IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12372

Fund Transfer using Block-chain application

Arghadeep Basak[1], Feon Jaison[2]

Masters Student, School of CS & IT, Jain University, Bengaluru, India[1]

Assistant Professor, School of CS & IT, Jain University, Bengaluru, India[2]

Abstract: Abstract uses blockchain technology to reduce the efficiency and cost of fund transfers. Blockchain offers important properties such as record immutability and decentralization that apply to subsequent transactions. By eliminating intermediaries during transactions and speeding up the process, this process can represent a fundamental change in the way things are done. Ethereum aims to use blockchain technology to create a decentralized treasury transfer application. By following contract restrictions, the use of smart contracts facilitates the elimination of intermediaries.

Index Terms: Blockchain, Smart-contract, Ethereum, Fund Transfer

I. INTRODUCTION

Blockchain is a decentralized, distributed public record used to conduct peer-to-peer network transactions. A block is a unit of time-stamped data storage that is linked chronologically before entering the block. The block body and block header are two parts of every block. The block header contains the block sequence number, timestamp, block size, and hash value of the previous block. Transaction counters and transactions form the body of the block. The storage and transmission of data in a blockchain system is no longer dependent on a centralized point; instead, it now occurs freely between communication points through consensus methods.

Transaction data recorded in blocks cannot be decrypted using asymmetric encryption techniques. In permissionless blockchains, anyone can participate in the verification process, meaning that no license is required to participate in the verification process, and users can contribute computing power, usually in exchange for a monetary reward. Checkpoints are authorized blocks pre-selected by a central authority or consortium. For the second categorization we have: In public blockchains, anyone can read and send blockchain transactions.

A private block restricts access to users within an organization or group of organizations. The goal of this article is to suggest a blockchain-based decentralised banking application for money transfers. So, if a Money Transfer application is created utilising blockchain technology, transactions are recorded on the blockchain permanently and can be traced back to their place and time of occurrence. Here the deposit and the previous deposit cannot be changed and the current deposit cannot be broken because all transactions are verified by points in the network. This article aims to build a decentralized network that will serve as a platform to transfer money quickly, cost-effectively, and user-friendly without the need for intermediary banks. From the right perspective, Blockchain technology can help reduce costs, enable faster transactions, and provide a complete infrastructure for financial transactions.

II. LITERATURE REVIEW

About a decade ago, Satoshi Nakamoto, the man/anonymous group behind Bitcoin, explained how distributed peer-to-peer structural blockchain technology can be used to maintain the order of transactions and avoid the double-spending problem (Nakamoto, 2008). Bitcoin orders transactions and groups into limited structures called blocks that share timestamps. Network nodes (miners) are responsible for linking blocks to each other in chronological order, each block containing the hash of the previous block to create a block (Crosby et al., 2016). Thus, the blockchain contains a secure and auditable record of all transactions.

Blockchains have fundamentally disrupted established business processes, as applications and processes that previously required centralized systems or third-party authentication are believed to be able to run at the same level of decentralization. Transparency, robustness, audibility, and security are hallmarks of blockchain architecture and design (Greenspan, 2015a, Christidis and Devetsikiotis, 2016). Blockchain is a type of distributed database where the blocks are immutable and arranged in a list. This is convenient for the banking industry because banks can collaborate on the same platform and promote customer transactions. In addition to transparency, this method facilitates the verification of blocking operations. Companies invest in this technology, seeing the potential to decentralize their architecture and reduce operational costs because it is more secure, transparent, and, in some cases, faster. That's why rumors aren't just rumors.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12372

The literature review for blockchain-based cash transfer applications will include existing studies and research on blockchain technology and its applications in financial services. Will review the following areas:

Blockchain Technology: This will include an overview of blockchain functionality, security features, and potential applications in the financial sector. Traditional Treasury Transfer Methods: This will include an overview of the current state of traditional treasury transfer methods, including their limitations and weaknesses.

Blockchain-based financial services: This will include an overview of existing blockchain-based financial services, including their features and limitations. Based on this literature review, the course will then discuss the potential of blockchain-based fund transfer programs and areas for further research and development.

