International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

Enhancing and Evaluating the Privacy of User in Bitcoin Transaction

Swarnalashmi R[1], Menaka R[2]

U.G. Student, Department of Information Technology, Velalar College of Engineering and Technology, Thindal, Tamil Nadu, India[1]

Associate Professor, Department of Information Technology, Velalar College of Engineering and Technology, Thindal, Tamil Nadu, India[2]

ABSTRACT: The increase in transactions of some multinational organizations are within the chance of losing their identity provided. To substantiate the security and privacy of the user variety of the cryptographic algorithms are used. This paper helps in enhancing the user's privacy by using some hash algorithms like MD5. Bitcoin and Blockchain plays a big role that shares the value during a cryptocurrency manner. Bitcoin is a digital and global money system currency. It allows people to send or receive money across the internet. Blockchain is a distributed ledger technology (DLT). It protects the transaction from the third party. Bitcoin has been criticized for its use in illegal transactions. To beat the illegal transaction blockchain concept is utilized to protect the transaction from illegal purpose. The transactions are stored within the blocks. Hence, it's decentralized. There isn't any possibility that the data if lost cannot be recovered. The blockchain technology is also practically applied to any industry.

KEYWORDS: Blockchain, Bitcoin, hash algorithm, user privacy, Decentralized network.

I. INTRODUCTION

A blockchain is a decentralized, distributed and public virtual ledger that is used to file transactions throughout many computer systems in order that any involved file can't be altered retroactively, without the alteration of all next blocks.This allows the individuals to confirm and audit transactions independently and relatively inexpensively.A blockchain database is managed autonomously using a peer-to-peer community and a disbursed time stamping server. They are authenticated with the aid of mass collaboration powered by means of collective self-interests. Such a design facilitates robust workflow where individuals' uncertainty regarding information security is marginal. The use of a blockchain eliminates the characteristic of countless reproducibility from a virtual asset. It confirms that each unit of price was transferred simply once, solving the long-standing hassle of double spending. A blockchain has been defined as value-alternate protocol. This blockchain-based exchange of fee can be forced quicker, more secure and cheaper than with conventional systems. A blockchain can preserve name rights because, whilst properly installation to detail the trade agreement, it offers a file that compels offer and acceptance. A blockchain is immune to the amendment of data. It is "an open, distributed ledger that can file transactions between two parties efficiently and in a verifiable and permanent way. A blockchain is a decentralized, distributed, and frequently public, virtual ledger that is used to report transactions throughout many computer systems in order that any involved report cannot be altered retroactively, without the alteration of all subsequent blocks. A blockchain is a decentralized, allotted, and generally public, virtual ledger that is used to file transactions across many computers in order that any involved report cannot be altered retroactively, without the alteration of all subsequent blocks.

II. SCOPE OF THE PROJECT

The blocks and the contents within them are covered by using effective cryptography, which guarantees that preceding transactions with in the community cannot be either cast or destroyed. Here,Smart contracts are often visible as a highly effective software of blockchain technology. These contracts are truly pc programs which can oversee all components of an agreement, from facilitation to execution. Blockchain gives a superb stage of security, thanks to independent verification procedures that take region at some stage in member computer systems on a blockchain network. In digital foreign money cases, this verification is used to approve transactions before they may be added to the chain. This mechanism could just as easily be implemented to other varieties of verification procedures, including identity verification and lots of other packages as well.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

A transaction is a switch of Bitcoin value this is broadcast to the community and collected into blocks. A transaction usually references previous transaction outputs as new transaction inputs and dedicates all input Bitcoin values to new outputs. Transactions aren't encrypted, so it's far possible to browse and view every transaction ever accrued right into a block. Once transactions are buried under sufficient confirmations, they may be taken into consideration irreversible.

Bitcoin is a cryptocurrency, meaning it's supported by a supply code that uses highly complicated algorithms to prevent unauthorized duplication or creation of Bitcoin units. The code's underlying principles, referred to as cryptography, are primarily based on advanced mathematical and pc engineering principles. It's simply impossible to interrupt Bitcoin's supply code and manipulate the forex's supply.

Bitcoin presently creates two distinct script Public Key pairs. These are described below. It is possible to design more complex types of transactions, and hyperlink them collectively into cryptographically enforced agreements. These are referred as Contracts. A Bitcoin address is handiest a hash, so the sender can't offer a complete public key in script Public Key. The script verifies that the provided public key does hash to the hash in script Public Key, after which it also checks the signature towards the general public key.

