International Journal of Engineering & Technology, 7 (4.6) (2018) 398-400

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Blockchain Based Aadhaar Security

Sankaranarayanan P.J *, Geogen George[2]

SRM Institute of Science and Technology
Chennai, India (TN)
**Corresponding author E-mail: sankaranarayanan_periyandavar@srmuniv.edu.in*

Abstract

A blockchain is a decentralized, disseminated and digital ledger that can't be altered retroactively without modifying every single blocks and the consensus of the network. Blockchain can be used in smart contracts, Banks, IoT devices, Database management, etc., Due to recent times flaws and leakage of Aadhaar information (Aadhaar which is the largest government databases of the Indian citizens) in Internet the security and privacy of Aadhaar became questionable. In order to ensure the security of Aadhaar, Blockchain has the potential to overcome security and privacy challenges in Aadhaar. In this project we are going to create a Blockchain for Aadhaar database and implement light weight algorithm for efficiency, optimization and scalability along with the Blockchain securing algorithm.

Keywords: *Blockchain, Aadhaar, Lightweight cryptography.*

1. Introduction

Blockchains are cryptographically signed digital ledgers where transactions are framed into blocks. Each blocks are linked to previous block with its hash value which is generated cryptographically. When new blocks are added, it is reflected across all copies of the ledger in the network.

Blockchains are distributed network without a central repository and central authority implemented as digital ledger systems. At their initial level, they enable a group of users to record transactions in a ledger which is public to that group, such that no transaction can be changed once published. This technology became widely known starting in 2008 when it was applied to enable the growth of electronic currencies where digital transfer of money take place in distributed systems. It has enabled the success of e-commerce systems such as Bitcoin, Ethereum, Ripple, and Litecoin. Due to this, blockchains are often viewed as bound to Bitcoin or possibly e-currency solutions in common. However, the Blockchain technology is more useful and the availability is for various applications.

Whenever a transaction occurs, that transaction is signed by whoever is authorizing it. That includes public key of the user which will be signed digitally by users private and public keys. This gets registered to the ledger of the Blockchain network. Consensus plays a vital role in the Blockchain network. The goal is to achieve a joint state, meaning everyone agreeing on a certain state of the Blockchain. As in a distributed system, there is no central authority to decide which new blocks are valid and which are not. Every node has to decide on its own if it accepts a new block or not. The basic consensus algorithm is simple: The only valid chain is the chain that contains the genesis block, only valid blocks according to the network rules and is the longest one. All other chains are not accepted. Longest chain means that the chain contains the most blocks.

Blockchain which is a decentralized network will help UIDAI which is governing authority for India's 1.2 billion citizen's identity database, Aadhaar. But privacy of Aadhaar and its security is questionable, due to recent incidents and reports on the leak of Aadhar details of many Indian citizens over internet.

2. Related Works

Personal Health Records of patients are recorded and are stored in cloud platform[1] from where they can be retrieved for future references by any Health Care provider which has conventional solution due to lack of complexity and accessibility in cloud storage the Blockchain is implemented to the PHR of all the patients which can be more efficient, secured and easy accessibility. It also deals with the solution on challenges faced while linking huge database to the Blockchain, the idea of the off-chain data storage is suggested by many, where the data kept outside the blockchain database is distributed in a standard way, and the data of hashed value is stored in the blockchain. The healthcare information is stored in off-chain fashion so that data can be secured, erased and collected as required. But the immutable hashed values of the healthcare information are upended on blockchain for validating the authenticity and accuracy.

Individual information, and sensitive information when all said is done, must not be confided in the hands of outsiders, where they are helpless to assaults and abuse [2]. Rather, clients should have control to their information without trading off security or constraining organizations and expert's capacity to provide customized administrations. Our stage empowers the above stated by joining with blockchain, reused with a new purpose as an entrance guidance arbitrator, by an off blockchain stockpiling arrangement. Clients are not needed to trust any outsider and are constantly given the knowledge of the information that had being gathered about them and the way it has been utilized. In addition, the blockchain is aware of the clients as the proprietors of their

own information. Organizations can centre around using information without being excessively worried about legitimately securing and dividing them into sections. Moreover, with a decentralized stage, settling on legitimate and administrative choices about gathering, putting away and sharing sensitive information have to be less difficult. Also, laws and directions could be customized into the blockchain itself, with the goal that they are maintained naturally. In different circumstances, the record can go about as lawful confirmation for getting to (or putting away) information, since it is (computationally) designed carefully. At long last, we examined a few conceivable future expansions for blockchains that could saddle them into a balanced answer for put stock in processing issues in the public arena.

