WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Resource Allocation Using Blockchain For Disaster Relief

Om Pant[1], Shiksha Srivastava[2], Dhruv Sharma[3], Ms. Rashmi Tiwari[4]

[1]CSE-IOT Student RKGIT, Ghaziabad ompant624@gmail.com
[2]CSE-IOT Student RKGIT, Ghaziabad shikshasrivastava957@gmail.com
[3]CSE-IOT Student RKGIT, Ghaziabad dhruvpandit206@gmail.com
[4]Assistant Professor, CSE-IOT RKGIT, Ghaziabad rt45720@gmail.com

ABSTRACT—

Blockchain is a technology for distributed databases. that allows data to be transparent inside the system and safeguarded using cryptographic operations. It is widely utilized in a variety of use cases, including supply chain management, e-governance, financial instruments, and many more. Because an integrated information system is deficient, it is made expressly for disaster control and management, which would facilitate effective decision-making. Blockchain facilitates safe transaction processing for asset trades. To enable reliable and consistent information exchange and preservation, we want to bring all necessary stakeholders together on a single platform. This study offers a system paradigm for various user scenarios during times of crisis. The model presents a complete picture and explains the unfortunate occurrences. Efficient financial resource management and timely, efficient delivery of supplies to impacted areas with little processing time is critical to the success of disaster response and relief operations. Several factors determine how long it takes to transport goods from their point of origin to the affected region, but the one that can be reduced the most is the amount of time needed for paperwork and legal compliance. We propose a resource management system that utilizes the Hardhat architecture on top of a blockchain platform to expedite humanitarian relief distribution and reduce paperwork. This provides a conduit for information amongst the network of relief businesses and groups, an opening for the public to donate goods, and a method for levies to provide their services to the active non-profits on the property.

Keywords— blockchain; latency; security; distributed system; hardhat; smart contracts.

I. INTRODUCTION

Information on crises is essential to making any kind of sensible decision. Much more crucial is protecting the data from illegal access points. Blockchain is a secure database system that provides encryption techniques, consensus methods, distributed data storage, and point-to-point transmission.[1] It is extensively relevant in many domains where numerous parties are engaged, such as the healthcare supply chain[2], financial services[3], Internet of Things, privacy rights, e-governance, etc. In times of crisis, blockchain can be very helpful to society and the government. Many nations' governments take the lead through websites such as NDM and SERS. Information systems are used extensively in many corporate sectors; however, they are not as often used in disaster management.

Blockchain provides a way to monitor particular requirements and assets. Smart contracts are used to handle requests and inquiries to the blockchain. A smart contract is a business agreement that is implemented with transactions and is included in the transaction database within the blockchain. Here, we suggest a new design for a resource management system that would enable users to request aid at their location or a safer house during a disaster. The system would also establish a portal where all parties involved can be verified and would give affected individuals access to basic information like location beacons, weather information, shelters that are close by, and resource locations.

Every second matters in the chaotic aftermath of a calamity. The goal of the blockchain-based system is to create processes that expedite information sharing and shorten response times. In times of crisis, real-time data processing guarantees that all relevant parties have access to current, reliable information, facilitating quicker and better-informed decision-making. Ensuring the authenticity and accuracy of information is crucial for effective disaster management. The blockchain technology is renowned for its tamper-resistant and transparent nature. By implementing robust validation protocols, this system will provide an immutable ledger for critical disaster-related data, from emergency alerts to resource allocation. This will significantly enhance trust and accountability in disaster response efforts. In an age of cyber threats and data breaches, the security of sensitive information is paramount. The disaster management system built on blockchain concentrates on strengthening security protocols to protect sensitive data. Access restrictions and encryption methods will stop unwanted access, safeguarding not just the data's integrity but also the privacy of those impacted by natural catastrophes.

For effective decision making by the government and the people in time, disaster management is a complicated and disorganised process involving collection, analysis, storage, and dissemination of information. Now the government is unable to coordinate the process of rescue without keeping proper records in real time. During all stages of disasters like risk reduction, preparedness, response, and recovery, the government can effectively utilise funds, launch the rescue operation through the disaster management team, and provide food and shelter, medical and rehabilitation centres, transport facilities, water and electricity supply, and other necessities to victims and people in their direct circle.