III. RELATED WORKS

Traceable monero: Anonymous cryptocurrency with Enhanced Accountability

Yannan Li, Guomin Yang, Willy Susilo, Yong Yu, Man HoAu, Dougxi Liu (2019) - Monero offers a high stage of anonymity for both users and their transactions. However, many criminal activities probably devoted with the safety of anonymity in cryptocurrency transactions. Thus, user accountability (or traceability) is also vital in Monero transactions, which is sadly lacking in the modern literature. This technology fill this gap by introducing a new cryptocurrency named Traceable Monero to balance the user anonymity and accountability. This framework relies on a tracing authority, but is optimistic, in that it is only involved when investigations in certain transactions are required. Then formalize the system model and security model of Traceable Monero. Present a detailed construction of Traceable Monero by overlaying Monero with two types of tracing mechanisms, tracing the one-time addresses with money flows and tracing the long-term addresses. Thus, prove the security of Traceable Monero and implement a prototype of the system, which demonstrates that Traceable Monero incurs merely a very small overhead in generating and verifying a transaction compared to Monero transactions.

A Survey on Security and Privacy Issues of Bitcoin

Mauro Conti, Sandeep Kumar E, Chhagan La, Sushmita Ruj (2018) - Bitcoin is a popular cryptocurrency that records all transactions in a distributed append-only public ledger called blockchain. The security of Bitcoin heavily relies on the incentive compatible proof-of-work (PoW) based distributed consensus protocol, which is run by the network nodes called miners. In exchange for the incentive, the miners are expected to maintain the blockchain honestly. Since its launching 2009, Bitcoin economy has grown at an enormous rate, and it is now worth about 150 billion of dollars. This exponential growth in the market value of bitcoins motivate adversaries to exploit weaknesses for profit, and researchers to discover new vulnerabilities in the system, propose countermeasures, and predict upcoming trends. In this paper, we present a systematic survey that covers the security and privacy aspects of Bitcoin. We start by giving an overview of the Bitcoin system and its major components along with their functionality and interactions within the system. We review the existing vulnerabilities in Bitcoin and its major underlying technologies such as blockchain and PoW-based consensus protocol. These vulnerabilities lead to the execution of various security threats to the standard functionality of Bitcoin. We then investigate the feasibility and robustness of the state-of the-art security solutions. Additionally, we discuss the current anonymity considerations in Bitcoin and the privacy-related threats to Bitcoin users along with the analysis of the existing privacy-preserving solutions. Finally, we summarize the critical open challenges, and we suggest directions for future research towards provisioning stringent security and privacy solutions for Bitcoin.

Privacy Preservation of Users in P2P E-Payment System

Albert Kofi Kwansah Ansah, Daniel Adu – Gyamfi, Stephen Anokye (2019) - Bitcoin ecosystem is supposed to be anonymous and untraceable. Nonetheless, Bitcoin offers weak anonymity in practice. The linkable pseudonymity of Bitcoin system raises privacy concerns for users. There are inputs and outputs of vulnerable to possible link ability and traceability of users' identity, that can lead to information leakage. Input and output addresses of transactions miss unlink ability in Bitcoin. Several attempts to solve unlink ability and untraceability of users' transactions found not to satisfy all requirements of a practical anonymity for users to transact business with bitcoins

securely and privately. In this paper, the authors focused on preserving identity and transactional behavior of users in bitcoin cryptocurrency transactions. A secure privacy-preserving scheme is presented. The paper incorporates bilinear pairing, elliptic curve (ECC), ring signature and Zero Knowledge Proof to curb users' privacy breaches. The authors theoretically analyzed, and evaluated proposed scheme, which is proven secure and robust to implement for preserving users' privacy in bitcoin transactions. The proposal adds a compatible privacy preserving layer on top of the Bitcoin blockchain, and consistent with the current Bitcoin architecture without offering any modification.

