



IJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: <https://doi.org/10.22214/ijraset.2023.49791>

www.ijraset.com

Call: ☎ 08813907089

E-mail ID: ijraset@gmail.com

Execution of IoT System using Blockchain with Authentication and Data Protection

M. Rubika¹, Prof. S. Senthilvelan², N. Sneka³

Department of MCA, Paavai Engineering College, Namakkal

Abstract: Blockchain allows users and data providers to ensure authentication, authorization and data validity with proper multi-key exchange authentication for user identity and hash key for Blockchain so that the data is not just stored but also validated each time the user access. In this paper, we apply Zero Knowledge proof to a Strong rooms using RFID Card reader and Camera module IoT systems to prove that a prover without disclosing information such as public key enhances the anonymity of Blockchain.

Keywords: IoT, RFID Card Reader, Block Chain, Strong room, Zero Knowledge Proof

I. INTRODUCTION

Internet Of Things (IoT) is the extension of internet connectivity into physical devices and everyday objects. These devices can communicate and interact with others over the internet, and they can be remotely monitored and controlled. The paper introduces Blockchain which is a digital record of transactions. The name comes from the structure, in which individual transactions/records, called blocks are linked together to a single list called chain. Blockchain records transactions and each transaction added to the Blockchain is validated by multiple consumers. These systems are configured to monitor specific types of Blockchain transactions, form a peer-peer network. They work together to ensure each transaction is valid before it is added to the Blockchain. This decentralized network of computers ensures a single system cannot add invalid blocks to the chain. When a new block is added to the Blockchain, it is linked to the previous blocks using a cryptographic hash generated from contents of previous block. This ensures that the chain is never broken and that each block is permanently recorded.

II. PROBLEM STATEMENT

Blockchain technology consumes more energy than any centralized system. Not only does their redundancy cause them to consume more power than an average centralized cloud-based system, but their transaction validation method plays a great role too. First, they require more storage than any other system. The Approaches of authentication use centralized servers, which increases the chances of a single point of failure and the servers getting hacked. The hacking of servers can cause loss of valuable information. To avoid this problem, we need a decentralized system that allows us to identify and authenticate users. The other issue related to centralized servers is that they are managed by a third party, which can modify the data with no user permission. A new system is needed to keep the activity records of a particular user in an immutable way.

III. PROPOSED SYSTEM

IoT, Blockchain Server and Client Application. We have taken the environment of strong room in police station. Smart cards will be given to few authorized staffs working in police station, and when the person swipes card to enter into the strong room, the RFID Card reader scans the value of that particular card swiped by the person, and the camera fixed at a place captures the image of the person swiping the card. The "RFID tag+image" is a transaction which gets stored in the Blockchain ledger. Client on the other hand, to view the transaction, should get registered to the Blockchain server initially. During the registration, Blockchain server shares a secret key to the client on request by encrypting it with the public key by providing the private key. Once the client gets registered and obtains the private key from the Blockchain, that client is said to have been authenticated and authorized. Again, when the client wants to view transactions, he has to regenerate the shared secret by encrypting it with the private key. Blockchain, upon receiving, decrypts it with the public key and checks if the shared secret key is the same given to the client while registering. Once the combination of the secret key is found to have been the same, Blockchain concludes that the client is an authorized person and allows the recent transaction to move to the respective user blocks. Once the transaction moves to user blocks, that particular transaction will be removed from the Blockchain ledger, hence no security breach and data tampering. In order to check the security breach, a hacker application has been developed where in, when a hacker modifies the transactions, then that particular transaction is viewed as a "bug" icon in the user block.

IV. DESIGN & ARCHITECTURE

Smart grids are intelligent grids that combine IT technology with traditional grids to enhance the efficiency of the energy utilization. In a smart grid environment, each Advanced Mitigation Infrastructure (AMI) is deployed in users and facilities, and can be used to measure energy production and utilization and provide services such as resale. In a smart grid environment, smart meters are needed to measure power consumption. The smart meter is installed at the end of each device to record the power consumption and production of the device, and the accumulated data can analyze the power usage pattern. Security vulnerabilities for smart meters have privacy concerns that analyze patterns using power usage eavesdropping and traffic analysis. There is also the risk of moderating the power data transmitted from the smart meter to charge lower or higher costs. So we need to introduce smart meter authentication technology.

