IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96114

Transaction transparency using Block chain

Yashaswini BR[1], Prof. Rajeshwari N[2]

[1]Dept. of MCA Bangalore Institution of Technology, Bengaluru , India.

[2]Dept. Of MCA, Assistant Professor, Bangalore Institute of Technology, India.

Abstract: Due to the Covid-19 epidemic, there has been a greater-than-ever rise in entrepreneurship. Even though some of the pandemic-era firms failed due to investor withdrawals that scared the economy since startups are seen as sources of employment development, innovation, and economic robustness. Many e-commerce Businesses emerged and also use online transactions because they are convenient, affordable, and quick. when it comes to raising capital for startups and new businesses have gained preference. The number of bitcoin transactions increased in 2021, indicating that the use of blockchain data platforms for digital asset trading is becoming more widespread. Blockchain technology offers solutions to risks with online cryptocurrency transactions related to decentralized finance, security, money laundering, traceability, scams, and illegal transactions. When combined with blockchain technology, we present a framework that can offer a fix for transaction transparency and safety problems. This project involves a crowdfunding and blockchain-based startup fund-raising application. where investors may follow their investments across different startups. Decentralized, unchangeable, transparent, and traceable are all characteristics of blockchain. distributed database system made up of several independent nodes connected using peer-to-peer technology. It keeps track of all transaction details, has an effective and transparent workflow, and highly secure data.

1. INTRODUCTION

A startup's inability to develop can be caused by a variety of factors, but one of the main ones is finance. The entrepreneur must know the precise amount of money they need, as well as their company plan, leadership style, and other factors. It's a win-win situation when business networking of increases and if startup income grows investor or shareholder net worth increases. But raising money is a difficult process that necessitates confidence between a number of stakeholders, including funders, middlemen, and organisations that act as a repository for temporary funding for recipients. In order to entice investors to provide money to fund beneficiaries, fundraising primarily rely on this trust.

By using blockchain technology to analyse the procedures often found in fundraising platforms, it may be possible to boost funders' trust, which might have an impact on how much money companies are able to raise. this money as well as smart contract technology that enables startup business owners to easily obtain these funds if all requirements are satisfied. The use of blockchain technology not only fosters trust but can also be utilised by investors as verification that money are coming from reputable sources, as well as to verify cryptocurrency funds and the reliability of companies.

[1]The principle of crowdfunding simply entails pitching a business idea to a certain group of people online and persuading them to donate a fixed amount of money apiece in order to raise the necessary capital to make the idea a reality. This means that a project's ability to attract investors may depend on how lucrative it seems. Crowdfunding can take many different forms. Investors can lend money to businesses and expect to get their principal and interest back over time.Investors can exchange their money for shareholder status, which entitles them to dividends and voting rights. Investors can also choose to give money simply without expecting anything in return.possible difficulties with crowdfunding If investor concerns are not protected by law, illicit activities may become the norm as a result of improper administration of regulations. Any financial choice must account for information asymmetry, and the security of participating in a crowd contract may be hampered by inaccurate information about the credit ratings of fundraisers and a lack of a clear description of investors' rights. How do we safeguard shareholders' interests? How can we stop unlawful enterprises from using a crowdfunding contract to raise money? The market for crowdfunding is expanding quickly, thus it is important to consider the security of the transactions that take place there.

[2]Currently most of e-commerce businesses have relied on banks to act as reliable third parties in the processing of digital payments. The trust-based model's underlying flaws are still present in the system, despite the fact it functions adequately for the majority of transactions. if transactions are completely irreversible are not actually feasible since banks must mediate disagreements. A larger cost is the loss of capacity to make non-reversible payments for non-reversible services. The cost of mediation raises transaction costs, lowering the minimum practicable transaction size. The requirement for trust grows as a result of the likelihood of reversal. Merchants must be predetermined proportion of fraud hence a blockchain technology is best suited approach to avoid third parties in process of payments. Blockchain technology enables any two parties to do business directly with one another without the requirement of a trustworthy third party, which is essential for a system of online payments based on cryptographic evidence rather than trust. Transactions that are computationally challenging to reverse would shield company against fraud. In this paper, solution to the double-

