Timestamp for the Blockchain Based Banking System

Timestamp for the Blockchain Based Banking System

**Abstract**  
The digital transformation in the world introduced Blockchain technology which can solve the busiest sector i.e. Banking Sector. Blockchain technology was presented with the concept of cryptocurrency bitcoin, a form of cash that can be sent peer-to-peer without the need of a central bank or any authority to maintain the ledger which was decentralized, faster, secure, cost-effective, transparent and non -vulnerable. Through this paper, we are introducing how the timestamp algorithm can be used as an address for a node of a blockchain. In this algorithm with every block creation, the previous block transaction hash and a unique value is used to create the transaction hash of that particular block node.

**Keywords**

Blockchain, Timestamp, Hashing, Salting, Smart Contracts

1. **INTRODUCTION**
   1. **Overview**

A blockchain is a decentralized database that is shared across computer network nodes. A blockchain acts as a database, storing information in a digital format. Blockchains are well recognized for their critical function in keeping a secure and decentralized record of transactions in cryptocurrency systems like Bitcoin.

The structure of the data on a blockchain differs from that of a traditional database. A blockchain organizes data into groupings called blocks, each of which contains a collection of data. Blocks have specific storage capabilities, and when they're full, they're closed and connected to the preceding block, producing a data chain known as the blockchain. All additional data that comes after that newly inserted block is assembled into a new document.

A Blockchain act as decentralized ledger that keeps track of transactions between two parties effectively. Although these parties have simultaneous access to update digital ledger constant and system virtually impossible to hack.

A consensus algorithm is a process in computer science used to achieve agreement on a single data value among distributed processes or systems. By this procedure, all the peers reach a common agreement about a present state.

The timestamp is a small data stored in each block as a unique serial and whose main function is to determine the exact moment in which the block has been mined and validated by the blockchain network.

* 1. **Background**

Today, banks are continuously exploring new ways to do transactions quicker for enhanced customer services by assuring transparency to customers and regulators while ensuring cost efficiency. Blockchain is an essential technology with promising application scenarios in banking industry nowadays. It can transform banking industry and make process more democratic, transparent secure and efficient.

* + 1. *Timestamp Algorithm*

Timestamp is an algorithm of blockchain which plays an important role in different business processes. We can timestamp digital content through it. As amount of digital content is rapidly increasing, so there are different methods of timestamping which can help us in easily digitalization in our day to day life, as now, we are using two types of methods for this- Traditional and Decentralized trusted time stamping. The basic approach for the first type was one way hash functions which was to secure and determine integrity of hash algorithms and the other is based on inserting integrated digital fingerprints into cryptocurrency blockchain system. The common fingerprint in this case is SHA-256 which is based on checksum followed by the definition of RFC-6234.Concluding that time stamping services are used to preserve the data integrity on blockchain, prevention of counterfeiting and securing our processes.

* + 1. *Salting*

In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. Salts are used to safeguard passwords in storage.

A salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. Salts are used to safeguard passwords in storage.

* + 1. *Hashing*

Hashing is a process of scrambling a piece of information or data beyond its original form. It is a process where original data is passed through a hash function which changes into a hash value also referred to as digest. The hashing algorithm that is used here is SHA-256, referred as Secured Hashing Algorithm, which mainly consists of 4 families SHA-0, SHA-1, SHA-2, SHA-3. SHA-256 referred to 2nd family.

Process of Hashing through SHA-256:

1. Padding bits: Message which is to be hashed is added with extra bits known as padding bits such that length is exactly 64 bits short of multiple 512.The first bit should be one, and the rest filled with zeroes.
2. Padding length: 64 bits of data can be added to make final plaintext a multiple of 512.
3. Compression: Entire message breaks into multiple blocks of 512 bits each. It puts each block through 64 rounds of operation. Output of first serves as input for second. The procedure is repeated until it reaches 512-bit block, final hash digest
   * 1. *Consensus Algorithm*

Consensus, it is a process in computer science used to achieve agreement on a single data value among distributed systems. In a distributed computing environment, a consensus algorithm is a technique that allows all participants in a blockchain network to reach a shared understanding (consensus) on the current data state of the ledger and trust unknown peers. Therefore, Consensus Algorithms helps to achieve reliability in network of blockchain and build a trust between unknown peers, where the consensus protocol is added to blockchain which is the only version on which every other node agrees upon. Consensus algorithms has some objectives to be clear before making an agreement that will be beneficial for whole network. Firstly, it agrees for an agreement, collaborate, equal right to nodes and compulsory participation of every node in the process. There are 4 major types of consensus algorithms in details to get a better understanding over the topic:

1. Proof of Work (POW):

This algorithm rewards the first node to complete all the necessary calculations received from the blockchain network, where all the nodes compete against each other by increasing the capacity of computing resources, which is less energy efficient.

