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, the authors have presented a design andimplementation of the Time Lock Wallet. ThisTimelock model utilises blockchain technology. The primary goal of time-locked wallets is to secure funds for a specified period. Afterthe stated date has passed, only the designated person or beneficiary may withdraw money from 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 specific deadline, but it would be detrimental to our interests if the info were leaked immediately. A straightforward example is a public procurement tender, where there are deadlines for submission and for opening the bids, as well as sharing the most crucial bid qualities, such as the offered price. This is why the procurer does not want any further assistance from the bidders; hence, the sensitive material must either not be encrypted 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 centre, or trust. While Bitcoin and other cryptocurrencies make considerable use of blockchain technology, it can also be applied to different purposes. An inventory of blocks is a blockchain. An address to a hash is contained in each block of data. Deals are the primary use case 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

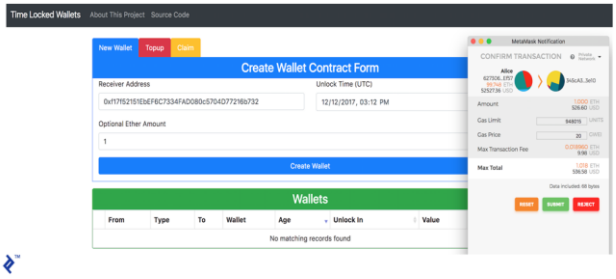


Figure 1. The visual illustration of the model.

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 an extended period without worrying about them being stolen. [4]. Time-locked wallets are also a good idea for those who want to hold onto their Bitcoin for a specific period but don't trust themselves not to sell prematurely. 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 thedecentralised ledger of all transactions in a peer-to-peer network. With the use of this technology, participants can confirm transactions without the need for a central clearing institution. Applications may requireyou 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 specific date, in case something were to happen to you, but youwant to keep it hidden. The cash in the wallet may only be withdrawn by theselected person/beneficiary, and after the specified date has passed.

III. PROPOSED METHOD

a. Generating the encryption key

An encryption key is often a random string of bits specifically designed to both encrypt and decrypt 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 the modulus N. This condition can be met by partitioning the data into 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 disclosure to the public. In a hybrid system, a symmetric key is first used to encrypt the data, which can be extremely large in size. Then the encryption key of the asymmetric cryptosystem encrypts the symmetric key. The encrypted data and the encrypted symmetric key are transmitted to the receiver, who first decrypts the symmetric key using the decryption key of the asymmetric system, thereby obtaining the open symmetric key. The receiver then decodes the data using this key. The key size ofsymmetric cryptosystems (e.g., AES) is smaller than the modulus N used by RSA, yet it provides the same level of security. We fill the unused bits with random values. Hereinafter, 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 partners 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 modulus N into a new "time-lock encryption" class smart contract of the blockchain, storing it in a state variable within the constructor 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 encryptedby their public key also in a state variable mapped totheir wallet identifier to show the wallet which factor to use as an exponent parameter in the function of the smart contract. They download the encrypted factorand decrypt it with their private key. The encrypted Cis public, but the decryption is only possible by the Algorithm used [9].

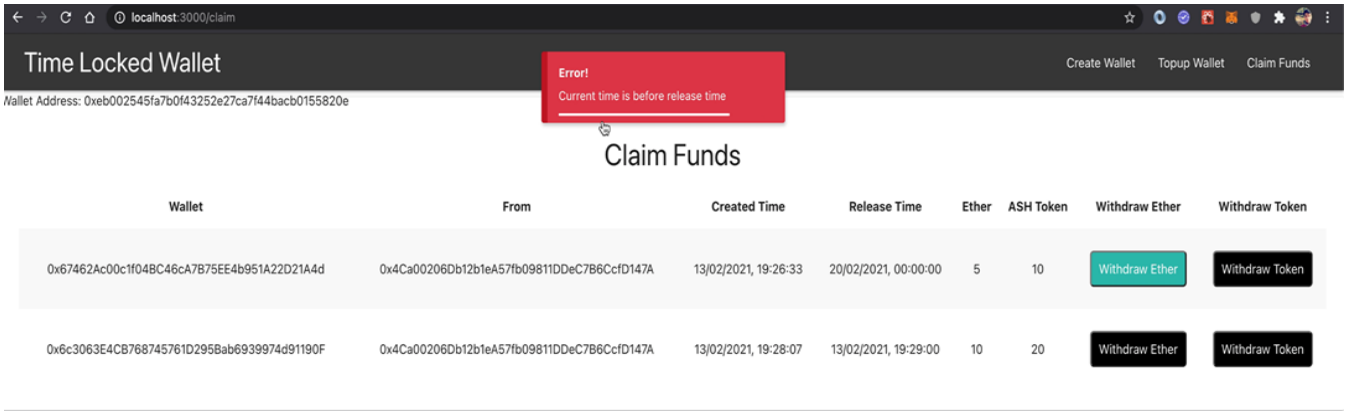


Figure 2. The figure below illustrates the model's operation.

c. *Decryption*.