A Survey on Anonymity and Privacy in Bitcoin – like Digital Cash Systems

Merve Can Kus Khalilov and Albert Levi (2018) - Bitcoin is the most widely known distributed, peer to-peer (P2P) payment network without existence of a central authority. In Bitcoin, users do not use real names; instead, pseudonyms are used. Managing and verifying transactions and issuing of bitcoins are performed collectively by peers in the network. Since pseudonyms are used without providing any identity, it is perceived that Bitcoin provides anonymity. However, it is one of the most transparent payment networks since all transactions are publicly announced. Blockchain, which is the public ledger of Bitcoin, includes all transactions to prevent double-spending and to provide integrity. By using data in the blockchain, flow of bitcoins between transactions can be observed and activities of the users can be traced. When the implications obtained from the blockchain are combined with external data, identity and profile of a user can be revealed. This possibility has undesirable effects such as spending history of a user becomes accessible to other people, or cash flow of a merchant becomes exposed to competitors. There are several proposals as extensions or alternatives to Bitcoin, which improve anonymity and privacy. This survey presents an overview and detailed investigation of anonymity and privacy in Bitcoin-like digital cash systems. We examine the studies in the literature/web in two major categories: (i) analyses of anonymity and privacy in Bitcoin, and (ii) extensions and alternatives to Bitcoin, which improve anonymity and privacy. We list and describe methods and outcomes for both categories and group studies according to these methods and outcomes. We also present relationships between outcomes of analyses and the improvement methods. We compare performances of the methods and show relationships between the proposals. Moreover, we present guidelines for designing an anonymity/privacy improvement and discuss future research directions.

ProvChain: A Blockchain based Data provenance Architecture in Cloud Environment with Enhanced privacy and Availability

Xueping Liang, Sachin Shetty, Deepak Tosh, Charless Kamhoua, Kevin Kwiat, Laurent Njilla (2017) - Cloud data provenance is metadata that records the history of the creation and operations performed on a cloud data object. Secure data provenance is crucial for data accountability, forensics and privacy. In this paper, we propose a decentralized and trusted cloud data provenance architecture using blockchain technology. Blockchain-based data provenance can provide tamper-proof records, enable the transparency of data accountability in the cloud, and help to enhance the privacy and availability of the provenance data. We make use of the cloud storage scenario and choose the cloud file as a data unit to detect user operations for collecting provenance data. We design and implement ProvChain, an architecture to collect and verify cloud data provenance, by embedding the provenance data into blockchain transactions. ProvChain operates mainly in three phases: (1) provenance data collection, (2) provenance data storage, and (3) provenance data validation. Results from performance evaluation demonstrate that ProvChain provides security features including tamper-proof provenance, user privacy and reliability with low overhead for the cloud storage applications.

IV. EXISTING SYSTEM

The Bitcoin is a kind of cryptocurrency. It is used for the transaction money to a particular individual. The bitcoin has no currency it is able to be transferred to the particular person and information of the transaction are best proven to the receiver. When conditions are met, clever contracts may be completely self-executing and self-enforcing. For proponents of smart contracts, these tools provide a greater secure, greater automated alternative to conventional settlement law, as well as an application that is faster and inexpensive than conventional methods.

The information which has been shown is stored within the database so the data can be regarded in later part if any query arises. When redeeming coins which have been sent to a Bitcoin address, the recipient provides each the signature and the public key. The information of transaction is secured but the records which has been transacted isn't secure due to the fact the encryption technique has been implemented in this process and the information has the threat of having attacked by using the third party in computerized format.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

