JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Trust Building With Technology Exploring Blockchain and Smart Contract in Charity

Akhila Menon[1],Asst. Prof. Divya Premchandran[2]

Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India

ABSTRACT

This research delves into the cost-effective utilization of blockchain technology and smart contracts on the Binance Smart Chain to transform and enhance the transparency of distributing charitable funds.In the philanthropic landscape, where ensuring that donated funds serve their intended purpose is paramount, the affordability and efficiency of the Binance Smart Chain offer an ideal platform for creating a transparent and automated system. This innovative system verifies and records each transaction, guaranteeing that funds are allocated exclusively for approved charitable activities, thus mitigating the risk of misallocation or misuse.By harnessing the Binance Smart Chain's cost-efficient capabilities, this study presents a practical solution for bolstering donor confidence, trust, and transparency within the charitable sector. The decentralized and tamper-resistant features of blockchain ensure an immutable and verifiable transaction record, providing stakeholders with instant Consequently, this study adds to the ongoing conversation about utilizing blockchain for societal benefit, underscoring the transformative possibilities of emerging technologies in improving the efficiency of charitable initiatives and fostering a commitment to conscientious philanthropy.

Keywords ---blockchain, smart contract,charity, trust

1. INTRODUCTION

The combination of blockchain technology and smart contracts has become a revolutionary force in the ever-changing field of philanthropy, transforming the fundamental principles of allocating philanthropic funds. The contemporary philanthropic sector faces a pressing need for transparency and accountability, where the efficient deployment of donated funds is paramount. In light of this necessity, blockchain technology emerges as a symbol of creativity, providing a decentralized and tamper-resistant ledger that functions as an unalterable documentation of financial transactions. Complementing this decentralized ledger, smart contracts introduce programmable automation, enabling self-executing agreements that can autonomously verify and enforce the terms of charitable fund allocations.

This study delves into a detailed examination of the intersection among blockchain, smart contracts, and philanthropy, emphasizing the Binance Smart Chain, a platform known for its cost-effectiveness and scalability.The collaboration of blockchain and smart contracts offers an innovative solution to the issues affecting conventional methods of distributing funds in the charitable sector.As the research delves into the intricacies of cost-effective utilization of these technologies, it endeavors to bridge the gap between theoretical concepts and practical implementation. Beyond theoretical constructs, the study envisions a future where philanthropy is liberated from traditional constraints, embracing a new era of trust, efficiency, and accountability It aspires to contribute not only theoretical insights but also a pragmatic blueprint for philanthropic organizations seeking to navigate the complexities of the modern socio-economic landscape. The immutability of smart contracts and the integrity and transparency of blockchain ecosystems inspired a new direction in financial systems such as auctions or banking services based on blockchain[1].

II. WHAT IS BLOCKCHAIN AND SMART CONTRACT?

Blockchain: Blockchain is a decentralized and distributed ledger technology crafted to enable secure and transparent transactions. It functions as a secure and tamper-resistant recording system across a computer network. Essentially, it operates as a sequence of blocks, with each block containing a set of transactions..Transactions on a blockchain involve the transfer of digital assets or information from one participant to another..through the digital money or cryptocurrency know as Bitcoin. This technology ensures trust, transparency, and immutability, making it suitable for various applications beyond cryptocurrencies, such as supply chain management, voting systems, and smart contracts. Immutability: That's of the most effective features of Blockchain in which when a user entered the data then the data can't be tampered by anyone, this can be called as "immutability."[2]

Smart Contract:

A smart contract is a self-executing contract guided by code, featuring explicitly outlined terms.Once predefined conditions are met, it autonomously enforces and executes the terms of the agreement. These contracts operate on blockchain platforms, serving to facilitate, verify, or enforce contract negotiations or performances. Smart contracts are essential components within decentralized applications

(DApps) that operate on blockchain networks.Binance Smart Chain (BSC) and Ethereum exemplify blockchain networks that uphold the functionality of smart contracts.These DApps can include various functionalities such as decentralized finance (DeFi) protocols, non-fungible tokens (NFTs), and more.The term "smart chain" can be used more broadly to describe any blockchain that incorporates smart contract capabilities, allowing for the creation of decentralized and programmable applications.