spending issue using a p2p distributed server to generate computational verification of the chronological sequence of transactions. The system is secure as long as the legite nodes collectively control more computing power than any collection of attacker nodes.[3]The major goal of the blockchain is to solve the ever-growing issues, particularly with trust. Blockchains are distributed ledgers that can withstand harm when applied. Blockchain is a global ledger of all completed transactions that is shared with all participants and is stored in a distributed database that is confirmed by a majority of the system's consensus. Additionally, information entered cannot be erased. Every transaction that has ever been made is recorded on the blockchain and can be confirmed. Blockchain is a global database of transaction records that is distributed, verified, and maintained by computer networks.

Since Bitcoin and Ethereum are some of the most popular decentralised digital currency. The majority of the market capitalisation for cryptocurrencies is made up of these two currencies. By using our proposed system, companies may obtain funding from a variety of investors using their cryptocurrency wallet with Bitcoin and Ethereum coins, and the investors can keep track of the money they have invested in companies.

2. RELATED WORK

[4]Although the concept of digital money is not brand-new, it has only lately been put into practice with success. According to Chaum's article, public key cryptography may be used to create electronic mail, return addresses, and digital pseudonyms that are untraceable. His method didn't need a reliable third party, and correspondents could remain anonymous. Public key cryptography was also used by Law et al. to propose the notion of digital money, but their model was designed to be used in conjunction with financial institutions acting as central trust authorities.

[5]This paper proposed system a decentralized resource sharing system . They dealt with the issue of P2P network blocks that consume more network resources than they produce. A blocks karma is raised with each contributions , and it is lowered with each consummation. The records of each block's karma are kept by a group of blocks. These methods, meanwhile, either necessitated the use of banks as a reliable third party or fell short of fully resolving the issue of double spending. In a centralised solution, banks or other reliable authorities can stop attempts to issue two transactions in tandem, but in a decentralised system, like a cryptocurrency, this issue is very significant. Additionally, because there is no central authority, In order to prevent potential attackers from compromising the system with fake data, users must keep the P2P network in a consistent condition.

[6]This paper describes how blockchain technology enhances productivity and fosters trust in the startup funding process, both of which have an impact on today's businesses and sectors. It is addressed how to create a block chain-based distributed ledger that is decentralised and records transactions or other events related to startup funding. Startups are having trouble finding the necessary funding. Entrepreneurs who want to start new firms or grow existing ones have access to a variety of funding sources, including family, bank loans, the internet, online crowd fundraising platforms, and many more. The key issue, however, is how to monitor money and ensure that it is properly distributed, used, and tracked. With the use of blockchain technology, this suggested approach could be able to address the problems with crowd funding contracts. This project aims to provide a solution to the problems of security, investor abuse, and unauthorised transactions in the crowdfunding process. The proposed system is employ Ethereum-based smart contracts to manage connections between fundraisers, vendors, and the project manager or idea person in a safe and efficient manner. Blockchain-enabled, distributed platforms are used to prevent fraud, monitor funds received from various contributors, and distribute them fairly. The suggested solution would address these issues by utilising blockchain technology to establish confidence and see proper money distribution by developing smart contracts for utilising the funds collected by the people. Blockchain technology offers a more affordable, simple, secure, and practical way to transmit information provide the solution to all crowdfunding problem.

This article outlines research needs in the fields of Economics and Finance for two FinTech applications: crowdfunding and blockchain. These analysis reveals that current FinTech research is fragmented and lacks theoretical underpinning; (ii) crowdfunding and blockchain can be seen as two innovations that may disrupt traditional financial intermediation, though in different ways; (iii) crowdfunding platforms act as both a new intermediary and a replacement for traditional financial intermediaries, without doing away with the need for intermediation, Blockchain-enabled, distributed platforms are used to prevent fraud, as well as to monitor the appropriate usage and distribution of funds received by various contributors.