Blockchain, initially proposed as the underlying technology for cryptocurrencies, has now become a robust tool with far-reaching implications across industries beyond the financial sector. Its decentralized and tamper-proof nature, coupled with the use of advanced cryptography, offers a secure and transparent platform for data management and transactional processes. Based on the distinctive features of blockchain, disaster management can be transformed, making coordination efficient, information sharing enhanced, and stakeholder trust improved. The objective of this project report is to establish the potential of blockchain for disaster management and present its many applications, advantages, and challenges. The objective of this report is to analyse the potential of blockchain for disaster management and offer insight into its many uses, advantages, and limitations. In this report, we will first present the most significant challenges to traditional disaster management systems, including data integrity issues, coordination issues, and accountability issues. We will then present the fundamental concepts of blockchain technology, including its decentralized nature, consensus mechanisms, and cryptographic methods used to offer data security and immutability. Next, we will discuss the specific applications of blockchain in disaster management. These include identity management for impacted persons, transparent tracking and allocation of relief resources, real-time data sharing and stakeholder collaboration, and safe smart contracts for efficient financial and logistical operations. This research will also examine the advantages that blockchain technology provides for disaster management. These benefits include heightened accountability, efficiency, openness, and stakeholder trust-building. We will also investigate the possibility of using blockchain technology to support recovery and reconstruction operations following a disaster.

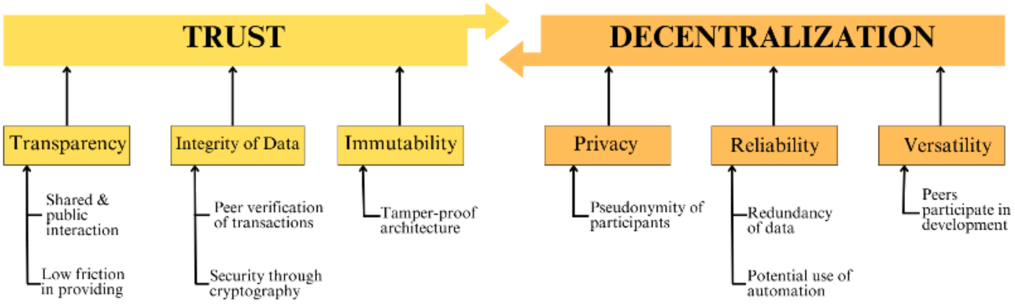
TRUST
DECENTRALIZATION
Transparency
Integrity of Data
Immutability
Privacy
Reliability
Versatility
Shared & public interaction
Low friction in providing
Peer verification of transactions
Security through cryptography
Tamper-proof architecture
Pseudonymity of participants
Redundancy of data
Potential use of automation
Peers participate in development

Fig 1. Characteristics of Blockchain Technology.[1]

Fig 1. presents a list of properties which are traditionally linked with blockchain technology. Such principles are typically included in systems that utilize blockchain for several purposes. But it of note is the use of blockchain in disaster management is far from being free of challenges. This report will address the scalability, technical, and regulatory issues with regard to blockchain adoption, and also possible privacy 4 problems and the need for interoperability with current systems. To verify the findings and the analysis, this project report will use a range of sources, including scholarly research papers, case studies, industry reports, and authoritative views. The data will be combined with care and properly cited to guarantee the validity and integrity of the report, ruling out any chance of plagiarism. Lastly, the use of blockchain technology in disaster management has vast potential to revolutionize the field. By solving the big issues related to transparency, coordination, and data integrity, blockchain enables the efficiency and effectiveness of disaster response programs. We hope that this project report to provide useful inputs and ideas to stakeholders interested in leveraging blockchain for future disaster management programs. Blockchain is a method for tracking particular requirements and assets. Smart contracts deal with requests and inquiries to the blockchain. Within the blockchain network, a smart contract is a commercial agreement that is included in the transaction database and carried out in tandem with transactions. Through this project report, we aim to provide valuable insights and recommendations for stakeholders interested in leveraging blockchain for future disaster management initiatives.

Blockchain is a tool for tracking particular requirements and assets. Smart contracts manage queries and requests to the blockchain. Within the blockchain framework, a smart contract is a commercial arrangement that is integrated into the transaction database and carried out in tandem with transactions. In [4] In this case, we suggest a new architecture for a resource management system that would establish a verifiable portal for all parties involved and give impacted individuals access to basic information like location beacons, shelters close by, weather information, and resource locations in addition to the option to request assistance at their current location or a safer house.

Our planet is faced with an unprecedented influx of data. 20% of the world's data is thought to have been gathered in the past two years, a recent report says. The largest social networking site, Facebook, has reached 300 petabytes of private data from the beginning — even more than the Library of Congress has accumulated over more than 200 years. Data is constantly being compiled and monitored under the Big Data regime,
which promotes economic growth and innovation. Organizations and institutions utilize information they convene to customize services, rationalize internal decision-making, forecast future trends, and so on. Information is a precious commodity in our economy today. A society based on data is good. all of us, user privacy is a growing public concern. Public and private centralized bodies collect a lot of private and confidential data. Individuals have scarcely any autonomy of how their data is stored and utilized. Of late years, public media has reported a number of controversial privacy breaches. Two of the best-known instances are the history of government spying and Facebook's massive scale scientific research, which appears to have been carried out

without participants' knowledge.

