International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 07 | July - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Secure Online Transactions using Blockchain

Ms. K Annsheela
Assistant Professor,
Department of Computer College
Thassim Beevi Abdul Kader College for Women

ABSTRACT:

Blockchain is the most commonly used distributed database or ledger for digital currency exchanges and secure transactions. Each network participant has access to a ledger that is updated with each new transaction. The blockchain ledger is a collection of all transactions made in the past. A blockchain ledger is an ever-evolving tamper-proof data structure that contains blocks containing individual batches of transactions. This work will help understand the various security algorithms used for electronic transactions and payments. Hashing methodology is used to secure the transaction in Blockchain. Blockchain technology and its impact on companies and industries. The blockchain supports a decentralized, invariant, consistent, and secure hashing algorithm in which Proof-of-Wok is used. This systematic study helps you understand how is secure a transaction.

I. Introduction:

Advances in digitalization have revolutionized people's lives. As technology advances, we use internet-based banks, and various e-commerce payment systems are growing when shopping. It is designed to increase, improve and deliver secure electronic payment transactions. People are also interested in electronic payment systems because they reduce paperwork and transaction costs.

The system is easy for business people to use and takes less time than manual processing and latency to help businesses expand their reach to the market. The ePayment system is a method of processing or paying goods and invoices via electronic media without using cash or checks. This is called an online payment system. E-Payment uses electronic devices and various types of trading cards such as customers, productions, financial companies, etc. as a medium of computer technology to issue payment instructions directly or indirectly via a network to make payments and remittances. , Refers to the parties to electronic transactions.

II.Literature Review

Prince will Aigbe et, al[3],2014, In their study, a complete review of the different categories of online payment systems in terms of online payment processes, authentication mechanisms, and authentication types analysis

reveals that online payment systems with authentication mechanisms involving two or more authentication factors such as token encryption, digital signature, PIN tend to be more secured, reduced fraud vulnerability, and boost users' confidence in using electronic payment systems. Their work reveals that e-payment systems with authentication mechanisms involving two or more authentication factors have to be secured and reduced fraud and boost users' confidence e - payment systems

Satoshi Nakamoto et.al [4] 2016**.**Mentioned their work Online Payments or transactions were directly sent from one party to another without going through a financial institution that undergoes peer-to-peer communication. Digital signatures play a role in protection at a limit. The proposed system uses the verification of data and secures the transmission of money through bank validation.

NiturkarPallaviPravinet.al[5],2020 mentioned Blockchain technology for protecting the banking transaction without using tokens. Blockchain technology is a distributed system that works on total verification and validation of data without consideration of Miners or Tokens. Eliminating the use of miners or tokens may lead to creating a transparent and load-free network, which increase in survivability of transaction. By adopting blockchain in the distribution of databases on banking systems one can reduce attacks on the system. Blockchain without tokens plays an avital role in building a system that is more reliable for banking to perform transactions that have to be secure at a very high level.

Joseph Gualdoniet.al[4],2017, mentioned the Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication. The Secure Online Transaction Algorithm (SOTA) would benefit not only the account holders but also the credit card companies. Our model works by using two-factor authentications and a random code that the consumer would be generated and supplied on an application. The Secure Online Transaction Algorithm creates a new level of security that has not been implemented into credit cards yet. This algorithm could instrumental in reducing the number of fraudulent purchases made with stolen credit cards.

III.Blockchain

A blockchain is a distributed database shared between nodes in a computer network. As a database, blockchain stores information electronically in digital format. Blockchain is best known for its important role in cryptocurrency systems like Bitcoin for maintainingsecure and decentralized records of transactions. Blockchain innovationis to ensure the fidelity and security of data records and to create trust without the need for a trusted third party. The main difference between a typical database andblockchain isthe structure of the data. Blockchain collects informationin groups called blocks that

contain a set of information. A block has a certain amount of storage capacity, is closed when it is full and is linked to a previously full block to create a chain of data called a blockchain. The new information that follows this newly added block is compiled into the newly formed block and added to the chain when it is full.