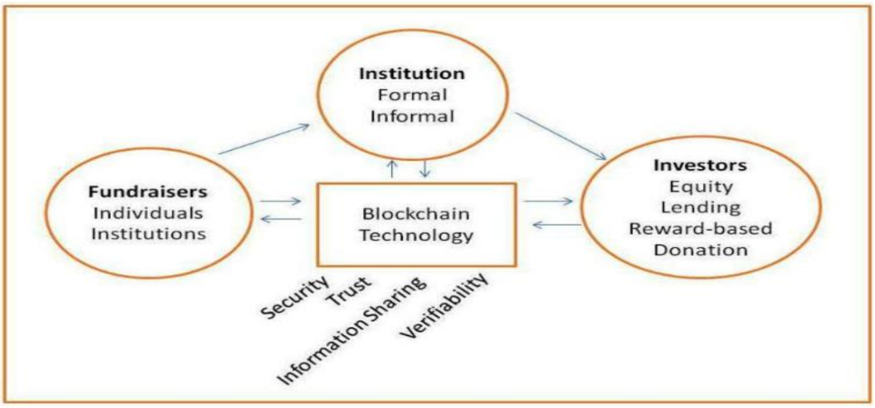
[7] The paper's focus is on how cryptocurrencies will impact the banking industry and other industries through the blockchain technology platform. the impact of modern technology on industry, particularly financial processes. The core assumption of the argument is that blockchain has significantly impacted the financial industry and has the potential to profoundly change not only that sector but also how we buy and sell items. Utilizing the information that is now available and the synthesis of knowledge from the fields of technology, economics, finance, and politics. The scenario approach is combined with trend analysis, which highly confidently supported the basic assumption. The study's findings show that the technology being studied, blockchain, is already having a big influence on There is a strong likelihood that these

changes will become significant during the following five to ten years in the financial industry and that it is only now starting to affect a number of other businesses.

[8]Crowdfunding is a method of getting funds from investors to finance start-up businesses. Various crowdfunding sites like Kickstarter are available to facilitate crowdsourcing. A easy method of getting investors to contribute money to companies is through crowdfunding websites. The main drawback of traditional crowdfunding platforms is that users must pay a small portion of their donations to the sites as convenience charges. the Users must pay a platform transaction charges to the processors in addition to the convenience charges. In this work, we suggest a decentralised and secure blockchain-based crowdfunding system. The suggested crowdfunding technique does away with the necessity for current crowdfunding platforms, which cost business owners money in the form of convenience charges. The suggested approach offers an irreversible log of transactions between investors and entrepreneurs and enables entrepreneurs to utilise the full amount of money collected from investors.

3. METHODOLOGY

The literature review technique was employed in this work. In order for them to be utilized as references from this writing, this work draws on sources from journals that have been published both worldwide and domestically as well as additional pertinent articles. The basic basis for the blockchain-based crowdfunding system is further explained in the figure below. To understand the possible uses of blockchain technology in the execution of crowdfunding contracts, take into account the existing research on both crowdfunding and blockchain technology. We divide investors into four types, take into consideration the fact that fundraisers may be either individuals or companies, and demonstrate how getting rid of institutions (such as crowdfunding platforms) and replacing them with blockchain technology may boost productivity and ensure security.



[9]Blockchain technology might eventually totally replace the job of trusted third party as a result of the inclusion of crowdfunding contracts. crowdfunding Contracts can be carried out instantly online.The use of blockchain technology in crowdfunding might serve as the foundational technology to address the majority of the apparent difficulties associated with executing crowdfunding contracts

Under a typical Crowdfunding contract, funders are people or organizations searching for a simple, low-cost approach to generate money to assist their enterprises. There are a variety of financing options available for fundraisers to choose from in order to finance their operations, but the majority prefer to use crowdsourcing because of the relatively cheap transaction costs associated with it. Fundraisers in a startups ideas would require institutional approval before being implemented and an Etherum blockchain-based framework would. Utilizing block chain technology that platforms may keep track of information like business registration capital raising and retail record keeping for the company. Of the fundraisers and , making this information easily available to investors. our system is bound by a crowdfunding agreement are responsible for serving as the trusted participants between fundraisers and investors. our website act as a middleman to prevent investment fraud and maintain confidence between the investors and startups. The website engage in a number of activities to ensure the fundraising campaign is successful Maintaining confidence and offering investor safety is the system's most important issue in this situation, and difficult. In a Etherum block chain-based Crowdfunding, the technology is known as a trusted machine, which may help the Crowdfunding sites in to maintain the safety and security of the contracts.

