International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

DECENTRALIZED BLOCKCHAIN SERVICES USING CARDANO NETWORK

Akash Kumar D[1], Avinash Khanna R[2], Shashang P[3], Surash T[4], Ms. Lakshmi R[5]

[1,2,3,4] *Student, Department of IT, SRM Valliammai Engineering College, Tamilnadu, India*
[5] *Assistant Professor, Department of IT, SRM Valliammai Engineering College, Tamilnadu, India*

Abstract - *The System will be using the Cardano, which is a blockchain of a crypto coin. Due to the usage of the Cardano network, our blockchain will consist of three segments: DATA, Block's HASH, Previous Block's HASH. In case of Cardano the data will be further divided into 3 components, FROM, TO and AMOUNT. This project also revolves around brining web-based services such as E-commerce into the blockchain. Currently the blockchain is used in very few industries and its majorly occupied by cryptocurrencies. The entirety of blockchain is used only for crypto transactions. Our innovation here lies in the implementation of E-commerce services into the blockchain. To attain said goals we will be using the web3 prototype websites powered by blockchain servers to host our website for the E-commerce products. Any transaction happening on the web3 websites will be implemented on the blockchain by default due to its hosting server being a blockchain server (Cardano). A transaction is only completed after using the PoW or Proof of Work method. This method ensures transactions on the blockchain are absolute and maintains its integrity and security. These elements of the blockchain makes it difficult to crack through and change its data. Ultimately once the transaction is verified by the PoW, it will pass through, and the respective product purchased will drop into the buyers E-wallet or crypto wallet.*

Key Words: Cardano, Blockchain, Hash, E-Commerce, Web3, PoW (Proof of Work), E-wallet.

1. INTRODUCTION

A blockchain is a collection of blocks that are inter-linked on a network. Blockchain networks are used to strengthen security and anonymity of transactions that happen on the blocks. This project revolves around decentralizing services such as E-commerce services on the blockchain to implement them on to the web3 prototype websites. We will be using the Cardano Blockchain to attain said goals. Cardano is a blockchain that offers a crypto coin called Cardano ($ADA). ADA is used to make transactions on the cardano Blockchain network. We will be implementing the Cardan blockchain server on our web3 prototype site for E-commerce to sell products using ADA as the method of payment. The payments are made using E-wallets which can hold your ADA(s) and use them for your purchases. The purchases are done using a PoW or Proof of Work method which verifies every transaction on the blockchain and brings integrity and security to our transaction to avoid it from being attacked by external networks and change its values. Once the minimum number of verifications required for a transaction to complete is attained on the Cardano network using the Proof of Work method, the transaction will go through and be completed successfully. Upon completion of a successful transaction, the purchased product will then be sent to the E-wallet of the user in form of a token.

2. LITERATURE SURVEY

The proposed system has gone through various papers on blockchain and its services, impacts etc. on the financial sectors from the past decade. Insights of these papers bring light on various fields and its flaws that need to be investigated while creating networks on the blockchain. Some the referred papers are given below along with their insights.

Those references are listed as follows.

1. Victor Changa, Patricia Baudierb, Hui Zhangc, Qianwen Xua, Jingqi Zhanga, Mitra Arami - How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees (2020). Deals with impact of blockchain on the financial sectors.

2. Omar Alia, Mustafa Allyb, Clutterbuckc, Yogesh Dwivedi - The state of play of blockchain technology in the financial services sector: A systematic literature review (2020). Deals with the state of blockchain in the sector of finance.

3. David Berdika , Safa Otoum⁎,b , Nikolas Schmidta , Dylan Portera , Yaser Jararweha - A Survey on Blockchain for Information Systems Management and Security (2020). Deals with impacts and benefits of blockchain on the Information Systems.

4. QIHENG ZHOU, HUAWEI HUANG (MEMBER, IEEE), ZIBIN ZHENG(SENIOR MEMBER, IEEE), JING BIAN - Solutions to Scalability of Blockchain: A Survey (2016). Deals with the scalability issues faced by the blockchain technologies and methods to overcome them.