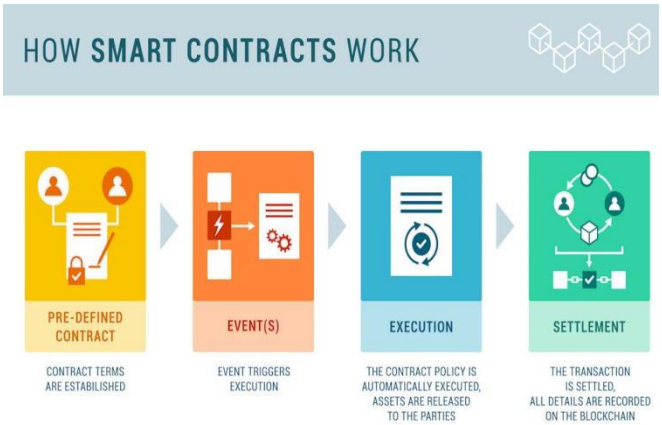

Fig. 1 How smart contract work

III. METHODOLOGY

BINANCE SMART CHAIN

While Ethereum was introduced to address several shortcomings of the original Bitcoin blockchain, it still faces challenges related to block time, scalability, and cost issues. Binance Smart Chain(BSC)was introduced in 2020 after three years of launch of Binance Chain in 2017 by Chapeng Zhao Yi He[14] removing the barriers of Ethereum[3]. Its consensus is based on the PoSA [4] (Proof of Stake and Authority) combining elements of both Proof of Stake (PoS) and Proof of Authority (PoA). Binance Smart Chain (BSC) distinguishes itself through its compatibility with Ethereum dApps, allowing seamless support for smart contracts that are compatible with the Ethereum ecosystem. Binance Smart Chain (BSC) stands out in the blockchain landscape for its remarkable interoperability, notably with Ethereum-based decentralized applications (dApps). This interoperability significantly broadens the horizons for dApps that can seamlessly operate within the BSC network, contributing to the cultivation of a more expansive and diverse ecosystem.

The strength of Binance Smart Chain extends beyond its technical prowess to encompass strategic partnerships and collaborations. Actively participating in ecosystem partnerships, BSC strategically aligns with various entities to fortify its overall functionality. These collaborations introduce additional resources, tools, and functionalities, fostering an environment of continuous development and heightened effectiveness within the BSC network.A key player in the BSC ecosystem is Binance, a globally recognized cryptocurrency exchange. Binance assumes a pivotal role by leveraging its well-established infrastructure and integration points, facilitating frictionless fund transfers between the exchange and the BSC. The dynamic character of BSC is underscored by its commitment to overcoming challenges observed in other blockchain networks, notably Ethereum. Through the embrace of strategic partnerships and the utilization of Binance's robust infrastructure, BSC positions itself as a versatile and interoperable blockchain solution. This adaptability not only broadens its functional capabilities but also enriches the overall user experience, positioning the Binance Smart Chain as an enticing and compelling choice within the swiftly evolving realms of decentralized finance and blockchain technology. In navigating this dynamic landscape, BSC emerges as a frontrunner, embodying adaptability, innovation, and collaborative synergy.

ZERO KNOWLEDGE PROOF

Zero-knowledge proof (ZKP) is an advanced cryptographic method developed to validate the truth of a statement without disclosing any specifics about the information being affirmed. In a zero-knowledge proof exchange, the prover endeavors to persuade the verifier that they have particular knowledge without revealing the exact details.The essence of "zero-knowledge" lies in the fact that the proof reveals nothing beyond the validity of the statement. This ensures that even if the interaction is observed by an external entity, they gain no additional knowledge about the information being proven.ZKP operates on the principle of mathematical protocols that allow the prover to showcase the truthfulness of a claim, such as possession of a password or private key, without exposing the sensitive content.

Fig. 2 Zero-knowledge proof

CROSS-BORDER PHILANTOPHY

Blockchain can streamline the process of currency conversion and fund transfer across borders. Smart contracts could automate the conversion process based on real-time exchange rates, reducing the need for intermediaries and associated fees.Blockchain's decentralized nature and smart contract automation can significantly improve the speed and efficiency of cross-border transactions. This is particularly crucial in times of urgent humanitarian aid or when responding to global crises.Leveraging blockchain guarantees openness in monitoring the transfer of funds from donors to recipients. Each transaction is logged on the blockchain, creating a publicly accessible and unchangeable ledger that illustrates the allocation and utilization of funds. Smart contracts can be coded to release funds only upon meeting specific conditions, ensuring accountability and mitigating the risk of fraud.This openness can aid in building trust with regulatory entities. Blockchain-based decentralized systems have the potential to boost confidence in the distribution of assistance.By removing central authorities and introducing transparency, it becomes easier to verify that aid reaches its intended destinations, especially in regions with potential corruption challenges.Smart contracts can be employed to establish the conditional distribution of assistance. In the current philanthropic landscape, there is an urgent requirement for transparency and accountability, with a focus on the effective utilization of donated funds. In response to this imperative, blockchain technology stands as a beacon of innovation, offering a decentralized and tamper-resistant ledger that serves as an immutable record of financial transactions. Complementing this decentralized ledger, smart contracts introduce programmable automation, enabling self-executing agreements that can autonomously verify and enforce the terms of charitable fund allocations.

