IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 6, June 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006226|

Blockchain based Privacy Preserving Enforced Bill Collection System using Smart Contract

Pooja L[1], Prof Madhuri J[2]

M. Tech Student, Department of Computer Science and Engineering, Bangalore Institute of Technology, Bangalore, Karnataka, India[1]

Assistant Professor, Department of Computer Science and Engineering, Bangalore Institute of Technology, Bangalore, Karnataka, India[2]

ABSTRACT: Blockchain technology is being used for electronic invoicing. Additionally, it has the power to fundamentally change how payments are processed, invoices are created, and transactions are validated. These distributed ledgers are still best known as the basis of cryptocurrencies like Bitcoin and are a perfect fit for payment reconciliation. They are built on blocks, each of which records a transaction. A document that can be accessed and modified by numerous people concurrently on a decentralised blockchain network keeps track of who made changes and when. It is transparent and impenetrable. Since all transactions are visible to all parties and each record or block is linked and safeguarded using cryptography, there is no need for a middleman. The use of a blockchain-based invoicing system will enable automatic payments from clients to a company's digital wallet. It is simple to track and monitor transactions, and the blockchain allows for the download of an exchange's full history. The suggested solution is based on the usage of smart contracts and accountable ring signatures.

KEYWORDS: Cryptocurrencies, Ring signature, Smart contract, Zero Knowledge.

I. INTRODUCTION

Blockchain is a distributed ledger system that uses encryption on a point-to-point basis. User privacy is now seriously under risk due to statistical techniques like sociological mining and data mining as well as the open and public blockchain ledger. As a result, the current focus of blockchain technology research is privacy protection. An encryption method that is widely used in the privacy protection industry is ring signature technology. As a result, this study creates a ring signature-based security system for blockchain privacy. For data security and user identity privacy in blockchain applications, this solution developed a privacy data storage protocol based on the ring signature on the elliptic curve. analysis of the suggested plan's accuracy and safety.

Smart Contract

To effectuate the terms and conditions of a particular agreement, smart contracts use software codes and computational infrastructure. They function as self-executing and self-enforcing programmes. The underlying blockchain network is made more functional by the decentralised programmes known as smart contracts. The program's immutability and cryptographic verification make it trustworthy. Some of the functionality of smart contracts are derived from the underlying blockchain technology. Smart contracts can be used in many different industries thanks to their qualities. In general, peer-to-peer smart contract execution takes place without the intervention of a centralised third party. Without the requirement for centralised infrastructure, they provide services. Enable automated transaction execution when pre-established criteria are met.

Here are listed the key properties of blockchain-based smart contracts.

1.Elimination of Trusted Third Party and Autonomous Execution

Decentralization is the key benefit of blockchain-based smart contracts. When a certain system is merged with blockchain-based smart contracts, the need for trusted middlemen like brokers, agents, or service providers may be removed. The power and costs associated with transactions imposed by centralized institutions will decrease with the elimination of a trusted third party. One of the most notable instances is bitcoin, which adopted smart contracts to change the function of dependable third parties like central banks. The centralized third parties operate as the ultimate

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006226|

regulating body while imposing hefty transaction fees. The rules imposed by the centralized authorities must be followed by the users.

Smart contracts, in contrast, allow participants to determine the agreement procedure themselves, enhancing democracy [49]. Upon mutual agreement, the participants set the guidelines and criteria for the deployment of the smart contract. Once a particular predefined state of the blockchain has been reached, the programmed condition and flow of events are meant to be carried out. Upon approval from all participants in the blockchain network, the precise status will be specified in the smart contract. Any condition, including a certain wallet amount, a time limit, etc., can be this state. Following that, the execution is automatic without the involvement of a centralized third party. Since the operation runs peer-to-peer and is not dependent on a centralized third party, the service availability is ensured. The correctness of the operation without human error or even biased acts is ensured by the autonomous execution according to the conditions. In light of this, the smart contract holds promise for the majority of applications that call for substitutes for trustworthy third parties.