Paper[3] first examines about the basics of crypto-currencies for the audience which have none or zero knowledge about it. Further it talks about the advantage and disadvantages of bitcoin with its implementation. The author finally concludes that how poorly and overhyped the bitcoin is. But it also implies that Blockchain, the root technology behind bitcoin has a huge scope in different fields in the near future. Also the paper discusses about the various attacks and vulnerabilities that the bitcoin has faced till now. It is a correct decision not to call Bitcoin a currency. Cash may be a unit of account, store of import and medium of exchange. Bitcoin is none of these, in any serious sense. Bitcoin has several issues that needs to be answered. Associate anonymous and localized payment system may so revolutionize the economy, facilitate to finish the disproportionate power of some banking systems and democratize financial exchange. A system created by associate anonymous cryptologist might not be the method of the future; true openness is required for future experiment to achieve success. A blockchain can be seen as a decentralized database in which information can be saved. This database is distributed across all participating nodes, resulting in a decentralized network. All nodes agree upon a certain set of rules, defining the allowed behaviour in the network and the structure of information to be stored. The rule set defines the purpose and the functionality of the Blockchain.

The blockchain based e-voting is easy [4], to use a digital-currency method, Blockchain enabled e-voting provide a “wallet” with a credential to each voter. Each voter receive a “coin” representing a chance to vote. When we Cast our vote, the voter’s coin will be transferred to the candidate’s blockchain wallet, and the coin can be spend only once by voter. Nevertheless, vote can changed by the voter before the deadline. By this, we can define that we can overcome two of the most common concerns (voter access and voter fraud) in voting methods today by using blockchain. Blockchain enable tamper-proof audit trails for voting.

Mobile devices can use simplified payment verification [5], based on Trust zone through isolation and verification done by secure execution environment and block header are not readable through encryption. This design is a secure lightweight blockchain wallet for securing private keys.

3. Requirement Analysis

Blockchain based Aadhaar will follow the data protection and privacy of the users. This will permit data to be collected, maintained and used explicitly with the knowledge of the information to which person it belongs.

When using Aadhaar in blockchain, we can see more trusted UIDAI nodes where state governments and other legal entities can be as a part of trusted UIDAI nodes. These Trusted nodes only can validate the transaction and add new blocks in the blockchain, they can also perform decryption on the data that has been stored in the blocks. Since, we can find numerous nodes contained in the peer-to-peer network and we can find a full copy of the blockchain in each and every node, this will be an advantage if any node gets compromised the blockchain will not be affected. When attacker wants to validate a malicious transaction then he must take control of at least 51% of the nodes.

From this large size of the information and needed bandwidth, it might become difficult to implement a similar system. A solution for the above stated problem is to gather the original data in a central server as they store now, the blocks with the original data will have a pointer assigned to them in the centralized database. We will be encrypting the stored pointer and we will be decrypting to see the original data node. By this method, the bandwidth required for implementation will be very less because we can utilize all the data it has stored in the existing infrastructure. Moreover, implementing Lightweight cryptographic algorithm to the existing Blockchain security algorithm that will reduce the complexity, time constrains and increase the efficiency of the system.

4. Challenges

The Popular technique blockchain faces few challenges. We list few critical challenges and recent enhancements as follows.

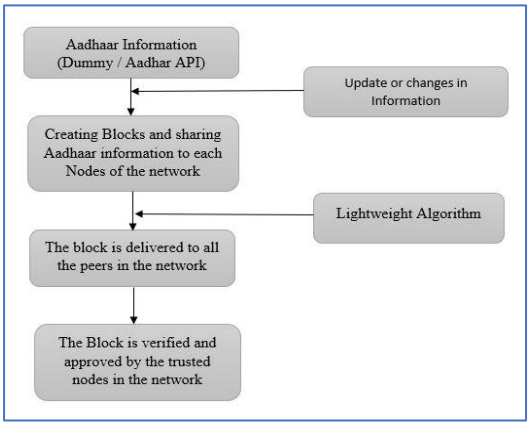
Scalability: As the number of transactions in our day to day life are increasing, the size of blockchain is becoming bigger. Every node in network will store all transactions and verify them with blockchain as they have to verify whether source of current transaction is spent or not. Bitcoin blockchain approximately process 7 transactions per second due to block size restriction and time interval in generating new block, which is not enough to fulfil the requirement in real-time as it has to process millions of transactions. The blocks capacity are very small, so this may result in delay between minor transactions because the miners prefer these transactions with higher transaction fee.

Human error: When we send information into the database it needs to be of high quality and we use blockchain as a database. It is untrustable to store data in blockchain because of this events are recorded and monitored accurately.

Unavoidable security flaw: In bitcoin and other blockchains we can find a security flaw, the lie will become the truth when more number of computers are working as nodes to service the network . This is known as '51% attack' and was highlighted by Satoshi Nakamoto when bitcoin is launched by him. So, the community closely monitors bitcoin mining pools, ensures no one will gain such network influence unknowingly.