A hash pointer is a pointer that has an encrypted hash of the data it points to. If you are new to hash functions, think of a hash of your data as a short code that represents your data. We cannot undo the original data from this code, but we can verify that the new data matches the original data by hashing the new data and comparing this new code with the stored code. Each node in the linked list is called a block, stores some data, and references the previous block in the blockchain. The first block on the blockchain is called a genesis block because it does not point to any other block. The latest block added is called Head

Blockchain is the technical backbone of "Bitcoin" and was introduced in 2009 as a secure and fast connection technology that enables exchange. In the blockchain, each user transaction creates a block and adds it to the chain of transactions. This creates a trail of interconnected blocks. Each block is sent and added to your ledger. Application of blockchain technology in payment of Blockchain functions corresponds to the requirements of the payment base.

- **Safe.**
- **Processing speed**
- **Traceability**
- **Global Registry (Ledger)**

The distributed ledger makes it possible to connect all the parties to real-time financial transactions for quick processing while maintaining the audit trail. Processing is distributed over the network, it is almost impossible to change or manipulate data, or manipulate fraud prevention and safety stops. Blockchain, we can ship money without using banks. Describes the simplicity and elegance of such systems and understands the process of creating ourown blockchain in the Python programming language to explain nuances. Working from a blockchain:

Block or ledger and this updated block are displayed to wait for the verification node at a specific time interval. Block Verification: When an Inner work node receives an updated block validation request, the node searches other nodes in the network in network to process to repetitive process to check the block. Blockchain: If all transactions are approved in the block, the new block is connected to the current block and closes the latest status of the block into the remaining blocks on the network.

IV.Methodology:

SSL:

SSL, or Secure Sockets Layer (SSL), is the most widely used security measure to secure Internet communications. SSL provides a secure communication layer between computers on a network.SSL supports security protocols such as encryption, and authentication, and ensures that requested and transmitted data is actually forwarded to the SSL provides security with 128-bit encryption, so sensitive information transmitted over the Internet during online transactions remains private.

SET:

The SET is a system that ensures the security and integrity of scripted electronic transactions made with credit cards. Secures online credit card payments using a variety of encryption and hashing methods. The SET protocol supports development by major organizations such as Visa, MasterCard, Microsoft providing Secure Transaction Technology (STT), and Netscape providing Secure Sockets Layer (SSL) technology.

Hashing in Proof-of-Work Consensus Algorithm:

Blockchain is an ever-evolving ledger that continues an everlasting report of all of the transactions which have taken place, in a stable, chronological, and immutable manner. To stable information, blockchain makes use of a hash characteristic. The hash characteristic is one of the maximum broadly used cryptographic algorithms in blockchain technology. These are cryptographic (however now no longer encryption) algorithms designed to defend the integrity of information. In a nutshell, a hash set of rules is a mathematical characteristic that turns any enter into an output of a set length. To be cryptographically stable - and usable in blockchain technology - a hash should be collision-resistant, this means that it`s very hard to locate inputs that produce the identical output.

Types of cryptographic hash features:

- **Secure Hash Algorithms (SHA2 and SHA3)**
- **RACE primitive integrity evaluation message summary (RIPEMD)**
- **Message Algorithm 5 (MD5)**
- **BLAKE2**

To do this, a hash characteristic should have the subsequent properties:

• **One-manner**: It is feasible to move from entering to output in a hash characteristic, however now no longer vice versa. This makes it not possible to opposite engineer a collision from the preferred hash output

• **Large output area:** The handiest manner to locate hash collisions is thru brute pressure seek. According to the Pigeon Cage principle, this calls for checking as many inputs because the hash has feasible outputs. This quantity

should be huge and sufficient to make a brute-pressure seek not possible

• A hash set of rules is taken into consideration stable tilla collision may be located for it. Once this happens, it`s formally obsolete, much like MD5 and SHA1. Using hash features inside the blockchain Hash features are frequently used to defend the integrity of information. With a dependable information hash, it's far feasible to compute the hash of the information and evaluate values. If they match, the information won't have been modified for the reason that a unique hash turned into generated. The blockchain`s virtual ledger is designed to keep treasured records that might advantage an attacker if modified in their favor. Furthermore, this ledger is saved and transmitted with the aid of using a community of nodes that might be suspicious of every other.

