good example of harnessing the power of blockchain is China government. It is the first to use blockchain for egovernment purposes. It helps to strengthen the trust between the producers, government and citizens. It is used for ensuring the quality of the perishable food. The application safely shares the status of the produce at each stage. The stages include manufacturing, transportation and marketing[3]. China has a large population like India. Despite this fact, it has successfully used Blockchain to increase the trust of the people towards the government by making the production of the food resources transparent. This helps in equal distribution of the resources to the people and increases the accountability of the Government since all the transactions are recorded and can be viewed in case of disparity. Similar use cases can be implemented for India to manage its huge population. Blockchain is being used by financial institutions to increase cyber security. The advantages of blockchain are that it is fast, cheaper, has a decentralised registry and provides secure payment information[4]. In India, an Aadhar number is issued to all Indian citizens that asserts their biometric data along with their location and other details. The Aadhar can be utilised along with Blockchain technology for many applications like healthcare and voting[5]. Data loss due to single point failure and privacy disclosure can be eliminated through Blockchain[6]. Consensus protocol is of a large significance as it decides the parameters on which the new node is validated. An inappropriate consensus protocol may lead to undesirable results while using the application[7]. The challenges faced by a blockchain application are the need of resources and scalability[8].

III. PROBLEM STATEMENT

Donors have every reason to fear that charitable funds will not reach people who really need them. According to the same HSE survey in 2017, 68% of citizens are willing to donate more if there is evidence of where and what they are going. By law, foundations are required to maintain public records (in particular, to publish reports on their websites), and now all reports are prepared by employees of a foundation manually .The problem of mistrust of donors and overloading of funds can be solved by organizing an external database, records in which are recorded in the blockchain. Therefore, it is important to develop a social platform based on blockchain technology that can help non-profit organizations, foundations, volunteers and social entrepreneurs in their work and make donation processes transparent and understandable for all parties. Blockchain will allow all users of the platform to see their account and a description of each payment of the organization it supports. Also, the technology of distributed ledger will guarantee a donor that the amount will reach the goal, and without any intermediaries According to Rosstat research, in 2017 there were more than 9600 charitable foundations and about 1700 charitable organizations.

IV. PROPOSED METHODOLOGY

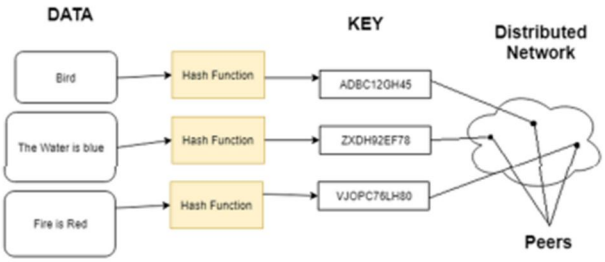
The system model has been presented in this section. The users of the application are classified on the basis of their roles viz a viz Donor, Organization, Retailers, Government official.



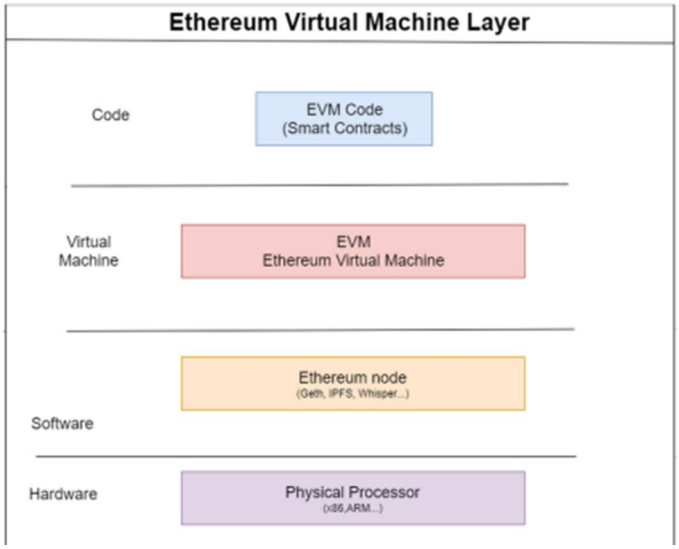
1) *Organization (Beneficiary):* These are charities, NGOs or other social enterprises in need of resources (monetary or otherwise). They will be able to publish their requirements in a predefined format on the Charity-Chain system. They will also play an important role in mining.
2) *Retailers:* These are the entities who pitch their tenders and quote the price. The retailer with most optimal pitch is selected by the government officials.
3) *Donors:* They are the entities who will view the requirements published by various organizations and the accepted tender choose to donate as per their capabilities and preferences to the cause.
4) *Government Official:* This entity will authenticate the requirements published by the organizations and validate the smart contracts. Only after authentication by the official will the donor be able to donate.