3. PROPOSED WORK

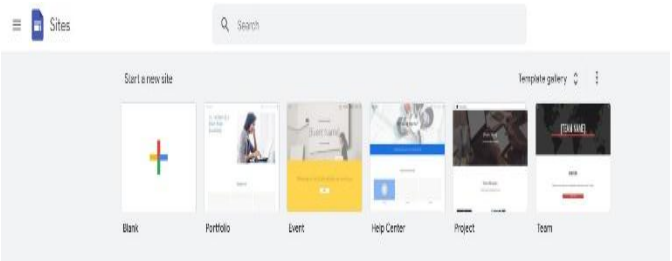
The proposed system aims to challenge the flaws faced by the current system. One of the major issues faced by the current encryption algorithms such as the SHA algorithms are that they are very vulnerable to attacks such as Man-In-The-Middle Attacks and BOOMERANG Attacks. These attacks make the encryptions vulnerable and destroy the confidentiality of the data that is being processed on the blockchain. Various Tech giants in the current E-Commerce market use SHA algorithms. To overcome the issues faced by them we will be using the BLAKE algorithm. BLAKE algorithm is faster and more vulnerable to attacks in comparison to the SHA algorithm. BLAKE algorithms is the key component of the ADA or Cardano Blockchain. Using BLAKE algorithms helps one to overcome the issues faced by the current tech giants.

Another important factor is the usage of blockchain technology. Since BLAKE algorithm is based on a blockchain cryptocurrency, it by default helps the framework of the E-commerce site to reach the blockchain technology. Due to this we are passively supported by the blockchain technology in terms of security and protocols.

3.1 CHOOSING BLOCKCHAIN & SETTING UP SERVER AND WEBSITE

In this module we decide the suitable blockchain for the system through various research papers and technical background checks. Through all the above mentioned methods we landed on the Cardano blockchain due to its fluid hashing rate and fast bit rate. Another important reason would be the resistance to various attacks that cause data breaches in algorithms like SHA.

Fig-1: Shows the google sites hosting platform.



3.2 CREATING PRODUCTS & METADATA

This module will be focusing on products that the E-Commerce website we host will be selling. For the sample sakes of the system, we will be selling electronic products such as iPhone etc. Once the product for the system is decided, we will need to create metadata for the products individually. Metadata help us get a background data about the products on the blockchain. Metadata plays crucial role for finding the information of items on the blockchain.

Fig-2: Metadata.

3.3 UPLOADING PRODUCTS TO THE BLOCKCHAIN

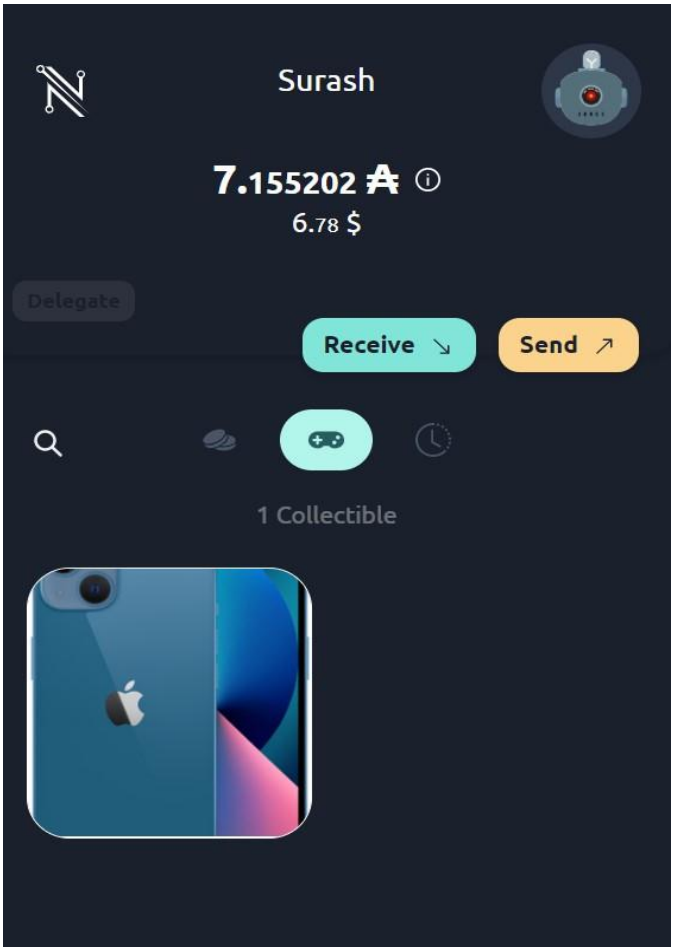
This module will focus on uploading the product to the NFTMAKER.IO Blockchain server using VS Code or Visual Code. The code to upload files on the blockchain server is written in JavaScript and consists of various external libraries. Once the files are uploaded to the blockchain, it will be available to mint for anyone.