As a result, blockchains have some exclusive makes use of for the hash features and integrity safety they provide. Some of the maximum not unusual place that makes use of hash features in blockchain include:

Uses of Hash:

• **Digital signature**: Hash features are a vital part of virtual signature algorithms, summarizing information right into a compact price even as retaining its integrity. Digital signatures are used to hold information integrity and authenticate transactions and blockchains

• **Merkle Tree**: The Merkle tree summarizes the listing of transactions contained in a block right into inside the block header. They use hash features to make certain that no Merkle timber with the identical root hash can't be located. In this manner, with the aid of using storing the unique hash inside the block header and retaining the integrity of the block header, the integrity of the transactions contained inside the block frame is likewise protected.

• **Proof of Work consensus**: The Proof of Work consensus set of rules determines that a legitimate block is a block whose header has a hash price under a positive threshold. The collision resistance of the hash characteristic is vital right here because it guarantees that it's far very hard to discover a legitimate block.

Hash function security for blockchain

The safety of hash features for hash features inside the chain is vital to defend the immutability of the virtual ledger. If the hash utilized by a blockchain is broken, an attacker can locate conflicts for crucial hashes (consisting of the blockchain chain or the Merkle tree price). This will make it simpler for malicious nodes to rewrite the blockchain community records and motivate the blockchain gadget to crash. For this reason, the safety of hash features is vital to blockchain safety. The safety of a hash characteristic may be threatened in of the ways:

• **Algorithm strength**: Hash features are designed to face up to collisions, however cryptographic algorithms occasionally break.

If the vulnerability is observed in a hash characteristic, this may correctly locate collisions inside the hash characteristic.

• **Hash output period**: Hash features are designed to make the nice manner to discover a collision is a brute pressure seek, with the hunt area being the identical length as the gap of feasible has outputs. Might also additionally have. If the sort of area does emerge as searchable - because of using a hash whose output period is just too short - then the hash is now no longer collision-resistant and liable to attack.

Conclusion:

Online payment transactions use blockchain, the purpose of which is to ensure the security of the entire process. It uses a one-way hashing algorithm and Proof-of-Work in a consensus Algorithm to securely transmit data to miners. Miners also use a proof-of-work algorithm to verify transactions using the submitted hash value. Therefore, this paper aims to provide a secure process for online transactions by overcoming attacks such as man in the middle attack and eliminating third-party ports that speed up the whole process of the Hash function using proof-of-Work. Compared to Previous algorithms like SSL, and SET, the Proof-of-Work and hashing algorithms using blockchain got the better results. In the future optimizing the hash value in blockchain and increasing the security of transactions using blockchain algorithms

References:

(1)What is Blockchain Technology? A Step-by-Step Guide For Beginners. Available Online: https://blockgeeks.com/guides/ is-blockchain-technology/

(2)Nakamoto, Satoshi. ”Bitcoin: A peer-to-peer electronic cash system.” (2008). Available Online: https://bitcoin.org/bitcoin

(3) ParitoshBanchhor, DurgeshSahu, Ankit Mishra, Mohammed BakhtawarAhmed,”A Systematic Review on Blockchain Security Attacks, Challenges, and Issues,(2021)

(4)KarthikeyaThanapal, DhirajMehta, KarthikMudaliar, and BushraShaikh,” Online Payment Using Blockchain(2020)

(5)Fan Yang, Wei Zhou, Qingqing Wu, Rui Long, Neal N. Xiong, (Senior Member, IEEE), And Meiqi Zhou, Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism,IEEE access, august 2019.

(6)Applicationofblockchain,Availableonline(https://www.businessinsider.in/finance/news/the-growing-list-of-applications-and-use-cases-of-blockchain-technology-in-business-and-life/articleshow/74447275.cms) (accessed on march 2020)

(7)Prasanth Varma Kakarlapudi and Qusay H. Mahmoud, A Systematic Review of Blockchain for Consent Management, in mdpi journal, Healthcare 2021, 9, 137.

(8)Masihuddin, M.; Islam Khan, B.U.; Islam Mattoo, M.M.U.; Olanrewaju, R.F. A Survey on E-Payment Systems: Elements, Adoption, Architecture, Challenges, and Security Concepts. Indian J. Sci. Technol. 2017, 10, 1–19. [CrossRef]