V. SYSTEM DEVELOPMENT

1) *Blockchain:* Blockchain is decentralized ledger designed to be a secure way of handling data based on a peer-to-peer architecture[1]. The two features of blockchain technology are transparency and distributed data architecture. Blockchain technology acquires transparency by removing the centralized node or any third party need for processing. It is a sequence of blocks of data linked to each other with different connected nodes which forms the chain-network of blockchain. Once a new transaction is approved by consensus, it is encrypted and linked to the previous transaction. Once a piece of data is added to the chain, it cannot be deleted. If there are any modifications to be done in any created block, a new block is created stating the modifications, if this block is approved by consensus of the network, it is appended to the chain. In this way, if an impostor tries to tamper with the recorded data, he/she can never mend already created data without the consent of the network. The approximate time taken for a blockchain network to create a single block in the blockchain is called block time. The block time for Ethereum blockchain is from 14 to 15 seconds. The included data becomes verifiable by the time of block completion. A Distributed blockchain networks are safe against any vulnerability that crackers can exploit in centralised computer system. Security methods used are based on public-key cryptography. A public key for a node (a long, randomly generated string of numbers or characters) used to address a node on the blockchain. Tokens transferred over the blockchain are logged as association to that address. A private key is a secret keyword which can give its owner access to their assets or it can be used to utilize the various features that blockchains now provides. Data stored over the network is considered unexploitable or incorruptible. The heart of our proposed system is the blockchain network that is to be built for secure and speedy donations to the beneficiary. As blockchains are transparent, decentralized and immutable, the proposed system will be best suited for the features that blockchain provides. Ethereum is very variable programming language for smart contracts.
2) *IPFS:* The InterPlanetary File System is based on the distributed peer-to-peer architecture[9]. IPFS is used as the storage system in the blockchain technology because the working of IPFS is similar to that of a blockchain. Every block in the blockchain is associated with hash value which is generated by the cryptographic hash function. This value is used as an index for storage purposes. The file or block is retrieved using this unique hash value. IPFS is an attempt in creating a permanent and decentralized web. An HTTP request can be represented as http://11.32.45.60/folderdirectory/filename.png An IPFS request can be represented as /ipfsdirectory/OqL9IpXyuK7j/folderpath/filename.png Unlike HTTP, IPFS uses representation of the content instead of using location. It is achieved using a hash generation encryption function on file and then the output of function is used as node address.The hash also represents a root and other objects can be found in its directory. In HTTP we focus on asking about something at a particular location whereas in IPFS we focus on a particular object on a path. Because of some similarities in the structure of IPFS and Blockchain both the technologies work well together. To record data IPFS uses a Distributed Hash Table or DHT.

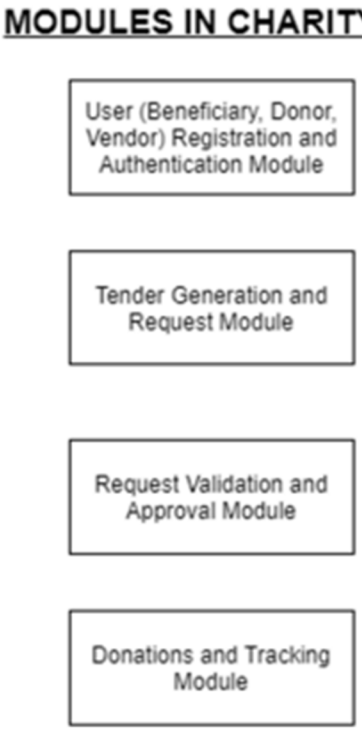


3) *Smart Contracts:* Smart contracts can be considered to be the soul of the blockchain network which controls all the transactions taking place in blockchain network. [10] Smart contracts are defined to make decision for all the transactions. We can say that the smart contracts are the rules designed to process any transaction that take place in blockchain network. A Smart contract can be lines code running on top of blockchain, which contains a set of rules under which multiple parties agree to that contract for interaction.If and when these predefined rules are met, the smart contract is automatically enforced.A smart contract can form a relationship between people, institutions and the assets they own. A Smart can extremely reduce the transaction costs.We can say that is an Auto-enforceable code, means it standardizes transactions rules and it indirectly reduces transaction cost of: Reaching an agreement, Formalization, Enforcement. Using such smart contracts a Dapp is created. DAPP stands for Decentralized Application It can be a message or any asset. Upon creation of a transaction, every transaction is charged with a certain amount also known as Gas. The purpose of this is gas is to limit the amount of work which is needed for the transaction and also to pay for its execution. While the EVM is executing a transaction, the gas is depleted gradually according to some rules specified in smart contract. The gas price is set by the creator of the transactions, who has to pay gas_price * gas up front from the sending account.