Fig-3: Shows the file on the server.

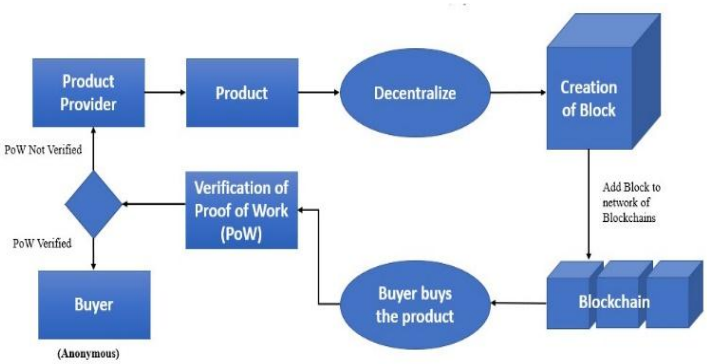
3.4 MINTING THE PRODUCTS USING $ADA

This module will focus on minting the products using $ADA or Cardano crypto currency using our E-Wallet. Once minted, the blockchain will run a PoW or Proof of Work to verify the transaction's legitimacy. Once the PoW is confirmed by the nodes on the network (more than 50% of the nodes) then the product will be sent to the user's wallet.

Fig-4: Shows the file on the E-wallet.



4. SYSTEM ARCHITECTURE



5. METHODOLOGY

The process will start by choosing a crypto blockchain, in our case the Cardano Blockchain. The Cardano blockchain is rather fast and scalable comparing to the other crypto currencies like BTC and ETH. Another important reason would be the implementation of BLAKE Algorithm which is fast and resistant to various attacks.

6. EXISTING SYSTEM

The existing system faces a lot of technical issues such as Security issues faced due to the poor encryption of SHA in comparison to the BLAKE Hashing Algorithm. It is also very vulnerable to Man in the Middle Attacks and BOOMERANG Attacks which impact the privacy and confidentiality of the data that is processed during a crypto transaction on the blockchain.

The SHA algorithm is the most used hashing algorithm as per the research done on various papers. SHA deals with slow hashing speed and bit rate. When we compare this with BLAKE Algorithm, its inefficient and less fast in hashing elements.

7. CONCLUSION AND FUTURE ENHANCEMENT

The project will work with ease and fluidity for all transactions and is efficient in terms of processing speed. Other conclusions drawn from the system would be the implementation of blockchain to the E-commerce which help promote anonymity and security in the field of E-commerce. Building of the servers of blockchain around the BLAKE algorithm in return boosts the resistance to various attacks such as Man-In-The-Middle attacks and BOOMERANG attacks. It also improves in terms of hash rate and bit rate.

Flaws that were detected during the testing and running of the system would include congestion of network during high traffic period. Traffic refers to the occurrence of transaction on a blockchain. If the number of transactions exceed the amount that the blockchain can handle, then it will lead to congestion on the network which will slow down transaction and fluidity on the server. Other possible enhancements could be implementation of such blockchain server and technology to various other field that could prove helpful for various sectors in terms of security and integrity.

REFERENCES

[1] Victor Changa, Patricia Baudierb, Hui Zhangc, Qianwen Xua, Jingqi Zhanga, Mitra Arami - How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees (2020)

[2] Omar Alia, Mustafa Allyb, Clutterbuckc, Yogesh Dwivedi - The state of play of blockchain technology in the financial services sector: A systematic literature review (2020)

[3] David Berdika , Safa Otoum,b , Nikolas Schmidta , Dylan Portera , Yaser Jararweha - A Survey on

Blockchain for Information Systems Management and Security (2020)

[4] QIHENG ZHOU, HUAWEI HUANG (MEMBER, IEEE), ZIBIN ZHENG(SENIOR MEMBER, IEEE), JING BIAN - Solutions to Scalability of Blockchain: A Survey (2016)

[5] RUI ZHANG and RUI XUE - Security and Privacy on Blockchain (2019)

[6] MAYANK RAIKWAR , DANILO GLIGOROSKI , AND KATINA KRALEVSKA - SoK of Used Cryptography in Blockchain (2019)