International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-12 Issue-8, July 2023

Design and Implementation of Time-lock Wallet using Blockchain Technology

Aman Anand, Chirag Sharma, Neel Bhardwaj, Amit Kumar

Abstract: ***In this work, authors have presented a design and implementation of the Time Lock Wallet. ThisTimelock model n This is done by using Blockchain Technology. The main goal behind time-locked walletsis to lock the money for a specific amount of time. After the stated date has passed, only the designated person/beneficiary may take money out of the wallet.***

Keywords: Time-lock, Blockchain, and RSA[1] Blockchain; Blockchain operations; distributed digital tally technology; Blockchain Tools

I. INTRODUCTION

There are times when we must provide someone with sensitive information by a certain deadline, but it would be detrimental to our interests if the informationleaked out right away. A straightforward example is a public procurement tender because there are deadlines for submission and for opening the bids and sharing the most crucial bid qualities, such as the ffered price. This is why the procurer does not want any more assistance from the bidders, hence the sensitive material must either not beencrypted or have the decryption key attached. However, the bidder does not want to rely on the reliability of an uncontrolled party and wishes to keepthe bid secret until the official opening. The answer isan encryption method where the decryption is technically impossible before a given time and is not required. Co-operation between the parties after the submission [6]. Authorities in the center, or trust. While Bitcoin and other cryptocurrencies make considerable use of blockchain technology, it may also be used for other things. An inventory of blocks is a blockchain. An address to a hash is contained in each block of data. Deals are the main usage of blockchain. A decentralized record that cannot be commuted to.

Manuscript received on 25 June 2023 | Revised Manuscript received on 07 July 2023 | Manuscript Accepted on 15 July 2023 | Manuscript published on 30 July 2023.

*****Correspondence Author(s)

Aman Anand*, Graduate Student, School of Computer Science and Engineering, Galgotias University, Greater Noida (U.P), India. E-mail: anandaman141@gmail.com, ORCID ID: 0009-0000-0084-1190

Chirag Sharma, Graduate Student, School of Computer Science and Engineering, Galgotias University, Greater Noida (U.P), India. E-mail: chirag.sharma.1005n@gmail.com, ORCID ID: 0009-0008-0063-7470

Neel Bhardwaj, Graduate Student, School of Computer Science and Engineering, Galgotias University, Greater Noida (U.P), India. neelbhardwaj5@gmail.com

Amit Kumar, Assistant Professor, School of Computer Science and Engineering, Galgotias University, Greater Noida (U.P), India. E-mail: amit.kr@galgotiasuniversity.edu.in

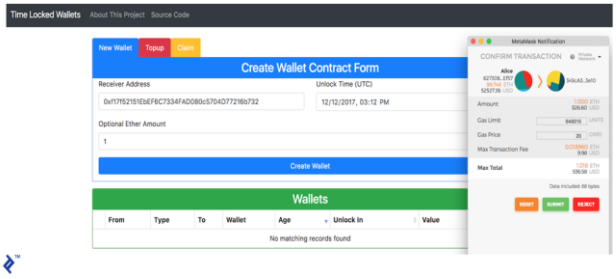


Figure 1. The visual illustration of the model.

twill benefit the employee in the following ways: Time-locked wallets are safer than regular cryptocurrency wallets because no one, not even hackers, can remove the coins before the set date or block height. This means that those who have faith in Bitcoin's long- term prospects can lock their coins up for a long period without having to worry about them being stolen. [4]. Time-locked wallets are also a good idea for those who want to keep their Bitcoin for a certain amount of time but don't trust themselves not to sell early. Putting funds in a time-locked wallet ensures that the devil doesn't make work for your idle thumbs and you stick to your convictions.