III. CATEGORIES IN BLOCKCHAIN

3.1 Permissionless blockchain or public blockchain:

In permissionless blockchains, all users are allowed to create their own addresses and initiate interactions with the network by sending transactions and adding entries to the ledger. Each node in the network can use the mining protocol to validate transactions through mining operations in exchange for mining fees and block rewards. Permissionless blockchains use proof of work, which is derived by solving complex mathematical formulas, in exchange for validating transactions that are added to the ledger. Digital currencies such as Ethereum, and blockchain networks also support smart contracts. A smart contract is an automated transaction that automatically executes when certain criteria are met [1].

In order to take security measures against server attacks, the purpose of the study is to know how companies use honeypots to protect their servers against cyber-attacks. Surveys can include questions such as:

3.2 Permissioned Blockchain:

A permissioned blockchain is like a closed ecosystem where users cannot freely participate in the network. International Journal of Computer Sciences and Engineering Volume 7(3), March 2019, E-ISSN: 2347-2693 © 2019, IJCSE View all. Recorded History All rights reserved 77 or publish your trades. Permissioned blockchains are preferred by centralized organizations that use the power of the network for their internal business operations. A permissioned blockchain has a set of trusted parties to perform verification, and additional verifiers can be added with the consent of existing members or central authorities. Permissioned blockchains are intended to be compatible with existing applications. It can be a fully private blockchain or a consortium. Since the network's actors are named, the intent is that they are also legally responsible for their actions. The advantage of permissioned blockchains is scalability. In a permissionless blockchain, every node verifies every transaction, and the data is stored on every computer on the network. Any significant increase in the number of transactions will definitely lead to fewer users and more focus to perform this processing and validation. With permissioned blockchains, there are only a few select participants as miners, and large institutions can scale up their computing power to handle the ever-increasing number of transactions. Pre-selected participants make it easy to change results and easily reject transactions

IV. IMPLEMENTATION OF SMART CONTRACTS

When specific criteria are satisfied, a smart contract leverages blockchain to automatically and securely carry out its commitments. The smart contract is created to function independently of a central authority, just as other blockchain-based technologies. A smart contract has the ability to execute and enforce itself. Smart contracts use simple "if this, then that" Boolean logic to function. In this method, an item or amount of money is placed into software, which then executes this code to automatically validate and decide whether the asset should be returned to the original owner, given to another person, or refunded. Ethereum is a platform for deploying internet services, and smart contracts are the fundamental building blocks of this platform. Three major parts make up the smart contract:

State Variables: The contract has two state variables, the account balance and the account owner. The balance stores the amount of funds in the account, and the owner stores the address of the account owner.

Functions: The contract has three functions:

The first function is a constructor that initializes the balance and owner of the account.
The second function is a deposit function that allows the account owner to add funds to their account. The function takes an input parameter for the amount of funds to be added, and updates the balance accordingly.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12372

The third function is a withdraw function that allows the account owner to withdraw funds from their account. The function takes an input parameter for the amount of funds to be withdrawn, and checks if the account has sufficient funds to cover the withdrawal. If the account balance is sufficient, the function updates the balance and sends the requested funds to the account owner's address.

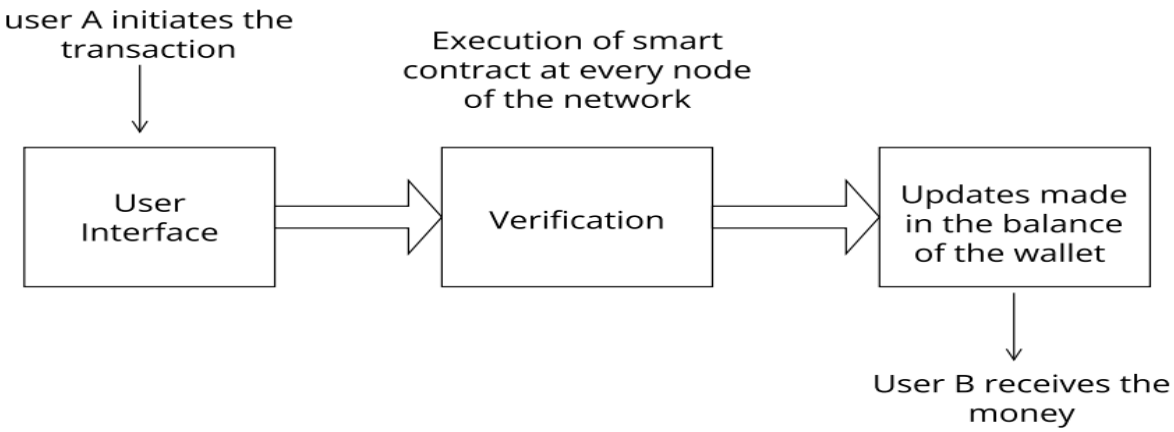
External Entities: The external entities in this contract are the account owner and any other contracts or wallets that interact with the contract.