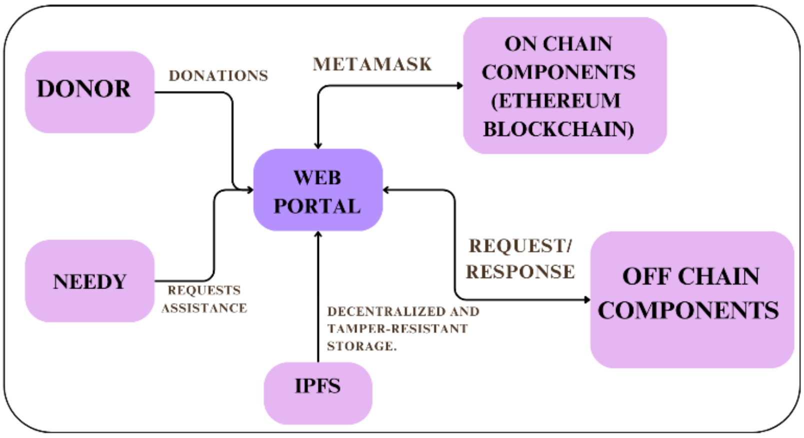

Fig 2. Overview of Model[5]

Fig 2. depicts the architecture that combines the security and transparency of the Ethereum blockchain with the decentralized file storage capabilities of IPFS. The off-chain components, including the use of MetaMask, enhance user interactions and facilitate the seamless transfer of digital assets within the system.

Multiple disaster calamities occur for example drought, and an earthquake so more than half of the earth's land surface is susceptible to drought, making it a common and unexpected natural disaster. In recent decades, India has experienced frequent and severe droughts (once every three years), making it one of the world's most vulnerable nations when it comes to droughts. Notably, several areas of Gujarat and Rajasthan state (in the west of the country) have recently experienced a severe drought. These areas experience droughts because of unseasonably high temperatures, unfavorable weather patterns, and unlucky monsoon seasons.

A. Problem Statement

Information must be gathered, processed, stored, and distributed to the public and government in a timely and efficient manner as part of the complicated and chaotic process of disaster management. Because of the present disaster management information systems' lack of integration, data from different catastrophe stages is fragmented, which makes it more difficult for the government to plan rescue operations, distribute resources, and make prompt judgments.

Manual data verification in the existing system leads to manipulation, redundancy, and data integrity issues, causing misinformation, unreliability, and ambiguity in victim certificates and fund allocations, posing significant challenges for the disaster management team.

B. Objectives

The following goals are being pursued by this initiative, which intends to develop a disaster management system based on blockchain technology. The initiative is motivated by the realization of how crucial it is to have a well-stocked disaster kit that includes necessities like food, water, first aid supplies, and critical papers.

- To develop mechanisms to reduce response time and improve real-time data processing during disaster situations.
- To put strong validation procedures in place to guarantee the veracity and correctness of data kept on the blockchain.
- To focus on enhancing the security measures of the platform to safeguard sensitive information and prevent unauthorized access.

II. RELATED LITERATURE SURVEY

A study published, by Vinayak G. B et al. [6] suggests a resource management system that aims to tackle the difficulties related to a lot of paperwork while relief supplies are being deployed for disaster relief. They advise utilizing a blockchain-based web application built on Hyperledger Fabric to speed up this process. However, the report did point out that one potential disadvantage of their recommended strategy could be transaction delay.

Sujit Biswas et al. Scalable Blockchain Framework for Secure Transactions in the Internet of Things [4]. This article explores the possibilities of combining Internet of Things

(IoT) and Blockchain technology. The Internet of Things (IoT) offers sophisticated automation across numerous industries, whereas blockchain is known for its secure transaction processing in asset exchanges. It is noteworthy that the research does not offer an assessment grounded in real-time transactional data, hence providing opportunities for additional pragmatic evaluation and execution.

Sobha P. et al. [7] have produced a paper describing a conceptual model for utilizing blockchain technology in disaster assistance. This paradigm is currently at the conceptual stage and has not yet been incorporated into any systems, even though it offers relevant information for improving disaster response and recovery.

In the context of financial innovation, Wang et al. [8] focus on a maturity model for blockchain adoption. They evaluate different aspects of this model, which is essentially based on the well-known capacity maturity model, using a comparative analysis method. According to their findings, blockchain systems are still not at the optimal stage of maturity, which highlights the necessity of conducting extensive feasibility studies before introducing blockchain technology into the financial industry.

Seebacher et al. [1] emphasize the potential advantages of blockchain technology as a service system enabler. Blockchain technology makes decentralization possible, which can improve privacy protection. Pseudonymization techniques make it possible to handle sensitive data securely. Systems establish a flexible and dependable service delivery environment. Service systems are more reliable because of blockchain's tamper-proof and decentralized architecture.

