International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 13, Issue 4, April-2024, Impact Factor: 8.285
Presented at "ICRETETM-2024", Organized by GSMCOE, Pune, on 22nd - 23rd April 2024

# Blockchain Based Secure Transaction Management System

Pranjali Ghode[1], Jayshri Mankar[2], Kalyani Zore[3]

[1,2,3]Computer Department, Genba Sopanroa Moze College of Engineering.
Balewadi, Pune, Maharashtra, India

## ABSTRACT

A new business paradigm called e-commerce depends on autonomous transaction management on gadgets. The management structure for blockchain-based e-commerce requires independence, portability, and legality. We use blockchain to develop an autonomous transaction management system for e-commerce since it is a cutting-edge technology capable of controlling a decentralized network. However, present blockchain technologies, most notably cryptocurrencies, have the fatal flaws of being unserviceable and having a significant processing cost, making them inapplicable to blockchain-based e-commerce. In this research, we suggest a normalized autonomous transaction settlement system for e-commerce based on blockchain. The ability for the banking industry to monitor and, if necessary, manage the transaction without infringing on the privacy rights of specific users. To record and maintain track of the transactions taking place in a merchant's business, a device can operate a block chain server on the merchant's property. By adding a digital identification layer, the users' true identities are shielded. With permission from the concerned bank, the official can oversee the transaction by gaining access to the bank layer.

**Keywords**— Block Chain, Secure Transaction, E-Commerce, Transactions, JAVA, Cryptocurrency.

## INTRODUCTION

The foundational technology of the digital currency Bitcoin is blockchain. The blockchain is a decentralised database that contains copies of all performed transactions and other digital events that were shared among participants. Every transaction is confirmed by the vast majority of system users. It includes every single transaction record. A blockchain is a public ledger that everyone can view and is not under the jurisdiction of a single entity. It is a technology that makes it possible for people and businesses to work together openly and honestly. The next major advancement in information technology is thought to be driven by blockchain technology. a novel trade paradigm that achieves transactions from person to machine (P2M) or even machine to machine (M2M) rather than person to person (P2P) as in traditional Ecommerce. For instance, Amazon Dash is a one-click button that instantly buys the specified item. This is a typical illustration of converting the P2P to P2M transaction paradigm in e-commerce. The CEO of JD.com, a major Chinese e commerce company, has also recently committed to full autonomy and anticipates that robotics and M2M algorithms would eventually take over its supply chain. In addition, JD completed the construction of the largest completely autonomous logistics facility in the world in Shanghai in 2017. Therefore, it is plausible to envision a future for e-commerce in which all levels of settlements are carried out in a wholly autonomous and M2M manner. But existing Blockchain- based E-commerce platforms frequently use a jumble of dispersed, light-weight Blockchain devices. An autonomous, responsible, and lightweight M2M system must be implemented to control this dispersed structure. Blockchain is ideally suited for building a self-management system on devices due to its capacity for managing decentralised networks. Current blockchain systems may build trust and function autonomously without the need for a centralised authority because to strict cryptography. Additionally, it provides virtually flawless data integrity with its hash connected chain data structure. Thus, there is considerable confidence in the storage and sharing of transaction data. Smart contracts, which work as digital contracts strengthened by codes, can be used to further boost device autonomy.

### Problem in Hand

Traditional methods are frequently unwieldy, prone to mistakes, and painfully sluggish. To mediate the situation and settle disputes, intermediaries are sometimes required. Obviously, this causes tension and costs money and effort. Users believe the block chain to be  more efficient, transparent, and less expensive.

## LITERATURE REVIEW

We provide a method for traversing Merkle trees that only needs logarithmic time and space1. Our algorithm computes sequential tree  leaves and authentication path data for a tree with N nodes in time Log2(N) and space less than 3Log2(N), where the computation units  are hash function evaluations or leaf value computations and the computation units of space are the number of node values stored. We  demonstrate the necessary and sufficient nature of our constraints with respect to this algorithm. Over all other earlier conclusions (such  as the finding that measuring cost equals space time), this result represents an asymptotic improvement. We also demonstrate that our  approach's complexity is optimal: There is no Merkle tree traversal technique that uses less than O(Log2(N)) time and less than  O(Log2(N)) space. Our technique can improve previous traversal algorithms that loosen space limitations to increase speed, making it  particularly useful when space efficiency is necessary. [1]