To use this contract in a fund transfer application, a user would create a new instance of the contract and specify the account owner's address and initial account balance. The user could then call the deposit and withdraw functions to add or remove funds from the account. The contract would automatically enforce the rules and logic defined in the functions, ensuring that the account balance is accurate and that the account owner can only withdraw funds that they have available.

V. SYSTEM DESIGN

5.1 BLOCK-DIAGRAM:

In the proposed Block Diagram in the user initiates a transaction through their account or wallet using the regular mechanism a smart contract is then executed at each node in the network as part of a verification process to confirm the transactions. The balances are updated accordingly in their wallet, and then finally the receiver receives the money from the sender.



5.2 FLOW-CHART:

The proposed Flow Chart allows users to log in and check their balance, along with that they can also initiate a transfer to a particular address of other user, It is followed by organising the execution of smart contracts. Balances are updated only when the requirements of smart contracts are met.

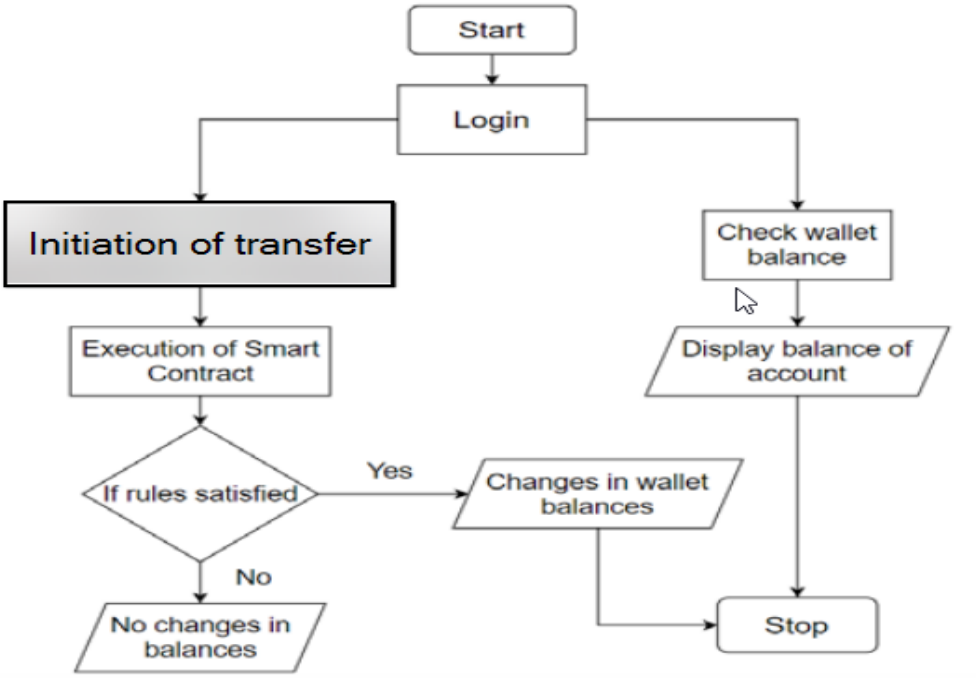
This assures that the system operates under a set of carefully adhered-to standards, preventing any fraud activities.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12372