1. Proof of State (POS):

In this algorithm, node with greater number of resources get chosen to generate the next block in the blockchain which more energy efficient than Proof of work and also promotes centralization of work to a particular node

1. Proof of Capacity (POC):

This algorithm allows mining devices in a network to use their primary or secondary memory space to decide mining rights. This consumes less energy compared to proof of work and proof of capacity.

* 1. **Research Objective:**

To prove the address generated by hashing and salting the Timestamp of the any transactions is untraceable.

1. **Literature Review**

As stated by [2] could have additional trust than ever before because the dealings is immutable and clear. Success in crypto-currency and different technical areas highlights several engaging options of the blockchain technology that may profit additional aspects of recent society. Time Banking may be a generalized exchange economy not supported cash, however values everyone's contribution on identical scale, the time exhausted.

As stated by [3] the effectiveness of this policy has remained polemical as many of us believe that policy manufacturers ought to promote freedom and transparency by empowering the general public to directly interfere and alter the system for public interest. this text makes an attempt to synthesize and analyses offered data with a spotlight on the role of blockchain, a money tool that may probably play a vital role within the property development of the world economy

As stated by [4] the utilization of Blockchain technology while not tokens to guard info regarding banking transactions, namely, transfer amounts, card details, names of participants, etc. this subject has relevancy, since the digital economy is changing into associate degree integral a part of fashionable life.

As stated by [5] Singh block chain has a stimulating support of bit coin, the digital crypto currency with Associate in Nursing ever increasing sphere of users worldwide. But, blockchain

in itself is far over simply bit coin, it's the new generation security system encapsulating processes nonparallel of blocks to produce a secure method of recording transactions and it's circulated among signatories, or any target cluster being the participants within the method. It attracts it charm out of the very fact that it achieves this while not the requirement of any central authority.

As stated by [6], Blockchain innovation offers the banking industry numerous interesting chances. For observable effects to happen in the financial industry, certain difficulties should be overcome. In any case, notice that new protection laws should be trailed by the financial business for utilizing this innovation. Security laws should be followed for the wellbeing of both people and associations.

As stated by [7] The paradigm of net of Things (IoT) is paving the means for a world, wherever several of our daily objects are interconnected and can move with their setting so as to gather data and modify sure tasks.

As stated by [8] blockchain technology platform on the financial sector through cryptocurrency, and an impact on other industries. The subject of research is not only this technology but also its commercial exploitation. In order to understand the platform, the starting point of this research is an analysis of how the technology functions, after that the advantages for business and economic transaction are identified, and finally the paper deals with an impact of new technology on business, above all on financial operations.

As stated by [9] The formation of storage contracts between peers. Contracts area unit agreements between a storage supplier and their consumer, shaping what knowledge are going to be keep and at what worth.

1. **METHODOLOGY**

**3.1 Implantation Tools**

* Ganache for creating the blockchain
* Solidity for writing Smart Contracts
* Web3.js for interacting with the smart contracts and interacting with database
* Etherscan to check the addresses stored by the blockchain
* MY-SQL workbench for storing and managing database of banking system
  1. **Implementation Details**
* The object that contains the transaction details that need to be pushed to the blockchain as part of the block is created for all four of the processes being processed by the applications.
* But for storing the customers’ details and transaction details a separate relational database is set up. The customer table contains account number (email id), password (hashed value), balance, customer id, name, CNIC number, Date of Birth, debit card details, card status and registration details
* Similarly, for every transaction, the transaction details are also stored in a relational database table pushing alongside to blockchain. The transaction details contain transaction id, sender id, amount, receiver id and date of transaction.
* As the details are inserted by the customer for the transfer the user's table updates first of all by subtracting the transferred amount from the sender and adding the amount to the receiver. If the balance of the sender is less than the amount entered for the transfer the applications show up the error and the transaction won’t be processed alternatively if the transaction is processed it is followed by inserting a row in the transactions table
* In order to first push any data into the blockchain, we have to validate the block which is done by the miners. Miners validate the block and then it is added to the chain; the block is verified by a consensus algorithm
* The timestamp is a small amount of data stored in each block as a unique serial whose main function is to determine the exact moment in which the block has been mined and validated by the blockchain network. Verification is done by hashing the current block timestamp unique value with its previous block unique hash value.
* Since the timestamp is unique there is a zero percent chance that two blocks will have the same hash ID. Then we conclude that there are no collisions in the series and the series itself will remain unique.
* Every fund transfer transaction record is present in the Blockchain server as well as in SQL Server. Because SQL Server and Blockchain Server are synced. If we try to forcefully delete the Fund Transfer Transaction record from the database table then the deleted record will be immediately rolled back using the blockchain node data.
  1. **Why Timestamp**

For any point in time, the timestamp turns out to be 13-digit number. After salting it 5 times at random with different salting strings the combination is 28 digits. After using sha256 algorithm hashing we get a 256-bit result. Which can give around 100^8 + 100^7 +100^6 different addresses. Now the “fastest bitcoin rig” can generate 44TH/s. That means they can generate 44 tetra hash per second.