II. METHODOLOGY

Blockchain is a method of storing data that makes it difficult or impossible to change the system, hack it, or cheat. A network of computer systems known as ablockchain merely copies and disseminates a digital log of transactions across the whole network. It is thedecentralized ledger of all transactions in a peer-to- peer network. With the use of this technology, participants can confirm transactions without a central clearing institution. Applications may require you to make payments, seal business deals, cast ballots, and do a variety of other things [2]. If you are driven by market emotions to panic sell amid price volatility, locking these funds away in awallet might be a good idea. The last will - If you want to leave your family somemoney that they can access after a certain date in theevent that something were to happen to you, but youwant to keep it hidden. The cash in the wallet may only be withdrawn by the selected person/beneficiary and after the specified date has passed.

III. PROPOSED METHOD

a. Generating the encryption key

An encryption key is frequently a random string of bits designed specifically to muddle and unmuddle data. Each encryption key is unique and surprising because of the algorithms employed to create them.

The longer the key is generated in this technique, the more challengingit is to decrypt the data [3].

b. Encryption

The RSA method maps the remainder classes of N that are coprime with the modulus to a new remainder classof N, which is considered the crypto value. First, the encrypted data must be assigned to a remainder of N. Itis easy because any digitally stored data can be interpreted as a positive integer. The assignment is bijective if the integer representing the data is smaller than modulus N. This condition can be met by partitioning the data to blocks and encrypting them or by using a hybrid cryptosystem. We use the latter, because in a public blockchain the decryption of the data itself would mean a disclosure to the public. In a hybrid system first, a symmetric key is used to encrypt the data, that can be huge. Then the encryption key of the asymmetric cryptosystem encrypts the symmetric key. The encrypted data and the encrypted symmetric key is transmitted to the receiver, who first decrypts the symmetric key using the decryption key of the asymmetric system, getting the open symmetric key, then decrypting the data with that key. The key size ofthe symmetric cryptos (e.g. AES) are smaller than modulus N used by RSA, providing the same level of security. We fill the unused bits with random values. Here in after, we consider the symmetric key as dataN to be encrypted. Data source encrypts the data by computing the crypto value C = De mod N [4].

Distribution of the factors of the decryption key Let's take an implemented blockchain system (e.g. Ethereum). Let's suppose that we have at least k collaborative partner with a smart contract-enabled wallet to operate the time-lock encryption service. Thedata source hands over the data encrypted by the symmetric key to the recipient(s) with the identifier ofthe smart contract where the symmetric key will beavailable after t2, and also selects k wallets of the collaborative partners and sends them the di=1..k factors of the decryption key d, encrypting them by thepublic key of the wallet. If the number of partners isbigger than k, then one factor can be sent to multiplepartners, but the difference between the most and leastshould not exceed one (most even distribution) [8].

Uploading the crypto data into the blockchain The data source uploads crypto data C and modulusN into a new "time-lock encryption" class smart contract of the blockchain to a state variable, in theconstructor function. The collaborative partner's wallets have access to the functions of this smartcontract however, anybody can see crypto data C.They get their key factor di in the contract encrypted by their public key also in a state variable mapped totheir wallet identifier to show the wallet which factorto use as an exponent parameter in the function of thesmart contract. They download the encrypted factor and decrypt it by their private key. The encrypted Cis public, but the decryption is only possible by the Algorithm used [9].