VI. METHODOLOGY

The user of this app has to sign in and register their details like name, mobile number, and password. The user must enter their cellphone number and pin number in the login step in order to use the mobile application. Figure: The architecture of Firebase The Google Firebase, a real-time database, stores the blocks of each user, the total number of users, and the user's transactions. Details of the group of users who want to conduct their transactions in this mobile blockchain with the other registered users are stored in Firebase, a cloud database. User information such the user's name, phone number, and pin number are stored in the firebase. If the user information is valid, it is input; otherwise, users are prompted to enter accurate values. Every client has two keys: the open key and the private key, and these keys are utilised in safe transactions. The transaction is verified by the sender node and publicly revealed to other users. The receiver node will sign the transaction details with his private key in order to access them and disseminate them to other users. The adoption of a proof-of-work consensus mechanism necessitates that all nodes take part in the process of generating and verifying blocks. Four modules make up the Mobile Wallet application: the Registration, Login, Edit Contactor Updating of Details, and Transaction modules. It shows each client's square, together with its hashing evaluation, Merkle root, nonce, and hash estimation of the previous square, in addition to the time stamp shown as a long number. The Merkle root which has the hash of the considerable number of exchanges underneath, which will empower new clients to download the exchanges. The Merkle tree can be used to download the transactions if a new user downloads the Blockchain and any transactions break during the download process. When more than 51% of users in this peer-to-peer network confirm a transaction, proof of work consensus is obtained. The double-spending attack is carefully avoided by chronologically organising the timestamps of the transactions, which also prevents forking of the chain. We developed this way because there isn't a Meta mask wallet implementation like this in mobile applications. Mobile applications have not yet adopted Meta mask, which is used in permissionless blockchains (such as Ethereum) and decentralised applications to validate transactions. User information, including the user's login and cell number, is encrypted and stored in Firebase with our Android app in encrypted form, each user's total transaction count as well as the origins and receivers of their payments are displayed as well.. As a result, this programme protects both the payer's and the payee's anonymity. Both the encryption details and the user details are displayed. The transaction details of a successful transaction, including the user's public key, are provided in Log Cat along with the user validity of the chain. Homomorphic encryption is a type of encryption in which computations can be carried out in ciphertext while still producing the same results as when they are carried out on plain data. Customers can store their data in distributed storage using homomorphic encryption, which provides security and protection-preserving features. Any anonymous person or cloud service provider who wishes to conduct data mining operations can do so using encrypted data rather than actual data. As a result, it is a decentralized programme that protects privacy.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12372

VII. IMPLEMENTATION

A safe technique for the transaction is the block-chain based peer to peer money transfer using cryptocurrency. Steps for implementation are:
1. To open a new account, a user must first fill out the following information: username, email, mobile number, aadhaar card number, phone number, and user photo.
2. The user logs into the account after registration by entering their user ID and password.
3. After signing in, the user opens their account and can deposit money there.
4. The user can log out or go back to the act as access after making a deposit.
5. Withdrawal is still an option that is possible.
6. After withdrawing money, a user may log out or go back to the account panel.
7. The transfer amount to another account option is the application's final choice.
8. The transaction field allows you to view every transaction.
9. The user can log out of the account after completing his transaction.

VIII. CONCLUSION

Blockchain-based shared funds in this project do not merely go to customers and carriers who individually spend and profit from advance funds. The underlying findings of computerised money exchange tests, using the popular general advanced wallet of cryptographic finances and cloud databases, also demonstrate the protected cost-viability in computerised money exchanges and oversight between payer and payee in proposed blockchain-based distributed money move. Additionally, the suggested blockchain-based decentralized cash movement concept includes the following features:

- Constantly prepared for the next execution, bringing excellent cost investment funds;
- Purchasers' exchange records cannot be deleted.
- It is still hard to forecast buyers in order to ensure the privacy of individual data.

• If buyers have any questions about the exchange to request, they must present the exchange receipt or show that they have the right of entry to the payee's location. All trade information is transparent and unambiguous. With high level consistency, the de-united and the unaltered information is noticed by the blockchain development as the primary trade information.

The following summarises the advantageous conditions of the proposed blockchain-based shared cash move:

• For consumers: Because the sharing of information is transparent and easy to understand, consumer rights and interests are protected. Since the transaction is tenable and the timestamp is accurate. Buyers can gradually successful and tenable evidence from the proposed framework when they are compelled to offer their trades to their customers.
• For Business: Relying on all digital exchange data, businesses can do measurements and counts for their employment strategies. This may lessen mistakes made when manually recording results. The quantifiable data can be combined with store inventory management to guarantee that goods and resources are equal in value and to establish the job in accounting accuracy and wage costs.
• For the government: Progressively tenable evidence can be accommodated for reference during the time spent resolving the exchange dispute. The problem of the paper becoming illegible or lost can also be resolved by the electronic exchange receipts. We shall equip supervision capabilities for the government's financial administrative element as soon as possible.