Number Of Second = 100^length of string/computer speed

Therefore, the Second for 28-digit string is:

Number of seconds = (100 ^ 28 /44) = 2.27e54

Number of years = 3.1e + 7

1. **Conclusion And Future Work**

In this paper, we justified why using timestamp algorithm, then hashing and salting its values can increase the security of blockchain by a lot of margins and make the addresses quite untraceable taking its computing power to around 3.1e+ 7 years. This computation is not possible in single life time.

The Roll-back of data can also change the local database which is currently now restricted to smart contracts. This will not change the final balance but the deleted transactions can now be printed.

Time Warp Attack can also be addressed as repeated salting and hashing can increase the risk of the same

**References:**

**[1]Bakaul, Masum & Das, Nipa & Moni, MadhabiAkter. (2020). The Implementation of Blockchain in Banking System using Ethereum. International Journal of Computer Applications. 177. 50-54. 10.5120/ijca2020919895.**

**[2]R. C. Merkle, "Protocols for Public Key Cryptosystems," 1980 IEEE Symposium on Security and Privacy, 1980, pp. 122-122, Doi: 10.1109/SP.1980.10006.**

**[3]S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *URL:***[***http://www.bitcoin.org/bitcoin.pdf*,**](http://www.bitcoin.org/bitcoin.pdf)**2008.**

**[4]X. Lin, R. Xu, Y. Chen and J. K. Lum, "A Blockchain-Enabled Decentralized Time Banking for a New Social Value System," 2019 IEEE Conference on Communications and Network Security (CNS), 2019, pp. 1-5, Doi: 10.1109/CNS.2019.8802734.**

**[5]Q. K. Nguyen, "Blockchain - A Financial Technology for Future Sustainable Development," 2016 3rd International Conference on Green Technology and Sustainable Development (GTSD), 2016, pp. 51-54, Doi: 10.1109/GTSD.2016.22.**

**[6]N. A. Popova and N. G. Butakova, "Research of a Possibility of Using Blockchain Technology without Tokens to Protect Banking Transactions," 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2019, pp. 1764-1768, Doi: 10.1109/EIConRus.2019.8657279.**

**[7]V. Naik, R. Pejawar, R. Singh, A. Aher and S. Kanchan, "Expeditious banking using Blockchain Technology," 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE), 2020, pp. 1-6, doi: 10.1109/CISPSSE49931.2020.9212253**

**[8]S. Sakho, Z. Jianbiao, F. Essaf and K. Badiss, "Improving Banking Transactions Using Blockchain Technology," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), 2019, pp. 1258-1263, doi: 10.1109/ICCC47050.2019.9064344.**

**[9]Chowdhury, M. ,Suchana, K. , Alam, S. and Khan, M. (2021) Blockchain Application in Banking System. *Journal of Software EngineeringandApplications*,14,298-311.doi:**[**10.4236/jsea.2021.14701**](https://doi.org/10.4236/jsea.2021.147018)**8.**

**[10]T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," in IEEE Access, vol. 6, pp. 32979-33001, 2018, doi: 10.1109/ACCESS.2018.2842685.**

**[11]Knezevic, Dusko. (2018). Impact of Blockchain Technology Platform in Changing the Financial Sector and Other Industries. Montenegrin Journal of Economics. 14. 109-120. 10.14254/1800-5845/2018.14-1.8.**

**[12]S. King, “Primecoin: Cryptocurrency with prime number proof-of- work,” July 7th, 2013.**

**[13]J. J. Kishigami, “Blockchain contract: A complete consensus using blockchain,” in Consumer Electronics (GCCE), 2015 IEEE 4th Global Conference on. IEEE, 2015, pp. 577–578.**

**[14]S. King and S. Nadal, “Ppcoin: Peer-to-peer crypto-currency with proof- of-stake,” self-published paper, August, vol. 19, 2012.**

**[15]G. Wood, “Ethereum: A secure decentralisedgeneralised transaction ledger,” Ethereum Project Yellow Paper, vol. 151, 2014.**

**[16]E. Dufﬁeld and K. Hagan, “Dark coin: Peertopeer cryptocurrency with anonymous blockchain transactions and an improved proof\_of\_work\_system,” Mar-2014 [Online].**

**Available: https://www.dash.org/wpcontent/uploads/2014/09/DarkcoinWhitepaper.pdf, 2014.**

**[17]“A brief survey of cryptocurrency systems,” in 2016 14th Annual Conference on Privacy, Security and Trust (PST). IEEE, 2016, pp. 745–752.**

**[18]F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Communications Sur- veys& Tutorials, vol. 18, no. 3, pp. 2084–2123, 2015.**