International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT1206233

Crowdfunding Using Blockchain

K. Bhavya Sri*, J. S. Supriya, M. Pranathi Sai, P. Siva Prasad

Computer Science and Engineering, Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India

ABSTRACT

Crowd funding is the practice of raising money from large number of individuals for the purpose of financing a project, venture, business or cause. Conventionally, crowdfunding has been carried out via events and door-to door fundraising. However there are lot of risk features like security of your business idea, developing a successful crowd funding campaign is an effort and time consuming. Crowd funding is not a charity, fees charged, risk of failure etc. Here comes the role of blockchain to nullify the potential risks of the conventional method of fundraising. A decentralized approach to crowd funding allows us to eliminate all the potential risks faced by the conventional approach of crowdfunding.

Keywords : Bitcoin, Blockchain, Hashing, Smart contracts, Digital Tokens, Consensus, Mining, Digital Signatures, Ethereum.

I. INTRODUCTION

Bitcoin is most popular type of decentralized digital currency also known as crypto currency that was first created by Satoshi Nakamoto. It was launched with the intention to bypass the centralized nature of government concurrency controls and simplify online transactions without the need for third party payment processing intermediaries. Blockchain and bitcoin are not the same. However there are closely related.

Bitcoin ⟵ Blockchain.

People often used bitcoin to mean blockchain but it was not true. Blockchain is the underlying technology that maintains the bitcoin transaction ledger. In simple terms we can say bitcoin is an application of blockchain.

II. BLOCKCHAIN

Blockchain is an incorruptible distributed public ledger. Also blockchain is a chain of blocks that contain information which cannot be backdated or tampered and acts as a permanent database. The blockchain is used for the safe and secure transfer of items like money, property, contracts, etc. without requiring third party intermediaries. Each block contains all the information and data about one transaction, a hash. There three main features of blockchain technology [1][9].

- ✓ Scalability
- ✓ Decentralization
- ✓ Security

Scalability is required for the Blockchain technology to gain abroad adoption. Decentralization is necessary to cut costs (Third party intermediaries) and build trust. Security is the most vital concept, and without it, the technology would be unusable. The other two

important aspects of blockchain are miners, users. Firstly, without miners and good mining algorithms, there will not exist a technology called blockchain. Secondly, technology developed needs user who make use of the offerings of the tech. Hence to make blockchain a sustainable technology, it has to cater to different users and different needs.

A. BLOCK

Block can be thought as a page in ledger. Each block is composed of various components and roughly these can be divided into the block header and block body.

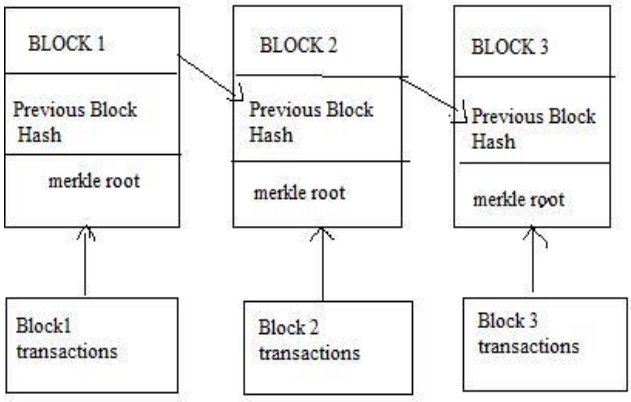

Figure 1 : Blockchain Architecture

1) Version: The block version number. This can signal which protocol to be supported by the miner according to his version number.

2) Time: A timestamp in the block itself. The time is given in seconds.

3) Hash of block: Hash of the previous block is contained in the hash of the new block, the blocks of the blockchain all build on each other. This component helps in maintaining connection and chronology between each block.

4) Hash of Merkle: All transactions in a block can be aggregated in to a hash. This is termed to be the root hash for the merkle tree.

5) Nonce: Nonce is a variable incremented by the proof of work. In this way, the miner guesses a valid hash, a hash that is smaller than the difficult target.

III. TYPES OF BLOCKCHAIN

A) Public blockchains: Public blockchains are open source and allow anyone to participate in the network including users, miners, developers and others. The transactions taking place in this network are fully transparent and anyone can view the transaction related details. Bitcoin and ethereum are the instances of public blockchains.

B) Private Blockchains: Not everyone can gain access to participate in this network. Participants need permission or consent to join the network and only they can make transactions or view any details. The instances of private blockchains are hyper ledger and Quorum.

3) Hybrid blockchain: Hybrid blockchain offers the benefits of both private and public blockchain. It combines the permission consent feature of private blockchain with the security and transparency features of the public

blockchain. It provides flexibility to the businesses/organizations to keep their data public/ transparent or private according to their choice.

IV. HASHING

Hashing is a process in which an input string of variable length is given to the hash function which produces an output of a fixed length. In the context of cryptocurrencies like Bitcoin, the transactions are taken as input and run through a hashing algorithm (mostly uses SHA-256) which gives an output of a fixed length [4].

Cryptographic hash functions:

A Cryptographic hash function is a different class of hash functions that has various useful properties which enhances cryptography [5][6].

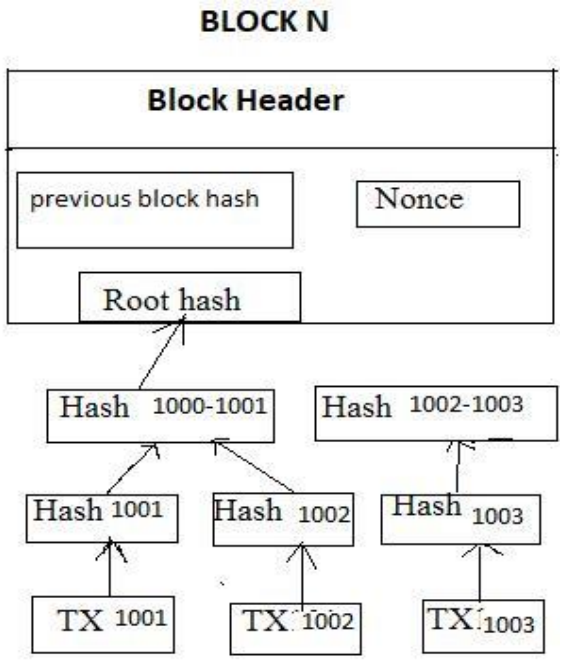

Figure 2 : Block Structure

Properties of cryptographic hash functions are:

Property 1: Deterministic

This property plays a vital role in hashing and make sure that no matter how many times you parse a given input through a hash function, always get the same result. This is crucial because if you get different hashes every single time it will be impossible to keep track of the input.

Property 2: Quick Computation

The hash function must be able to return the hash of input quickly. If the process is not fast enough then the system won't be efficient.

Property 3: Pre-Image Resistance

Pre-image resistance property states that for a given Hash

(A) it is impossible to determine A, where A is the given input and Hash (A) is the output hash value. It is well known that it's impossible to determine the original input from the hash value.

Property 4: Change in input Changes the hash

Even the change in your input is a minor one the changes that will be reflected in the hash will be huge.

Property 5: Collision Resistant

Consider two inputs A and B where Hash (A) and Hash (B) are their respective hashes values, it is impossible for Hash

(A) to be equal to Hash (B). No two hash values will be same that means for each input will have its own unique hash.

V. SMART CONTRACTS

A smart contract is defined as an agreement between buyer and seller being directly written into lines of code. These agreements therein exist across a decentralized, distributed blockchain network. These lines of code in the agreement control the execution and keep track of the transactions. Smart contracts allow trusted transactions and agreements to be carried out among various anonymous parties without the need for a third party intermediaries, legal system, central authority or external enforcement mechanism. The most familiar primary benefits of smart contract are firstly Independence- You don't have to depend on intermediaries. This cuts cost, increases efficiency, and prevents fraud from a third party. Because smart contracts are decentralized. Secondly Trust- There is no need to trust an individual; all you have to trust is the system. Thirdly Security- This ties in with trust. Blockchain is decentralized- there is no possibility of an attack. For a thief to just hack into your bank account, they would have to take over 51% of the network in order to control anything. Smart contracts, which are encoded into blockchain, are just secure or accurate- they are fast. And it is not just because it

removes wait times for lawyers and notaries. It is completely automated process [2].

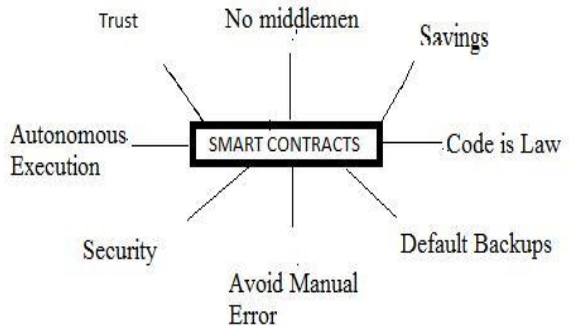

Figure 3 : Smart Contracts

VI. CONSENSUS

A consensus mechanism is defined as a fault-tolerant methodology that is used in blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems, such as cryptocurrencies. It is useful in maintaining of records, of variety of things. There are various kinds of consensus algorithms which work on different principles. The proof of work (POW) is the most popular consensus algorithm used by the most popular cryptocurrency networks like bitcoin and litecoin. It requires a particular node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain. However, this whole mining mechanisms of bitcoin needs high energy consumption and longer processing time [9].

The proof of stake (POS) is another familiar consensus algorithm that evolved as a low cost, low energy consuming alternative to POW algorithm. It allocates responsibility in maintaining the public ledger to a participant node in proportion to the number of virtual currency tokens held by it.

Proof of Capacity (POC) is a consensus algorithm which allows sharing of memory space of the contributing nodes on the blockchain network. The more hard disk or memory space a node has the more rights are granted for maintaining the public ledger.

VII. DIGITAL TOKENS

A digital token is defined as a unit of cryptographic information that is useful for felicitating a real-world transaction. The transaction can be anything from an online money transfer to subscribing from an online money transfer to subscribing to a service. Ethereum and bitcoin

are two blockchains that offer digital tokens. You can use Bitcoin as digital money whereas ethereum is ETH token has several developmental use cases. There are mainly two types of digital tokens one is security tokens and other is the utility tokens.

A. Security Tokens: Security tokens are same with an investment contract, which implies security tokens represent shares in a company, earning streams, an entitlement to dividends or interest payments

B. Utility Tokens: utility tokens provide access to a company's product or service. They are not regulated, and are not investments. These tokens are independent of jurisdictional intervention and only applicable inside the company ecosystem.

VIII. DIGITAL SIGNATURE

A digital signature is defined as an assurance scheme for presenting the authenticity of digital messages or documents. A valid digital signature make a recipient to believe that the message was originated from a genuine source(sender authentication), that the sender cannot deny having the sent the message technically called non-repudiation, and that the message was not altered which ensures integrity. Digital signatures embody asymmetric cryptography technique which is also termed as public key cryptography (PKI), uses both public and private keys to encrypt and decrypt data [7].

Working of digital signatures:

- ✓ Generate the hash of the data

- ✓ Produce the digital signature
- ✓ Sent to recipient
- ✓ Receiver checks the hash generated by the sender
- ✓ Regenerate the hash value from the data and match with hash sent by the sender.

Also, the receiver makes use of the same hash function to generate the hash value of the original content. If this newly generated hash matches with the hash sent from the sender, and then the receiver gets the assurance that the digital signature is valid.

IX. MINING

Mining is the mechanism that allows the blockchain to be a decentralizes security. It secures and enables a bitcoin system without a central authority. Miners validate new transactions and record them on the public ledger. Miners always compete to solve a complex mathematical problem based on a cryptographic hashing algorithm. The solution identified is called PROOF-OF-WORK [3].

X. ETHEREUM

Ethereum is an open source, distributed and decentralized public block chain network that helps users to create and run various decentralized applications. Ethereum is a distributed computing platform that enables the development of smart contracts for decentralized applications, also known as Dapps (Decentralized Applications). Ethereum uses ether a decentralized digital currency, also known as ETH. Ether is paving the way for a more intelligent decentralized financial platform. A smart contract is auto-executing, programmed agreement between buyer and seller that is recorded on the ethereum blockchain. In the ethereum, miners work to earn ether, a type of crypto token that fuels the network. Ether is used by developers to pay for transaction costs and services on the ethereum network. Ganache is a personal Ethereum blockchain for testing your solidity contracts. It mimics the nature of a real ethereum network, including the availability of a number of accounts funded with test Ether.

XI. Proposed Blockchain crowd funding System

To avoid the existing problems like centralized system, private ledger, hacking, double spending, transactional fee of current crowd funding system we have developed a crowdfunding system using following. Our crowdfunding system contains following Decentralized features depicted as follows.

A. Public access of ledger:

The transaction that is recorded are made available to everyone and they can see all the transaction history on the etherscan there can be no manipulation.

B. Hacking:

The transactions that are made are immutable so they cannot be hacked. To change a transaction they need large computational resource to change single transaction which is costly than the transaction itself.

C. Double Spending:

Double Spending can be avoided in the block chain because before a transaction is added to the block the entire history of the money is checked. Double spending is not allowed because of basic structure of block chain itself.

D. Transaction fee:

By using the block chain there will be minimal or no transaction fee for the transaction.

By considering above benefits we have developed a crowdfunding system using the block chain where there will be different ideas listed and funds to be gathered. Different projects are created by projected initiators who want to finance their idea. The funder can login to the system if he has already a metamask account in the system otherwise he has to create one. After login to the system the user can select a project after viewing its details and current status. Then the funder can start funding to his interested project in the list and amount (ethers) to be transferred along with the ethereum account address. We used ethereum platform for developing the crowd funding system using blockchain. The user can transfer funds in ethers. If the project status is expired then there is a refund to all the contributors. All the transactions and funds of an organization are available to all because block chain is a public ledger.

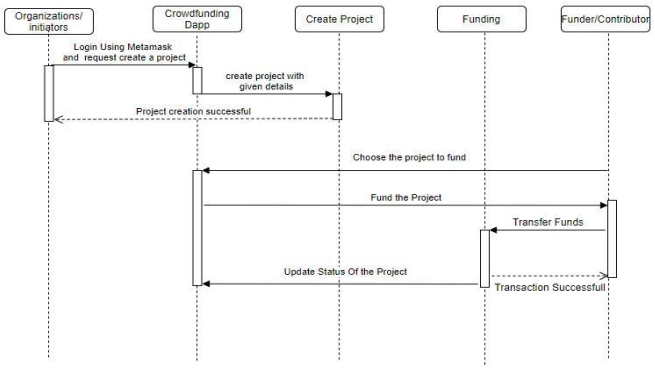

Figure 4 : Sequence of Operations in the proposed Crowdfunding Dapp.

XII.CONCLUSION

To solve the problems associated with the conventional method of crowdfunding, this system proposed the blockchain based crowdfunding, which can store information about the organizational projects and make funds transfer using blockchain network. The funds spending for a project will be transparent, can ensure data integrity, the information of the projects and current status will be updated accordingly. So this blockchain based based crowdfunding platform helps resolve the potential risks associated with existing crowdfunding techniques in term of saving time, reaching to a large group of potential users within less time span etc,

XIII. REFERENCES

[1]. Liufei Chen, Yushan Li, Hong Wen, WenXin Lei, WenJinHou, Jie Chen Block Chain Based Secure Scheme For Mobile Communication.

[2]. Gareth W. Petersz, EfstathiosPanayiy Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money.

[3]. Buterin, Vitalik. 2014b. A next-generation smart contract and decentralized application platform. White Paper.Likas Kolisko, 'Do we need mining in private and permissioned blockchains?', A Medium Corporation, 2018. Online]. Available:https://medium.com/@lkolisko/do-weneed-mining-in-private-and-permissioned-blockchain1a69b4c2c7a1.

[4]. Jayamine Alupotha, 'How to calculate the hash of block inbitcoin?',AmediumCorporation,2018. online].Available: https://medium.com/hackergirl/how-to-calculate-the-hash-ofa-block-in-bitcoin-8f6aebb0dc6d.

[5]. Saraiah Gujjunoori, Taqi Ali Sted, Madhu Babu J, Avinasg D, Radhesh Mohandas, and Alwyn R.Pais, "Throttling DDoS Attacks," Proceedingd of SECRYPT 2009, Milan, Italy, 7-10 July 2009, pp. 121-126.

[6]. Dennis Fisher. Experts debate risks to crypto, Mar 2002. Also available as http://www.eweek.com/ article/0,33658,s=720&a=24663,00.asp.

[7]. Marc Waldam and David Mazieres. Tangler: A censorship resistant publishing system based on document entanglement. In Proceedings of the 8th ACM Conference on Computer and

Communication Security, Nov 2001. Also available as http://www.cs.nyu.eddu/waldman/.

[8]. David Mazieres. Self-certifying File System. PhD thesis, Massachusetts Institute of Technology May 2000. Also available as http;//scs.cs.nyu.edu/dm/.

[9]. Zibin Zheng1, Shaoan Xiel, Hongning Dai2, Xiangping Chen4, and HuaiminWang3 :An Overview of BlockChain Technology: Architecture, Consensus, and Future Trends.

Cite this article as :

K. Bhavya Sri, J. S. Supriya, M. Pranathi Sai, P. Siva Prasad, "Crowdfunding Using Blockchain", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 128-134, March-April 2020. Available at doi : https://doi.org/10.32628/CSEIT1206233
Journal URL : http://ijsrcseit.com/CSEIT1206233