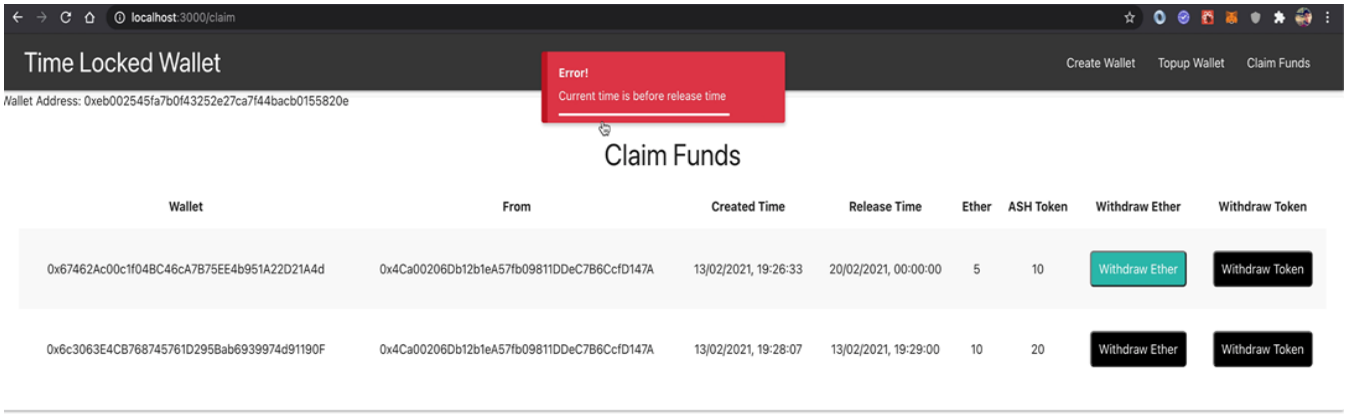


Figure 2. Below figure show the working of the model.

c. *Decryption.*

Decryption is the process of restoring data that has been encrypted to its original state. Typically, the process of encryption is reversed. Decryption requires a secret key or password, thus it decodes the data so that only an authorized user may decrypt the information [13].

IV. SMART CONTRACTS

Smart contracts can be understood as dealing machines with no cashier. There's no central station in the blockchain network. For the development of smart contracts, some tools are needed that are used to maketheframe and emplace them on the blockchain. Smart contracts are simply programs stored on a blockchainthatrun when destined conditions are met. For illustration, NFTs are like special coins that can not betraded for other coins. They're made using a special computer program that gives someone power of the coin and if theysend it to someone different, the power changes too. It's like having a special agreement between the people buying and dealing with the coin that's written in computer language [7].

V. EXPERIMENTATION

The block height can be used to perform actions over time. If you know the average block time, then you can calculate roughly how many blocks will be mined in a specific time frame. We will use this concept to create awallet contract that unlocks at a specific block height. Such a contract can be useful if you want to bestow tokens to someone after a certain time period.

Imagine that in the crypto-future you want to put some money aside for when your child comes of age. Naturally you would do this by means of a smart contract! [11]. From our main projects folder, we create a new projectclarinet new time-locked-wallet.

Inside the time-locked-wallet into the folder, we createthe contract files using the following command:
clarinet contact new time-locked-wallet
Instead of starting to code straight away, let us take a moment to consider the features we want to have [14].
A user can deploy the time-locked wallet contract.

- Then, the user specifies a block height at whichthe wallet unlocks and a beneficiary.
- Anyone, not just the contract deployer, can sendtokens to the contract.
- The beneficiary can claim the tokens once thespecified block height is reached.
- Additionally, the beneficiary can transfer the right to claim the wallet to a different principal. (For whatever reason.)
  With the above in mind, the contract will thus feature the following public functions:
- lock, takes the principal, unlock height, and an initial deposit amount.
- claim, transfers the tokens to the tx-sender if and only if the unlock height has been reached and the tx- sender is equal to the beneficiary.
- bestow, allows the beneficiary to transfer the rightto claim the wallet [14].

There are several applications for Ethereum smart contracts. The two that are now most popular are token sales for crowdfunding, commonly known as initial coinofferings, or ICOs, and cryptocurrencies (implemented as ERC20 tokens). A good illustration of a utility ERC20 token is the Motoro Coin. In this blog article, we'll look at an uncommon idea—locking money in contracts for Bitcoin wallets. Numerous applicationsmay be made of the idea itself [5]. Alternatively, a smart contract might work as a cryptocurrency will. Consider the case where we desireto save our bitcoin holdings in a contract that our heirs can only access after our passing. Imagine that we needto call a contract function on a regular basis to 'check in'with the wallet. They may take the money out if we don't show up whenwe're supposed to on the grounds that we were hurt. Theamount of money that each family member would get might be specified in the contract or left up to the family members' discretion [10].