Decryption is the process of restoring encrypted data 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 automated machines that operate without human intervention. There's no central station in the blockchain network. For the development of smart contracts, specific tools are needed to create the framework and deploy them on the blockchain. Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. For illustration, NFTs are like special coins that cannot be traded for other coins. They're created using a special computer program that grants someone the power of the coin, and if they send it to someone else, the power is transferred as well. 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, you can roughly calculate how many blocks will be mined within a specific time frame. We will use this concept to create a wallet contract that unlocks at a particular block height. Such a contract can be helpful if you want to bestow tokens to someone after a specific 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 through a smart contract. [11]. From our main projects folder, we create a new projectcalled Clarinet New Time-Locked Wallet.

Inside the time-locked wallet in the folder, we createthe contract files using the following command:
Clarinet contacts a 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
  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 concept itself [5]. Alternatively, a smart contract might function similarly to a cryptocurrency. Consider the case where we wish to safeguard our Bitcoin holdings in a contract that our heirs can only access after our passing. Imagine that we needto call a contract function regularly to 'check in'with the wallet. They may take the money out if we don't show up whenwe're supposed to, because we were hurt. Theamount of money that each family member would get might be specified in the contract or left up to the familymembers' discretion [10].

VI. RESULT AND DISCUSSION

We want to RSA encrypt a document with the condition that no other party can decipher it 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 on the blockchain in a secure manner. A smart contract is constructed in a way that controls the wallets performing the modular power operation exactly once with every key exponent factor, with a maximum of one transaction per block. The shortest time of decryption can be set by defining the frequency of transactions in units of block time [12].

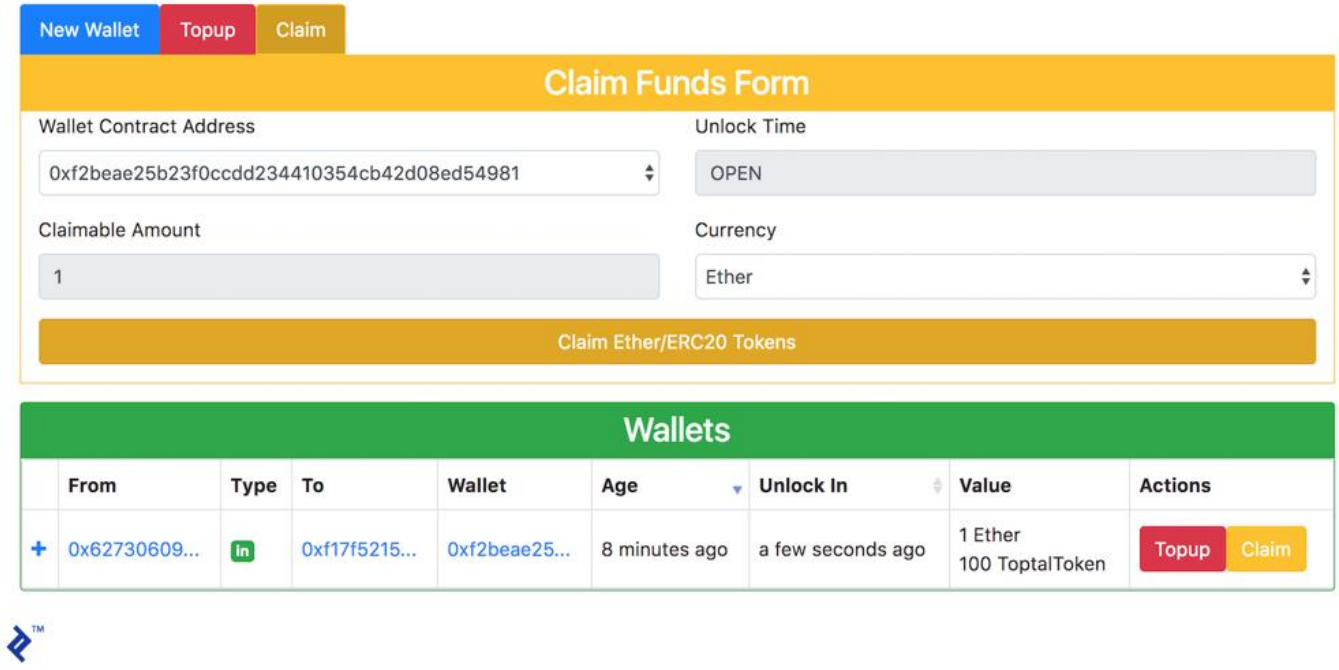


Figure 3. Showing the sample dataset.