2) Forge Resistance and Immutability

Digital signatures are used to confirm the accuracy of the transaction records in distributed ledgers [50]. Additionally, each transaction was reviewed and approved before being added to the ledger. The ever-expanding ledger is made up of immutable approved transactions. The modification cannot be carried out by a person. On the blockchain, smart contract code is immutable. Various methods can be used to distribute the code to every node. as an executable contained in the container, as an illustration. The altered smart contracts cannot be performed since the smart contract code is tamper-evident. On the other hand, smart contracts can be changed, if necessary, with the consent of blockchain network nodes. As a result, everyone involved in the blockchain network can have faith in the smart contract and know that the code that is executed contains the logics that were disclosed to and approved by each participant in the blockchain network.

3) Transparency

One of the key differentiating characteristics that the smart contracts have inherited from the blockchain is transparency. The smart contract is transparent in two different ways. First off, both the public and intervening parties can see the code stated in smart contracts. Second, the group of transactions contained in the blocks are also open to public scrutiny. Therefore, the blockchain network's intermediary parties can have faith in its logic and transactions. In a more specific case, if the smart contract logic is set by a governing body that is a member of the blockchain network, the specific operation carried out in accordance with the logic can be viewed as trustworthy and unbiased because the code is publicly available. To promote confidence, the transaction that is put to the ledger is also made available to the general public. The centralized service design, in contrast, lacks transparency and is vulnerable to man-in-the-middle attacks and other flaws. If any alterations to the data at rest occur, it is impossible to trace them in the centralized databases. Members of the blockchain ecosystem can openly verify the correctness of its execution thanks to the transparency of smart contract code.

Existing System and their Drawbacks

1. In many of the Existing System the RSA algorithm are used. But RSA signature is slower than elliptical curve digital signature.
2. In some of the existing system they have used the zeroknowledge proof but the Requires a large amount of computing power.
3. Homomorphic encryption has been employed in certain existing systems, but it is expensive and requires specialist client-server software in order to function.

Drawbacks:

1. Computation power is more.
2. Slow and low efficiency of the system.
3. User Privacy is not taken as serious issue.
4. The invoice sent by the bill Collector was not able to verify by the user.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006226|

II. RELATED WORK

Ahmet Önder Gür et al. [1] proposed a concentrate on keeping a harmony among insignificance and recognizability is a principal issue in security protecting frameworks. Isshiki et al. proposed a personality the executives framework in view of gathering marks in which a specialist co-op namelessly decides if clients of the assistance are authentic individuals, and just a bill authority can recognize clients for the motivations behind sending those solicitations. It is especially important that, under the Isshiki framework, the specialist co-op isn't expected to oversee individual data, for example, client records, which permits the framework to beat other as far as saving client protection and overseeing individual data spillage risk. It is additionally critical that the Isshiki framework just considers cases in which the bill authority recognizes clients who have utilized the assistance and that, truth be told, distinguished clients who overlook solicitations can involve the help free of charge. In this paper, we expanded the Isshiki framework by adding a brilliant agreement empowered authorization bill assortment usefulness. Under this usefulness, stores made by clients who don't pay an assistance expense are naturally moved to the bill authority. Due to their unified construction, bunch marks are not appropriate to blockchain frameworks, subsequently, the proposed framework utilizes responsible ring marks as building blocks. The security saving upheld bill assortment framework is executed utilizing the responsible ring mark conspire created by Bootle et al. also, Ethereum brilliant agreements. To decrease the gas costs related with running brilliant agreements, the shrewd agreement isn't run except if the client disregards a receipt, and fundamental strategies are run by means of an off-chain channel. To stay away from the utilization of weighty cryptographic calculations in doing the responsible ring mark plot for running brilliant agreements, we utilized standard elliptic curve digital signature algorithm (ECDSA) marks without particularly having an impact on the state to be checked in shrewd agreements.