IV. CHALLENGES IN TRADITIONAL METHOD

A. Lack of Transparency:

Traditional methods often lack transparency in the allocation and utilization of charitable funds. Donors may not have real-time visibility into how their contributions are being used, leading to a diminished sense of trust.

B. Bureaucratic Inefficiencies:

Conventional philanthropic models are often hindered by bureaucratic processes and intermediaries, resulting in delays and increased administrative costs. The smart contract deployment streamlines the fund allocation process, eliminating unnecessary intermediaries and automating approval procedures.

C. High Administrative Costs:

The involvement of multiple intermediaries, paperwork, and manual verification processes contributes to high administrative costs. This reduces the overall efficiency of charitable activities, with a significant portion of funds allocated to administrative overhead.

D. *Fraud and Mismanagement:*

Centralized systems are susceptible to fraud and mismanagement. Without robust verification mechanisms, funds can be misallocated or diverted for purposes other than the intended charitable activities.

E. Limited Accountability:

Establishing accountability in traditional methods can be challenging due to the involvement of numerous intermediaries. The smart contract deployment creates a transparent and auditable system, enhancing accountability by providing a verifiable record of every transaction.

F. Slow Response to Emergencies:

Conventional approaches may encounter challenges in delivering a prompt and efficient response in times of emergencies or disasters. Bureaucratic hurdles and complex approval processes can impede the quick deployment of resources.

G. Geographical Barriers:

Philanthropic organizations using traditional methods may struggle to reach remote or underserved areas due to logistical challenges. This limits the effectiveness of charitable initiatives in certain regions.

H. Dependency on Intermediaries:

Depending on banks, financial institutions, and other intermediaries introduce dependencies that may result in extra charges, delays, and possible points of failure in the process of allocating funds.

V. PROPOSED SYSTEM

A. OPERATION OF BLOCKCHAIN IN THIS SECTOR

Figure 3 depicts the partial operation specifically focused on the blockchain.

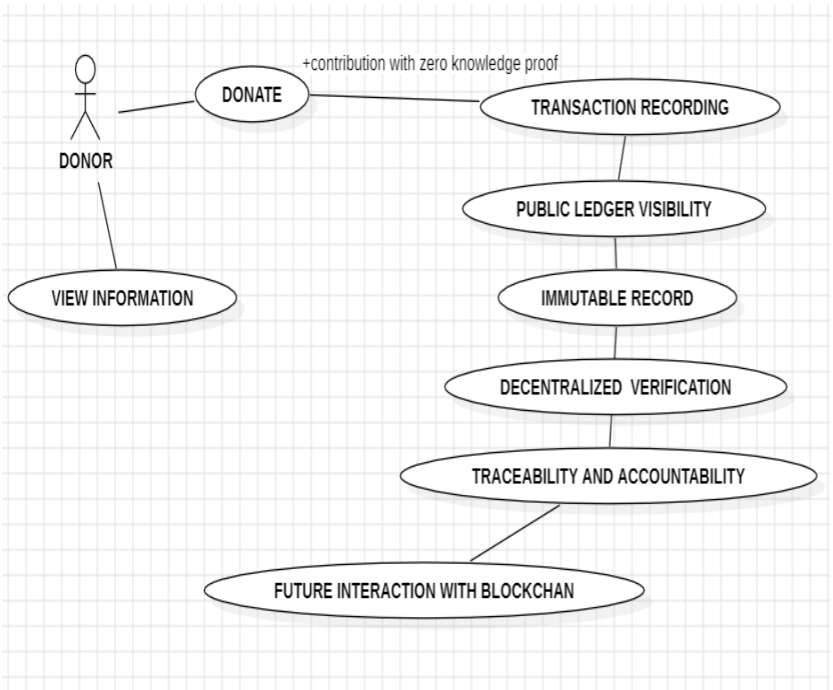

Figure 3

i. Donor Contribution with Zero-Knowledge Proof:

When opting to donate funds, a donor creates a zero-knowledge proof to validate the legitimacy of their contribution. This proof enables them to affirm that they are making a genuine donation without disclosing specific details like the precise amount or the donor's identity.

ii. Confidential Transaction Recording:

The donation, accompanied by the zero-knowledge proof, is recorded on the decentralized ledger of the Binance Smart Chain. This ensures the incorporation of the donation into the transparent and immutable record of the blockchain while preserving the confidentiality of sensitive information.