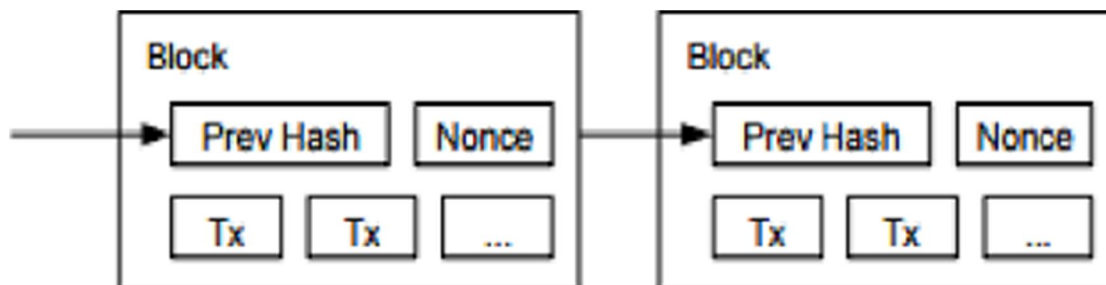


Fig. 1. Block Chain Concept Map

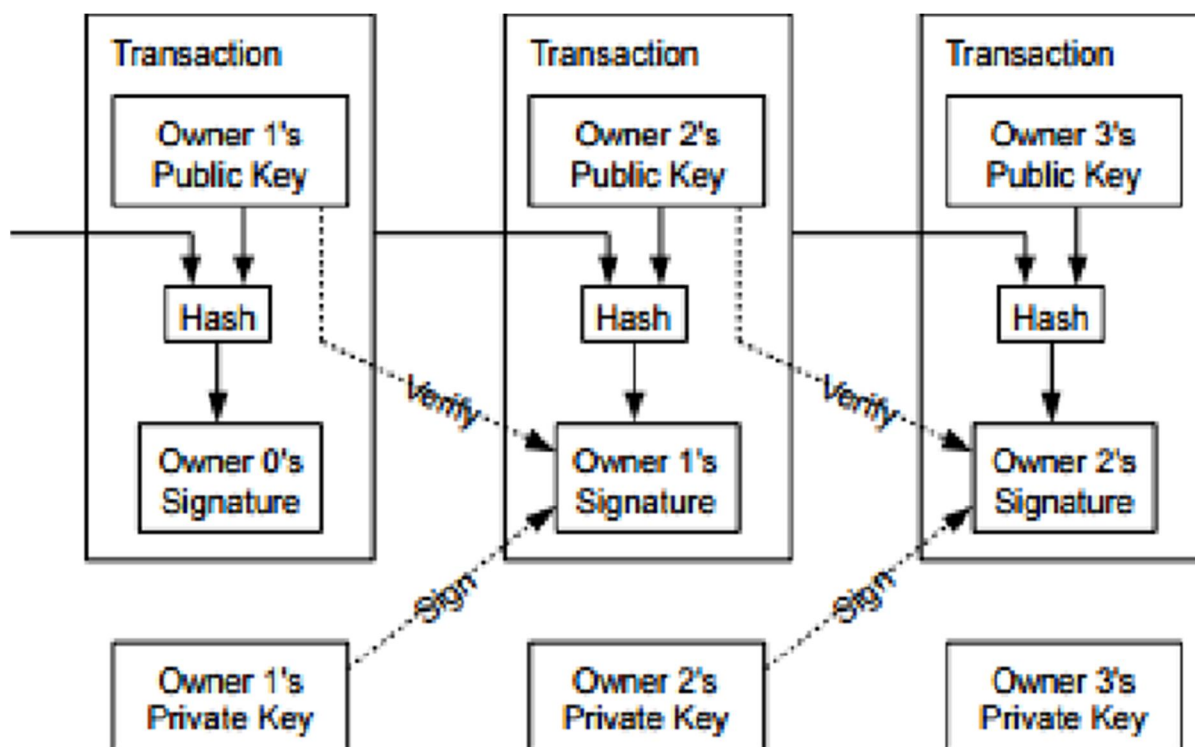


Fig. 2. Transactions in a block chain

Block chain has been applied to bitcoin and Ethereum using security technologies such as electronic signatures, public keys, and hash functions. The bitcoin developed by Satoshi Nakamoto is getting attention, and it is also studying the utilization method in financial and non-financial areas including virtual currency. In the bitcoin, the block chain is a kind of distributed digital book that stores the history of the bitcoin, which is a currency issued periodically. This ledger is made of cryptographic techniques that can not be counterfeited or modulated and is made as a verification step to prevent forgery and tampering of transactions through transaction processes and hash values for the transfer of ownership.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)