4) *Embark:* Embark is a simple, fast and powerful framework to develop and deploy Decentralized Applications (DApps). Embark is integrated with Ethereum blockchains,[11] Distributed peer-to-peer storages (IPFS) as well as Distributed peer-to-peer communication platforms (Whisper and Orbit). 6) ReactJS: ReactJS is a declarative, component-based library. ReactJS is developed with JavaScript as the base. React has been designed from the start for gradual adoption. 7) Consensus Protocols: A consensus protocol is a very important part of blockchain. It is required to reach to an agreement on a single value of data among distributed and peer-to-peer processes or systems. Whenever a new transaction is to be added to the network,all the participants are alerted about this new transaction. They can either approve it and add it to the chain or ignore it. When a majority of participants approve the transaction, consensus is achieved.As blockchains are not controlled by a central authority, bad participants can cause faults and disrupt valuable transactions. In absence of a strong, full proof consensus algorithm, the bad peer is able to post faulty transactions, nullifying the reliability promised by blockchains. To make things worse, there is no central authority to take charge and mend the errors.This ensures reliability and consistency in a network involving multiple unreliable and random nodes. It is difficult to imitate or replicate consensus protocols as they are extremely costly to carry out, in terms of time and the computing resources required. Depending on the blockchain within which they are validating the blocks, the methods of consensus vary. There is a consistent ongoing debate as to what is the most effective and efficient method of consensus. There are many protocols that are being used by the Blockchain applications. Some of these are Proof of Work(PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Delegated Byzantine Fault Tolerance (dBFT), Proof of Existence (PoE), Proof of Activity (PoA)[12]. Charity Chain System uses Byzantine Agreement[13], i.e. the decision will be in favour of the majority of people.Suppose there are ‘m’ participants who don’t approve the transaction, Byzantine Agreement states that for every m there should be at least 3m participants who approve the transaction.In other words, ⅔ of the participants should be in favor of the transaction.

If more than ½ participants disapprove the transaction, it is ignored. Most users possibly send decisions that will be received by almost every other user within a specific time bound. This protocol is used as it provides less latency. The consensus algorithm should not be a bottleneck for the donation process. It makes sure that users never have different views of confirmed transactions[14]. The system developed comprises of a number of modules namely:- A. User registration and authentication Module B. Tender generation module C. Request validation and approval module D. Donations and tracking module The system will be built on Ethereum platform, using Embark framework.The smart contracts will be written in Solidity. The GUI of the system will be built on React. The modular diagram for the system is shown below:



A. User Registration and Authentication Module

The user needs to first register in the system as a beneficiary or as a donor. Accordingly, he will submit his details to the Charity Chain system. The details of the beneficiary will include the name of the organization, its contact and website link for further information. These details along with authentication details will be stored in the user database.

B. Tender Generation Module.

The beneficiaries post their requirements in the form of a tender in a predefined format provided by the Charity Chain System. This includes the details of the requirements along with the estimated cost of each item. These tenders will be available to the donors as well as the government officials.

C. Request Validation and Approval Module

The tenders are validated by the government officials through the system based on the authenticity of the organizations and their requests.

D. Donations and Tracking Module

Once the donations are approved by the government officials, the donors can donate any amount to the organization according to their capabilities and preferences. The genesis node will be created at this stage. The entire transaction pertaining to the charity will be visible to the donors on the charity's profile page. This will help the donor to make informed decision and donate accordingly. The donor will also be able to track the entire journey of the transaction till it reaches the beneficiary.

VI. CONCLUSION

In this research, a blockchain-based solution was proposed that would increase transparency and trust between NGOs and donor agencies in third-world countries. Some of the interesting objects and data structures that were used are: (i) an invalidation record that can be inserted into the blockchain to invalidate a previous transaction; (ii) a time-keeping table that each node maintains, to allow an entity, whether NGO or donor, to insert its records only if has participated as an active member in the system; and (iii) a table of purposes, that lists a valid range of a sum of money, for a given purpose, and is also used to detect duplicate/fake claims of two distinct funds. This article also includes a description of some of the distributed algorithms employed including: (i) how nodes calculate whether the signatories of a transaction have spent enough time to be allowed to insert records into the ledger; (ii) how transaction records and invalidation records are verified for correctness and inserted into the ledger by consensus; and (iii) how the nodes agree on when a set of outstanding records can be made into the next block of the blockchain.