In this research study, Kamble et al. [2] give a methodology for supply chain analysis of blockchain applications technology. They employed three adoption theories in their model: the Theory of Planned Behavior (TPB), the Technology Acceptance Model (TAM), and the Technology Readiness Index (TRI). This research will attempt to clarify the factors impacting the application of blockchain technology in Indian supply chains, concerning the vision of decision-makers and technologists. It also provides an entire system outlining this process.
The theoretical application of blockchain to disaster management is covered in [7]. It highlights how blockchain technology might be used in emergency situations. It's crucial to remember, though, that the ideas discussed in the paper are still theoretical and conceptual and have not yet been applied to any systems.

In the study, Sreelakshmi et al. [9] developed a plan for using blockchain technology to aid in disaster relief. Their plan lays a heavy emphasis on the need for doing research, developing usable technologies, and creating legislative frameworks in order to increase the efficacy, accountability, and transparency of disaster relief initiatives. They do, however, admit that blockchain networks might have issues with scalability and transaction processing speed, particularly in public blockchains, which might prevent widespread adoption in catastrophic situations.

Information technology is used in response, recovery, preparedness, and risk reduction phases of disaster management, as demonstrated in the work by Sakurai et al. [10]. The lack of a decentralized implementation, however, is highlighted and raises the possibility of a constraint in discussing the advantages and difficulties of decentralized approaches to disaster management.

A comparative analysis method is used in the by Svein et al. [11] to evaluate several features of a maturity model. But the investigation shows that the model is mostly useful for storage needs.

The work published by Shrier et al. [12] examines the use of blockchain technology in infrastructure, with a focus on data and identity security in particular. It highlights how blockchain technology might transform infrastructure management by removing the difficulties brought on by a lot of paperwork. On the other hand, the study doesn't go into detail about how blockchain technology is used in this situation.

To establish a personal data management platform that emphasizes privacy, Data Zyskind et al. [13] talk about the application of off-blockchain storage and blockchain technologies. The safe storage of personal information is the main priority. The study does stress that while this method works well for storing data, it is not appropriate for processing data.

In their work Betti et al. [14], the authors propose to improve hyperconnected logistics by using blockchain and smart contracts, with an emphasis on achieving transparent supply chain activity tracking. They acknowledge that more improvements are required and that problems like scalability and access control must be dealt with in this environment.

The report discusses the application of blockchain technology to trade financing. By Bogucharskov et al., [3], which highlights its benefits and offers suggestions for enhancing its effectiveness. Although the article mentions openness, it does not go into detail about possible problems with data security and privacy in blockchain-based trade finance.

With an emphasis on increasing automation and transparency, the Ernest Chang et al. [15] study proposes re-engineering supply chain processes utilizing blockchain technology. However, there can be challenges to overcome when applying blockchain to supply chain management in the real world. These include integrative, technological, financial, legal, and human factors, all of which require careful thought.

III. PROPOSED ALGORITHM

The goal is to work together with a range of stakeholders, including the local government, government, non-governmental organizations, the disaster team, transportation, energy, communication services, hospitals, rehabilitation facilities, financial services, and residents, to create a single platform where information can be securely shared and exchanged for efficient disaster management and recovery.

A. Feasibility Study

This survey is being conducted to better handle the disaster situation by providing funding. Current Disaster systems have closed the gaps of various problems in disastrous situations but there are a lot of issues in current existing disaster management systems. There is no focus on smooth transactions to prevent them from fraud. There is a lack of trust among the concerned authorities, NGOs, and donors in the transactions and data shared on these systems as they can be tampered with easily. The problem statement of this research paper is to use blockchain technology to make a decentralized application in which problems of transparency, security, and latency will be improved and various concerned entities will take part in the blockchain nodes to see the details of transactions happening.

B. Proposed Design

The following is included in the proposed work for the disaster assistance system based on blockchain technology:

- Creating an easy-to-use online interface for government organizations to communicate with the disaster assistance system based on blockchain technology.
- Developing a financing mechanism based on smart contracts so that monies for disaster assistance can be transferred directly from higher government entities to lower government entities, eliminating the need for middlemen.
- SHA-256 and Keccak256 algorithm integration to prevent corruption and manipulation with the disaster relief system.
- Creating a Proof of Stake consensus technique to verify transactions and guarantee the disaster assistance system's immutability.
- Deploying and testing the Ethereum and Polygon networks' disaster relief solutions.
- Assessing how well the system works to increase openness and decrease corruption in the way the government finances disaster aid.

Overall, the proposed work aims to provide a more transparent and secure system for government financing and a secure system for government disaster relief financing.

C. Key Terminologies

- Web3: The latest version of the World Wide Web, referred to as Web3.0 or Web3, blends token-based economics, blockchain technology, and decentralization. Gavin Wood, a co-founder of Ethereum, popularized it in 2014. Investments from IT businesses and cryptocurrency enthusiasts sparked interest in it in 2021. Andreessen Horowitz, a venture capital firm, traveled to Washington, D.C. to promote Web 3.0 as a possible solution to web regulation issues.
- IPFS: To store and distribute data, this distributed file system makes use of a peer-to-peer network, hypermedia, and a protocol. It enables users to distribute content across the World Wide Web and to host and receive content. The decentralized user-operator design of IPFS allows peers to locate and request content through the use of a distributed hash table. Ethereum-based on blockchain technology, Ethereum is a decentralized global software platform best known for its native cryptocurrency, ETH. Because it is decentralized, safe, programmable, and scalable, programmers and businesses prefer it. It supports smart contracts, an essential part of decentralized applications across multiple industries.