REFERENCES

[1] H. Kuzuno and C. Karam, "Blockchain explorer: An analytical process and investigation environment for Ethereum," APWG Symposium on Electronic Crime Research (eCrime), Scottsdale, AZ, Published on 2017, pp. 9-16.
[2] Tian, Feng. "An agri-food supply chain traceability system for China based on RFID & blockchain technology." Service Systems and Service Management (ICSSSM), International Conference on. IEEE, Published on 2016.
[3] Ali, Muneeb, et al. "Blockstack: A Global Naming and Storage System Secured by Blockchains." USENIX Annual Technical Conference, Published on 2016.
[4] Larimer, D., N. Scott, V. Zavgorodnev, B. Johnson, J. Calfee, and M. Vandeberg "Steem: An incentivized blockchainbased social media platform,". Published on 2016
[5] Buba, Zirra Peter,and Gregory Maksha Wajiga. "Cryptographic algorithms for secure data communication." International Journal of Computer Science and Security (IJCSS), Published on 2011, pp .227- 243.
[6] Stapleton, Jeff, and Ralph Spencer Poore. "Tokenization and other methods of security for cardholder data." Information Security Journal: A Global Perspective 20.2, Published on 2011,pp 91-99.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Vol. 12, Issue 3, March 2023
DOI: 10.17148/IJARCCE.2023.12372

[7] Swan, Melanie, "Blockchain: Blueprint for a new economy," O'Reilly Media, Inc.", Published on 2015.
[8] Szydlo, Michael. "Merkle tree traversal in log space and time," International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg", Published on 2004.
[9] Grinberg, Reuben. "Ethereum: An innovative alternative digital currency."Published on 2011.
[10] Gilbert, Henri, and Helena Handschuh. "Security analysis of SHA-256 and sisters", Selected areas in cryptography. Springer Berlin/Heidelberg, Published on 2004. [11] Fox, Geoffrey. "Peer-to-peer networks." ,Computing in Science& Engineering , Published on 2001 pp. 75-77.
[12] Preibusch, Sören, et al. "Shopping for privacy: Purchase details leaked to PayPal," Electronic Commerce Research and Applications, Published on 2016, pp. 52-64. [13] Antonopoulos, Andreas M, "Mastering Ethereum: unlocking digital cryptocurrencies," O'Reilly Media, Inc.", Published on 2014. [14] Mathieu, Florian, and Ryno Mathee. "Blocktix: Decentralized Event Hosting and Ticket Distribution Network," (2017), https://blocktix.io/public/doc/blocktix-wp-draft.pdf [15] Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine general's problem," ACM Transactions on Programming Languages and Systems (TOPLAS), Published on 1982, pp. 382-401. [16] Gervais, Arthur, et al. "Is Ethereum a decentralized currency?" IEEE security & privacy 12.3, Published on 2014, pp. 54-60. [17] Buterin, Vitalik. "Ethereum network shaken by blockchain fork." Ethereum Magazine 12 (2013). [18] Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things."IEEE Access 4 (2016): 2292-2303. [19] Buterin, Vitalik. "Ethereum white paper." (2013), https://github.com/ethereum/wiki/wiki/White-Paper [20] Noether, Surae. "Review of CryptoNote white paper," http://monero.cc /downloads /whitepaper _review.pdf. [21] González, Andrés Guadamuz. "PayPal: the legal status of C2C payment systems," Computer law & security review 20.4(2004): 293-299. [22] Ortiz, C. Enrique. "An introduction to near-field communication and the contactless communication API," Oracle Sun Developer Network. Retrieved on Jun 30 (2008): 2010. [23] Karame, Ghassan O., Elli Androulaki, and Srdjan Capkun. "Double-spending fast payments in Ethereum." ACM conference on Computer and communications security. ACM, Published on 2012.