It is hoped that this detailed solution given in this article leads to an implementation that has the impact that is being envisaged: significantly improving the amount of trust and transparency in the transactions among the NGOs and donor agencies of a third world country. The implementation of the model is under process and the results will be published shortly. Furthermore, the Raft consensus algorithm is being implemented.

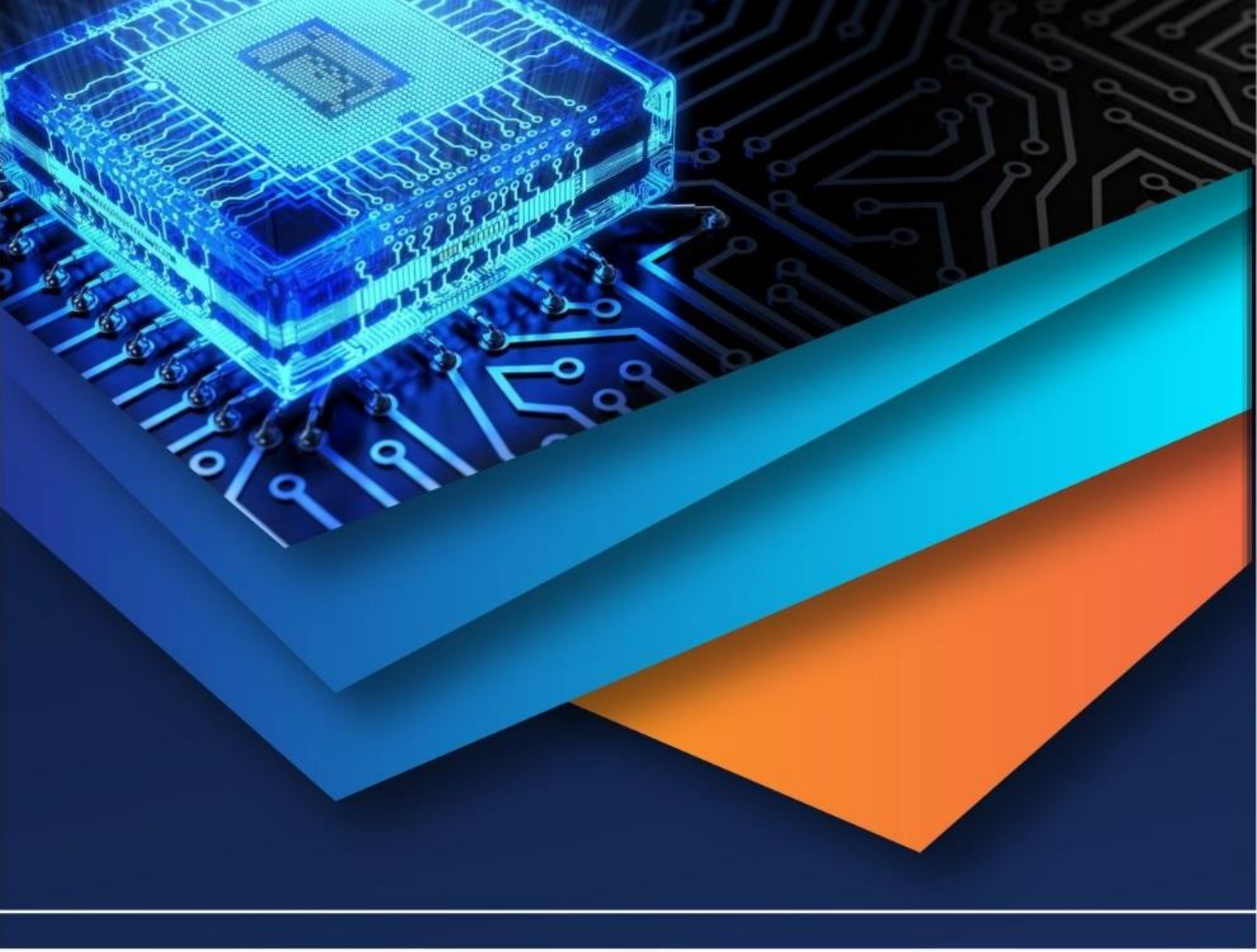
VII. ACKNOWLEDGEMENT

I would like to express my deep gratitude to Professor Mr. Sunil Sonawane Sir, our project guide, for their patient guidance, enthusiastic encouragement and useful critiques of this research work. I would also like to thank Mrs. V.R. Palandurkar, for her advice and assistance in keeping my progress on schedule. I would also like to extend my thanks to the technicians of the laboratory of the Information Technology department for their help in offering me the resources in running the program.