D. Methodology

Working of Smart Contracts in Donations-

- The donations have been made in the form of smart contracts.
- These smart contracts make the transactions between two parties by involving everyone and removing the middleman.
- The manager will start the campaign for the victims and raise donations.
- The donors will donate the money through smart contracts.
- If the manager has to spend this money to the victims supply, then he/she have to take the permission of more than 50% of the donators.
- The smart contract will help to secure the money to not go into the manager's account.
- The smart contract helps to make the money go into the account of victim supply joint account with the help of more than 50% of the donors.
- In this way, Smart contract make the transparency, security, and accountability of the funds donated by the donator.

E. Smart Contract Algorithm For Smooth Transactions

The line // SPDX-License-Identifier: Unlicensed tells us the license we are working with. This would help us to prevent from any errors. pragma solidity >0.7.0 <=0.9.0 tells us the solidity version we are working on.

We will create the contract by calling the function contract and naming it "Campaign". We will make these state variables as public function because we want to anyone to call it.

- State variables: These variables will be stored in the blockchain: - title : It will be used to store the title of the campaign to be started by the requestor. It is of string datatype.
- RequiredAmount: It would be used to store the required amount requested by the users. It is of uint datatype.
- Image: We would save the link of the image as a string we get from IPFS as storing the image in the blockchain is very costly.
- Story: This variable will store the Reason or detail of the campaign.
- Owner: It would store the address of the creator or owner of the creator. • ReceivedAmount: It would store the amount received from the donor. We would use the event function to integrate the smart contract values with the front end.

The Constructor Function:

- The constructor is the first function to run as we would make sure that only the creator of the campaign would call the contract.
- We can set arguments with memory keywords so that these would not save in the blockchain and will be used till we call the constructor function
- The arguments in the constructor are – campaignTitle, requiredCampaignAmount, imgURI, storyURI, campaignOwner
- this constructor would be assigned to the state variables as:

title = campaignTitle;
requiredAmount = requiredCampaignAmount;
image = imgURI; story = storyURI;
owner = payable(campaignOwner);

The Donation Function:

- This function is used to run the donation process smoothly.
- We use the payable keyword if we want to receive or transfer the funds. • msg.value is the global variable which is used to fetch the value of transaction or funds.
- msg.sender is a global variable that is used to fetch the value of the owner. • We would use receivedAmount += msg.value to increase the value of the received amount whenever someone donates it.
- We would increase the received amount till (requiredAmount > receivedAmount) is satisfied.
- emit is used to get the values from the donate function to use these with the front end.
- block.timestamp is used to give the value of the current block running.

The Campaign Factory function :

- This function is used to store the deployed addresses of all the previously created contracts and functions.
- address[] public deployedCampaigns is used to store deployed addresses of campaigns.
- We would create a new function to create the campaign as function createCampaign().
- emit campaignCreated() is used to fetch the values of createcampaign function for frontend use.

F. The algorithms that protect this portal

Consensus Algorithm

To reach a consensus on the current state of the blockchain among all network nodes in our blockchain-based portal, we employed a consensus method. We employed the Proof of Stake (PoS) consensus process, which is widely adopted by other blockchains, like as Ethereum and Polygon.

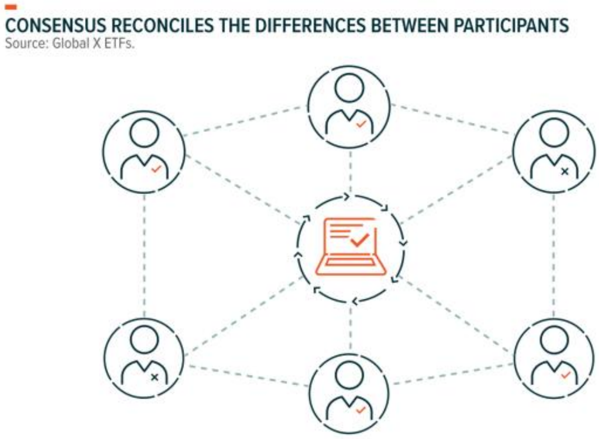

Fig 3. Consensus Algorithm

Proof of Stake

The level of cryptocurrency validators staked decides what is brought in as new blocks to the blockchain in proof of stake. Validators stake a portion their bitcoin as collateral that they would lose if they act dishonestly. They are encouraged to act honorably and comply with the rules of the network consequently. A validator has a greater likelihood of being selected to attach a new block to the blockchain, the more cryptocurrency they have pledged.