Kyawt May Hlaing et al. [2] proposed a review on an Ethereum, a blockchain-based dispersed processing stage, gives shrewd agreement usefulness. It additionally gives Ethereum virtual machine (EVM) that can execute shared agreements across decentralized network. Notwithstanding, the gas utilization of savvy contract is exorbitant to such an extent that it becomes one of the significant issues to be addressed. The motivation behind this paper is to give a theoretical outline of blockchain based power charging framework fully intent on reducing gas utilization of the brilliant agreement. In this framework, Firebase is utilized as an information stockpiling while Ethereum blockchain goes about as both a digital money installment framework and a confirmation channel. Also, this paper delineates two-factor verification by using Ethereum record and Firebase Authentication as a confirmation channel. Results show that by using Firebase with blockchain, the exchange cost of every exchange made on Ethereum is diminished by roughly 73%.Feng Gao et al. [3] proposed an assessment on as a basic piece of VehicaltoGrid(V2G) organizations, ElectricalVehicals(EVs) get power from the framework as well as different EVs and may much of the time feed the power back to the matrix. Installment records in V2G networks are helpful for separating client ways of behaving and working with decision-production for enhanced power supply, booking, evaluating, and utilization. Sharing installment and client data, notwithstanding, brings genuine protection worries up notwithstanding the current test of secure and solid exchange handling. In this study,propose a blockchain-based protection safeguarding installment system for V2G organizations, which empowers information sharing while at the same time getting touchy client data. The component presents an enlistment and information support process that depends on a blockchain strategy, which guarantees the obscurity of client installment information while empowering installment examining by advantaged clients. Our plan is carried out in light of Hyper record to painstakingly assess its plausibility and adequacy.

Zhitao Guan et al. [4] proposed an assessment on with the approach of the Industry 4.0 period, the improvement of shrewd urban areas in view of the Internet of Things (IoT) has arrived at another level. As a critical part of the Internet of Things (IoT), the security of remote sensor organizations (WSN) has gotten boundless consideration. Among them, Energy Internet, as a significant part to help the development of brilliant urban communities, its security and dependability research is turning out to be increasingly significant. In the Energy Internet, conveyed energy exchange model is a promising way to deal with supplant the conventional incorporated exchange model and has turned into the main heading of advancement in energy exchanging. As the hidden help, blockchain innovation is drawing in increasingly more consideration because of its benefits, i.e., respectability and nonrepudiation. Be that as it may, most blockchain-based exchanging models deal with the issue of security divulgence. In this paper, to take care of this issue, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is acquainted as the center calculation with reproduce the exchange model. In particular, we fabricate an overall model for appropriated exchanges called PP-BCETS (Privacy-saving Blockchain Energy Trading Scheme). It can accomplish fine-grained admittance control through exchange discretion in the ciphertext structure. This plan can expand the assurance of protection data, and impressively work on the security and dependability of the exchange model. Also, a believe ability based value verification agreement component is proposed in PP-BCETS, which can significantly expand the activity effectiveness. The security

