**Reliability On Timestamp Algorithm for The Banking System Using Blockchain**

**Ms. Akanksha Dhamija[[1]](#footnote-2),** **Rajat Kumar[[2]](#footnote-3), Pushan Verma2, Avnish Singh2 and Navneet Lohchab2**

**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, which was decentralized, faster, secure, cost-effective, transparent, and non-vulnerable. Through this paper, we demonstrated how hashing and salting the timestamp algorithm's values may significantly improve blockchain security and render addresses almost untraceable.

**Keywords**Blockchain, Timestamp, Hashing, Salting

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

A decentralized database which is shared among nodes of a computer network is known as blockchain. A blockchain works as a database, stores the information digitally. Blockchains are well known for their critical functioning, keeping the transactions secure and decentralized for cryptocurrency systems like bitcoin.

The data structure in a blockchain is different from database which is traditional. A Blockchain contains clusters of data known as blocks, each cluster have a collection of data. Blocks have some specific capabilities in storage, when they get full, they get closed and connects to the preceding block, maintaining a chain of data called as the blockchain. All additional data gets assembled into a new document when a new block is inserted.

A Blockchain maintains a track of transactions of two parties acting as decentralized ledger. Each party has their own access to modify digital ledger constant which makes the system impossible to hack, making it safe.

An algorithm which is used to achieve agreement on a single data value among distributed systems or processes is called consensus algorithm. Through this procedure, a common agreement is reached among all the peers about a present state.

In Timestamp, data is stored in a unique serial block and its primary function is to specify the exact moment, when the block has been mined and validated as per the blockchain network.

* 1. **Background**

To make transactions quicker and safer, banks continuously explore new methods so as to give their customer a better experience while banking which intact transparency to customer as well as maintaining cost efficiency. Blockchain which is referred to as distributed ledger between two peers. The power of decentralization can be extremely useful to banking sector [[11]](#References). It has the ability to streamline most of important feature that bank provides to customer offline which can be more time consuming and not cost efficient. Due to Decentralization, the process is completely transparent and assures safety of transactions. Decentralized system helps in making payments which is the most integral part of the banking system fast and secure at lower cost. Distributed Ledgers decrease the cost of operation and transactions are real time between any kind of institution. It can also be very useful in KYC, where the user information is stored in a decentralized block which makes it much faster and reliable as compared to doing everything online by visiting banks. It also prevents frauds since user information since blocks stores information of user are hashed using hashing and salting algorithms which prevent them from any kind of vulnerability. It can also help in tokenizing the securities like stocks, bonds, where this information will be stored in a public blockchain and can be a potential interoperable capital market.

* + 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 [[13]](#References). 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 [[12]](#References), 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 [[14]](#References), 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 the dealings are immutable and clear [[2]](#References), we can have additional trust than ever gained before. Success that we got in crypto-currency and other technical areas displays several engaging fields of the blockchain technology that can help our society in various aspects. Time Banking can be a normalized exchange economy; however, everyone's contribution was valued on identical scale in which the time exhausted.

This policy's effectiveness has always been critical as we believe that all the policy manufactures need to support freedom and transparency [[3]](#References) by giving power to the general public interfering and altering. this text takes effort synthesizing and analyzing data having role of the blockchain, a money tool that can play an important role in development of the world's economy.

The Blockchain technology utilizes while not guarding information regarding bank transactions, namely transfer amounts, details of card, participant names, etc. this subject contains relevant stuff, as the digital economy [[4]](#References) is converting into associate degree, which is an integral part of fashionable life.

Bitcoin supports blockchain in simulating way, the digital crypto currency associates nursing in every sphere of users all over the world, but blockchain itself is far over bit coin, blockchain is today's security system expressing processes non-parallel of blocks [[5]](#References) producing secure way of recording transactions and its circulation is done among signatories, or any target group being the participants in the method. it puts light on the fact that it achieves this not requiring any central authority.

Blockchain innovation gives the banking industry various chances. certain difficulties need to be conquered to let observable effects [[6]](#References) happen in the financial industry. in any case, the financial business should trail the new protection laws. Security laws need to be followed for the welfare of both associations and people.

The world is being paved by the paradigm of net of things (IoT), wherever many of our objects of daily use are interconnected [[7]](#References) to each other and can change with their setting, gathering data and changing sure tasks.   
  
The impact of blockchain technology on the financial sector and other industries through cryptocurrency. Not only this technology but also its exploitation is as subject of research. for understanding the platform, the initial point of research is analysis of works of this technology, after that identification of the advantages for business and economic transactions is done, and then in end, the paper evaluates the technology's impact on business, above all on financial operations [[8]](#References).

The storage contacts formation between peers [[9]](#References). it contracts agreements of area unit between their customer and storage supplier, shaping the importance of the knowledge and its worth.