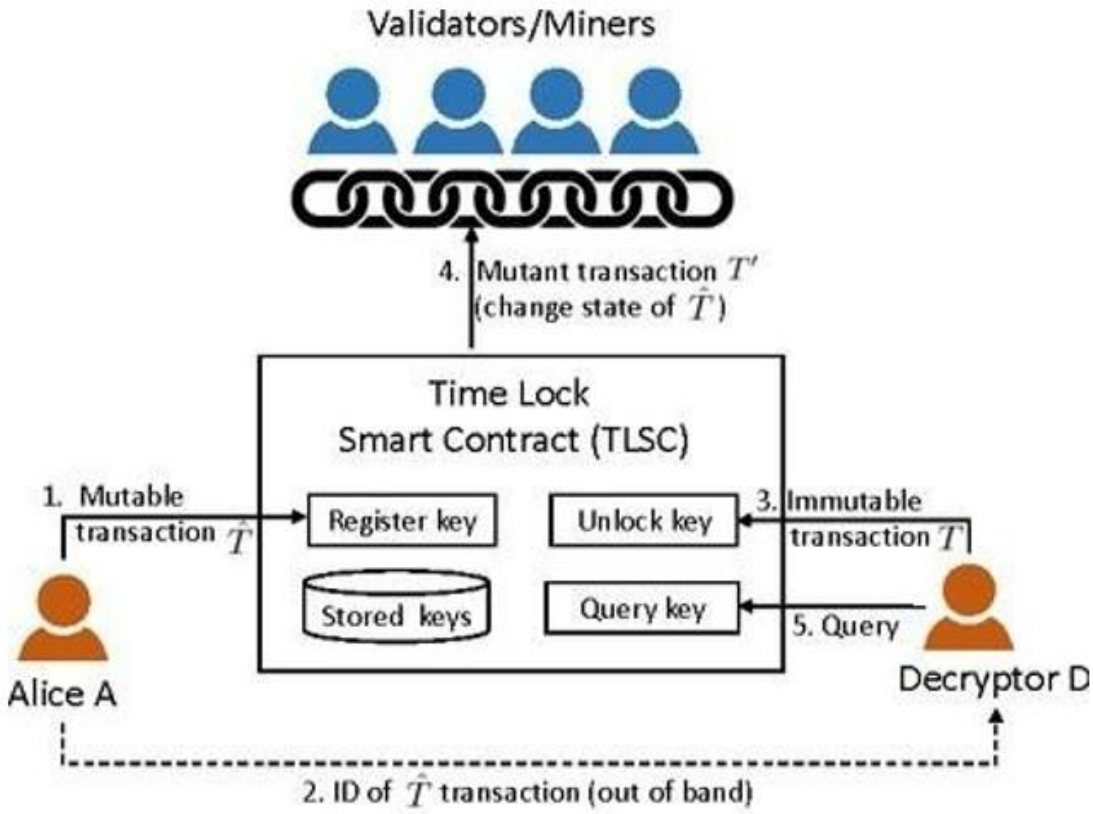


Figure 4. The above figure is for demonstration.

