A SURVEY ON PROTECTION AND SECURITY OF TRANSACTION USING BLOCKCHAIN

Dr. Rachna Somkunwar, Anil Kumar Gupta, Akshita Koul,
Srushti Rajput, Pallavi Bansode, Purnankita Kavitake
Department of Computer Engineering
Dr. D. Y. Patil Institute of Technology, Pimpri Pune

ABSTRACT

A blockchain is a series of digital blocks that hold transaction data, as the name suggests. Each blockis linked to the blocks that come before and after it. To avoid detection, a hacker would have tochange the block containing that record as well as those linked to it, making it difficult to tamper with a single record. This may not appear to be much of a deterrent on its own, but blockchain has some intrinsic qualities that provide further protection. Cryptography is used to secure the records on a blockchain. Participants in the network each have their own private keys, which are associated with the transactions they conduct and serve as a personal digital signature. If a record's signature is changed, the signature becomes invalid, and the peer network is notified immediately. The importance of early notice in preventing futured image cannot be overstated. Unfortunately for those determined hackers, blockchains are decentralized and spread across peer-to-peer networks that are updated and kept in sync on a regular basis. Blockchains have no single point of failure and cannot be modified by asingle computer because they are not stored in a central location.

Keywords: Blockchain, Smart contracts, Traceability, Paymentsystem, Payment safety.

INTRODUCTION

Blockchain: Stuart Haber and W. Scott Stornetta, two research scientists, first discussed blockchain technology in 1991. They intended to offer acomputationally feasible approach for time-stamping digital documents in order to prevent them from being backdated or tampered with. Blockchain is not a distributed computing system. Scalability is a problem. Some Blockchain solutions use excessive amounts of energy Users Are Their Own Bank: Private Keys. Blockchains are Sometimes Inefficient

.Not Completely Secure. Blockchains Cannot GoBack — Data is Immutable. Bitcoin is the first successful blockchain implementation. Today, blockchain technology is being used in a variety of industries where trust without the involvement of a centralized authority is desired. So, welcome to the Blockchain world. Secure Electronic Transaction :TheSET Consortium, which was founded in 1996 by Visa and Mastercard in collaboration with GTE, IBM, Microsoft, Netscape, SAIC, Terisa Systems, RSA, and VeriSign, developed SET. [1] The consortium's purpose was to create a single standard that would unify the card associations' similar but incompatible protocols (STT from

Visa/Microsoft and SEPP from Mastercard/IBM).SET let parties to safely identify themselves to one another and exchange information. X.509 certificates withdifferent extensions were used to bind identities. A credit card is required for use. When the payment is little, it is not cost-effective. There is no anonymity, and it can be traced. Client software installation isrequired due to the network effect (an e-wallet).Cost and complexity for merchants to provide support, compared to the existing SSL-based alternative's comparatively cheap cost and ease. Certificate delivery logistics on the client's end. The internet'ssecurity is improving. As the usage of the Internet forcommerce grows, so does the technology used to protect financial transactions. It is easy to extend fundamental technologies to safeguard multicastcommunications, and this is likely to happen as multicast becomes more widely used.

LITERATURE REVIEW

In this Paper, The resilient payment routing is investigated in this study by designing two node-disjoint payment channels for a payment request in PCNs. A robust payment routing is expected to satisfy a set of desired qualities since it has a number of distinguishing characteristics. First, a reliable payment routing protocol should be efficient, i.e., it should reduce routing and payment delay by sendinga payment across several payment pathways at the same time. Second, because PCNs lack a central administrative operator, a robust payment routing must fulfil distributedness. RobustPay is a robust payment routing protocol that we propose. Welooked at the resilient payment routing protocol in this study to see if it could withstand payment transaction failures in PCNs. We started by proposinga set of critical design goals for payment routing, which we called robustness, efficiency, and distributedness. We presented RobustPay, a distributed robust payment routing protocol with three stages: Payment Path Construction, HTLC Establishment, and Payment Forwarding, based on these design aims. RobustPay established robustness in payment path construction by establishing two payment paths, each of which may satisfy the payment request. Furthermore, we converted the original HTLC protocol to the robust paymentrouting protocol and changed it to enhance efficiency**[1].**