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006226|

examination and exploratory assessments are directed to demonstrate the legitimacy and practicability of the proposed conspire.Ahmad Alsharif et al. [5] proposed an assessment on the high level metering foundation (AMI) networks permit service organizations to gather fine-grained power utilization information of power buyers for load checking and energy the executives. This brings genuine security worries since the fine-grained power utilization information can uncover purchasers' exercises. Security safeguarding information conglomeration methods have been utilized to save shoppers' protection while permitting the utility to get just the buyers complete utilization. Be that as it may, the greater part of the current plans don't consider the complex idea of force utilization where power utilization can be ordered in light of the utilization type. They likewise don't consider multisubset information assortment in which the utility ought to have the option to acquire the quantity of customers whose utilization exists in a particular utilization range, and the general utilization of each arrangement of shoppers. In this article, we propose an effective and security protecting multidimensional and multisubset information assortment plot, named "MDMS." In MDMS, the utility can get the all out power utilization along with the quantity of customers of every subset in each aspect. Moreover, for better adaptability, MDMS permits the utility to appoint charge calculation to the AMI organizations' passages involving the encoded readings and following the unique costs where power costs are different in light of both the time and the utilization type. In addition, MDMS involves lightweight activities in encryption, collection, and decoding bringing about low calculation and correspondence overheads as given in our exploratory outcomes. Our security investigation shows that MDMS is secure and can oppose intrigue goes after that expect to uncover the purchasers' readings.Jie Xu, Kaiping Xue et al. [6] gives blueprint of the report on with the significantly expanding arrangement of the Internet of Things (IoT), remote checking of wellbeing information to accomplish wise medical services has gotten extraordinary consideration as of late. Be that as it may, because of the restricted registering power and capacity limit of IoT gadgets, clients' wellbeing information are by and large put away in a unified outsider, like the medical clinic data set or cloud, and cause clients to fail to keep a grip on their wellbeing information, which can without much of a stretch outcome in security spillage and single-point bottleneck. In this paper, we propose Healthchain, an enormous scope wellbeing information security safeguarding plan in light of blockchain innovation, where wellbeing information are encoded to direct fine-grained admittance control. In particular, clients can successfully deny or add approved specialists by utilizing client exchanges for key administration. Besides, by presenting Healthchain, both IoT information and specialist conclusion can't be erased or messed with to keep away from clinical questions. Security examination and test results show that the proposed Healthchain is relevant for shrewd medical care framework.

Axin Wu et al. [7] proposed an assessment on Attribute-based encryption, particularly ciphertext-strategy property based encryption, assumes a significant part in the information sharing. During the time spent information sharing, the mystery key doesn't contain the particular data of clients, who might impart his mystery key to different clients for benefits without being found. Furthermore, the property authority can produce the mystery key from any trait set. Assuming the mystery key is mishandled, it is challenging to judge whether the manhandled private key comes from clients or the quality power. Also, the entrance control structure normally releases delicate data in a circulated network, and the effectiveness of trait based encryption is a bottleneck of its applications. Luckily, blockchain innovation can ensure the respectability and non-renouncement of information. Considering the above issues, an effective and security safeguarding discernible trait based encryption plot is proposed. In the proposed plot, blockchain innovations are utilized to ensure both trustworthiness and non-renouncement of information, and the ciphertext can be immediately produced by utilizing the pre-encryption innovation. Also, ascribes are concealed in unknown access control structures by utilizing the trait blossom channel. At the point when a mystery key is mishandled, the wellspring of the manhandled secret key can be examined. Security and execution investigation show that the proposed plot is secure and productive.Junqing Lu et al. [8] gives diagram of Group mark is a cryptography crude that has been broadly investigated. It finds some kind of harmony between computerized signature and the client's interest for namelessness. A legitimate part in the gathering can create a mark for the entire gathering. The general population can realize that it was given by a legitimate gathering part and advance nothing about the genuine personality of the endorser while checking a gathering mark. Backes et al called attention to that the current unique gathering mark conspires certainly expect that the enrollment of everybody in the gathering is available to the general population. In this way, they set forward a property called enrollment security for dynamic gathering mark. In this paper, we plan a unique gathering mark plot with enrollment security on top of Signature Proofs of Knowledge (SPK) and BBS+ signature. Moreover, dynamic aggregator system is taken on to renounce a gathering part's position to sign. Then, at that point, a security examination exhibits that the proposed bunch signature plot fulfills join-leave protection. At long last, quantitative examination and test results show that the proposed bunch signature plot accomplishes the less signature size and less calculation upward contrasted and Backes' plan.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006226|