Advantages of Proof of Stake

PoS is superior to other consensus algorithms in several ways.

- Energy efficiency: Proof of Work (PoW), a consensus process that forces validators to carry out intricate computations that use a lot of electricity, uses a lot more energy than PoS.
- Security: PoS is safe because it encourages truthful behavior from validators. They will forfeit the bitcoin they have staked if they attempt to assault the network.
- Decentralization: Since PoS does not require specialized hardware to function in the network, decentralization is encouraged.

Fig 4. Proof of Stake

Plasma security

Polygon offers "Plasma Guarantees" for several attack scenarios. The following are the top two examples:

- The user is dishonest.
- Chain operator is dishonest

In any scenario, if users' resources on the plasma network are being hacked, they need to begin mass exodus. Useful root network smart contract structures are offered by Polygon. For more details, including technical specifications, on this building's architecture and the possible attack paths, keep reading. By effectively riding atop Ethereum's security, Polygon's Plasma contracts provide security. Users' money is never at risk, not unless Ethereum succeeds. In other words, a plasma chain's consensus process is equally secure as the main chain's. This shows that to preserve security, the plasma network might employ incredibly basic consensus techniques.

Developers must create their special custom predicates for their smart contracts if they want to create dApps on Polygon with the Plasma security assurance. All that needs to be done is draft external contracts that address the conflict scenarios caused by Polygon plasma structures.

Hybrid

Additionally, developers have the option to employ a hybrid strategy, which essentially entails receiving guarantees on specific dApp operations from both Proof of Stake and Plasma. Pure Proof of Stake and pure Proof of Plasma Security are both feasible with dApps running on Polygon.

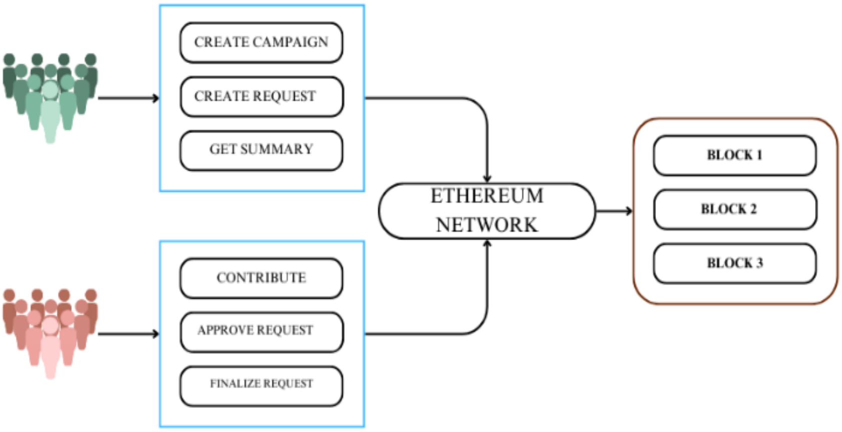

Fig 5. Proposed Model

IV. IMPLEMENTATION

The general workflow of the Modules blockchain-based funding portal project is summarized as follows:1. Connect wallet & Create Campaign
2. Create a Request Module
3. Request-Approval Module
4. Final Module

1. Connect Wallet & Create Campaign: First, link your Ethereum wallet to the website using MetaMask, a browser plugin that allows you to approve transactions. Next, go to the page and click on the "Create Campaign" option. Make sure you have enough funds to cover the transaction costs associated with initiating a campaign if you're starting one or contributing to one.

Complete the campaign information that you wish to create. Including the details of the campaign, including Your Name, Campaign Title, Goal, and End

Date. It could also be necessary for you to upload the picture in the designated area labeled "Campaign Image" to highlight the campaign. Log in to the platform using your MetaMask account, then allow the campaign to be established. This will initiate a blockchain-based smart contract that will retain the funds raised during the campaign and then automatically distribute rewards to backers in compliance with the terms specified in writing by the campaign organizer.

2. Develop the Request Module: After the campaign is launched, donors will contribute and assist it. The user needs to register a request for utilization before they can use the funds immediately. For example, if the user wants to buy something for the project, he needs to send in a detailed purchase request that contains the address of the seller. After that, something will happen, and a new block will be added to the blockchain. He is unable to spend the money immediately since doing so would expose him to the many scams that sometimes occur on crowdfunding sites.

3. Module for Request-Approval: The campaign author will request funds to purchase more items or accessories after providing proof. The designer will then inform every investor that they have to buy anything. Therefore, if the investor so desires, he must approve the idea. An investor may only receive one approval. All investors should cast their votes at the same time. There will be a record of each request approval in the block. The investor will not be able to do it again after that.

4. Final Module: In this module, the money will automatically go to the person who started the campaign after it has been approved by the two or three funders who have contributed the most to that specific campaign. The blockchain records every transaction. When sending money, the recipient's address and specific campaign creators must be provided by the developer. The campaign information, including a synopsis, will be emailed after the funds have been sent and on that platform, a history of your developed campaigns is available.