iii.Selective Public Ledger Visibility:

While the transaction is logged in the public ledger, the use of zero-knowledge proofs enables the donor to selectively choose which information to disclose.

iv. Immutable Record with Confidentiality:

Incorporating zero-knowledge proofs into the transaction procedure guarantees that the documented transaction becomes an indelible component of the blockchain.

v. Decentralized Verification:

Inherent to blockchain technology is its decentralized nature, which facilitates a distributed consensus mechanism. Multiple nodes scattered across the network independently verify and validate the donation transaction.

vi. Traceability and Accountability with Privacy:

The traceability capabilities of blockchain enable stakeholders to follow the fund's journey from donor to recipient. However, the integration of zero-knowledge proofs adds an extra layer of confidentiality, guaranteeing that only crucial information is disclosed for the sake of accountability.

vii. Future Interaction with Blockchain:

As the charitable organization obtains additional donations or participates in fund allocation tasks, each interaction with the blockchain adheres to a comparable sequence involving recording, verification, and transparency.

B. OPERATION OF SMART CONTRACT IN THIS SECTOR

Figure 4 shows the functionality of the smart contract

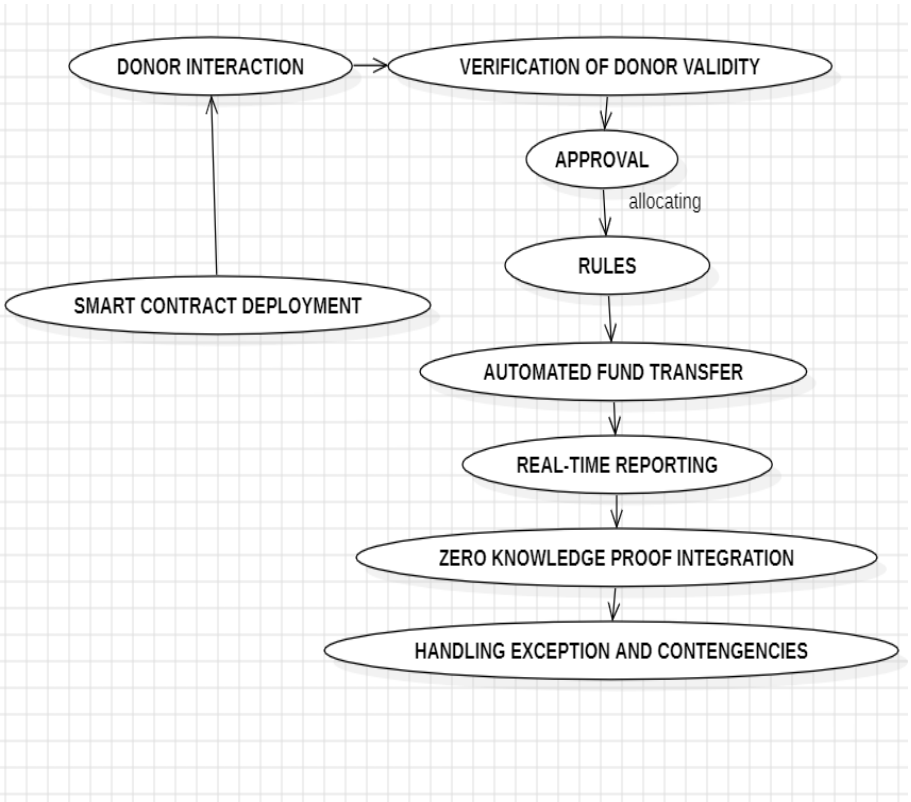

Figure 4

i. Smart Contract Deployment:

In the intricate domain of charitable giving, initiating a smart contract on the Binance Smart Chain signifies a crucial and foundational stride towards establishing a transparent and effective fund management system for philanthropic organizations.

ii. Donor Interaction with Smart Contract:

Upon the donor's contribution of funds, the smart contract becomes operational, commencing an interactive engagement with the donor. This engagement triggers the execution of predefined functions encoded within the smart contract, streamlining the entire process and laying the foundation for a seamless fund allocation journey.

iii. Verification of Donation Validity:

The smart contract performs a critical role in scrutinizing the validity of the donation. Leveraging the information stored on the blockchain, it meticulously validates the donation, cross-referencing details with any zero-knowledge proof employed during the donation process.

iv. Allocation Rules Execution:

Upon approval, the smart contract independently carries out the guidelines for distributing funds. This could involve dividing the funds among specific charitable activities, projects, or beneficiaries based on predefined criteria.

v. Automated Fund Transfer:

Once the allocation rules are diligently applied and approved, the smart contract takes the helm in initiating seamless fund transfers. Funds are efficiently transferred to the precisely identified recipients or addresses linked to approved charitable activities.

vi. Real-Time Reporting:

The smart contract, serving as a dynamic and real-time recorder, consistently updates the blockchain ledger. An overarching view of the advancements in charitable endeavors is available to donors and stakeholders.

vii. Zero Knowledge Proof Integration:

When there is a need for heightened privacy by integrating zero-knowledge proofs into the donation process, the smart contract is meticulously crafted to smoothly integrate these proofs.

