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

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.134181

IMPLEMENTATION OF IOT USING BLOCK-CHAIN WITH AUTHENTICATION AND DATA PROTECTION

Darshan M[1], Viswanth D[2], Chethana P[3], Chandana C P[4]

Department of CSE, Dayananda Sagar university Bengaluru, India[1-4]

Abstract: In a humanity loaded of new technology, the menace of sting is constantly multiplying. In the shields assiduity, this threat was long before the use of technology. Congress legislated the shields Act of 1933 to battle the menace of sting and misrepresentation in the trade of armors. By challenging chock-full exposure, investors possess the occasion to make informed opinions previous to investing. still, Distributed Autonomous Associations(“ DAOs ”), through the use of blockchains and smart - contracts, engage in the trade of securities without completely telling the pitfalls or complying with the enrollment conditions of the Securities Act of 1933. Compliance with the burdensome conditions of enrollment , still, would destroy this new technology and system of conducting business. To avoid this reversal, Congress must amend the enrollment conditions to give an impunity for DAOs. This impunity, although reducing current enrollment burdens, must still bear DAOs to expose certain information, there by icing investors are informed previous to investing. likewise, due to the unique nature of the blockchain, smart contract, and DAOs, Congress must put a fiduciary duty on the generators of DAOs to insure compliance with the exposure conditions. Further, Congress should consider the allowance of burden - shifting following the original crowd trade. In a block-chain IoT atmosphere, when data or device authentication information is lay on a block chain, particular information may be blurted through the evidence- of- work course or declamation hunt. In this document, we refer Zero Knowledge evidence to a sharp cadence network to demonstrate that a prover without telling information similar as public key, and we've studied how to enhance obscurity of block chain for sequestration protection.

Index Terms: Transaction, Transaction of insurance,bank transaction details, block-chain, Cloud -storage , Zero knowledge proof , Evolution of block chain.

I. INTRODUCTION

In our increasingly connected world, the Internet of goods(IoT) has came up as a transformative technology, allowing indefectible communication between bias, and furnishing vast breaks for automation and data- driven decision- timber. still, with these advancements come new challenges, particularly in the realm of security and data protection. As IoT bias come more integrated into our day-to-day lives, it's consummate to ensure the confidentiality, integrity, and authenticity of the data they induce and exchange. Our design," performance of IoT System using Blockchain with Authentication and Data Protection," aims to address these enterprises head on. We recognize that the integration of blockchain technology, robust authentication mechanisms, and data protection protocols is essential for creating a secure IoT ecosystem. The Internet of goods(IoT) is swiftly expanding and converting various industriousness, including healthcare, transportation, and manufacturing. As the number of IoT bias continues to grow, so does the volume of data they induce. This data can be largely precious, but it also raises enterprises about security and insulation. Blockchain technology, with its decentralized and tamper- substantiation nature, offers a promising result to address these enterprises in IoT systems. This design aims to apply an IoT system that utilizes blockchain technology to enhance authentication and data protection. In today's connected world, Internet of Things (IoT) devices play a crucial role in making our lives easier. These devices, ranging from smart thermostats to health trackers, gather and share data. However, ensuring the security of this data is a top priority.

Fig. 1. Transaction in the block chain

DOI: 10.17148/IJARCCE.2024.134181

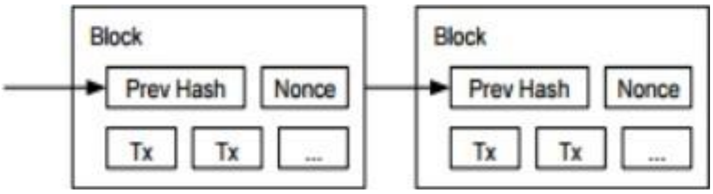


Fig. 2. . Block Chain Concept Map

II. CONCEPT MAP

Smart Contract was first introduced by Nick Szabo in 1994 and is defined as a protocol that enables the motorized deals to be decoded by rendering the necessary rudiments of the contract(10). This is a technology that enables the need for a good third party to be minimized(11).

Ethereum is a representative block chain with smart contracts. Etherium was proposed by Vitalik Buterin in 2013 and introduced smart warranties as well as virtual currency, enabling inventors to apply operations directly. Software updates can be used to produce operation platforms that can apply colorful DAPPs, similar as IoT or operation services(12).