VI. RESULT AND DISCUSSION

We want to RSA encrypt a document with the condition that no other party can decipher before a given time. The exponent of the decryption key is generated as a product of random values and the encrypting exponent is calculated from that. The said factors of the decryption key are made accessible to selected wallets of the blockchain on a protected way. A smart contract is constructed in the way that controlsthat the wallets that perform the modular power operation exactly once with every key exponent factor, maximum one transaction in a block. The shortest timeof decryption can be set by defining the frequency of transactions in units of block time [12].

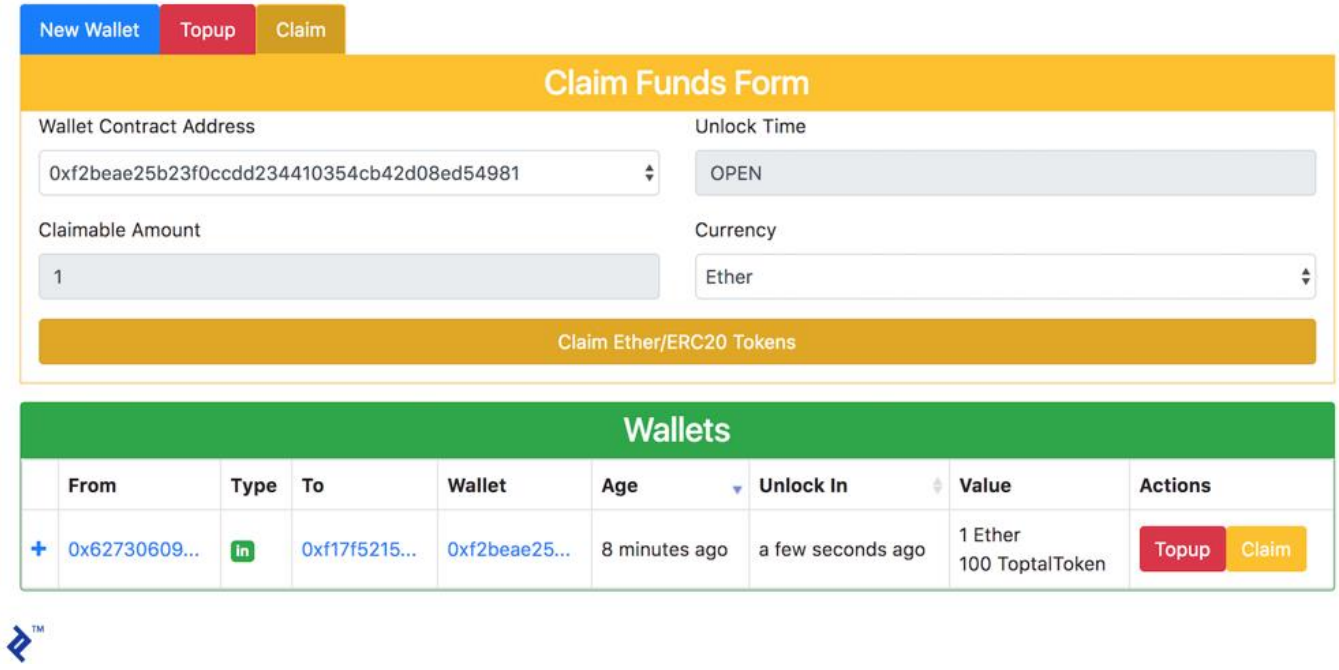


Figure 3. Showing the sample dataset.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