There are several reasons why investors donate their money, but it should be noted that they do not want to be taken for granted. In the case of crowdfunding, some investors may donate without anticipating any kind of reward. They want to be certain that their investment is in a legitimate company that fits the description given on the platforms. Investors desire security and safety for their capital and will not put money into a company that where they can't withdraw it back.

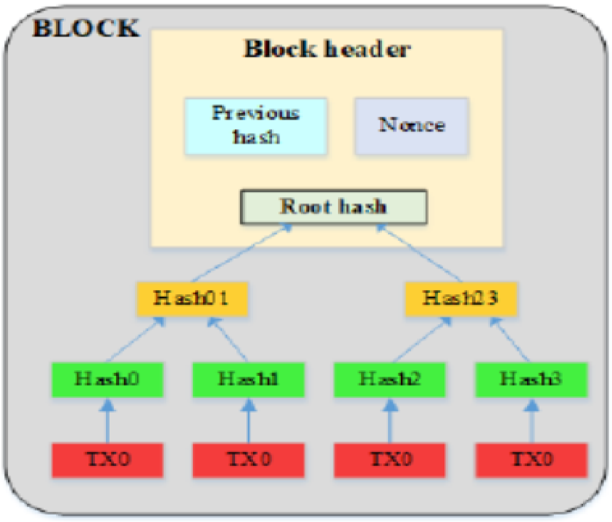
DOI: 10.17148/IARJSET.2022.96114

Blockchain-based crowdfunding will guarantee transperency and information regarding funds to investors in making wise selections.

4.Mathematical Model:

[5]By requiring each node to validate the transaction, any Sybil attack may be stopped on the Bitcoin network. To demonstrate that they are legitimate network members, the nodes must do certain demanding computations. All legal transactions will take place as long as our nodes' combined processing power exceeds that of the attacker nodes, keeping the system stable. A block is declared by a collection of transactions, the preceding block's hash, and a nonce. A timestamp server hashes a block and publishes the result, demonstrating that the information inside the block must have been there at the moment of hashing. The timestamp server must confirm that the block's timestamp is less than two hours in the future and higher than the timestamp of the block before it in the chain. the chain of these hashes is referred to as a blockchain. The ability to trace transactions back to any point in history is a key feature of the blockchain.

Bitcoin utilises hashing algorithm based on the SHA-256 hash function. By increasing a nonce in the block until a value is obtained that contains the necessary quantity of zero bits at the beginning of the block hash, the proof-of-work is carried out. Once completed, it cannot be undone without carrying out the calculations again. Every block after that would contain incorrect hashes if it were altered in some way by an evil attacker. According to the rule, the longest chain with the greatest amount of network consensus is the right one. If an attacker wants to modify a block, he must have sufficient computing power to override the votes of the vast majority of trustworthy nodes. therefore contributing to the racial issue. In a Merkle tree, the transactions included in a block are hashed. A Merkle tree is a particular kind of binary tree with several leaf nodes, each of which has a root that is a hash of its descendents. A Merkle tree of transaction hashes made up a Bitcoin block. The Merkle tree is essential for long-term maintainability since any irregularity in the tree will manifest itself somewhere along the chain.Make room on the nodes' storage systems for the blockchain. The Bitcoin blockchain is currently 144.8 GB in size. after a block containing the transactions has been created and validated. Simplified Payment Verification (SPV), which simply requires the nodes to retain a copy of the block headers from the longest chain rather than a complete record of transactions.



