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

DECENTRALIZED BLOCKCHAIN CRYPTOCURRENCY TRANSACTION

[1]Dr.S.Durga Devi BE,ME,Ph.D., , [2]Sangeeth Sahana D, [3]Winselin a, [4]Valli s

[1] Head of Computer Science Department [2] UG Scholar, [3]UG Scholar,[4] UG Scholar
[1] Department of Computer Science and Engineering
[1]Vel Tech High Tech Dr. Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai. 600062

Abstract : Various sectors,use blockchain decentralized applications (dApps) to gain profit from this technology. The current Blockchain technology (BT) inspires benefits in trustability, non-manipulation of data, collaboration, and transparency.In this project, we've researched to show how open science can benefit from this technology and its characteristics. For this, we determined the needs of the current society and then compared it with the properties of Blockchain Technology(BT) to prove that this technology is suitable as an infrastructure. We will use Blockchain here for secure transactions of money between peers.

IndexTerms - Blockchain, Ethereum, Solidity, Smart Contract.

I. INTRODUCTION

Blockchain is an advanced circulated record of exchanges that are imitated, disseminated and decentralized across the entire organization of PC hubs on the blockchain. This system records information in a way that makes entirely impossible to manipulate, or hack the system. The concept of Blocks are the ones that make up the blockchain.Multiple blocks make up the blockchain and it consist of three fundamental elements.Data (i.e transactions), which has the hash of the previous block and the block current information. Hash value is unique, to identify an independent block. Therefore each block can reference or point to the block before, which means the four-block is taking a reference to the third one is taking a reference to the second, and so on and thus a chain of blocks is formed which we call a blockchain.

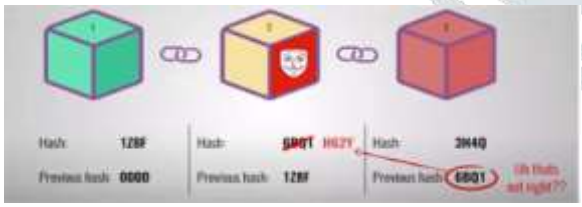

Fig 1

Cryptography + Blockchain Hashing Process = Immutability

The key element that makes blockchain immutable is cryptographic hashes, which is why blockchain is immutable.The data stored in blockchain is in the form of transactions. A blockchain transaction is a transfer of crypto money. A transaction is a new record of exchange of some value or data between two public addresses of the blockchain.One can think of a transaction as being a record that describes one account attempting to send money to another account. A transaction is created any time two accounts exchange some amount of money.

Ethereum: Here we have used Ethereum as the platform to create a Blockchain application. Here the consensus is reached using the Proof of Stake Algorithm(PoS). Ether is the native cryptocurrency that's used.

Smart Contracts and Solidity: For transactions, that is to add the block to the blockchain we have written a smart contract using a solidity programming language. The receiver's address, amount, message, and keyword with datatypes address payable, int, and memory are used respectively. This is appended under the file Transactions.sol file. This smart contract is deployed using the getContractFactory method that's under the javascript file deploy.js

Metamask: To perform a transaction on the blockchain network it is necessary to hold an account with a unique address, which can be created by using the meta mask extension in google chrome. This acts as a crypto wallet and the gateway to our decentralized web 3.0 app.

Hardhat: To run our solidity contracts locally, we have used HardHat as the Ethereum Virtual Machine (EVM). This is used as an alternative to truffle since it provides an error management tool such as console.log method.

Ropsten network To test our application without losing any actual funds, Ropsten Network is used where we can create free accounts and get around 1 ETh .

II. RELATED WORKS

This paper aims to study and evaluate recent research available in the literature on blockchain smart contracts and the methods used to test them, their results, and the experimentation used to achieve those results[1].

We identify the feasible conditions, which govern the feasibility of each financing model. We then develop the optimal rule, in the form of an algorithm, to determine the optimal financing choice[2].