Block chains with obscurity include Monero, gusto, ZCASH and so on. An anonymous block chain is a block chain that makes it insolvable to trace an account and sale contents, similar as an account,etc., in order to help particular information violation. They enforced an anonymous block chain using different security technologies. Monroe applied a technology to help dogging of being bit coins with digital means using Cryptonote protocol. It used a special encryption fashion called Ring Autographs, One- time keys. It is veritably sensitive for a third party to verify the contents of a sale because the key is mixed in a certain group and a private key is needed to confirm the sale(13). gusto is a fashion of ensconcing sale records through the fashion of coin joining. It started with the name of Dark Coin, but changed its name to gusto Coin for image improvement. It's delicate to track deals using a fashion of mixing coins to be traded by concocting a new type of knot called a master knot(20). ZCASH is a block chain of cryptographic grounded on zero knowledge evidence technology. Other than the information handed by the provider, it's designed so that it can't be known by the philanthropist. Depending on the choice, the provider may give information similar as the being block chain. ZCASH, enforced as a zero- knowledge evidence, distributes anonymized,non-traceable technology in coordination with Etherium and ZPMorgan(17).

A Zero knowledge evidence is a system of proving that information is known without telling any information. The conception of the zero knowledge evidence presented in the block chain is a evidence system that can prove a sale or a work without exposing the information or sale information of the virtual plutocrat to the outside. It's a evidence system which satisfies three parcels of absoluteness, impracticality, and Zero Knowledge. This simple concept map highlights the basic elements of blockchain technology and how they work together to create a secure, decentralized system for recording and managing transactions.

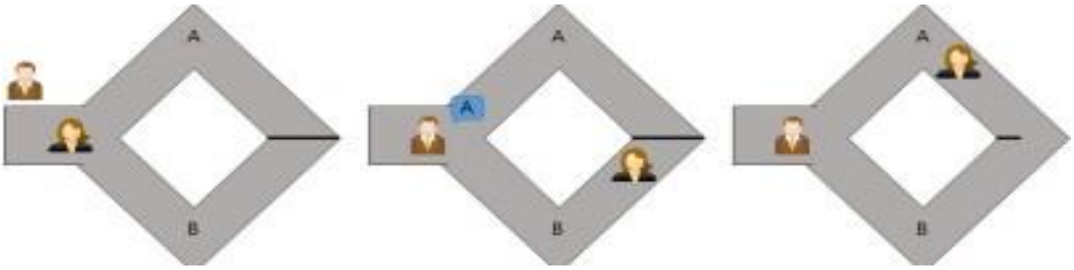


Fig. 3. Zero Knowledge proof

- **Benefits of Smart Contracts:**

Zero-knowledge proofs, or ZKPs, have multiple important applications in a variety of domains, most notably data privacy and cryptography. Here are a few main benefits:

Privacy: Using zero-knowledge proofs (ZKPs), a prover can demonstrate to a verifier that a statement is true without disclosing any details about the statement itself. This maintains privacy by enabling the verification of sensitive information without disclosing the data itself.

Security: Because ZKPs guarantee that information is kept private even throughout verification procedures, they offer a high level of security. This is especially crucial for sensitive transactions where data privacy is critical, including financial transactions or identity verification.

Efficiency: Compared to other cryptographic methods, ZKPs can be constructed with a comparatively small processing overhead.