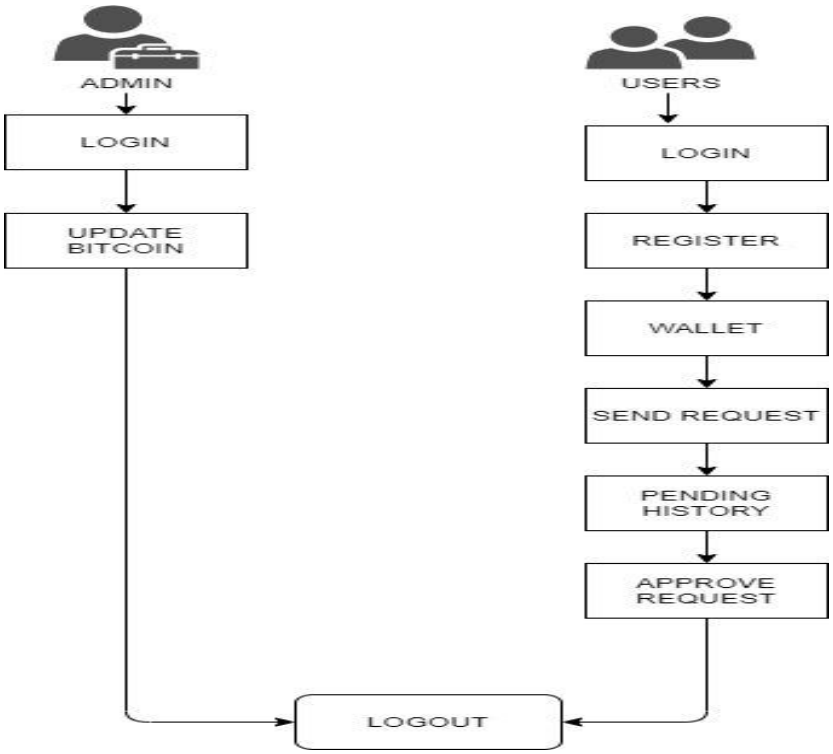
V. PROPOSED SYSTEM

In the proposed system the bitcoin is transferred in a blockchain manner which secures the transfer amount in a cryptocurrency. Blockchain technology allows for verification without having to be depending on third-parties. The data structure in a blockchain is append-only. So, the data cannot be altered or deleted. It uses protected cryptography to secure the data ledgers. Also, the current ledger is dependent on its adjacent completed block to complete the cryptography process. All the transactions and data are attached to the block after the process of maximum trust verification. There is a consensus of all the ledger participants on what is to be recorded in the block.

ARCHITECTURE DIAGRAM

MODULE DESCRIPTION

VERIFICATION:



The sender and the receiver both will get verified by their particular mail Id for the private account transaction. After the verification only certain transaction being done from one user to another user. The private account will be created.

TRANSACTION:

In this transaction process the sender will send the certain amount to the user. Before the transaction the receiver will wants to be verified weather the user has crypto currency or not. Before transaction the certain user will give request to the sender person who has the crypto currency. Then the sender will accept the request. The required amount will be transacted to the person who has request. Further the transacting the notification of each transaction was verified by the sender as well as receiver.

While transaction before and after transacting details where viewed for the sender and the receiver of transaction wallet of both the normal cash, crypto currency.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

VI. CONCLUSION

In this paper, the transaction of bitcoin is protected underneath the blockchain. The third-party can not attack the statistics easily. The transaction is completely encrypted ınd saved securely. In the business enterprise discipline here, the ledger consists of records that are saved as a reference purpose. Take, for instance, the land title. There are many cases of ambiguity in identify ownership. With blockchain technology, the records once saved cannot be altered. Any adjustments are time stamped. It's safer and extra secured.

REFERENCES

[1] Albert Kofi Kwansah Ansah, Daniel Adu-Gyamfi, Stephen Anokye, "Privacy Preservation of Users in P2P E-Payment System", (2019).
[2] Androulaki E, Karame G O, Roeschlin M, Scherer T, and Capkun S, "Evaluating User Privacy in Bitcoin", in Financial Cryptography and Data Security, (Vol.5) (2018).
[3] Mauro Conti, Sandeep Kumar E, Chhagan La, Sushmita Raj, "A survey on Security and Privacy issues of Bitcoin", (DOI 10.1109), (2018).
[4] Merve Can Kus Khalilov and Albert Levi, "A survey on Anonymity and privacy in Bitcoin Transaction-like Digital Cash Systems", (2018).
[5] Ruiyang Xiao, Wei Ren, Tianging Zhu, Kim-Kwang Raymond Choo, "A mixing Scheme Using a Decentralized Signature Protocol for Privacy Protection in Bitcoin Blockchain", (2019).
[6] Tengtei Xue, Cong Wang, Yuyu Yuan, "An Approach for Evaluating User Participation in Bitcoin", (vol.4) (2018).
[7] Volety T, Saini S, McGhin T, Liu C Z, and Choo K K R, "Cracking bitcoin wallets: I want what you have in the wallets," Future Generation Computer Systems, vol. 91, pp. 136–143, 2019.
[8] Xueping Liang, Sachin Shetty, Deepak Tosh, Charless Kamhoua, Kevin Kwlat, Laurent Njilla," ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability", (2017).
[9] Yannan Li, Guomin Yang, Willy Susilo, Yong Yu, Man Ho Au, Dongxi Liu, "Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability", (vol.3) (2019).
[10] Yi Liu, Xingotong Liu, Chajing Tang, Jiang Wang and Zei Zhang," Unlinkable Coin Mixing Scheme for Transaction Privacy Enhancement of Bitcoin", (vol.4) (2018).