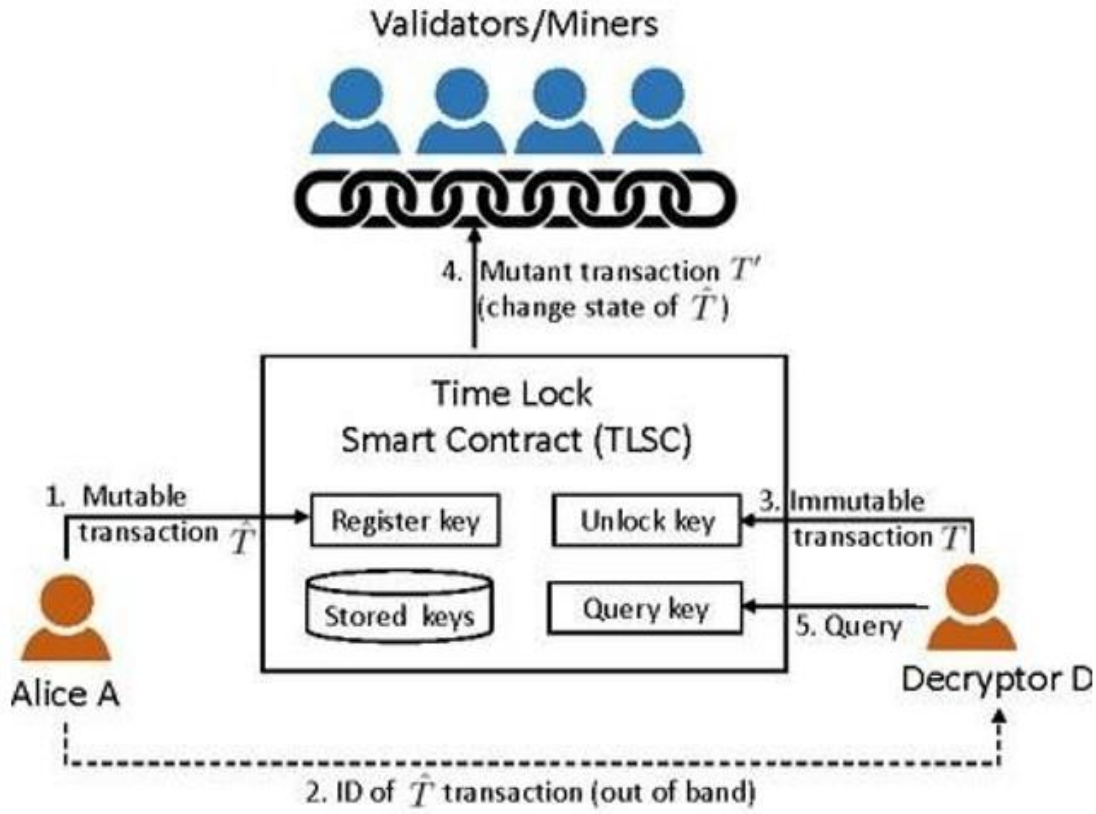


Figure 4. Above figure for demonstration.

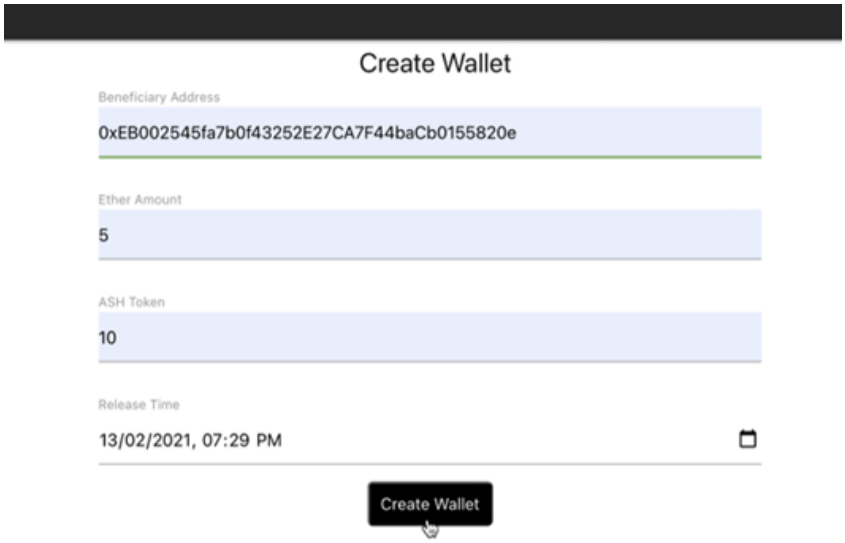
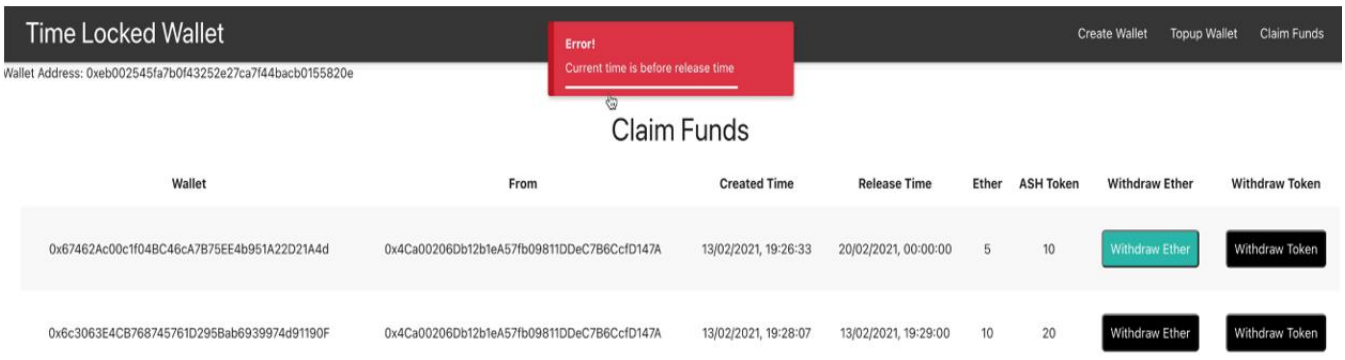