Each category has several subcategories. For each subcategory, we pick some of the most meaningful comments and highlight some statistics that we derived based on our survey responses to highlight the generalizability of the findings[3].

This paper proposes a specific software lifecycle approach to rationalize how to tackle the issue of smart contract security[4].

A smart contract is a distributed computer program that runs in a blockchain environment. Supported by the underlying blockchain. The two efforts are similar in their inability to protect deployed smart contracts and DeFi. In addition, they cannot fix vulnerabilities that have not been detected. Nor can they protect the assets in deployed smart contracts[5].

The ever-changing infrastructure realization of the decentralized blockchains probably means that we should not equalize Web 3.0 and decentralization. To address this challenge, HyperService designs UIP, a cryptography protocol between VESes and dApp clients to securely execute HSL executables on blockchains[6].

In this paper, we show how we build a secure IoT platform using a smart residing on a private Ethereum blockchain. We use g th to program Ethereum Virtual Machine. Miner creates a block after verifying the transaction received from the device A. The smart contract is recorded on the (n)th block and has its own[7].

Interoperability is one of the main challenges of blockchain technologies, which are generally designed as self-contained systems. This has led to users being forced to weaken their privacy, e.g. by using centralized exchanges, to move assets from one chain to another[8].

Blockchain technology has received tremendous attention from academia, industry, politics and media alike in the last decade. Since the introduction of blockchain technology with the cryptocurrency Bitcoin[9].

A new economic era with the Internet as the main driving force for the economic and social development of each country has been opened.Web3.0, websites are allowed to have the ability to learn on their own . Moreover, blockchain distributed storage technology is adopted to realize a decentralized autonomous network[10].

The proposed PackChain framework uses the Ethereum blockchain to offer a crowdsourcing platform for last-mile delivery with autonomous and transparent processes.The emulation results demonstrate the feasibility and cost-efficiency of the proposed solution[11].

This paper proposes a model to discover and recruit reputable talent by leveraging blockchain technology, which enables trustless networks and allows entities to conduct transactions without mutual trust, called the recruitment system[12].

In this research work, we will deliberate and recognize Blockchain arrangement, how Ethereum works, writing smart contracts, the introduction of web3.js, and wallet services.A record book holds all dealings, timestamps, the hash value of the preceding block, record book compensation, record book number, and others[13].

Decentraland by presenting the main details of the virtual world and by focusing on the economic impact of NFT trading on the description of the parcels.Online Social Networks gained a crucial role in people's everyday life, acting as the medium through which people can interact with each other[14].

The security and integrity of the smart contracts used to build these technologies should be of the highest priority.

In literature about testing smart contracts, the number of primary studies increases year over year due to the increasing demand for this domain[15].

This paper gives a model demonstration of the implementation of Blockchain Technology at the industry level. However, additional functionalities can be added in the future with enhanced compatibility.Cryptocurrency transactions are stored on a shared, digital ledger called a blockchain[16].

Cryptocurrency transactions are stored on a shared, digital ledger called a blockchain. Traceability, openness, immutability, and fault tolerance are some of the qualities of this technology that help maintain data privacy in IoT scenarios and thus create a safe environment[17].

This paper presents how to build a secure, trustful and efficient platform to combat malicious content and fake news by implementing NLP techniques including stop word removal, topic modeling. This paper presents how to build a secure, trustful and efficient platform to combat malicious content and fake news by implementing NLP techniques including stop words removal, topic modeling[18].

The software architecture of our energy trading platform is provided with example codes. We build smart contracts on Ethereum for determining the trading price. Blockchain architectures for P2P energy trading of surpluses and demands between consumers and neighborhood consumers without intermediaries[19].

The virtual–real interactions of three types of employees, as well as the virtual–real feedback of three closed loops in the parallel systems, DAO-based parallel management for enterprises can realize descriptive intelligence, predictive intelligence, and prescriptive intelligence. This case introduces the operation processes and illustrate the superiorities of the proposed DAO-based enterprise parallel management mode[20].