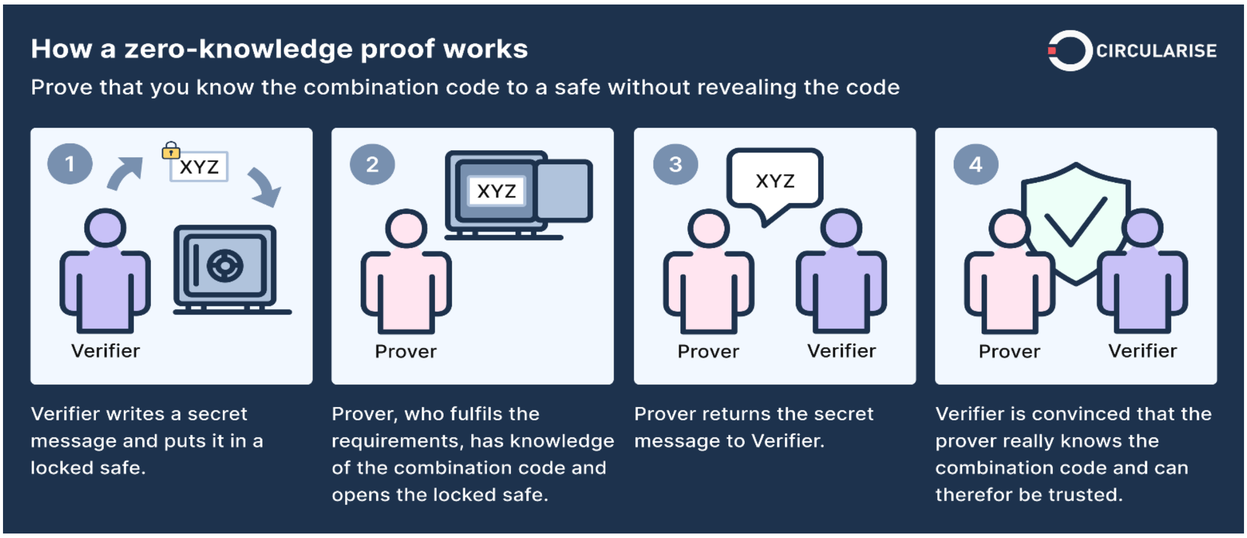
Lack of trust: ZKPs let parties to communicate and do business without requiring faith in a central authority or one another. In decentralised systems like blockchain networks, where users may not have complete faith in one another but still need to perform secure transactions, this trustlessness is extremely useful.

Scalability: Even if the size of the network or the complexity of transactions grows, ZKPs may be made to scale effectively. They operate well in large-scale distributed systems and networks because of their scalability.

Fraud Prevention: By allowing parties to confirm the validity and integrity of data without disclosing sensitive information, ZKPs can aid in the prevention of fraud. This can be especially helpful in fields like supply chain management, where it's critical to confirm the legitimacy of components or products.

Compliance: By enabling organisations to demonstrate compliance without disclosing sensitive information about specific individuals or their actions, ZKPs can help organisations comply with laws like the General Data Protection Regulation (GDPR).

Cross-organizational communication: Without the necessity for a reliable middleman, ZKPs allow for private, secure communication between several parties. This can encourage creativity and teamwork in a variety of fields, including research, healthcare, and finance, where it can be difficult to share sensitive data because of privacy concerns.



How a zero-knowledge proof works

Prove that you know the combination code to a safe without revealing the code

1 Verifier writes a secret message and puts it in a locked safe.

2 Prover, who fulfils the requirements, has knowledge of the combination code and opens the locked safe.

3 Prover returns the secret message to Verifier.

4 Verifier is convinced that the prover really knows the combination code and can therefor be trusted.

Fig. 4. Working of zero knowledge proof

Zero-knowledge proofs, or ZKPs, enable the prover to persuade the verifier that a statement is true without disclosing any details about the assertion itself. The key component of a ZKP is the ability to demonstrate knowledge of a particular topic without actually revealing it.

Setup: The cryptographic protocol to be used for the proof is decided upon by both the prover and the verifier prior to the start of the proof. Primitives of cryptography and mathematics are usually used in this protocol.

Statement and Secret: Without disclosing the value of the secret, the prover seeks to persuade the verifier that they are aware of it. Anything from a cryptographic key to a password might be this secret.

Interaction: The verifier and the prover interact with each other. In the course of this procedure, the prover communicates with the verifier in accordance with the prearranged.

DOI: 10.17148/IJARCCE.2024.134181

Challenge and Reaction: The verifier asks for evidence that the claim is factual in order to challenge the prover. In response to the challenge, the prover computes using the confidential data they have access to. These computations.

Verification: The verifier confirms that the prover's response complies with the established protocol by reviewing it. Without really finding out what the secret knowledge is, the verifier is persuaded that the prover knows.

Repeat (Optional): To boost confidence in the proof, the prover-verifier exchange may be repeated several times, depending on the particular ZKP protocol being utilised. In conclusion, the prover's claim is deemed legitimate if the verifier is content with the prover's responses and accepts the evidence, all without obtaining further knowledge about the secret itself.

It is vital to remember that ZKPs can be non interactive (like zk-SNARKs) or interactive (like Schnorr proofs), and that they can use a variety of mathematical procedures. Because each ZKP protocol has unique characteristics, benefits, and drawbacks, it can be used in a variety of settings and use cases.

All things considered, the beauty of ZKPs is their capacity to offer solid guarantees of truth without jeopardising privacy or disclosing private information. They are essential to contemporary cryptography because they provide safe authentication, privacy-preserving transactions, and many other features in a variety of applications.

Zero-knowledge proofs, or ZKPs, represent an exciting development in applied cryptography that will open up new applications in a variety of sectors, including supply chains, the Internet of Things, and Web 3. ZKPs have the potential to improve digital systems' efficiency, security, and privacy by discreetly authenticating information. We will examine the fundamentals of ZKPs as well as some emergent application cases in this post.

Consider the following scenario: you wish to demonstrate to someone that you are a citizen of a nation, but you don't want to reveal your name or passport number. It is possible to demonstrate your citizenship without disclosing your identity by using a ZKP-based identity solution. Beyond identity, ZKPs can improve the efficiency, privacy, and security of other systems in a variety of industries.

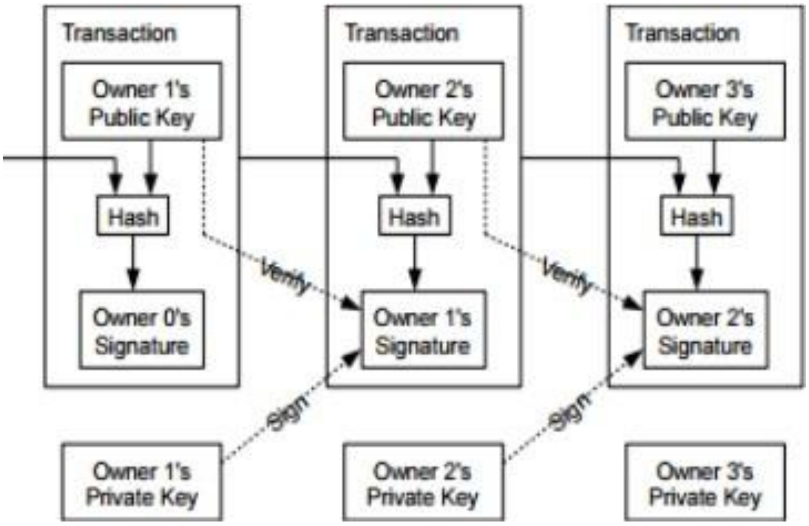


Fig. 5. Transaction inside blockchain

A blockchain transaction, to put it simply, is the transfer of a digital asset from one owner to another. The transaction itself will always contain the following information: the total amount, the funds' destination, and an authentic signature. Additionally, a blockchain transaction is typically started through the interface of a cryptocurrency wallet.

The transmission of digital assets between peers in a decentralised manner is the most apparent application of blockchain transactions. As you can see, a network of computers known as nodes stores, maintains, and processes the data on a public blockchain. In contrast to internet data, which is stored on servers with a single gatekeeper, blockchain data is stored on numerous nodes, each of which has a complete copy of the chain. This implies that peer-to- peer transfers can now be processed by blockchains in a manner.

DOI: 10.17148/IJARCCE.2024.134181

Nodes in a network handle transactions, so you don't need to depend on a centralised organisation. Additionally, you don't have to worry about strangers keeping their half of the contract because the network will ensure that they do.

A hash of the block is constructed and transaction information is gathered to determine whether or not it has been altered or fabricated. In this instance, the hash of the block is influenced by the hash value of the prior block as well. especially for its different scope of activities and consideration of both RGB video and profundity information.

- **Key Features:**

Immutability: A transaction cannot be changed or removed once it is registered on the blockchain. This is due to the fact that every block has a reference to the one before it, resulting in an impenetrable chain. This guarantees the data's reliability and integrity.

Transparency: Every transaction on the blockchain may be seen by the public, albeit user names may be kept anonymous. Within the network, this transparency promotes accountability and confidence.

Security: Cryptography, which includes hashing techniques and digital signatures,

Efficiency: Compared to typical financial transactions, blockchain transactions occasionally have the advantage of speed and cost savings. This is because they do away with the requirement for human processing.

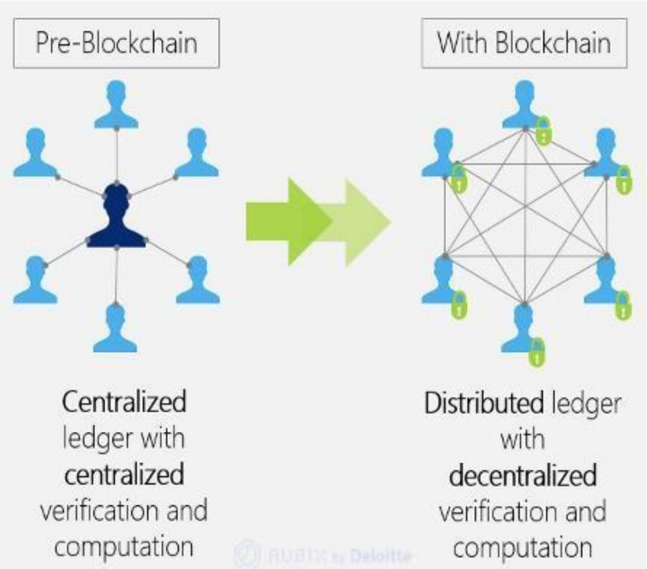

Pre-Blockchain
With Blockchain
Centralized ledger with centralized verification and computation
Distributed ledger with decentralized verification and computation
RUBIX by Deloitte

Fig 6. Blockchain transaction

Programmability: Smart contracts, or self- executing programmes that may automate the execution of transactions depending on predetermined criteria, can be created on some blockchains. This creates a plethora of new application.

Traceability: Using the blockchain, it is simple to follow a transaction's whole history. Asset movement tracking and auditing purposes can both benefit from this.

Atomicity: A transaction can be entirely completed or not at all. The absence of partial completion guarantees that the system's state doesn't change.

Benefits and Applications:

Security and Immutability: Transactions are impervious to fraud, tampering, and alteration since they are cryptographically secure and permanent. This promotes openness and trust in a variety of contexts. **Decreased**

Costs and Friction: Compared to traditional systems, the removal of intermediaries can simplify procedures and possibly lower transaction fees.

DOI: 10.17148/IJARCCE.2024.134181

Decentralisation and Transparency: By guaranteeing that no one party controls the network, distributed ledger technology reduces reliance on centralised authorities and fosters transparency.

Programmability and Automation: Smart contracts allow agreements to be automatically carried out in accordance with predetermined criteria, which may streamline complicated procedures and increase productivity.

Financial services include trade finance, fractional asset ownership, secure and effective cross-border payments, and alternative lending arrangements.

Supply chain management: Ensuring accountability and transparency by tracking the origin, transportation, and ownership of items across the supply chain.

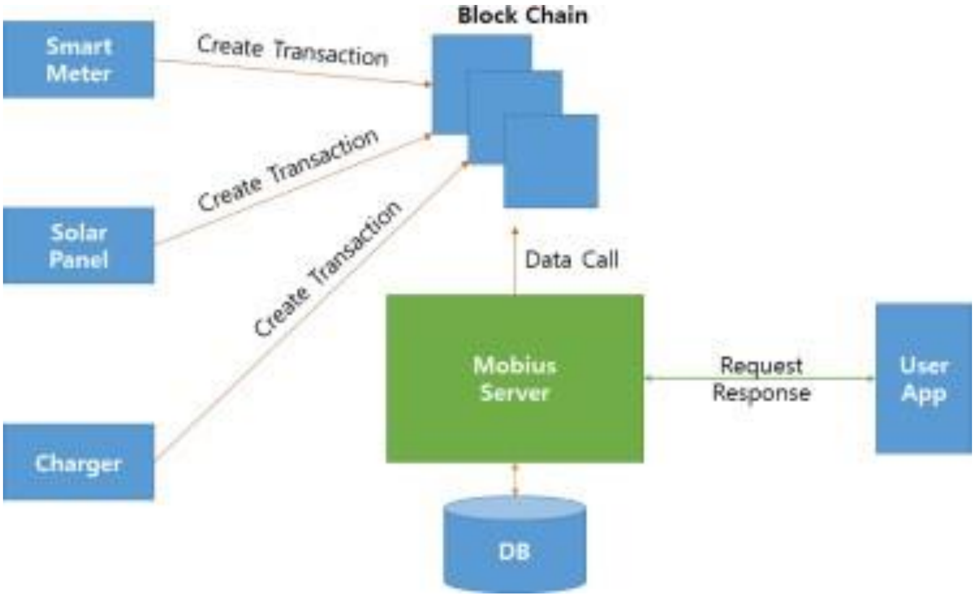


Fig 7.System architecture using block chain

Blockchain architecture is a breakthrough technology that is changing the way we think about data exchange and security in the quickly changing digital ecosystem. Fundamentally, blockchain architecture is cleverly crafted to provide a decentralised system, which stands in stark contrast to conventional centralised methods. Blockchain technology offers an immutable digital record that makes transactions on a peer-to-peer network safe and transparent. Understanding the fundamentals of blockchain architecture is essential as we explore its various facets, from the complex block structure to the broader network dynamics. With the goal of demystifying the intricacies of blockchain architecture, this overview intends to pave the way for a deeper comprehension of its constituent parts and the revolutionary potential they possess.

Since digital cryptocurrencies are so popular, the cornerstone of Blockchain—basically, a public digital ledger—has been able to transmit information in a reliable and safe manner. Blockchain technology and its uses have now extended beyond cryptocurrencies to a number of other industries, such as IoT, smart contracts, business process management.

This course is a collaborative effort between academia and industry, with the goal of covering Blockchain's conceptual and application features. This covers the system and security issues, as well as the basic architecture and building blocks of Blockchain, and a variety of use examples from various application sectors.

Decentralisation, accountability, and security are the three main tenets of blockchain technology. This method can greatly reduce expenses while increasing operational efficiency. Applications developed with blockchain architecture will continue to gain popularity and be used more often. Therefore, now is the ideal time to educate yourself on the subject.

III. EVOLUTION OF BLOCKCHAIN

Blockchain architecture's journey started long before it became widely known. When it was first conceived in 1991, the main goal was to develop a digital document timestamping system that would prevent digital documents from being altered or backdated. The basis for the current structure of blockchain was established by this fundamental concept. But it wasn't until 2008—thanks to Satoshi Nakamoto—that blockchain architecture started to take shape. The invention of Bitcoin by Nakamoto, a cryptocurrency built on a blockchain, was a turning point in the development of this technology. With this significant advancement, the blockchain's design moved from being a theoretical idea to a useful instrument that is revolutionising digital transactions. Gaining an understanding of this history is essential to comprehending the complex block structure of blockchain and to gain insights into possible future developments.

Bitcoin: The first decentralised cryptocurrency, Bitcoin operates on a peer-to-peer network that does away with the need for middlemen. An individual or group of individuals going by the nickname 2008 saw the creation of the Bitcoin cryptocurrency by Satoshi Nakamoto. The blockchain, which is a public ledger, records Bitcoin transactions. Currently, there are more than 18, as opposed to the 21 million Bitcoin tokens that are allowed to circulation.

Litecoin: Created in 2011, by Charlie Lee, a former employee of Google. He improved Bitcoin technology by adding cheaper fees, shorter transaction times, and a concentration of miners.

Ethereum: In July 2015, Vitalik Buterin unveiled Ethereum. Ethereum is currently the second-largest cryptocurrency by market capitalization, only surpassed by Bitcoin. Ethereum, a blockchain platform, has its own Solidity is a computer language; Ether (ETH) is its own digital currency.

Ripple: Similar to Bitcoin or Litecoin, Ripple is a type of cryptocurrency that operates on a decentralised, peer-to-peer network that is open-source and facilitates simple money transfers in any format. XRP is the currency of Ripple, a blockchain-based digital payment network and protocol.

NEO: Developed in China and originally known as Antshares, NEO is aggressively attempting to surpass other significant cryptocurrency players on the global scene. It centres on digital contracts, also known as smart contracts, which enable users to create and execute contracts without the need for an intermediary.

IOTA: An Internet of Things (IoT) application, IOTA was created in 2016. There will be billions of devices online by 2020. Data can be communicated between smart devices. and payment details in transactions made all day long in an Internet of Things environment with a multitude of other devices. IOTA aims to become the standard for conducting transactions on smart devices, displacing alternative ways.

Blockchain technology may prove to be highly advantageous in a future world where decentralised and centralised models coexist. The blockchain is an idea that, like any new technology, causes initial disruptions. However, in due course, it may facilitate the emergence of a broader ecosystem that encompasses both the traditional methods and the latest innovations. In the past, the introduction of the radio really resulted in a rise in record sales, and e-readers like the Kindle have driven up sales of books.

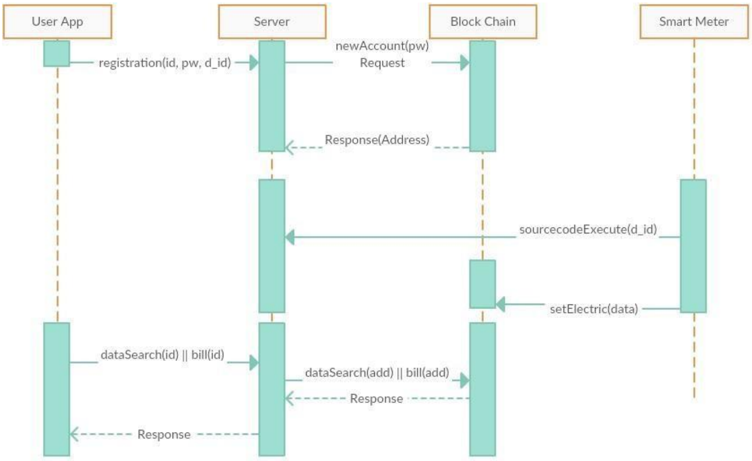


Fig.8.Device authentication and data transmission sequence diagram

DOI: 10.17148/IJARCCE.2024.134181

The smart meter's data transmission mechanism and authentication process in the suggested system are identical to those shown in Figure 5's sequence diagram. To register the member, the user sends the smart meter's "device ID," "user ID," and "password to be used as the block chain password" over the Mobius server. Using the password from the sent member data, the Mobius server requests a new account in the block chain and gets the account address answer. The account address, device ID, and user ID that are transmitted to the member application are stored in the database by Mobius. When the Smart Metre runs, it uses FTP to access the server's power measurement source code, which it then executes and stores. simply choosing the account address in the server's database, the amount of electricity used by the Smart Contract in the block chain. The smart contract gathers the power data that is sent in from the smart metre and uses the calculation method to apply the progressive tax on the day and month of the charge in order to request the transaction. Following the creation of the block, the user submits the member ID to the Mobius server in order to pay the fee or retrieve the power usage. The server then uses the block chain address to match the ID in the database to retrieve the data submitted to the block,application.

If the verifier or a third party in the suggested system simply knows the address of Through the block, information about the user, the amount of power used, and the cost paid may be found. This is a breach of personal information issue since it has the ability to analyse power usage.

user's behaviour pattern. Because the user can see whether the house is vacant, there is a chance that an attacker will commit a second offence, such theft. As a result, in this research, we suggest a technique to safeguard the system's personal data by including a proof of zero knowledge that may establish the accuracy of the data without requiring information from the verifier.

Breakthroughs in block-chain technology:

One of the biggest technological blind spots in history is blockchain. You could anticipate significant developments in virtualization, mobile, and cloud computing, but a unique distributed computing architecture built on public key cryptography? That was nearly entirely unexpected.

Unceremoniously, the 2008 release of the Nakamoto whitepaper ignited an innovative ferment that is still thriving today. If you were following the digital currency scene, which at the time was an even more geekier outpost of the already extremely geeky frontier of cryptography, it wasn't wholly surprising. The paper itself acknowledges the contributions of a number of earlier creators, such as Adam Back's Hash Cash whitepaper. Ethereum is the trunk from which the branches have extended if Bitcoin is the root from which the web3 tree has developed. Ethereum made the theoretical claim that, if we have a mechanism in place for confirming the legitimacy of transactions, perhaps we might create a virtual computer. There are nuances to be worked out carefully, as putting such a system into place is a significant obstacle, yet it is not only feasible but also opens features.

These programmes are generally referred to as distributed applications, or dApps. dApps are made up of standard web programmes that connect with smart contracts, which operate on-chain.

IV. SECURITY ANALYSIS

The information gathered by smart metres is utilised to determine power prices. As a result, to guard against manipulation, the gathered data needs to be integrity secured. A user may tamper with the data if, for instance, they want to pay less than the amount of power they consume. Furthermore, it is probable that the electricity supplier will alter the data in order to bill the user for more power than they have actually used. As a result, by validating the data sent by the smart metre, blocks may be created, and the ledger can be distributed to prevent data modulation and maintain integrity. Additionally, if the block chain disperses and distributes the data obtained from the smart metre across multiple users, the malicious.

By tracking the user's power usage over time, the attacker can examine the user's life patterns and save time by using the least amount of power. The attacker can determine whether the user is going out or taking a vacation based on this. As a result, the user's property and privacy may be violated if the data gathered by the smart metre is made publicly available through the block chain. To ensure secrecy without invading privacy, the public key produced by showing zero knowledge is stored in the suggested system. The original data can also be utilised for searches related to electricity pricing or usage and kept on the server to ensure availability.

DOI: 10.17148/IJARCCE.2024.134181

V. CONCLUSION

In this research, we present a zero-knowledge proof method and smart contract for data protection. Since IoT data is kept in a block chain, data manipulation and IoT device authentication may be avoided. By using block retrieval, zero-knowledge proof technology precludes outsiders from verifying the user's original material. Because of a number of issues, including data manipulation and fraud, inaccuracies in charge computation, and more, the current smart metre measurement and charging system uses a block chain.

Zero-knowledge proof smart contracts can provide secure and convenient transactions for prosumer power trading and car charges. We believe that our work may aid in someone's understanding of blockchain security concerns and technology. The security of the blockchain itself will be of more concern to users who utilise it for transactions. Additionally, we anticipate that our study will help researchers in their future work on blockchain technology development and blockchain security challenges. IoT for security protection and identity authentication. Additionally, we put out a blockchain-based approach for Internet of Things security and authentication. We also talked about the system's implementation in depth. Furthermore, we establish a test system utilising Hyperledger Fabric in order to validate the suggested approach. Compared to other works, our research offers the advantages of being simple and generic in character. It is appropriate for deployment on lightweight devices like the Internet of Things because to its minimal implementation cost.

Furthermore, the multi-chain structure offers extra security protection between several trust domains.

REFERENCES

[1]. Gungor, V. Cagri, et al. "A survey on smart grid potential applications and communication requirements." Industrial Informatics, Vol.9, No.1, 2013, pp. 28-42.
[2]. Gangale, Flavia, Anna Mengolini, and Ijeoma Onyeji., "Consumer engagement: An insight from smart grid projects in Europe.", Energy Policy, Vol.60, 2013, pp.621-628.
[3]. Luan, Shang-Wen, et al. "Development of a smart power meter for AMI based on ZigBee communication", Power Electronics and Drive Systems, 2009. PEDS 2009. International Conference on. IEEE, 2009.
[4]. Common Criteria for Information Technology Security Evaluation, Version3.1, CCMB, Setp.2006.
[5]. Youngu Lee, A Study for PKI Based Home Network System Authentication and Access Control Protocol, KICS '10-04Vol.35No.4
[6]. Kepco, Prosumer Power Trading,
[7]. Andreas M, Masteing Bitcoin: Unlocking Digital Cryptocurrencies, pp.49-68, O'REILLY, 2015
[8]. Sung-Hoon Lee, Device authentication in Smart Grid System using Blockchai, KAIST, 2016.
[9]. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
[10]. Nick Szabo, Smart Contracts, 1994.
[11]. Nick Szabo, The Idea of Smart Contracts, 1997.
[12]. The Cointelegraph, A Brief History of Ethereum From Vitalik
[13]. Buterin's Idea to Release, 2015
[14]. Jean-Jacques Quisquater, How to Explain Zero-Knowledge Protocols to Your Children, 1989.
[15]. KETI, Mobius IoT server platform, http://iotocean.com
[16]. Ryan Cheu, An Implementation of Zero Knowledge Authentication, 2014
[17]. Eli Ben-Sasson, Zerocash: Decentralized Anonymous Payments from Bitcoin, 2014
[18]. Surae Noether, Review of Ctyptonote White Paper, 2016
[19]. Charles RackoffDaniel R. Simon, Non-Interactive Zero- Knowledge Proof of Knowledge and Chosen Ciphertext Attack, Annual International Cryptology Conference, 1991
[20]. Evan Duffield,Daniel Diaz ,Dash: A Privacy-Centric Crypto- Currency, 2015