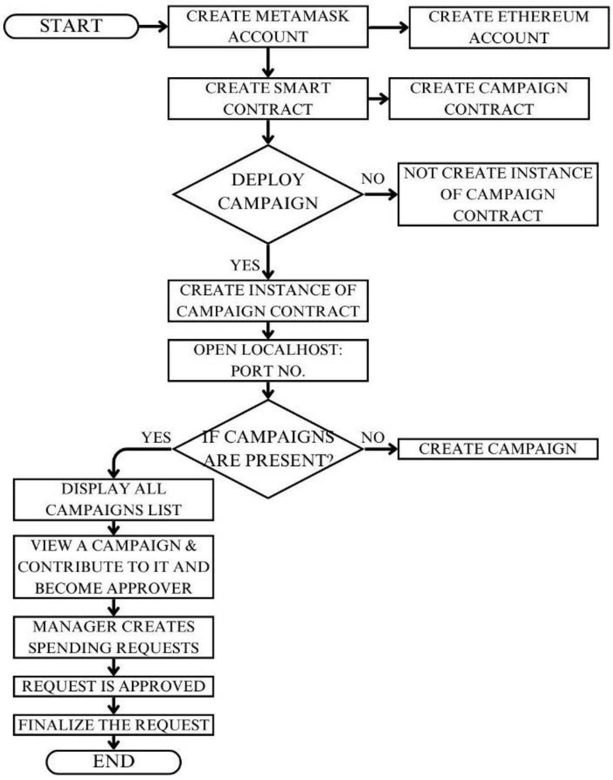
START
CREATE METAMASK ACCOUNT
CREATE ETHEREUM ACCOUNT
CREATE SMART CONTRACT
CREATE CAMPAIGN CONTRACT
DEPLOY CAMPAIGN
NO
NOT CREATE INSTANCE OF CAMPAIGN CONTRACT
YES
CREATE INSTANCE OF CAMPAIGN CONTRACT
OPEN LOCALHOST: PORT NO.
YES
IF CAMPAIGNS ARE PRESENT?
NO
CREATE CAMPAIGN
DISPLAY ALL CAMPAIGNS LIST
VIEW A CAMPAIGN & CONTRIBUTE TO IT AND BECOME APPROVER
MANAGER CREATES SPENDING REQUESTS
REQUEST IS APPROVED
FINALIZE THE REQUEST
END

Fig 6. Flowchart of the project

V. RESULT AND DISCUSSION

The integration of disaster response and recovery technologies with blockchain will make the recorded data accessible to all parties involved in the blockchain network. Transparency will be provided throughout the system and network by combining external data sources or databases onto a single platform. Every request and response made during the crisis was able to be handled promptly and without any misunderstanding among the network's participants. The blockchain network authenticates itself as a trustworthy solution by verifying and ensuring that every information sent over it is free from tampering.

All users in the network are validated, and there aren't any duplicates because of the legitimate processing carried out by the blockchain network's certificate authority. The malicious node will be able to be identified by the consensus process of the blockchain network, preventing any information from that node from being broadcast.

Blockchain protects user privacy by using its cryptographic hash function. Consequently, there is no need to worry about prejudice or danger when verifying the data in the network. As a result, the information will be more accurate and timely decision-making will be possible. Blockchain technology offers tamper-proof security for information. It's important to respond swiftly to requests for resources in a dynamic environment. Since all peers on a blockchain are connected to a single network, requests can be validated by the information technologies and disaster management blockchain. Every inquiry so gets a timely response. This will facilitate the speedy transfer of goods and funds between the concerned parties. If any modifications are made to any information that affects the hash value of a transaction, it is not practically possible to change the hash value of every block up until the genesis block. Thus, data transferred to a blockchain is extremely safe.

Here are a few comparison findings:

The speed at which we may retrieve the data from the server is faster; that is, server-side loading.

The results have been validated using PageSpeed Insights, and the screenshots of the comparison study have been attached. The latency of the transactions has been improved, and the computational load is relatively lower.

The final Dapp that is developed has the following buttons:

- Campaigns (included are all desired campaigns): Go to the campaign and send money.
- To initiate a campaign, click the "Create" button. Alternatively, you can submit files to IPFS and start a campaign.
- Dashboard (shows campaigns that the user has requested): a Visit the campaign: One give
- Click the "Connect" button to link your wallet.
- Buttons to swap between themes (theme toggles).
- Buttons for filtering data (button to view specific information about specific category): a food b medical c transport d all.

Following are some comparative results:

- We can fetch the data faster from the server i.e. Server- side loading is faster.
- Improved the latency of the transactions.
- Computational load is comparatively less.