The artificial enterprise DAO (EnDAO) corresponding to the actual enterprise is constructed, and they constitute a parallel system via virtual–real interaction and parallel execution.

III. TOOLS AND REQUIREMENTS

***PREFERRED IDE**:* VS CODE

LANGUAGE: SOLIDITY

***REQUIREMENTS AND DEPENDENCIES**:*

- NODE JS
- METAMASK EXTENSION
- VITE+REACT
- HARDHAT
- ROPSTEN TEST NETWORK
- ALCHEMY
- GIPHY Developer site

IV. EXISTING SYSTEM

Wild animals are a special challenge for farmers throughout the world. Animals such as deer, wild boars, rabbits, moles, elephants, monkeys, and many others may cause serious damage to crops
There are different existing approaches to address this problem which can be lethal and non-lethal

Agricultural fences: Agricultural fences are quite an effective wild animal protection technology. However, utilizing fences as a practice is often regulated.

Natural Repellents: Some farmers prefer using natural protection measures instead of mechanical or chemical protectivepractices. There are various ways to protect crops from wild animals.

V. PROPOSED SYSTEM

The proposed system aims to address the limitations of the existing system and enhance the overall experience of decentralized blockchain cryptocurrency transactions. Our methodology proposes to develop a React JS-based web application for cryptocurrency transactions between peers. These transactions between the peers are secured since there is no Central Server or System that either maintains the records of transactions or stores the data of the blockchain because here everything is decentralized. This Web 3.0 Blockchain Application will have a User Interface based on React JS framework and will be connected to the Blockchain at the backend. MetaMask pairing will be done for connecting the client's Ethereum wallet.
Solidity Programming language will be used for the Interaction with Smart Contracts and finally sending Ethereum via Blockchain Network takes place for effective cryptocurrency transactions between the peers. This will be a responsive website and each transaction will forever be stored in the Blockchain which in turn solves the issue of data manipulation and data privacy. We will also deploy our Web 3.0 application so that people can use it from anywhere all around the globe.

Key components of the proposed system include:

Scalability Solutions: The proposed system incorporates scalability solutions, such as sharding, layer 2 protocols (e.g., Lightning Network), or blockchain interoperability frameworks (e.g., Cosmos, Polkadot). These solutions enable the network to handle a larger volume of transactions, improving transaction throughput and reducing congestion.

Reduced Transaction Fees: The proposed system implements mechanisms to reduce transaction fees, such as optimizing transaction processing algorithms or utilizing off-chain transactions for lower-value transfers. This helps make transactions more affordable for users.

Enhanced Interoperability: The proposed system focuses on improving interoperability between different blockchain networks. It allows for seamless asset transfer and communication across different networks, promoting a more connected and efficient ecosystem.

Regulatory Compliance and Privacy Enhancements: The proposed system incorporates features to facilitate regulatory compliance, such as built-in know your customer (KYC) and anti-money laundering (AML) procedures. It also emphasizes privacy enhancements, such as zero-knowledge proofs or privacy-preserving techniques, to protect user data and transaction details.

Improved User Experience: The proposed system emphasizes a user-friendly interface, offering intuitive wallet management, transaction tracking, and easy integration with various devices and platforms. It aims to enhance the overall user experience and accessibility of decentralized blockchain cryptocurrency transactions.

Security Measures: The proposed system strengthens security measures, including advanced encryption techniques, multi-factor authentication, and robust smart contract auditing processes. It aims to mitigate vulnerabilities and protect against potential attacks or malicious activities.

The proposed system takes into account the existing challenges and limitations of decentralized blockchain cryptocurrency transactions. By incorporating scalability, reduced transaction fees, enhanced interoperability, regulatory compliance, privacy enhancements, improved user experience, and advanced security measures, it aims to offer a more efficient, secure, and user-friendly ecosystem for decentralized transactions.