XIAOFANG LI et al. [9] proposed an assessment on Blockchain is a highlight point dispersed record innovation in light of cryptographic calculations. Notwithstanding, the open and straightforward blockchain record enhanced by measurable strategies, for example, humanistic mining and information mining has made clients' security face significant dangers. Subsequently, security insurance has turned into a focal point of ebb and flow blockchain innovation research. Ring mark innovation is a generally involved encryption innovation in the field of security assurance. Subsequently, this paper builds a blockchain security assurance conspire in view of ring mark. This arrangement assembled a protection information capacity convention in view of the ring mark on the elliptic bend, and utilized the total secrecy of the ring mark to guarantee the security of information and client personality security in blockchain applications. The rightness and wellbeing evidence examination of the proposed conspire were additionally done.According to Chao Lin et al. [10], Blockchain is a distributed record technology that has the potential to be applied in a variety of contexts. Decentralized payment systems (such as Bitcoin) have been one of these applications that has received the most widespread support. While early schemes, like Bitcoin, were commonly used as payment by fraudsters (for instance, in ransomware incidents), they only provided pseudo-obscurity because anyone could deanonymize Bitcoin exchanges by incorporating data in the blockchain. Different arrangements, like Monero and Zerocash, have been suggested to strengthen the security assurance of decentralised payment frameworks. However, completely decentralised anonymous payment (DAP) systems can be misused for unlawful purposes, such as internet-based coercion and unauthorised tax evasion. We provide a unique definition of Decentralized Conditional Anonymous Payment (DCAP) and depict the contrasting security requirements after realising the importance of the guidelines. With our suggested mark of information in mind, we first plan a Condition Anonymous Payment (CAP) system whose security can be demonstrated using the defined formal semantic and security models. In order to demonstrate utility, we compare our proposition's presentation to that of Zerocash while maintaining comparable constraints and testing conditions.

Jong-Hyuk Im et al. [11] proposed an assessment on the advancement of brilliant meters that can much of the time measure and report power utilization brings empowered power suppliers to the table for different time-changing rates, including season of-purpose and constant estimating plans. High-goal power utilization information, nonetheless, raise genuine security concerns since delicate data with respect to a singular's way of life can be uncovered by dissecting these information. Albeit broad examination has been led to address these protection concerns, past methodologies have decreased the nature of estimated information. In this paper, we propose another protection saving power charging technique that doesn't forfeit information quality for security. The proposed technique depends on the original utilization of utilitarian encryption. Trial results on a model framework utilizing a true brilliant meter gadget and information demonstrate the plausibility of the proposed strategy.

Zhitao Guan et al. [12] gives layout of these systems will propose people that you share ordinary features with them as partners. Insight is perhaps the main perspectives in the improvement of our future local area. Going from savvy home to brilliant structure to shrewd city, this multitude of brilliant foundations should be upheld by wise power supply. Savvy network is proposed to address all difficulties of future power supply. In brilliant framework, to acknowledge ideal booking, a SM is introduced at each home to gather the close constant power utilization information, which can be utilized by the utilities to offer better shrewd home administrations. In any case, the close continuous information might unveil a client's private data. An enemy might follow the application use designs by examining the client's power utilization profile. In this article, we propose a protection safeguarding and productive information accumulation plot. We partition clients into various gatherings, and each gathering has a private blockchain to record its individuals' information. To safeguard the internal protection inside a gathering, we use pen names conceal clients' personalities, and every client might make various pen names partner his/her information with various pen names. What's more, the sprout channel is taken on for quick confirmation. The examination shows that the proposed plan can meet the security prerequisites and accomplish preferred execution over other famous techniques.

ABDULLAH AL OMAR et al. [13] proposed an investigation on a shrewd city guarantees quality support in assorted areas, to be specific resident wellbeing, security, medical care, transportation, and energy. Additionally, information protection and security have turned into an uprising worry for Electronic Health Records (EHR) in shrewd urban areas. This is on the grounds that the EHR stages are continually getting digital dangers from cybercriminals. Then again, health care coverage organizations offer specific explicit arrangements that require the relationship of patients' monetary information with EHRs. Subsequently, extra security concern emerges as false substances can modify these insurance contracts. An additional a test is set off as need might arise to approve their personalities independently while speaking with various savvy medical care elements. This is on the grounds that these medical care offices and insurance agency should guarantee credibility prior to offering any help for a person. Consequently, we have carried

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006226|

out a blockchain structure to defend patients' very own data and insurance contract. In this paper, we propose an answer for the medical care framework that gives information security and straightforwardness. Moreover, in the proposed framework, insurance contracts are consolidated in blockchain by means of the Ethereum stage and information security is protected with cryptographic instruments.

Yisen Cao, Yanjun Li et al. [14] gives blueprint of the gathering mark conspire is broadly utilized in military and monetary fields because of its effective secrecy and revocability. Notwithstanding, in an untrusted climate, past gathering mark conspires regularly experience the ill effects of the executives habitats or disavowal focuses, which diminishes the security of the plan. Simultaneously, the malignant gathering community and the mark beneficiary can recognize the endorser personality and furthermore undermine the secrecy of the program. It is demonstrated by estimation that the plan can keep up with the security and namelessness of the gathering mark calculation in an untrusted climate.

Rixuan Qiu et al. [15] proposed an investigation on Smart matrix is an exceptionally coordinated power framework that consolidates current progressed data and correspondence, sensor estimation and programmed control innovation, including countless shrewd gadgets, with dependability, adaptability, wellbeing and self-mending benefits an extraordinary assistance. In any case, gadgets, for example, shrewd meter in the organization face the issue of revealing client security while gathering, handling, and sending a lot of information. To tackle this issue, this paper advances a plan in light of further developed bunch signature and homomorphic encryption, utilizing further developed bunch mark to decide general society and private key of shrewd meter and the mark of power information, encoding and amassing the power information with homomorphic encryption. At long last, in the transmission of information, the power information is generally as ciphertext, and the gathering mark conspire with sending security can stay away from the mischief brought about by the exposure of the private key, in this way assuming a part in protection safeguarding.

Akash Suresh Patil et al. [16] gives layout of The Internet of Things gadgets produces an enormous measure of touchy information. AI is the standard handling worldview for shrewdly taking care of the gigantic measure of information. Tragically, the IoT gadgets have restricted assets to deal with the exhibition of large information highlight learning with AI strategies. IoT gadgets frequently compromise the protection of clients and make them defenseless against various digital assaults. In this paper, we propose a productive protection saving validation convention in light of blockchain innovation and the mysterious computational model of actually unclonable capacity (meant by PUF model). The proposed convention ensures the clients security with a decentralized brilliant agreement blockchain with the PUF model. Practically speaking, the proposed convention ensures that IoT gadgets and the digger are confirmed in a quicker verification process contrasted with current blockchain strategies. Moreover, Blockchain and PUF consolidate to guarantee information provenance and information straightforwardness in IoT organizations. Blockchain-based shrewd agreements give decentralized advanced records that can endure information altering assaults. This guarantees the security and protection of reevaluated huge information in IoT conditions. We likewise examined the protection ramifications of utilizing IoT gadgets with different security investigation, and roads for exploration to mitigate the protection worries in IoT conditions.

Huda Osman et al. [17] gives diagram of Organizations, organizations, even people can help the astonishing benefits of the cloud just when they observe that their information is safely handled and put away in the cloud. This makes it important to construct and foster methods and models to really keep up with information protection prior to re-appropriating it to the cloud. The vast majority of the current methods try to keep away from information divulgences that lead to protection spillage. Tragically, these methods actually experience the ill effects of certain kinds of assaults, adding to the issue of information utility that abatements due to execute the protection safeguarding tasks. This paper presents a model that maintains a strategic distance from two kinds of information exposures to forestall security spillage. The proposed model depends on consolidating one of the encryption methods, which is incomplete homomorphic encryption, with the anonymization strategy, which is k obscurity. The outcomes exhibited the viability of the proposed model in working fair and square of protection saving simultaneously diminishing the level of the lost information contrasted with a comparative present day model.