In this Paper, We'll set aside some of these issues and concentrate on how to perform economic transactions across IoT components that belong to various administrative entities. We take into account the fact that many common IoT components are built on low-end embedded systems with limited computationaland communication capabilities. As a result, we're looking for solutions that use a decentralized designto lower computing demands while also reducing communication. Our study introduces the Ticket- Based Verification Protocol (TBVP), a mechanismfor facilitating practical economic transactions in IoT systems. For establishing an economic value for IoT transactions, TBVP relies on blockchain technology. However, operating a blockchain client requires a lot of processing power and a lot of network bandwidth, which IoT devices don't always have. The high cost of deploying and operating IoT devices is the key barrier to mainstream adoption of IoT-basedsolutions for various societal issues. Horizontalintegration of IoT devices is a viable

strategy forlowering the cost of such solutions. The first stage in horizontal IoT device integration is to have a solid financing system. We presented a Ticket-BasedVerification Protocol for IoT devices in this work, which is an extension of the current blockchain-basedfinancial processes**[2].**

In this Paper, we look at the payment network balance planning problem, which entails determining the initial balances of payment channels based onprojected payment needs among nodes. PnP, a balance planning service that can be simply linked into existing payment networks, is something we designed. Even with estimating flaws, PnP can use knowledge of payment demands to reduce overall channel deposits. It does not rely on trustworthy third parties and can withstand malicious node attacks. It also has a low overhead in terms of transmission and computing. PnP achieves these results by resolving two major issues. Blockchain employs a number of clever ideas to ensure decentralization and consistency, but the consensus mechanism involving all nodes sacrifices scalability. At the moment, Bitcoin can only manage 7 transactions per second, while Ethereum can handle up to 15 transactions per second. This paper presents PnP, a payment network balance planning service Given inaccurately predicted payment demands, PnP can reduce the overall amount of money transferred into payment channels while ensuring a low risk of outage. Meanwhile, PnP does not require a trusted third partyand may withstand attacks by using an efficient cryptographic sortition process to choose a decision committee to perform balance planning algorithms. We use Lighting Network Daemon to implement PnP, and our results on a testbed of 30 nodes are promising**[3].**

In this Paper, Blockchain has remained a hot topic in the tech world since its inception in the early 2000s.It is a major player in both the consumer and commercial markets, providing an alternative to fiat currency . Companies are actively promoting it for complicated business solutions. People have discovered a niche in the public Blockchain throughout the years: having access to a massive amount of hardware resources, all working together for a shared aim and capable of providing supercomputer-like computational capacity. In practice, blockchain as a grid is a new sort of service. Furthermore, implementations such as Ethereum make APIs, SDKs, and a Turing-complete programming language available as service development tools that run on top of the current infrastructure. By enabling this cloud-like paradigm, one might generate assets and sell services without even owning the underlying resources, helping to support existing cloud-optimization regulations. In this work, we take advantage of this feature while also innovating by using the technique of latent transactions to make it easier to construct real-time applications on the Ethereum Blockchain. A latent transaction is an off-chain transaction in which a value-bearing asset owner receives specific guarantees before being paid for sharing an asset witha client. In this paper, We've created and tested a solution to address the issue of latency in Blockchain networks as it relates to the ability to conduct real- time services monetized with bitcoin. We've created an off-chain solution that makes it easier for vendors and customers to work out late payment agreements. In exchange for the delivery of services, providers may accumulate a set of latent-transactions from clients. They

can then claim the crypto-tokens as a reward for their efforts via our Ethereum Smart Contract**[4].**

In this Paper, The general procedure of bitcoin payment between consumers and merchants is defined by this standard. This procedure explains how a customer buys goods or services using bitcoin and receives fiat money in exchange. It involves a number of factors, including cryptocurrency payment operators acting as agents, cryptocurrency owners, merchants using a cryptocurrency payment platform, banks, and cryptocurrency exchanges**[5]**.