VI. METHODOLOGY

Initially, we will develop a User Interface with the help of React JS framework and use TailWind CSS for styles. This User Interface will be connected to the Blockchain at the backend. Metamask which is a chrome extension will be downloaded and added to the browser.

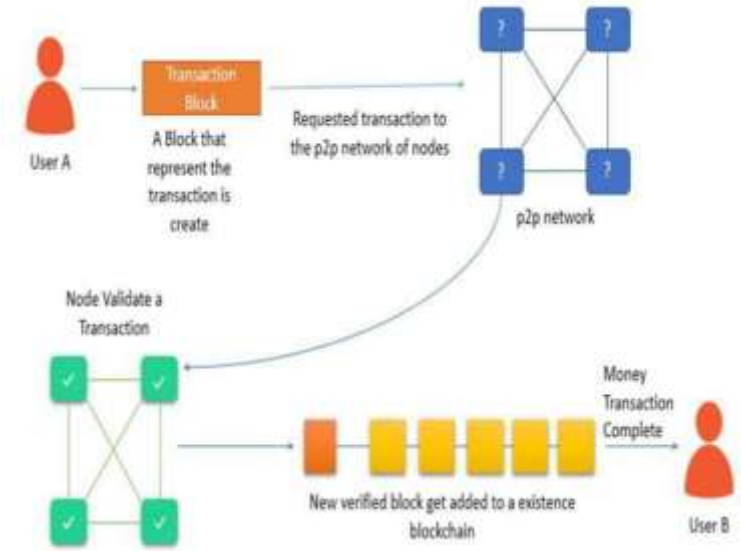

Fig 2

This is done to ensure the Ethereum wallet connection and pair it to the Blockchain Application. Further Smart Contracts will be written on Ethereum Network using Solidity Programming Language. For testing purposes, we have used the Ropsten test Network.

The Client will have to connect one's wallet which will trigger the meta mask extension and connect to an account of their own. Once connected the shortened address of their account will be visible on the User Interface for convenience. Additionally for cryptocurrency exchange, it is required to enter the address of the receiving account and the Ethereum amount.

Then a prompt to Metamask Confirmation will pop up, confirming which contract interaction takes place. On clicking the additional details, the date, time, and history of the transactions will be visible on the Etherscan. The latest Transaction will also be displayed on the User Interface as well with a GIF.

Deployment of the Web 3.0 application will be done using service providers like Hostinger.