Finally, I wish to thank my parents for their support and encouragement throughout my study.

REFERENCES

[1] Kravitz, D. Digital Signature Algorithm. U.S. Patent 5,231,668, 27 July 1993. Available online: https://patentimages.storage.googleapis.com/e6/de/c5/75aceb27607e59/US5231668.pdf (accessed on 11 April 2021).
[2] Satoshi, N. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 11 April 2021).
[3] Bhatia, S.; Wright De Hernandez, A.D. Blockchain Is Already Here. What Does That Mean for Records Management and Archives? J. Arch. Organ. 2019, 16, 75–84. [Google Scholar] [CrossRef]
[4] Irshad, S.; Brohi, M.N.; Soomro, T.R. Block-ED: The Proposed Blockchain Solution for Effectively Utilising Educational Resources. Appl. Comput. Syst. 2020, 25, 1–10. [Google Scholar] [CrossRef]
[5] Wu, H.; Zhu, X. Developing a Reliable Service System of Charity Donation during the Covid-19 Outbreak. IEEE Access 2020, 8, 154848–154860. [Google Scholar] [CrossRef]
[6] Sam, D. 30 Blockchain Applications and Real-World Use Cases Disrupting the Status Quo. Available online: https://builtin.com/blockchain/blockchain-applications (accessed on 11 May 2021).
[7] Akash, T. Top Blockchain Platforms of 2021. Available online: https://www.leewayhertz.com/blockchain-platforms-for-top-blockchain-companies/ (accessed on 11 May 2021)
[8] Bohme, R.; Christin, N.; Edelman, B.; Moore, T. Bitcoin: Economics, Technology, and Governance. J. Econ. Perspect. 2015, 29, 213–238. [Google Scholar] [CrossRef
[9] Abou Jaoude, J.; Saade, R.G. Blockchain Applications-Usage in Different Domains. IEEE Access 2019, 7, 45360–45381. [Google Scholar] [CrossRef
[10] Curt, T. Foreign Aid and the Education Sector: Programs and Priorities. Congr. Res. Serv. 2016, 1–23. Available online: https://fas.org/sgp/crs/row/R44676.pdf (accessed on 15 May 2021).
[11] Zwitter, A.; Boisse-Despiaux, M. Blockchain for Humanitarian Action and Development Aid. J. Int. Humanit. Act. 2018, 3, 1–7. [Google Scholar] [CrossRef]
[12] Farooq, M.S.; Khan, M.; Abid, A. A Framework to Make Charity Collection Transparent and Auditable Using Blockchain Technology. Comput. Electr. Eng. 2020, 83, 106588. [Google Scholar] [CrossRef]
[13] Gilad, Y.; Hemo, R.; Micali, S.; Vlachos, G.; Zeldovich, N. Algorand: Scaling byzantine agreements for cryptocurrencies. In Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai, China, 28 October 2017; pp. 51–68. [CrossRef]
[14] Al-Riyami, S.S.; Paterson, K.G. Certificateless public-key cryptography. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, 30 November–4 December 2003; pp. 452–473.
[15] Lamport, L. Time, clocks, and the ordering of events in a distributed system. In Concurrency: The Works of Leslie Lamport; Association for Computing Machinery: New York, NY, USA, 2019; pp. 179–196. [CrossRef]
[16] Whetten, B.; Todd, M.; Simon, K. A high performance ordered multicast protocol. In Theory and Practice in Distributed Systems; Springer: Berlin/Heidelberg, Germany, 1995; pp. 33–57
[17] Van Steen, M.; Andrew, S. Tanenbaum. Distributed Systems; Maarten van Steen: Leiden, The Netherlands, 2017.
[18] Nguyen, N.T. Consensus-based Timestamps in Distributed Temporal Databases. Comput. J. 2001, 44, 398–409. [CrossRef
[19] Awerbuch, B. Optimal Distributed Algorithms for Minimum Weight Spanning Tree, Counting, Leader Election, and Related Problems. In Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing, New York, NY, USA, 25–27 May 1987; pp. 230–240. [CrossRef]
[20] Abraham, I.; Dolev, D.; Halpern, J.Y. Distributed Protocols for Leader Election. ACM Trans. Econ. Comput. 2019, 7, 1–26. [CrossRef]



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY