International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206524

False Expenditure Prevention Using Blockchain

Harshit Khanna, Jasneet Singh Bhatia, Mayank Gupta
Department of Information Technology, Maharaja Surajmal Institute of Technology, Delhi, India

Article Info
Volume 7, Issue 5
Page Number: 128-133
Publication Issue :
September-October-2020
Article History
Accepted : 20 Sep 2020
Published : 30 Sep 2020

ABSTRACT

Blockchain is one of the latest disruptive technologies in the market. Primarily known for cryptocurrencies, it is now being used for various other applications that utilize the integrity and distributed mechanism employed by the blockchain technology. In this paper we intend to create a decentralized platform to eloquently solve the false expenditure and counterfeit problems which is prevalent in major crowd-funding applications.

Keywords : Blockchain, Cryptocurrency, Ethereum, Smart Contracts, Decentralization

I. INTRODUCTION

The number of stakeholders of the blockchain technology are increasing day by day[7]. The global blockchain market size is expected to increase from USD 1.2 billion in 2018 to USD 23.3 billion by 2023[7]. Blockchain was first introduced in the Bitcoin technology by Satoshi Nakamoto[6] in their paper. At the very basic, the blockchain is just a ledger. But there are many distinct features that differentiate it from a traditional ledger. Immutability and distribution are the key factors that ensure integrity. Unlike the traditional ledger, where each sector is standalone and could be easily modified, in the blockchain technology, each block is cryptographically linked to the previous block. Also, since it is a peer-to-peer technology, the same blockchain is present on many participating nodes. An attack on such infrastructure is difficult.

Apart from financial institutions, many other sectors are delving into the blockchain technology. The immutability and distribution allows many applications of practical use to be developed on blockchain. Major problems that can be addressed by it are property disputes, gun tracking, s1gnmg digital documents etc.

In this paper, we create a platform which solves the problem of false expenditure and is very helpful for creating trust-worthy transactions on a crowd-funding platform.

II. PRELIMINARIES

Blockchain: A blockchain is nothing but a growing collection of blocks. Itis a digital ledger which aims to provide integrity and security to data. All the blocks are cryptographically linked to each other. Blockchain technology has a lot of scope in the future

of finance, digital document signing and numerous other fields.

Cryptocurrency: A cryptocurrency is a digital or virtual currency that uses cryptography for security. Though theoretically possible, it is almost impossible to counterfeit a widely used cryptocurrency due to cryptographic security. Many cryptocurrencies are decentralized systems based on blockchain technology, a distributed ledger enforced by a disparate network of computers. A defining feature of a cryptocurrency, and arguably its biggest allure, is its organic nature; it is not issued by any central authority, rendering it theoretically immune to government interference or manipulation. [2]

Consensus Mechanism: The main power of Blockchain lies in it's decentralization property. The decentralized nodes should be synchronized and should always contain the same chain which is also the correct chain. Consensus mechanism is a protocol which provides a structured and safe way for the nodes to communicate and check the chain of every node. The latest chain, along with properties like timestamp, proof and previous hash gets copied to all the nodes.

SHA256 Algorithm: SHA256 or the Simple Hash Algorithm is an algorithm which produces a 256 bits. It is a one-way function which means the hash value can never be converted to the string it originated from. It is a deterministic function which means the same text will always yield the same hash value. Also, it follows the Avalanche effect i.e. even a small change in the text will cause the hash value to change completely.

Ethereum Blockchain: Ethereum, just like Bitcoin, is a Blockchain which is also distributed on the public Blockchain network. Ethereum is an open software platform which allows development of blockchain apps using the existing Ethereum blockchain. While Bitcoin is more focused on the financial aspects of Cryptocurrency and Blockchain, Ethereum Blockchain has emphasis on working on the programming code of any decentralized application.

Smart Contracts: Smart Contracts are self-executing contracts where the terms of contract between the two parties are coded on the contract. These contracts are executed when a certain condition is met. Smart Contracts are deployed on the Ethereum Blockchain and are coded on the Solidity language.

Solidity: Solidity is a contract-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms. Solidity allows the users to write self-implementing Smart Contracts embodied with business logic. It created non-repudiable and authoritative record of transactions.

Web3.js: Web3.js is a set of libraries which allows the user to interact with a local or a remote Ethereum node using internet or socket connections.

Remix IDE: Remix is a very powerful and open source tool that allows the user to write Smart Contracts in the Solidity language. It can be used locally or direct from the browser.

Metamask: Metamask is a cryptocurrency wallet that allows the user to manage multiple cryptocurrency accounts. It can be used to sign Blockchain transactions and it bridges the gap between the browser and the Ethereum network. MetaMask wallet can be used for storing keys for Ether and ERC20 tokens on three different web browsers. It also allows users to browse the Ethereum blockchain from a standard browser. MetaMask requires no login and does not store your private keys in any server, instead they are stored on Chrome and password protected.

III. LITERATURE SURVEY

In this section we will discuss about all relevant work we have reviewed in the field Blockchain and Cryptocurrencies.

[1] Blockchain has been considered a breakthrough technology- but does your company need it? There are many factors that need to be considered while making a big decision within an organization , let alone a decision like shifting all of company's data and functionality to a completely different technology. Blockchain is a rather unexplored territory and setting it up is a very expensive and complex affair. In this paper the author talks about when to use Blockchain in industries by providing a case study of practical use of Blockchain in the Insurance Sector. The analysis could easily be extended to other scenarios sharing comparable use cases, thus helping professionals make decisions in different contexts and sectors.

[2] A blockchain is a digitized , decentralized , public ledger of all cryptocurrency transactions. Constantly growing as 'comprehensive' blocks (the most recent transactions) are recorded and added to it in sequential order, it allows market participants to keep track of digital currency transactions without central recordkeeping. A word that often arises when talking about Blockchain is Bitcoin. Many people still confuse Blockchain with Bitcoin· however, they are not the same. Bitcoin is just on of many applications that utilize Blockchain technology. In this paper, the authors conduct a critical analysis of Blockchain applications and the challenges these face.

Major Blockchain Applications:

1. Cryptocurrency
2. Decentralized applications

[3] In the existing blockchain systems, there are four major consensus mechanisms: PoW (Proof of Work), PoS (Proof of Stake), PBFT (Practical Byzantine Fault Tolerance), and DPoS (Delegated Proof of Stake). Other consensus mechanisms , such as PoB (Proof of Bandwidth), PoET (Proof of Elapsed Time) , PoA(Proof of Authority) and so on, are also used in some blockchain systems. The two most popular blockchain systems (Bitcoin and Ethereum) use the PoW mechanism. Ethereum also incorporates the PoA mechanism and some other cryptocurrencies also use the PoS mechanism ' such as PeerCoin and ShadowCash.

[4] Since its inception, the blockchain technology has shown promising application prospects. From the initial stages of cryptocurrency to the current smart contract, blockchain has been applied to many fields. Although some studies have been done on the security and privacy issues of blockchain , there lacks a systematic examination on the security of blockchain systems. In this paper, the authors conduct a systematic study on the security threats to blockchain and survey the corresponding real attacks by examining popular blockchain systems. The author also reviews the security enhancement solutions for blockchain , which could be used in the development of various blockchain systems, and suggest some future directions to stir research efforts into this area.

[5] While there are controversies about Nakamoto 's true identity, one is for sure: he brought something revolutionary to the world , and it is up to the users to decide what they want to do with it. Some people will take this opportunity and develop their own application for solving various problems in the society, others will invest money in those ideas or simply trade with ups and downs of the cryptocurrencies ' values at the market. In this paper, the author has brought insight to the world of Blockchain and Cryptocurrencies. He started with

the Bitcoin essentials and proceeded to Bitcoin transactions and the Proof-of-Work Algorithm. The Bitcoin network starts with new transactions being broadcasted to all nodes. Each node acquires transactions into a block and works on finding proof-of-work , after which it broadcast its block to the network. After this, he proceeded to give insight on the 'Hard Fork' of Bitcoin i.e Bitcoin Cash and Bitcoin Gold. The author then proceeded to show how the limitations of B itcoin were addressed by Ethereum by introducing loops etc. The main difference is that Ethereum blocks contain not only the block number, difficulty, nonce, etc. but also the transaction list and the most recent state.

[6] The most important paper in any blockchain research. The author(s) proposed a system for electronic transactions without relying on trust using a decentralized ledger. This is implemented with SHA256 encryption and p2p networks. A purely p2p version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures deliver a part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double‐spending. They propose a solution to the double‐spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into a continuing chain of hash-based proof‐of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the order of events witnessed , but proof that it came from the largest pool of CPU power. As long as the majority of CPU cycles is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcasted on a best effort basis, and nodes can abandon and rejoin the network at will , accepting the longest proof-of-work chain as proof of what happened while they were gone.

IV. METHODOLOGY

Blockchain is an immutable and decentralized ledger. It's main power is that it involves not just a central server but multiple systems in remote locations. So even if a malicious user found out a way to change data in a single system, it would do no harm as the user would have to tamper with the data in multiple systems simultaneously which is nearly impossible.

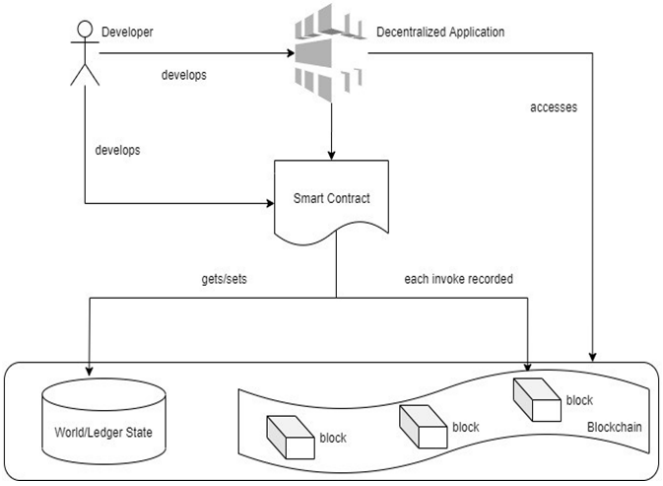

Fig. 1. Architecture of the decentralized platform

Firstly, we created a smart-contract which can somehow 'hold' the contributions from the crowd and directly initiates transactions with the vendors with whom the contract-creator wants to do transactions with. The contract was built using Solidity and various functions for spending request and voting etc. were introduced into it.

The contract was tested with Truffle so that no undetected loopholes were deployed.

The major problem was to somehow give the control of the money to the contributors. This was a really important step to solve counterfeits and false expenditure. We implemented a voting system inside the contract. First, the user would create a spending request which would go to all the contributors to

accept or reject. If a certain majority of them accepts the transaction, it will go through.

More testing using dummy accounts from Metamask and Ganache was done to ensure the basic aspects Blockchains are known for i.e.

- Greater Transparency
- Enhanced Security
- Improved Traceability
- Reduced Costs

Lastly, we created a web Application using the latest trend in the world i.e React.js which makes the interaction with the deployed smart contracts easy for both the developers and the users.

There were some design and implementation constraints that cropped up during the project design phase. There is one notable security flaw in blockchains: if more than half of the computers working as nodes to service the network tell a lie, the lie will become the truth. This is called a '51% attack' and was highlighted by Satoshi Nakamoto when he launched Bitcoin.

Also, there is problem with energy, notably electricity consumption with mining of cryptocurrencies.

As a digital technology, cryptocurrencies will be subject to cybersecurity breaches, and may fall into the hands of hackers. We have already seen evidence of this, with multiple ICOs getting breached and costing investors hundreds of millions of dollars.

Furthermore, we had to study the working of React.js to gain experience in that particular field. Study of React.js, next.js and next-routes was done. Also, frontend open-source libraries like Semantic-ui-react were studied and implemented in the project.

Also, as Blockchain is still an emerging technology, we had to use some libraries which had deprecated versions which aren't backward compatible like "web3": "^1.0.0-beta.37" and "solc": "^0.4.19".

V. CONTRIBUTION TOWARDS RESEARCH

The goal of the paper is to create a platform to prevent the counterfeits and false expenditures on major crowd-funding platforms.

Furthermore, a fully functional web app was created using latest front-end frameworks like react.js. This web app was fully integrated with the Blockchain network using node.js as the back- end framework. Smart Contracts were first conceptualized on the Remix IDE after being coded on Solidity and then they were deployed on the Ethereum network. The interface of communication between the web app and deployed Smart Contracts was web3.js.

VI. RESULT

A crowd-funding platform was successfully created which gave more power to users rather than the creator. This, by no means is a complete solution to false expenditure. A problem with this is that the creator can create another account and tell the users that it is the vendor's account. But many applications and solutions can be built on top of this.

In the application phase, firstly the Smart Contracts were conceptualized on the Remix IDE. Then these Smart Contracts were compiled using web3.js and a bytecode was obtained. Front- end was designed using React.js. Further, using web3.js, we interacted with the smart contracts using Metamask accounts. This allowed us to create a flow of information, hence implementing the application.

VII. FUTURE SCOPE

The scope of blockchain technology in the future is immense It is being adapted by organizations and governments at a rapid pace, hence the popularity. More and more transactions are happening via cryptocurrencies , hence it's share is steadily increasing in the market. This has prompted national banks to look into blockchain seriously. Many applications such as consumable media (books, music and movies) digital distribution , contract execution, preventing identity thefts and real estate management can be developed using a blockchain and smart contracts.

VIII. REFERENCES

[1]. Valentina Gatteschi, Fabrizio Lamberti, Claudio Demartini, Chiara Pranteda, Victor Santamaria, To Blockchain or Not to Blockchain: That Is the Question, IEEE Computer Society, March/April 2018, pp 64-72.

[2]. Pinyaphat Tasatanattakool, Chian Techapanupreeda, Blockchain: Challenges and Applications, ICION 2018, pp 473-475.

[3]. Aleksander Berentsen and Fabian Schar, A Short Introduction to the World of Cryptocurrencies, Federal Reserve Bank of St. Louis Review, First Quarter 2018, 100(1), pp. 1-16. https://doi.org/10.20955/r.2018.1-16

[4]. Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen, A survey on the security of blockchain systems, Future Generation Computer Systems, Elsevier, Received in revised form 11 July 2017, Accepted 14 August 2017. https://dx.doi.org/l 0.1016/j .future.2017.08.020

[5]. Dejan VujiCi6, Dijana Jagodi6, Sinifa Randie, Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview, 17th International Symposium INFOTEHJAHORINA, 21-23 March 2018.

[6]. Nakamoto, S., 2012. Bitcoin: A peer-to-peer electronic cash system, Oct,2008.

[7]. https://www.marketsandmarkets.com/Market• Reports/bl ockchain-technol ogy-market-90100890. html

[8]. http://www.investopedia.com/terms/ c/cryptocurrency. as- .P

AUTHORS

Harshit Khanna
Bachelor in Technology (Information Technology), Maharaja Surajmal Institute of Technology
Jasneet Singh Bhatia
Bachelor in Technology (Information Technology), Maharaja Surajmal Institute of Technology
Mayank Gupta
Bachelor in Technology (Information Technology), Maharaja Surajmal Institute of Technology

Cite this article as :

Harshit Khanna, Jasneet Singh Bhatia, Mayank Gupta, "False Expenditure Prevention Using Blockchain", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 5, pp. 128-133, September-October 2020. Available at doi : https://doi.org/10.32628/CSEIT206524
Journal URL : http://ijsrcseit.com/CSEIT206524