VII. OUTPUT AND RESULT

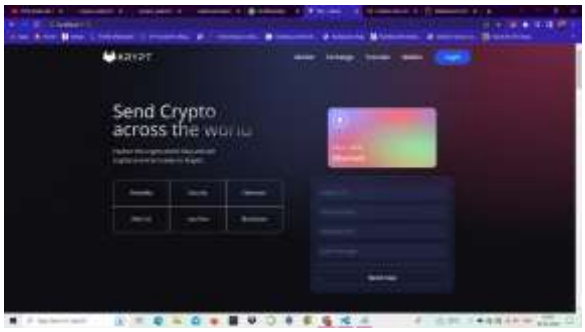

Fig 3

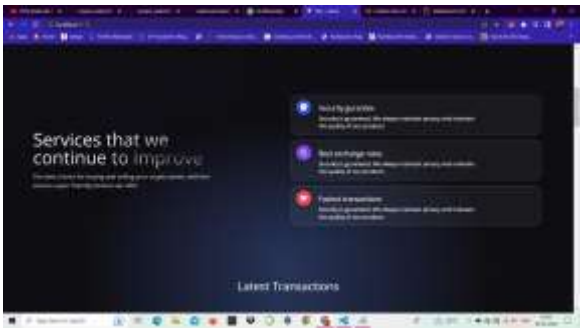

Fig 4

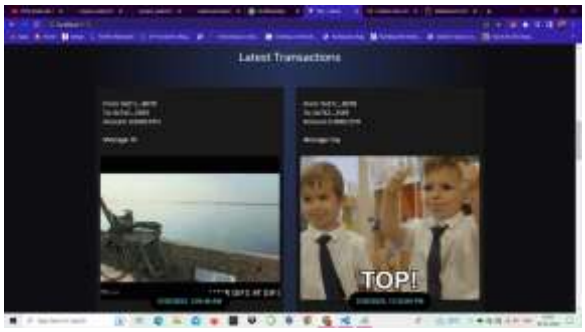

Fig 5

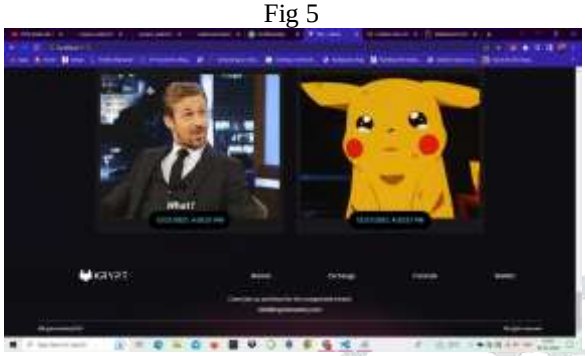

Fig 6

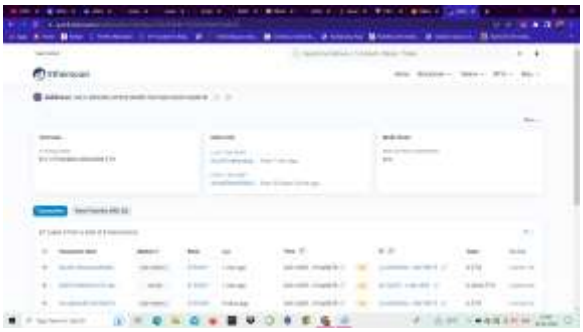

Fig 7

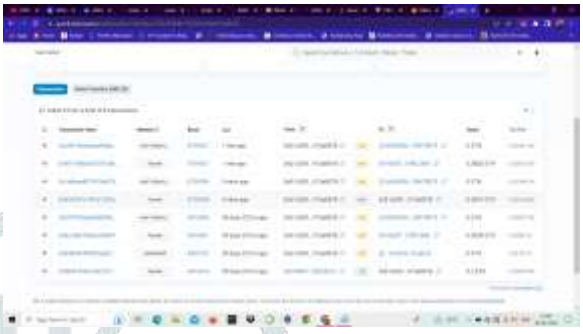

Fig 8

VIII. CONCLUSION

The proposed system helps in the safe transaction and cryptocurrency exchange between peers with the help of Blockchain Technology, Ethereum Network, Hardhat for the deployment of Smart Contracts, Solidity Programming Language for writing Smart Contracts and the development of an Interactive and Responsive User Interface deployed and hosted for users to access the Web 3.0 Application anytime, anywhere all around the globe.

IX. REFERENCES

[1]Al Khalil, T. Butler, L. O'Brien, and M. Ceci, "Trust in smart contracts is a process, as well," in Proc. 21st Int. Conf. Financial Cryptography Data Security, 2017, pp. 510–519.

[2] M. Alharby and A. van Moorsel, "Blockchain-based smart contracts: A systematic mapping study," CoRR, vol. abs/1710.06372, 2017. [Online]. Available: http://arxiv.org/abs/1710.06372.

[3] L. Alt and C. Reitwiessner, "SMT-based verification of solidity smart contracts," in Proc. Int. Symp. Leveraging Appl. Formal Methods, 2018, pp. 376–388.

[4] S. Amani, M. Begel, M. Bortin, and M. Staples, "Towards verifying Ethereum smart contract bytecode in Isabelle/HOL," in Proc. 7th Int. Conf. Certified Programs Proofs, 2018, pp. 66–77.