Daily life is being significantly impacted by the fast advancement of wireless networking, communication, and mobile technologies.  There is a high need for secure wireless information services and dependable mobile commerce apps due to the recent large growth in mobile device users. How to create secured mobile payment systems becomes a prominent research problem in both the ecommerce  research community and wireless commerce sector since wireless payment is a crucial component of the majority of wireless information  services and mobile commerce apps. In this research, a peer-to-peer wireless payment system called P2P-Paid is proposed. It enables two  mobile users to exchange wireless payments using Bluetooth connections. The system makes use of a 2-dimensional protected protocol  that not only facilitates peer-to-peer (P2P) payment exchanges via Bluetooth between two mobile clients, but also facilitates associated  secured exchanges between the payment server and mobile clients. This essay offers an overview of the system's functional components, system design, and employed technology. The P2P-Paid system's integrated security solution is also discussed. We report on the results  of our first phase of deployment and provide examples of applications that highlight the system's capabilities and viability. [2]

Without the need for a single custodial 3rd parties holding funds or mandating participants to have anything other than a computer  connected to the internet via a broadband connection, the bitcoin protocol can accommodate the total volume of financial transactions in  the world today that are made using all electronic payment systems. It is suggested that transactions be delivered over a network of  micropayment channels, also known as payment channels or transaction channels, whose value is transferred via a block chain. These  transfers may take place between untrusted parties along the transfer route by contracts that, in the event of uncooperative or hostile  participants, are enforceable via broadcast over the bitcoin block chain through a series of decrementing time locks. If Bitcoin  transactions can be signed with a new sighash type that addresses malleability, these transfers may take place between untrusted parties  along the transfer route. [3]
Cryptocurrencies, like Bitcoin and more than 250 other cryptocurrencies that are comparable to it, are fundamentally based on the block  chain protocol, which provides a way for a distributed network of processing nodes to regularly agree on a new set of transactions.  Designing a very scalable agreement process that is susceptible to manipulation by byzantine or purposefully malevolent nodes is an open  problem in security that must be addressed in order to create a safe block chain protocol. The block chain agreement mechanism for  Bitcoin is secure but does not scale; as present, it only handles 3–7 transactions per second, regardless of the available computing power.  In this article, we suggest ELASTICO, a brand-new distributed agreement system for permission-less block chains. The number of  transaction blocks picked per unit time increases as the network's computing power increases in ELASTICO, which scales transaction  rates practically linearly with available computing power for mining. When sending network communications, ELASTICO is effective  and can put up with byzantine opponents using up to one-fourth of the system's computing resources. Technically speaking, ELASTICO  parallelizes or uniformly divides the mining network into smaller committees that each execute a different set of transactions (or  "shards") in a safe manner. ELASTICO is the first contender for a safe sharding protocol with byzantine adversaries present, despite the  fact that sharding is widespread in non- byzantine environments. Our scaling tests on Amazon EC2, which support up to 600 nodes,  validate ELASTICO's theoretical scaling capabilities. [4]

Security and privacy are huge challenges in Internet of Things (Blockchain) environments, but unfortunately, the harmonization of the  Blockchain-related standards and protocols is hardly and slowly widespread. In this paper, we propose a new framework for access  control in Blockchain based on the block chain technology. Our first contribution consists in providing a reference model for our  proposed framework within the Objectives, Models, Architecture and Mechanism specification in Blockchain. In addition, we introduce  Fair Access as a fully decentralized pseudonymous and privacy preserving authorization management framework that enables users to  own and control their data. To implement our model, we use and adapt the block chain into a decentralized access control manager.  Unlike financial bitcoin transactions, Fair Access introduces new types of transactions that are used to grant, get, delegate, and revoke  access. As a proof of concept, we establish an initial implementation with a Raspberry PI device and local block chain. Finally, we discuss some limitations and propose further opportunities. [5]

The block chain paradigm when coupled with cryptographically-secured transactions has demonstrated its utility through a number of projects, not least Bitcoin. Each such project can be seen as a simple application on a decentralized, but singleton, compute resource. We can call this paradigm a transactional singleton machine with shared-state. Ethereum implements this paradigm in a generalized manner. Furthermore it provides a plurality of such resources, each with a distinct state and operating code but able to interact through a message passing framework with others. We discuss its design, implementation issues, the opportunities it provides and the future hurdles we envisage. [6]

Online underground economy is an important channel that connects the merchants of illegal products and their buyers, which is also constantly monitored by legal authorities. As one common way for evasion, the merchants and buyers together create a vocabulary of jargons (called "black keywords" in this paper) to disguise the transaction (e.g., "smack" is one street name for "heroin" [1]). Black keywords are often "unfriendly" to the outsiders, which are created by either distorting the original meaning of common words or tweaking other black keywords. Understanding black keywords is of great importance to track and disrupt the underground economy, but it is also prohibitively difficult: the investigators have to infiltrate the inner circle of criminals to learn their meanings, a task both risky and time consuming. In this paper, we make the first attempt towards capturing and understanding the ever-changing black keywords.