Figure 5. Illustration of Time Lock Wallet.



Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

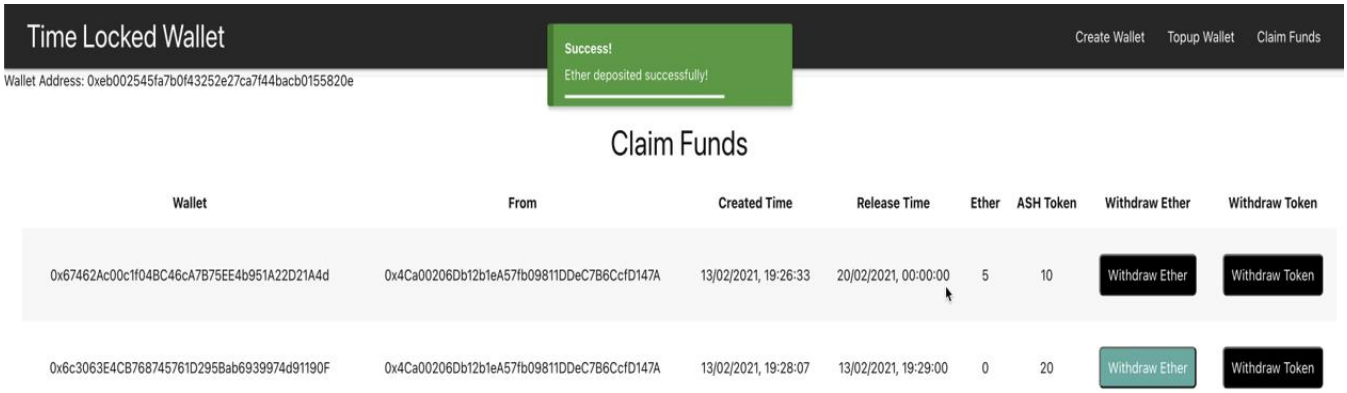


Figure 6. The snapshots of the working modules.

VII. CONCLUSION

The idea behind time-locked wallets is to lock the funds for a set period of time. The amount locked in the wallet can only be withdrawn when the set date is passed and only by the authorized person/beneficiary. This Timelock model is a restriction mechanism builtinto crypto transactions that define an actual time or block height to confirm a transaction on the blockchain network. Think of this as functionality for scheduling transactions. This is done by using Blockchain Technology. We have noticed that Time locked wallets are also a good idea for those who wantto keep their Bitcoin for a certain amount of time but don't trust themselves not to sell early.