A Bitcoin block with hashed transactions into a Merkle tree

Cryptocurrency network :A new cryptocoin that belongs to the block's inventor is created in the first transaction of every block. Due to the lack of a central authority issuing cryptocoin, this encourages nodes to verify transactions and put A coinbase transaction into circulation and disbrituton. The nodes have an to maintain their integrity in this model. One block should be generated by the Bitcoin network every 10 minutes or so. By progressively increasing the complexity producing new blocks, block time is kept about constant as computer power rises over time.

At the beginning of the Etherum blockchain network, new transactions are broadcast to all nodes. Every node compiles transactions into a block, searches for proof-of-work, and then broadcasts the block to the network. Only if all of the transactions included inside the block are accurate and have not yet been spent will the network nodes consider it as genuine. The chain is continued by producing the next block and adding the hash of the previously added block to it if the block is approved by the network.

The nodes are compensated with coins and by confirming transactions in addition to the payout based on block generation. Mining is the process of creating new blocks for the blockchain. The genesis block, which is the first block on the blockchain, is used to give the network its first set of currencies. Up until the reward drops, the block creation reward will continue to be cut in half. When considering distributed decentralised systems, there are instances in which many nodes broadcast the same block practically simultaneously with likely distinct sets of transactions. This circumstance, known as a fork, causes the network to be inconsistent. In essence, a number of chains have their roots in permissionless blockchain. The network responds to this circumstance in the same manner that it does every time. The problem is handled by ensuring that the longest chain in the network always continues. The proper path for the blockchain will eventually come to the network's agreement, and any chains created as a consequence of a fork will be invalid.

4. CONCLUSION

Our proposed application of Blockchain technology to raise capital for business and Blockchain technology is a sign of the potential to address most human-related issues with trust and security. The development of blockchain technology, which operates on a trust-free basis with minimum involvement from people, might provide a response to the request for investor safety and security in Crowdfunding smart contracts. The use of blockchain technology in crowdfunding smart contracts might offer the much-needed answer to the problems that crowdfunding contracts face in terms of abuse, trust, and secrecy. Blockchain technology offers a more affordable, simple, secure, and practical method for information sharing and money transfers. The system is programmable and, if necessary, may be expanded to accommodate any further enchancements in the smart contract. Future application of the technology might allow for the execution of smart contracts without the need for institutional platforms, even if it is presently possible to change the function of system.

5. ACKNOWLEDGEMENT

We would like to express our gratitude to Bangalore Institute of Technology's Department of Masters in Computer Application for allowing us to conduct this study. We also thank our professor **Rajeshwari N** for being ready to help us during this entire study process.

REFERENCES

[1]. Electronic copy available at: https://ssrn.com/abstract=3133176 1 The Applications of Blockchain Technology in Crowdfunding Contract
[2].Satoshi Nakamoto ,"Bitcoin: A Peer-to-Peer Elec-tronic Cash System" satoshin@gmx.com www.bitcoin.org
[3]. "Smart Contract and Blockchain for Crowdfunding Platform" Firmansyah Ashari, Tetuko Catonsukmoro, Wilyu Mahendra Bad, Sfenranto, Gunawan Wang
[4].D. Chaum, "Untraceable electronic main, return addresses, and digital pseudonyms," in Communications of the ACM, vol. 24, no. 2, pp. 84-88, February 1981
[5].Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview Dejan Vujičić, Dijana Jagodić, Siniša Ranđić Faculty of Technical Sciences in Čačak University of Kragujevac Čačak, Serbia
[6]. Ethereum Blockchain based smart contract for Secured transactions between Founders/Entrepreneurs and Contributors under Start-up Projects
[7].Disruption of financial intermediation by FinTech: areview on crowdfunding and blockchain
[8]. "Secure and Decentralized Crowdfunding Mechanism Based on Blockchain Technology",swati Kumari,Keyur parmar
[9]." The Application of Blockchain Technology in Crowdfunding Contract" - Hongjiang Zhao, Cephas Paa Kwasi Coffie