We investigated the underground business promoted through blackhat SEO (search engine optimization) and demonstrate that the black keywords targeted by the SEOers can be discovered through a fully automated approach. Our insights are two-fold: first, the pages indexed under black keywords are more likely to contain malicious or fraudulent content (e.g., SEO pages) and alarmed by off-the-shelf detectors; second, people tend to query multiple similar black keywords to find the merchandise. Therefore, we could infer whether a search keyword is "black" by inspecting the associated search results and then use the related search queries to extend our findings. To this end, we built a system called KDES (Keywords Detection and Expansion System), and applied it to the search results of Baidu, China's top search engine. So far, we have already identified 478,879 black keywords which were clustered under 1,522 core words based on text similarity. We further extracted the information like emails, mobile phone numbers and instant messenger IDs from the pages and domains relevant to the underground business. Such information helps us gain better understanding about the underground economy of China in particular. In addition, our work could help search engine vendors purify the search results and disrupt the channel of the underground market. Our co-authors from Baidu compared our results with their blacklist, found many of them (e.g., long-tail and obfuscated keywords) were not in it, and then added them to Baidu's internal blacklist. [7]

## DESIGN SYSTEM

The overall system design consists of following major modules:

### 1. UI Module

This module provides Front end UI of our system without blockchain support/storage. It shows banking transactions without blockchain i.e. using simple database storage.

It allows to client signup with system and makes transactions, request fund from trusted party by exchanging currency with crypto coins. Trusted party has rights to transfer fund on request.

System generates account identifier using SHA256 algorithm and uses GUID to differentiate transactions from each other. In addition of that, it provides interfaces for login, dashboard, send fund, receive fund and request fund etc. To make system more secure it uses OTP during login process.

### 2. Block Generator and Web Miner Module

In previous module, we have created required UI for customers for sending and receiving crypto coins without support of Block Chain Platform. In this module we are going to create block chain on a single node/server and a simple proof of work (mining) System. Block chain is a chain/list of blocks. Each block has their own hash/digital signature. Our block in block chain contains following. Assume following is a single block in chain We are going to generate next hash using SHA256 algorithm. We are calculating hash by pass following input to SHA256 Algorithm == > previoushash+timestamp+data+Nonce The first block will be genesis block and its previous hash will be "0" We are going to create chain of blocks using Linked List or Dynamic Array. Once block chain is formed then we will check its integrity by looping through blocks in block chain i.e. checking current block previous hash is same as previous block hash and current hash with newly calculated hash. This is called as "Proof of Work". Any tampering with old block – requires to create whole block chain again.

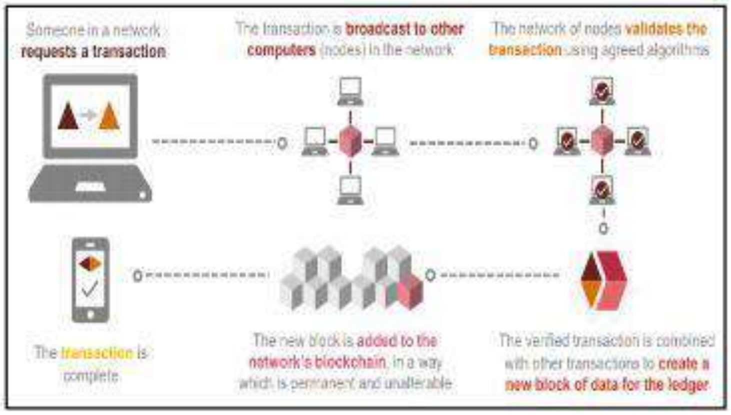

Someone in a network requests a transaction
The transaction is broadcast to other computers (nodes) in the network
The network of nodes validates the transaction using agreed algorithms
The transaction is complete
The new block is added to the network's blockchain, in a way which is permanent and unalterable
The verified transaction is combined with other transactions to create a new block of data for the ledger

**Figure no.1: System architecture**

### 3. Transactions and wallet Module

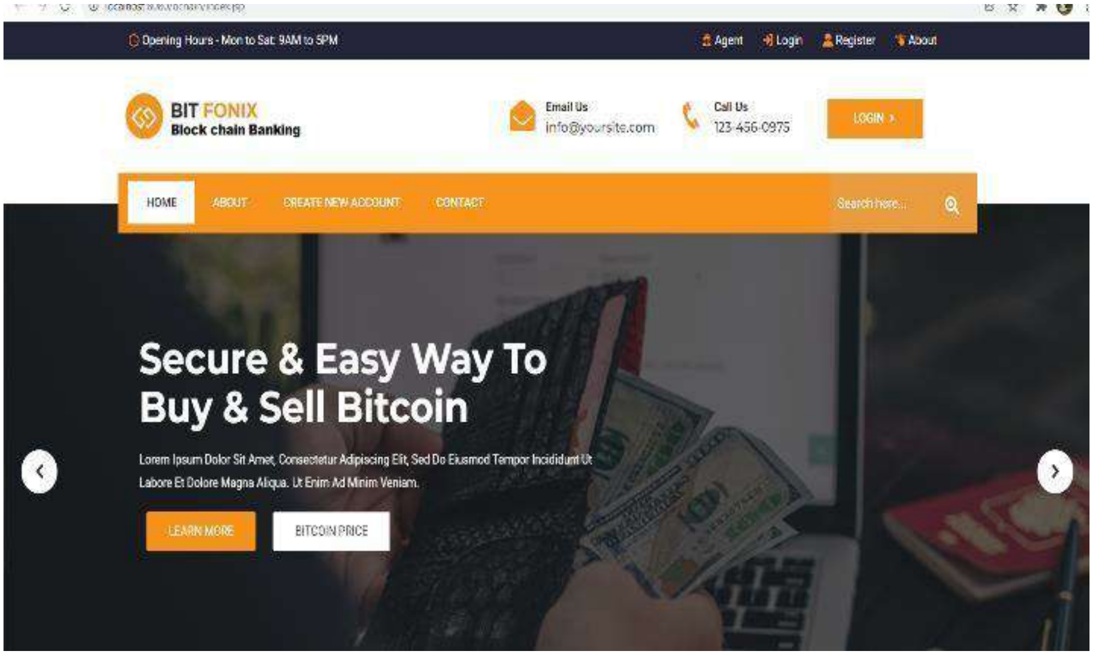
In module 2, we have stored only plain transaction message as data. In this module we are going to replace data with Transaction details and customer's wallet with public and private keys generated using Elliptic-curve cryptography For our crypto coin, public key will act as sender address hence it is OK to send share public key with others to receive payment. Our private key is used to sign our transactions so that nobody can spend/use our coins other than owner of private key. During transaction, public key will be sent and can be used to verify that our signature is valid and data is not tampered. Because signature consists of Sender+To+NoofCoins The private key is used to sign the data we don't want to be tampered with. The public key is used to verify the signature i.e. its integrity.

### 4. Peer to Peer Networks to Node

In Module 2, we have created only one node/server. In this we are going to create 2/3 nodes which will form P2P networks. Each node will maintain their copy of Blockchain and web miner will verify integrity throughout network. Here we are going to use Proof-of-Authority (PoA) is a consensus algorithm which can be used for permissioned ledgers. It uses a set of 'authorities', which are designated nodes that are allowed to create new blocks and secure the ledger. Ledgers using PoA require sign-off by a majority of authorities in order for a block to be created.

## RESULTS AND DISCUSSION

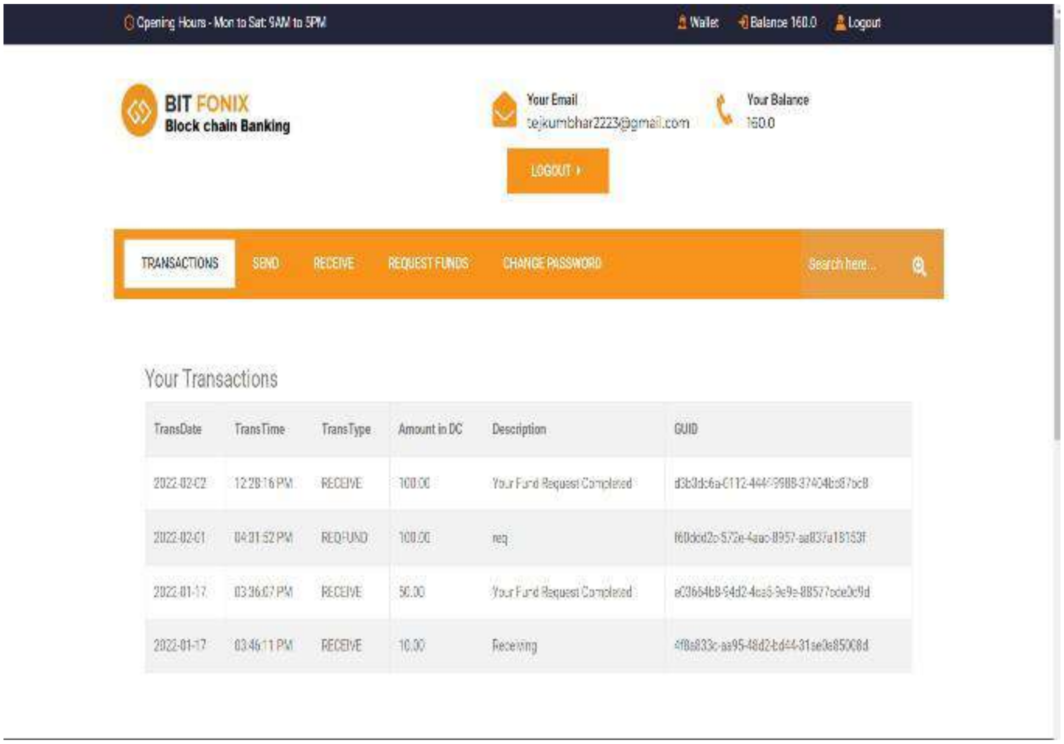
The ledger which holds the details of all transactions which happen on the Blockchain, is open and completely accessible to everyone who is associated with the system. Even though the complete ledger is publicly accessible, the details of the people involved in the transactions remains completely anonymous. Every single transaction is verified by cross-checking the ledger and the validation signal of the transaction is sent after a few minutes. Through the usage of several complex encryption and hashing algorithm, the issue of double spending is eliminated



Secure & Easy Way To Buy & Sell Bitcoin

Lorem Ipsum Dolor Sit Amet, Consectetur Adipiscing Elit, Sed Do Eiusmod Tempor Incididunt Ut Labore Et Dolore Magna Aliqua. Ut Enim Ad Minim Veniam.

Figure no.2: Initial Web page



Your Email
tejkumbhar2223@gmail.com

Your Balance
160.0

Your Transactions

| TransDate | TransTime | TransType | Amount in DC | Description | GUID |
|---|---|---|---|---|---|
| 2022-02-02 | 12:28:16 PM | RECEIVE | 100.00 | Your Fund Request Completed | d3b3dc6a-0112-4444-9988-37404bd87bc8 |
| 2022-02-01 | 04:31:52 PM | REQFUND | 100.00 | req | f60dcd2c-572e-4aac-8957-aa837a18153f |
| 2022-01-17 | 03:36:07 PM | RECEIVE | 50.00 | Your Fund Request Completed | e03654b8-94d2-4ca5-9e9e-88577cde0d9d |
| 2022-01-17 | 03:46:11 PM | RECEIVE | 10.00 | Receiving | 4f8a833c-aa95-48d2-bd44-31ae0e85008d |

Figure no.3: Transaction Page

## CONCLUSION

Thus, the system provides a secured transaction system with the help of blockchain which is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value. In future the project can be extended by implementing this secured payment system for every online transaction by increasing the encryption efficiency of the details such a way that no intruder any decrypt or corrupt it.

## REFERENCES

[1]. M. Szydlo, "Merkle tree traversal in log space and time," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2004, pp. 541–554.

[2]. J. Gao, K. Edunuru, J. Cai, and S. P. D. Shim, "P2p-paid: a peer-to-peer wireless payment system," in Mobile Commerce and Services, 2005. WMCS'05. The Second IEEE International Workshop on. IEEE, 2005, pp. 102–111.

[3]. J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," draft version 0.5, vol. 9, p. 14, 2016.

[4]. L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016, pp. 17–30.

[5]. A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Fairaccess: a new blockchain-based access control framework for the internet of things," Security and Communication Networks, vol. 9, no. 18, pp. 5943– 5964, 2016.

[6]. G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1–32, 2014.

[7]. H. Yang, X. Ma, K. Du, Z. Li, H. Duan, X. Su, G. Liu, Z. Geng, and J. Wu, "How to learn klingon without a dictionary: Detection and measurement of black keywords used by the underground economy," in 2017 IEEE Symposium on Security and Privacy (SP), May 2017, pp. 751–769.

[8]. F. Tian, "An agri-food supply chain traceability system for china based on rfid & blockchain technology,"in Service Systems and Service Management (ICSSSM), 2016 13th International Conference on. IEEE, 2016, pp. 1–6.