Viii. Handling Exceptions and Contingencies:

The smart contract is crafted to manage exceptions or unexpected events, ensuring that in the event of unforeseen circumstances, the fund allocation process can adjust and handle these situations transparently.

VI. CHALLENGES IN BLOCKCHAIN

1. Scalability: Blockchain networks, particularly those that are public, may encounter difficulties related to scalability.
As the volume of transactions rises, the duration and resources necessary for achieving consensus can affect the overall performance of the system.

2. Energy Consumption: Numerous blockchain networks, particularly those employing proof-of-work consensus mechanisms like Bitcoin and Ethereum, demand substantial computational resources, resulting in heightened energy consumption and triggering environmental apprehensions.

3. Block size: The maximum size for each block is one megabyte which can accommodate 2,200 transactions. Increasing block size is currently under discussion but so far no final decision has been reached[5].

4. Cryptography: Use of cryptographic tools is still incipient and the average Internet user cannot be expected to embrace its use in the short term[6].

5. Cost of Implementation: Implementing and maintaining blockchain networks can be expensive. The initial expenses, covering hardware, software, and skilled personnel, may pose a hurdle for smaller organizations.

6. Complexity and Understanding: Blockchain technology involves complex cryptographic principles, consensus algorithms, and decentralized structures. Understanding these aspects can be challenging for non-technical users, hindering widespread adoption.

7. Lack of Regulation: The absence of consistent regulations and standards in the blockchain industry can result in difficulties related to legal and compliance matters..This could impact the adoption of blockchain technology in particular industries and regions.

8. Bandwidth: Full nodes that want to be active in the network must have access to the right Internet bandwidth. Slow, unreliable connections are not welcome, especially when the current size of the blockchain is over 120 Gigabytes[7].

9. Slow Transaction Speed:
The duration needed to achieve consensus and append a block to the blockchain can result in decreased transaction speeds, particularly in times of elevated network activity. This can be a limitation in applications requiring real-time processing.

CONCLUSION

In summary, the utilization of blockchain technology and smart contracts on the Binance Smart Chain for the allocation of charitable funds emerges as a revolutionary solution. The Binance Smart Chain's cost-effectiveness and efficiency create an ideal environment for establishing a transparent and automated system, ensuring donated funds are utilized exclusively for approved charitable activities. This approach not only addresses the paramount need for accountability but also enhances donor confidence, trust, and transparency within the philanthropic sector. The collaboration between blockchain technology, smart contracts, and the Binance Smart Chain sets a

precedent for the future of overseeing charitable funds, emphasizing efficiency, security, and reliability. As advancements in technology persist in shaping the philanthropic landscape, the suggested model serves as a guiding light, utilizing innovation to generate positive outcomes.The openness, security, and decentralized characteristics of this solution not only address current challenges but also establish the foundation for a more responsible and reliable charitable ecosystem. Adopting these innovations empowers the charitable sector to reimagine its methodologies, ushering in a fresh era of thoughtful and impactful philanthropy.

REFERENCES :

[1] Menelaos Kokaras a, Magda Foti b -The cost of privacy on blockchain: A study on sealed-bid auction

[2] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang -An Overview of Blockchain Technology: Architecture, Consensus, and Future Trend

[3] Suhasini Monga & Dilbag Singh - MRBSChain a novel scalable medical records binance smart chain framework enabling a paradigm shift in medical records management

[4] Federico Cernera , Massimo La Morgia, Alessandro Mei - Token Spammers, Rug Pulls, and SniperBots: An Analysis of the Ecosystem of Tokens in Ethereum and the Binance Smart Chain (BNB)

[5] Iuon-Chang L., Tzu-Chun L., 2017, " A Survey of Blockchain Security Issues and Challenges

[6]Satarupa Saha1 , Jayanta Poray2 , Bappaditya Jana3 - Study on Blockchain Technology

[7] Roger W., Christian D., Conrad B., 2017 - Scalable Funding of Blockchain Micropayment Channel Networks