In this Paper, The modern industry has advanced to a new level as a result of the advancement of various technologies and the advent of novel concepts such as Big Data, Cloud Computing, Cyber Physical System (CPS), and so on. As a result, a smart factory has arisen, with the Industrial Internet of Things (IIoT) at its center, with the goal of realizing intelligent manufacturing. Different types of industrial equipment in a smart factory achieve cluster interaction through the IIoT, in which data is no longer separate. The transformation and upgrading of the intelligent and networked manufacturing process can be fostered by data collision and fusion, but platforms may produce unanticipated issues**.** We propose an innovative blockchain-based IIoT architecture in this research to aid in the development of a more secure and dependable IIoT system. We offer a new IIoT design and provide a full analysis of all architecture levels by assessing the drawbacks of the existing IIoT architecture and the benefits of Blockchain technology. In addition, we introduce the BLP and Biba models for designing secure assurance in theory. On this foundation, we outline the suggested architecture's essential technologies, flow, and protection measures. Finally, we analyses the benefits of retrofitting an existing automatic manufacturing platform vs a standard IIoT architecture. It demonstrates that the proposed architecture can significantly improve CIA needs**[6].**

In this Paper, The Internet of Things (IoT) is a new phrase that depicts how common devices are constantly connected. With the rapid adoption of IoT devices, incredible interactions between physical items are now possible, resulting in increased efficiency, accuracy, and economic benefits while eliminating human intervention. Gartner predicts that by 2020, there will be over 20 billion connected IoT devices around the world. In This Paper, We propose a blockchain-based safe system for IoT data storage and protection. Edge computing is used to manage data storage and to execute calculations on small IoT devices. Certificateless cryptography is used to create a simple authentication method for blockchain-based IoT applications, and blockchain addresses the disadvantages of certificate-based encryption by providing a platform for broadcasting a user's public key. We provide extensive methods for processing transactions and achieving authentication and accountability in such a system. To our knowledge, this is the first work to address the challenge of developing a secure and responsible storage system for large-scale IoT data, as well as the first to combine edge computing, certificateless encryption, and blockchain as a whole to serve IoT applications**[7]**.

In this Paper, The essential technology for ensuring information security is a cryptographic algorithm, and the security of blockchain technology is based on cryptographic security. Internationally recognizedcryptographic algorithm systems and related standards, such as SHA and RSA, have long been employed in blockchain. The State Cryptography Administration unveiled the "elliptic curve public keycryptography algorithm" (SM2), which wasindependently developed by the Chinese government, at the end of 2010 to substantially reduce the country's excessive reliance on foreign cryptographic technology and goods. The national secret algorithm is used in this system. It tackles the problem of key transmission in decentralized circumstances by establishing an automatic copyright "center." It overcomes the difficulties of copyright uploading, review, transaction, reporting, and distribution in the decentralized scenario by looking at copyright protection from the standpoint of a transaction. During the publicity and lock-up periods, transactions are possible. There are options for point-to-point payments, which need a minimal handling fee. The system has a high tolerance for single-point failure and minimal equipment costs because it is based on a decentralized idea. The system can handle multi- person income distribution and chain transactions. This system has a lot of advantages**[8].**