1. **METHODOLOGY**

**3.1 Implementation 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[[3]](#footnote-4) number. After salting it at random with 10 different[[4]](#footnote-5) salting strings the combination is 28 digits.



After using sha256 algorithm hashing we get a 256-bit result.



Which can give around 10e28[[5]](#footnote-6) different addresses.

The fastest bitcoin rig has the computation power of 5.6 TH/s[[6]](#footnote-7)



So, it would take around the 5.6e7 years with the fastest node to compute the address of next node in the blockchain.

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 5.6e7 years. This computation is not possible in single lifetime.

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.

1. **Acknowledgement**

Special thanks to HOD and other faculty members of CSE department of Bhagwan Parshuram Institute of Technology, Delhi for supporting the research work and providing the assistance and guidance for the same.

**References:**

1. Bakaul, Masum & Das, Nipa & Moni, Madhabi Akter. The Implementation of Blockchain in Banking System using Ethereum. International Journal of Computer Applications. 177. 50-54. 10.5120/ijca2020919895 (2020).
2. R. C. Merkle, "Protocols for Public Key Cryptosystems," IEEE Symposium on Security and Privacy, 1980, pp. 122-122, Doi: 10.1109/SP.1980.10006 (1980).
3. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” [*http://www.bitcoin.org/bitcoin.pdf*](http://www.bitcoin.org/bitcoin.pdf) (1999).
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), pp. 1-5, Doi: 10.1109/CNS.2019.8802734 (2019).
5. Q. K. Nguyen, "Blockchain - A Financial Technology for Future Sustainable Development," 3rd International Conference on Green Technology and Sustainable Development (GTSD), pp. 51-54, Doi: 10.1109/GTSD.2016.22 (2016).
6. N. A. Popova and N. G. Butakova, "Research of a Possibility of Using Blockchain Technology without Tokens to Protect Banking Transactions," IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 1764-1768, Doi: 10.1109/EIConRus.2019.8657279 (2019).
7. V. Naik, R. Pejawar, R. Singh, A. Aher and S. Kanchan, "Expeditious banking using Blockchain Technology," International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE), doi:10.1109/CISPSSE49931.2020.921225 (2020).

1. S. Sakho, Z. Jianbiao, F. Essaf and K. Badiss, "Improving Banking Transactions Using Blockchain Technology," IEEE 5th International Conference on Computer and Communications (ICCC), pp.1258-1263, doi:10.1109/ICCC47050.2019.9064344 (2019).
2. Chowdhury, M. Suchana, Kalam, S. and Khan, M. Blockchain Application in Banking System. Journal of Software Engineering and Applications, doi:[10.4236/jsea.2021.14701](https://doi.org/10.4236/jsea.2021.147018)8 (2021).
3. 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 Doi: 10.1109/ACCESS.2018.2842685 (2018).
4. Knezevic, Dusko. 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 (2018).
5. S. King, “Primecoin: Cryptocurrency with prime number proof of work” (2013).
6. J. J. Kishigami, “Blockchain contract: A complete consensus using blockchain,” in Consumer Electronics (GCCE), IEEE 4th Global Conference on. IEEE, pp. 577–578 (2015).
7. S. King and S. Nadal, “Ppcoin: Peer-to-peer crypto-currency with proof- of-stake,” self-published paper, August, vol. 19 (2012)

.

1. Assistant Professor

   CSE Department, Bhagwan Parshuram Institute of Technology, Delhi-89, India [↑](#footnote-ref-2)
2. Akanksha Dhamija [akankshadhamija12@gmail.com](mailto:akankshadhamija12@gmail.com)

   Rajat Kumar [rajat230616@gmail.com](mailto:rajat230616@gmail.com)

   Pushan Verma [pushanverma.99@gmail.com](mailto:pushanverma.99@gmail.com)

   Avnish Singh [singhavnish516@gmail.com](mailto:singhavnish516@gmail.com)

   Navneet Lochabh [navneet17012000@gmail.com](mailto:navneet17012000@gmail.com)

   CSE Department, Bhagwan Parshuram Institute of Technology, Delhi- 89, India [↑](#footnote-ref-3)
3. [The timestamp will contain digits till milliseconds](https://262.ecma-international.org/5.1/#sec-15.9.4.4) [↑](#footnote-ref-4)
4. [Using bycrpt npm package](https://www.npmjs.com/package/bcrypt) [↑](#footnote-ref-5)
5. The Time only contains 10 numerical values and of length 13 + salt of length 15 so total no of combinations possible are 1013 [↑](#footnote-ref-6)
6. [whatsminer-m21s](https://www.asicminervalue.com/miners/microbt/whatsminer-m21s) [↑](#footnote-ref-7)