DECLARATION

Funding/ Grants/ Financial Support	No, I did not receive any financial support for this article.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, this article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	All authors having equal contribution for this article.

REFERENCES

1. Balaskas, Anastasios, and Virginia NL Franqueira. "Analytical tools for blockchain: Review, taxonomy and open challenges." 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, 2018. [CrossRef]
2. Vacca, Anna, et al. "A systematic literature reviewof blockchain and smart contract development: Techniques, tools, and open challenges." Journal of Systems and Software 174 (2021): 110891. [CrossRef]
3. Oliveira, Luis, et al. "To token or not to token: Tools for understanding blockchain tokens." (2018).
4. Bergquist, Jonatan. "Blockchain technology and smartcontracts: Privacy-preserving tools." (2017).
5. Agustin, Farida, et al. "Utilization of blockchain technology for management E-certificate open journalsystem." Aptisi Transactions on Management (ATM) 4.2 (2020): 133-138. [CrossRef]
6. Piazza, Fiammetta S. "Bitcoin and the blockchain as possible corporate governance tools: Strengths and weaknesses." Bocconi Legal Papers 9 (2017):125.
7. Nguyen, Quoc Khanh. "Blockchain-a financial technology for future sustainable development." 2016 3rd International conference on green technology and sustainable development(GTSD). IEEE, 2016. [CrossRef]
8. Pradeep, Abhinaw Sai Erri, Robert Amor, and Tak Wing Yiu. "Blockchain improving trust in BIM data exchange: A case study onBIMCHAIN." Construction Research Congress 2020: Computer Applications. Reston, VA: American Society of Civil Engineers, 2020. [CrossRef]
9. Tran, An Binh, Qinghua Lu, and Ingo Weber. "Lorikeet: A Model-Driven Engineering Tool for Blockchain-Based Business Process Execution
10. Alharby, Maher, and Aad van Moorsel. "Blocksim: An extensible simulation tool for blockchain systems." Frontiers in Blockchain 3 (2020): 28. [CrossRef]
11. Azizi, Neda, et al. "IoT–blockchain: Harnessing the power of internet of thing and blockchain forsmart supply chain." Sensors 21.18 (2021): 6048. [CrossRef]
12. Benchoufi, Mehdi, and Philippe Ravaud. "Blockchain technology for improving clinical research quality." Trials 18.1 (2017): 1-5. [CrossRef]
13. Orji, I. J., Kusi-Sarpong, S., Huang, S., & Vazquez-Brust, D. (2020). Evaluating the factorsthat influence blockchain adoption in the freight logistics industry. Transportation Research Part E: Logistics and Transportation Review, 141, 102025. [CrossRef]
14. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.

AUTHORS PROFILE

Aman Anand is currently pursuing a Bachelor of Technology (B.Tech) degree in Computer Science and Engineering from Galgotias University, Greater Noida. He is in the final year of his undergraduate program and has maintained a strong academic record throughout his studies. Aman has a keen interest in the fields of BlockChain, artificial intelligence, and data science. He is so much interested in solving real life problems. Aman has also taken part in various hackathons and has a fair grip on web development and Data structures and algorithms.

Chirag Sharma is currently pursuing a Bachelor of Technology (B.Tech) degree in Computer Science and Engineering from Galgotias University, Greater Noida. He is in the final year of his undergraduate program and has a great grip on various programming languages and computer graphics. He has completed various projects in web development.

Neel Bhardwaj is currently pursuing a Bachelor of Technology (B.Tech) degree in Computer Science and Engineering from Galgotias University, Greater Noida. He is in the final year of his undergraduate program and has some serious interest in DBMS and computer graphics. And has competed in various hackathons. He has a keen intrest in Block chain and crypto currencies.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Mr. Amit Kumar is currently working as a Assistant professor in Galgotias University, Greater Noida. He has expertise in various domains of computer science. Has various papers under his name and projects supervised.

Retrieval Number: 100.1/ijitee.H9670071282
DOI: 10.35940/ijitee.H9670.0712823
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)