Chan Hyeok Lee et al. [18] proposed an investigation on In a square chain IoT climate, when information or gadget verification data is placed on a square chain, individual data might be spilled through the evidence of-work interaction or address search. In this paper, we apply Zero Knowledge confirmation to a brilliant meter framework to demonstrate

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006226|

that a prover without revealing data like public key, and we have concentrated on the most proficient method to improve namelessness of square chain for security insurance.

Tao Liu et al. [19] proposed an investigation on as another age of force framework, brilliant matrix has productive and supportable assistance abilities. Nonetheless, in most application situations, individuals just focus on the accessibility of information and overlook the security of the data.In request to take care of the issue of client information data spillage in the sharp network framework, we propose a blockchain-based protection assurance conspire for electric energy information. In the information procurement stage, the edge ElGamal homomorphic encryption calculation is utilized to total the energy estimation information. In the information stockpiling stage, the mix of on chain and off chain capacity mode is taken on to produce the declaration data of security information and transfer it to the blockchain. On the reason of safeguarding the protection and security of individual power utilization, the power utilization in the space is gathered to understand the protected stockpiling of private information, which gives reference to the energy dispatching of savvy framework later on.

Ashutosh Dhar Dwivedi et al. [20] proposed an assessment on Medical consideration has become quite possibly the most fundamental pieces of living souls, prompting a sensational expansion in clinical huge datum. To smooth out the finding and treatment process, medical services experts are currently embracing Internet of Things (IoT)- based wearable innovation. Late years have seen billions of sensors, gadgets, and vehicles being associated through the Internet. One such innovation far off tolerant observing is normal these days for the treatment and care of patients. Nonetheless, these advancements likewise present grave protection dangers and security worries about the information move and the logging of information exchanges. These security and protection issues of clinical information could result from a deferral in treatment progress, in any event, jeopardizing the patient's life. We propose the utilization of a blockchain to give secure administration and examination of medical care large information. Nonetheless, blockchains are computationally costly, request high transmission capacity and extra computational power, and are hence not totally appropriate for most asset compelled IoT gadgets implied for savvy urban areas. In this work, we attempt to determine the previously mentioned issues of utilizing blockchain with IoT gadgets. We propose a clever structure of adjusted blockchain models reasonable for IoT gadgets that depend on their appropriated nature and other extra protection and security properties of the organization. These extra protection and security properties in our model depend on cutting edge cryptographic natives. The arrangements given here make IoT application information and exchanges safer and unknown over a blockchain-based network.

III. CONCLUSION AND FUTURE WORK

Keeping a balance between anonymity and traceability is a crucial issue in privacy-preserving technologies. It is recommended to develop a safe bill payment system that protects your privacy. It supports a feature that enables customers to be forced to pay service fees. The foundation of this suggested solution is the application of ring signatures and smart contracts. As a result of the blockchain technology's decentralized architecture, which prevents a single point of failure that may bring down the entire system, the system is fault-tolerant. Additionally, the suggested system will offer defense against security threats including hacking and denial-of-service attacks. This proposed system is based on the smart contracts. The system is fault-tolerant as the blockchain technology provides a decentralized architecture which would avoid a single point of failure which can destroy the entire system. In the future work we can measure the service used using measuring devices and can add the service details along the Billing details. The user can be given option to pay his bills using online transactions.