In this Paper, Blockchain is nothing more than a chain of blocks. When the terms "block" and "chain" are used in this context, the primary topic of discussion will be digital data ("block") stored in a public database ("chain"). Information about transactions, participants in transactions, and information that distinguishes them from other blockswas stored in blocks. The network established between a firm and a supplier to distribute unproduced goods to end-users. It also keeps track of product and service information. The block chain technology is utilized throughout the supply chain to ensure transparency and end-to-end traceability (cryptography and bitcoin transaction). Blockchainusers digitize their physical data and establish a decentralized, immutable record for transparency and access**.** The numerous difficulties and related solutions encountered in the supply chain employing block chain technology are discussed in this paper. Data traceability and security are becoming easierand faster thanks to new block chain methods and technology. The use of block chain also provides structure to the supply chain, as well as a slew of other benefits. Blockchain allows for greater cost effectiveness in the supply chain. The research above will provide you a thorough understanding of themost recent supply chain security approaches. To meet their needs, the user should select the most appropriate and cost-effective method. Our next workwill assess how scalable different blockchain systemsand processes are using existing tools**[9].**

In this Paper, Although the Internet of Things (IoT) offers numerous prospects for digitalization, IoT devices are also becoming more attractive targets for cyberattacks. The constantly growing number of Internet-connected gadgets increases the potential for malicious behavior. Security solutions that work with restricted IoT devices are needed. Customized blockchain-based IoT security may be the answer. A blockchain is a peer-to-peer network that holds a continuously expanding linked list of data structures called blocks that is copied in each node. Blocks are made up of records of

transactions that blockchain users have initiated. Unauthorized IoT data activities can be avoided by recording all IoT data operations as transaction records in blockchain blocks. This chapter introduces blockchain technology and its security aspects, as well as its application to IoT security. The chapter gives some instances of how blockchain-based solutions might be used in various IoT scenarios**[10]**.

In this Paper**,** in recent decades, digitalization in information technology (IT) and communication has prompted significant economic and social developments around the world, making it one of the most significant sources of banking sector development [1]. However, Iraq's recent change has resulted in a significant expansion of financial markets and diversification of banking activity, necessitating the development of more sophisticated banking infrastructure. Iraq's banking system currently consists of 63 banks, with over 1068 branches . These banks are linked to the Central Bank of Iraq (CBI), which is in charge of currency issuance, cash reserve management, bank supervision and monitoring, and so on .This study offers a blockchain-based paradigm for electronic money transfers between Iraqi banks. The system demonstrates a high level of security by utilizing important blockchain capabilities such as immutability, tamper resistance, and irreversibility. To prevent data manipulation, asymmetric key encryption is utilized to transfer transactions between the relevant banks, as well as digital signatures to sign transfer requests. The method protects clients' privacy by segregating their personal information from their financial activities. The blockchain records transactions that are linked to bank codes and account numbers. As a result, no information about the client's identity is available, which is only known at the branch where the account is opened**[11]**.