[5] I. Anati, S. Gueron, S. Johnson, and V. Scarlata, "Innovative technology for CPU based attestation and sealing," in Proc. 2nd Int. Workshop Hardware Architectural Support Secur. Privacy, 2013, vol. 13, pp. 1–7.

[6] M. Aniche, C. Treude, I. Steinmacher, I. Wiese, G. Pinto, M.-A. Storey, and M. A. Gerosa, "How modern news aggregators help development communities shape and share knowledge," in Proc. 40th Int. Conf. Softw. Eng., 2018, pp. 499–510.

[7] ARM, "Arm security technology–building a secure system using trustzone technology," ARM Technical White Paper, 2009. [Online]. Available: http://infocenter.arm.com/help/ topic/com.arm.doc.pr d29genc009492c/PRD29%-GENC009492C_trustzone_security_whitepaper.pdf

[8] D. W. Barowy, S. Gulwani, T. Hart, and B. Zorn, "FlashRelate: Extracting relational data from semi-structured spreadsheets using examples," in Proc. 36th ACM SIGPLAN Conf. Program. Lang. Des. Implementation, 2015, pp. 218–228.

[9] M. Bartoletti, S. Carta, T. Cimoli, and R. Saia, "Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact," CoRR, vol. abs/1703.03779, 2017. [Online]. Available: http:// arxiv.org/abs/1703.03779.

[10] M. Bartoletti, T. Cimoli, and R. Zunino, "Fun with Bitcoin smart contracts," in Proc. Int. Symp. Leveraging Appl. Formal Methods, 2018, pp. 432–449.

[11] M. Bartoletti and L. Pompianu, "An empirical analysis of smart contracts: Platforms, applications, and design patterns," in Proc. 21st Int. Conf. Financial Cryptography Data Security, 2017, pp. 494–509.

[12] M. Bartoletti and R. Zunino, "BitML: A calculus for Bitcoin smart contracts," in Proc. 25th ACM SIGSAC Conf. Comput. Commun. Security, 2018, pp. 83–100.

[13] K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, N. Kobeissi, N. Kulatova, A. Rastogi, T. SibutPinote, N. Swamy, et al., "Formal verification of smart contracts: Short paper," in Proc. Workshop Program. Lang. Anal. Security, 2016, pp. 91–96.

[14] G. Bigi, A. Bracciali, G. Meacci, and E. Tuosto, "Validation of decentralized smart contracts through game theory and formal methods," in Programming Languages with Applications to Biology and Security. Berlin, Germany: Springer, 2015, pp. 142–161.

[15] S. Bragagnolo, H. Rocha, M. Denker, and S. Ducasse, "Smartinspect: Smart contract inspection technical report," PhD thesis, Lille, Department: Inria - National Institute for Research in Computing and Automation, France: Inria Lille, 2017.

[16] L. Brent, A. Jurisevic, M. Kong, E. Liu, F. Gauthier, V. Gramoli, R. Holz, and B. Scholz, "Vandal: A scalable security analysis framework for smart contracts," CoRR, vol. abs/1809.03981, 2018. [Online]. Available: http://arxiv.org/abs/1809.03981

[17] R. G. Brown, J. Carlyle, I. Grigg, and M. Hearn, "Corda: An introduction," R3 CEV, pp. 1–15, 2016. [Online]. Available: https://docs.corda.net/_static/corda-introductory-whitepaper.pdf

[18] M. Broy, "Challenges in automotive software engineering," in Proc. 28th Int. Conf. Softw. Eng., 2006, pp. 33–42.

[19] V. Buterin, "A next-generation smart contract and decentralized application platform," White Paper, 2014.

[20] C. Calcagno and D. Distefano, "Infer: An automatic program verifier for memory safety of C programs," in Proc. 3rd Int. Symp. NASA Formal Methods, 2011, pp. 459–465