REFERENCES

[1] Ahmet Önder Gür , ¸Safak Öksüzer , Enis Karaarslan, “Blockchain Based Metering and Billing System Proposal with Privacy Protection for the Electric Network,” Annual review of psychology, vol. 48, no. 1, pp. 61–83,2019
[2] Kyawt May Hlaing, Dim En Nyaung, “Electricity Billing System using Ethereum and Firebase”. IEEE, 2020
[3] Feng Gao, Liehuang Zhu, Meng Shen, Kashif Sharif, Zhiguo Wan, and Kui Ren, “A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks” Annual Review of Information Science and Technology, vol. 38, no. 1, pp. 87–143,2018.
[4] d Zhitao Guan a, Xin Lu a , Wenti Yang a , Longfei Wu b , Naiyu Wang a , Zijian Zhang c, “Achieving efficient and Privacy-preserving energy trading based on blockchain and ABE in smart grid”. Basic Books, 2020.
[5] Ahmad Alsharif, MDMS: “Efficient and Privacy-Preserving Multidimension and Multisubset Data Collection for AMI Networks”. IEEE 2021.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 6, June 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1006226|

[6] Jie Xu, Kaiping Xue, "Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data". IEEE, 2020.
[7] Axin Wu1,2 · Yinghui Zhang1,2 · Xiaokun Zheng1,2 · Rui Guo1,2 · Qinglan Zhao1,2 · Dong Zheng1,2, "Efficient and privacy-preserving traceable attribute-based encryption in blockchain".IEEE, 2019, pp. 492– 501.
[8] Junqing Lu, Rongxin Qi, Jian Shen and Tianxiang Zheng, "A Novel Dynamic Group Signature with Membership Privacy", IEEE 2022.
[9] XIAOFANG LI1 , YURONG MEI 2 , JING GONG3 , FENG XIANG4 , AND ZHIXIN SUN, "A Blockchain Privacy Protection Scheme Based on Ring Signature,"2020.
[10] Chao Lin , Debiao He , Xinyi Huang , Muhammad Khurram Khan, "DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain", IEEE 2022.
[11] Jong-Hyuk Im , Hee-Yong Kwon, Seong-Yun Jeon and Mun-Kyu Lee *, "Privacy-Preserving Electricity Billing System Using Functional Encryption",2019.
[12] Zhitao Guan, Guanlin Si, Xiaosong Zhang, Longfei Wu, Nadra Guizani, Xiaojiang Du, and Yinglong Ma, "Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities", 2018.
[13] ABDULLAH AL OMAR, ABU KAISAR JAMIL, "A Transparent and Privacy-Preserving Healthcare Platform With Novel Smart Contract for Smart Cities," IEEE,2021.
[14] Yisen Cao, Yanjun Li*, Ying Sun, Shubei Wang, "Decentralized Group Signature Scheme based on Blockchain," IEEE, 2019.
[15] Rixuan Qiu, Ming Ai, Fuyong Zheng, "Privacy-Preserving of Power Consumption Big Data Based on Improved Group Signature and Homomorphic Encryption," IEEE,2020.
[16] Brijesh Kumar Singh, Mansi Katiyar, Shefali Gupta and Nikam Gitanjali Ganpatrao, "A Survey on: Personality Prediction from Multimedia through Machine Learning." IEEE, 2021.
[17] Huda Osman , Maheyzah Md Siraj, Mohd Aizaini Maarof, "HAC: Model for Privacy-Preserving Outsourced Data Over Cloud" IEEE2021.
[18] Chan Hyeok Lee, Ki-Hyung Kim, "Implementation of IoT System using BlockChain with Authentication and Data Protection" IEEE,2018.
[19] Tao Liu, Xiaohong Cao and Jin Li, "Blockchain-based privacy protection scheme for electric energy metering data" IEEE 2020.
[20] Ashutosh Dhar Dwivedi, Gautam Srivastava 2,3,* , Shalini Dhar 4 and Rajani Singh 1, "A ecentralized Privacy-Preserving Healthcare Blockchain for IoT" IEEE,2019.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details