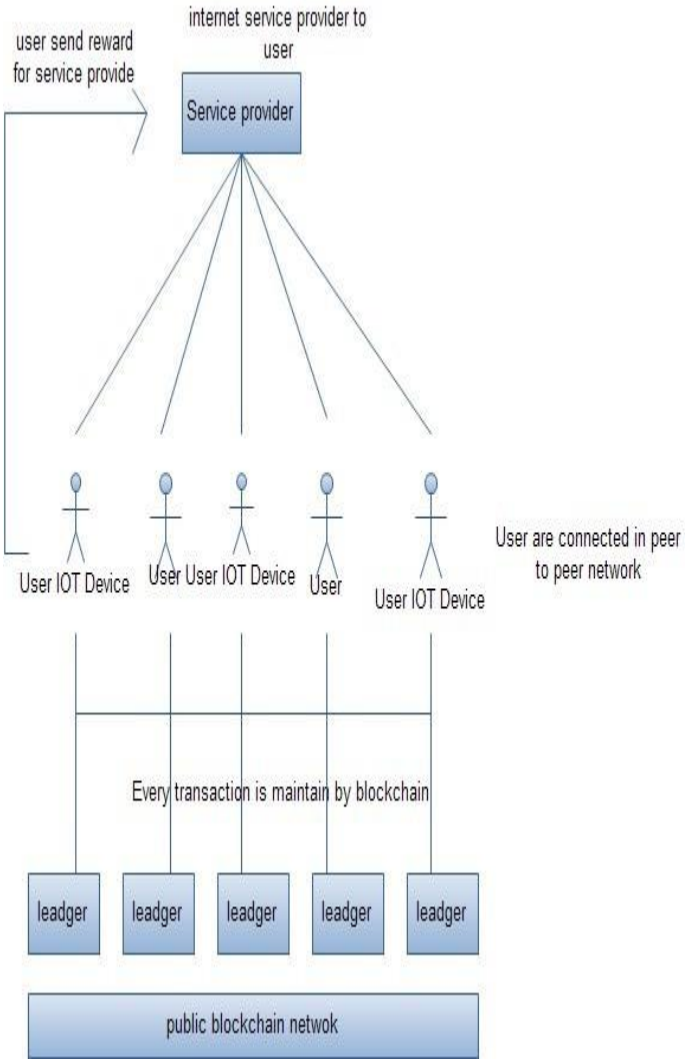
In this Paper, The set of mathematical procedures that allow us to determine the worth of money over time is known as financial mathematics. The value of this discipline lies primarily in its application to banking and stock market transactions, as well as economic issues and other areas of finance, because it allowsthe financial management to make the best decisions possible. As a result, the study of financial transactions, which describes the exchange of money flows available at various points in time and susceptible to quantitative alterations over time, falls under the umbrella of both mathematics and finance. This study looked at the major trends in global research on financial transactions from the publishing of the first article on the subject in 1935 tothe end of the last full year (2019). The bibliometric methodology was used to a sample of 1486 articles from the Scopus database for this purpose. This analysis allows for the identification of the main authors, institutions, and nations that contribute toworldwide research on financial transactions, as well as the evolution of scientific production and the main topic areas where the published papers arerelated[**12]**.

In this Paper**,** Individual entity transactions, particularly those involving money, require numerous processes and intermediaries to facilitate their interactions while maintaining confidence. As a result, typical transactions might be time-consuming and costly. Blockchain is a distributed ledger system that enables secure transactions in a network of independent entities without the use of a

third-party trustworthy third-party**.** Systems that facilitate financial transactions on a big scale must be able to manage huge numbers of transactions while maintaining a high level of operational availability. The limits of blockchain technology as a platform forconducting transactions among a network ofindividuals who do not need to trust each other were highlighted in this study. The availability and security of two architectural factors were investigated in depth to see how architectural approaches might beutilized to create blockchain-based systems to circumvent some of these restrictions. Blockchain systems have performance and scalability issues due to their decentralized nature. Because it is a trustless peer-to-peer network, each transaction must be authenticated at each hop, limiting the speed with which transactions may be processed and the number of transactions that can be completed in a given unit of time . We plan to look into performance and scalability issues in the future**[13]**.

MODEL ARCHITECTURE:

Blockchain is a method of storing data that makes it difficult, if not impossible, to alter, hack, or trick the system. Each block in the chain contains a number of transactions, and each time a new transaction takes place on the blockchain, a record of that transaction is added to the ledger of each participant.



SET stands for Secure Electronic Transaction. For all parties engaged in an e-commerce transaction, SET provides a secure environment. It also ensures that information is kept private. It uses digital certificates to offer authentication. A secured transaction is a loan or credit transaction in which thelender obtains a security interest in the borrower's collateral and has the right to foreclose or reclaim thecollateral if the borrower defaults.

LAYERED STRUCTURE OF PROPOSED SYSTEM.

In propose system blockchain network is distributed each ledger is store in different node. They are connected in peer to peer network. The blockchain system is tamperproof, distributed, secure and immutable. So user can store and upload their docson blockchain network. In this system service provider is provide service to user and with that service user give some rewards to the service provider. So we are use blockchain in between transaction. The attacker can query the transaction

amount and transaction address of both sides of the transaction, as well as extract the equivalent information by analyzing the transaction content, because every transaction is public in the blockchain. As a result, the blockchain's openness and transparency pose major privacy concerns for users.