A. COMPARATIVE ANALYSIS

These functionalities of the concerned websites have been obtained by Page Speed Insights:

Table I COMPARATIVE ANALYSIS

Functionality	Traditional Implemented	Proposed Implemented
Performance	06	71
Accessibility	87	88
Best Practice	75	93
SEO	83	73

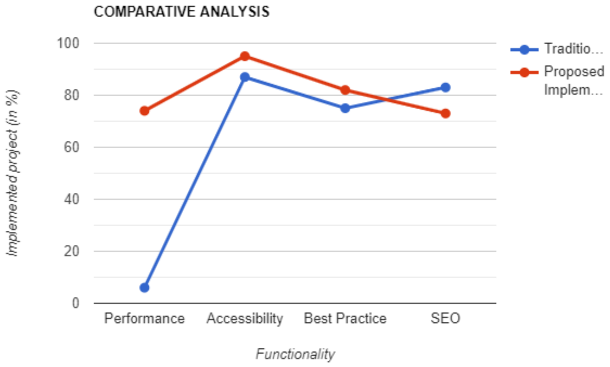

Fig 3. Displaying comparative analysis

The speed index of the website we implemented is 0.9 seconds, while the speed index of the official government website is 4.4 seconds.

VI. FUTURE SCOPE

Even though this project has put into perspective how blockchain technology can be used in relief of disaster, but there are some areas to be further researched and developed. Future studies on how blockchain technology will be utilized during disaster management will seek to maximize transaction throughput and scalability by the use of techniques such as sharding and layer-two solutions; creating standards for interoperability to facilitate data sharing across systems; solving privacy issues by using techniques such as secure multi-party computation; user-friendly design interfaces to facilitate broader adoption; and real pilot projects globally to ascertain the viability and performance of blockchain adoption. Through them, blockchain technology will be upgraded and widely utilized during disaster management, leading to the development of more dependable and efficient emergency response systems.

The ability to increase the efficiency, transparency, and dependability of numerous procedures involved in emergency response and recovery operations has been established by utilizing blockchain disaster management technology. Blockchain provides various benefits such as secure data sharing, smart automatic contracts, and decentralized decision-making with decentralized and immutable ledgers. The main uses of blockchain disaster management, as well as supply chain management, resource use, identity validation, and financial transactions, have been investigated and highlighted in this research.

VII. CONCLUSION

By offering a decentralized network where all peers can swiftly authenticate requests, blockchain technology provides an answer to the problems associated with disaster management and emergency preparedness. This makes it easier for the parties concerned to move goods and money quickly. Furthermore, the transparent and unchangeable nature of blockchain guarantees trust and accountability, and smart contracts automate the application of pre-established regulations to guarantee the prompt distribution of resources and services to impacted areas.

REFERENCES

1. Seebacher S, Schüritz R. Blockchain technology as an enabler of service systems: A structured literature review. Lecture Notes in Business Information Processing, Springer Verlag 2017, 12–23.

2. Kamble S, Gunasekaran A, Arha H. Understanding the Blockchain technology adoption in supply chains-Indian context. Int J Prod Res 2019; 57: 2009–2033.

3. Bogucharskov A V, Pokamestov IE, Adamova KR, Tropina ZN. Adoption of Blockchain Technology in Trade Finance Process. 2018.

4. Biswas S, Sharif K, Li F, Nour B, Wang Y. A scalable blockchain framework for secure transactions in IoT. IEEE Internet Things J 2019; 6: 4650–4659.

5. Sobha G V, Sridevi P. Usecase of Blockchain in Disaster Management-A Conceptual View.

6. Bhat VG, Pranaav HP, Mini S, Tosh D. Blockchain-centric Resource Management System for Disaster Response and Relief. 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), IEEE 2021, 540–545.

7. Sobha G V, Sridevi P. Usecase of Blockchain in Disaster Management-A Conceptual View.

8. Wang H, Chen K, Xu D. A maturity model for blockchain adoption. Financial Innovation 2016; 2.

9. Sreelakshmi S, Chandra VSS. Blockchain technology in disaster management: A high-level overview and future research dimensions. In: Blockchain for Industry 4.0: Blockchain for Industry 4.0: Emergence, Challenges, and Opportunities. CRC Press, 2022: 229–243.

10. Sakurai M, Murayama Y. Information technologies and disaster management – Benefits and issues -. Progress in Disaster Science 2 2019.

11. Ølnes S. Beyond Bitcoin enabling smart government using blockchain technology. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Springer Verlag 2016, 253–264.

12. Shrier D, Wu W, Pentland A. Blockchain & Infrastructure (Identity, Data Security). 2016.

13. Zyskind G, Nathan O, Pentland AS. Decentralizing privacy: Using blockchain to protect personal data. Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015, Institute of Electrical and Electronics Engineers Inc. 2015, 180–184.

14. Betti Q, Khoury R, Hallé S, Montreuil B. Improving Hyperconnected Logistics with Blockchains and Smart Contracts. 2019;

15. Ernest Chang S, Chen Y-C, Lu M-F. Supply chain re-engineering using blockchain technology: A case of smart contract-based tracking process.