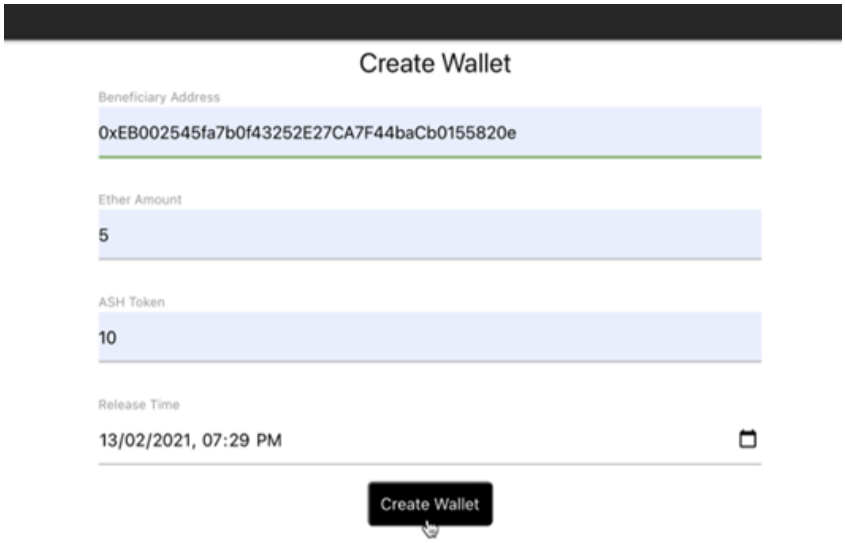
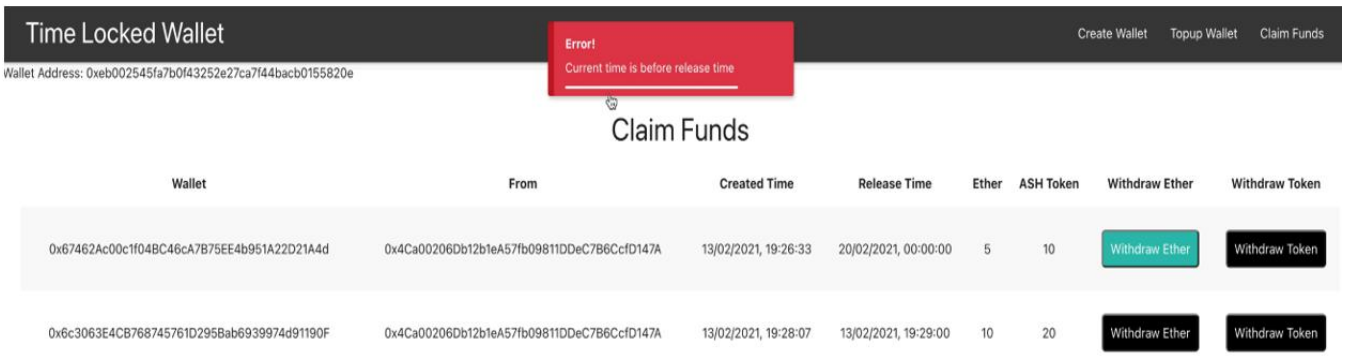


Figure 5. Illustration of Time Lock Wallet.



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)

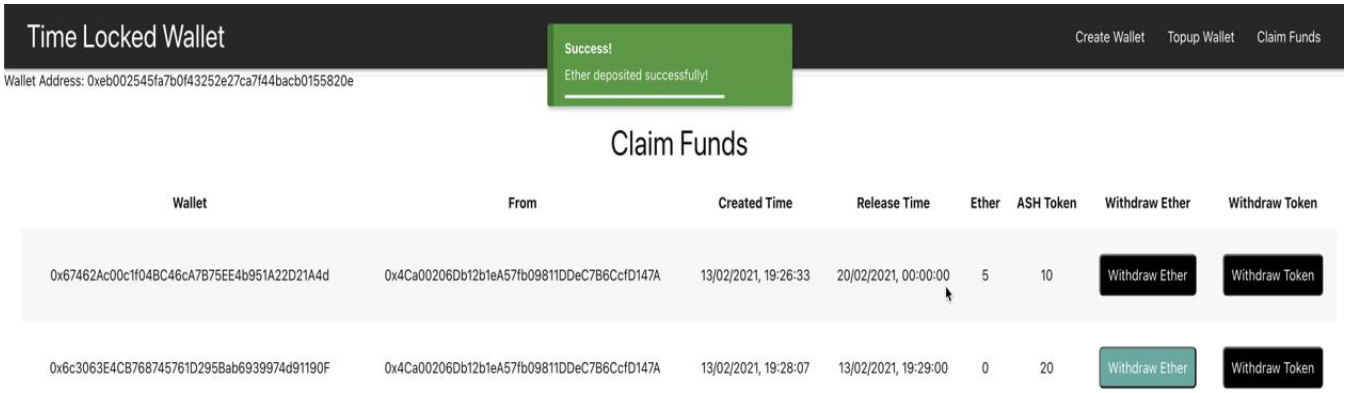


Figure 6. The snapshots of the working modules.

VII. CONCLUSION

The concept behind time-locked wallets is to secure funds for a predetermined period of time. The amount locked in the wallet can only be withdrawn after the set date has passed and only by the authorised person or beneficiary.This Timelock model is a restriction mechanism built into cryptocurrency transactions that defines a specific time or block height to confirm a transaction on the blockchain network. Think of this as functionality forscheduling transactions. This is achieved by utilising 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 or consent to participate, as it is based on evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	All authors have equal contributions to 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 review of 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 on BIMCHAIN." 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 the Internet of Things 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 his final year of undergraduate studies and has maintained a strong academic record throughout his program. Aman has a keen interest in the fields of BlockChain, artificial intelligence, and data science. He is very interested in solving real-life problems. Aman has also participated in various hackathons and has a solid grasp of web development, 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 firm grasp of various programming languages and computer graphics. He has completed multiple 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 a serious interest in DBMS and computer graphics. And has competed in various hackathons. He has a keen interest in blockchain and cryptocurrencies.

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