Advantages:

- Secure payment transmission between userand service provider
- Each transaction maintain record oftransaction of data
- Data maintain integrity during transaction.

CONCLUSION:

This project proposes a blockchain-based safe serviceprovisioning method for LCs. In addition, an incentive plan based on the credibility of SPs is beingdeveloped. A logical payment method will also be implemented. We employ blockchain as a proof recorder, which records all evidence of service provisioning from SPs to LCs. Because it has both public and private blockchain properties, a blockchain consortium is used. Licensed blockchain users are in charge of maintaining the blockchain. Other government users can utilize the blockchain to read and validate their services. A PoA consensus system is utilized, in which a set of validators ispicked and blocks are added to the blockchain. Validators are chosen depending on their network's trustworthiness. The amount of transactions that are true for that SP is known as reputation. The Keccak256 hashing algorithm is used to convert data of any size into a hash of xed size. Keccak256 is preferred over SHA256 and RIPEMD160 due to its lower gas usage. SC is used to validate the services provided by SPs to LCs. When an LC receives a service from the SP, the LC activates the SC forvalidation of the acquired service. Because service codes are delivered in an off-chain fashion, AES128is utilized to encrypt them before delivering them to LCs. The simulation results demonstrate that utilizing PoA reduces total gas consumption by 17% when compared to PoW. In comparison toRIPEMD160 and SHA256, the overall gas usage utilisingKeccak256 is reduced by 1.9 percent and 1.3 percent, respectively.

REFERENCES:

[1] Yuhui Zhang Dejun Yang," Robust Pay: Robust Payment Routing Protocol in Blockchain-based Payment Channel Networks".[2019].

[2] Arman Pouraghily and Tilman Wolf," A Lightweight Payment Verification Protocol for Blockchain Transactions on IoT Devices".[2019].

[3] Peng Li, Toshiaki Miyazaki, and Wanlei Zhouy," Secure Balance Planning of Off-blockchain Payment Channel Networks".[2020].

[4] Alin Bogdan Popa," Instant payment and latent transactions on the Ethereum Blockchain".[2018]

[5] Xiaofeng Chen, "IEEE Standard for GeneralProcess of Cryptocurrency Payment".[2020]

[6] Jiafu Wan, Jiapeng Li, Muhammad Imran, Di Li, Fazal-e-Amin," A Blockchain-Based Solution for Enhancing Security and Privacy in SmartFactory".[2019].

[7] Ruinian Li1 , Tianyi Song1 , Bo Mei2 , Hong Li3, Xiuzhen Cheng," Blockchain for Large-Scale Internet of Things Data Storage and Protection".[2018].

[8] Liming Liu; Wenqian Shang; Weiguo Lin; WeiHuang," A Decentralized CopyrightProtection, Transaction and Content DistributionSystem Based on Blockchain".[2021].

[9] Yaswanth Raj; Sowmiya B, "Study on Supply Chain Management using Blockchain Technology".[2021].

[10] Smitha Chowdary Ch; Srilakshmi Puli; Lakshmi Viveka K; M.V.B.T. Santhi," Machine Learning Based Data Security Model Using Blockchain forSecure Data Transmission in IoT"[2018].

[11] Sangwan, Raghvinder S., Mohamad Kassab, and Christopher Capitolo. "Architectural considerations for blockchain based systems for financial transactions." *Procedia Computer Science* 168 (2020): 265-271.

[12] Deer, Mohammed Sabri, Intisar Al-Mejibli, and AllaTalal Yassin. "Money Transfer System Using Blockchain Technology: A Case Study of Banks in Iraq."

[13] Westermeier, Carola. "Money is data–the platformization of financial transactions." *Information, Communication &Society* 23.14 (2020): 2047-2063.