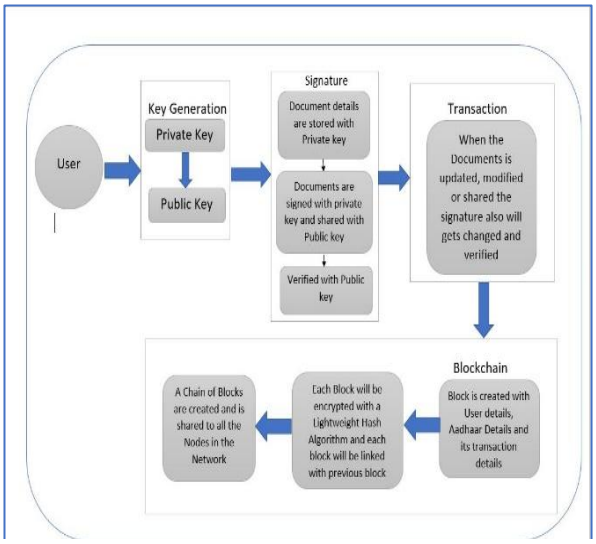
Complexity: More Complex Security algorithms are used for signing and verification. And also Hashing algorithm is used to securely share the Documents.

5. Proposed Methodology



In this project we are going to create a Blockchain for Aadhaar database and implement lightweight algorithm for efficiency, optimization and scalability along with the Blockchain securing algorithm.
In order to achieve this we have to create a genesis block in which user identification is uploaded with private key for which a public key is generated.
To add Aadhaar details like Address, Iris scan, Finger Print, etc,. and upload with a private key, sign (in general signature part use Elliptic Curve Algorithm) and share in the network which is should be verified.
To create a Block for a Aadhaar user, and secure it by SHA256 hashing algorithm, and try to make a conventional lightweight algorithm.
Whenever any modification is done the block gets updated and are shared to all nodes in the network.
To overcome the security challenges while implementing lightweight to the blockchain.

6. Conceptual Diagram



7. Comparison Table of Security Algorithm

Hash function	Digest size [bits]	Code size [bytes]	RAM data [bytes]	RAM state and others [bytes]	RAM stack	Cycle count (8-byte message)	Cycle count (50-byte message)	Cycle count (100-byte message)	Cycle count (500-byte message)
SHA256	256	1090	64	73	6	33 600	33 600	66 815	266 105
Keccak[r=1088,c=512]*	256	868	136	240	4	178 022	178 022	179 494	716 483
SPONGENT-256/256/128	256	364	16	96	5	1 542 923	3 856 916	6 170 900	25 454 100
(small) Keccak[r=144,c=256]	256	608	18	92	4	90 824	181 466	317 221	1 313 291
PHOTON-256/32/32	256	1244	4	68	10	254 871	486 629	787 896	3 105 396

Here we are supposed to find a best suitable lightweight security algorithm to replace SHA256. So that the size of the Block can be reduced without compromising the security level of the Blockchain.

8. Conclusion

Blockchain has much more potential which can be used in many ways. In this project we proposed to make Blockchain lightweight by replacing the standard algorithm without compromising the security. So that it can be used to store more data and secure 1.2 billion Indian citizen's Aadhaar details and the transaction usage records of each citizen's Aadhaar is maintained.

References

[1] Christian.E.Alfredo, S.D.Tortora, G.Chang.H, & Kim-Kwang.R, (January-February/2018) Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? IEEE Cloud Computing.
[2] Zyskind.G, Nathan.O & Pentland.A, (2015) Decentralizing privacy: using Blockchain to protect personal data. IEEE Security and Privacy Workshops. IEEE.
[3] A Guadamuz, & C Marsden (2015). Blockchains and Bitcoin: regulatory responses to cryptocurrencies. FirstMonday.
[4] Nir, K., & Jeffrey , V. (2018). Blockchain Enabled E-voting . IEEE Software.
[5] Weiqi, D., Jun, D., Qinyuan, W., Changze, C., Deqing, Z., & Hai, J. (2018). SBLWT: A Secure Blockchain Lightweight Wallet Based on Trustzone. IEEE Access.
[6] Zyskind.G, Nathan.O & Pentland.A. (2015). Decentralizing privacy: using Blockchain to protect personal data. IEEE Security and Privacy Workshops. IEEE.
[7] Christidis.K, Devetsikiotis.M, (2016) Blockchains and smart contracts for the internet of things. IEEE Access 4:2292–2303.
[8] Croman.K, Decker.C, Eyal.I, Gencer.AE, Juels.A, Kosba.AE, Miller.A, Saxena.P, Shi.E, Sirer.EG, Song. D, Wattenhofer.R, On scaling decentralized blockchains - (a position paper). In: Financial cryptography and data security - FC 2016 international workshops, BITCOIN, VOTING, and WAHC.
[9] Forte.P, Romano.D, Schmid.G, Beyond bitcoin - part I: a critical look at blockchain-based systems. IACR Cryptology ePrint Archive 2015
[10] Forte.P, Romano.D, Schmid.G (2016) Beyond bitcoin - part II: blockchain-based systems without mining. IACR Cryptology ePrint Archive 2016
[11] Gervais.A, Karame.GO, W¨ust.K, Glykantzis.V, Ritzdorf.H, Capkun.S, On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, vienna, Austria, October 24–28, 2016,
[12] pp 3–16
[13] Karame.G, 2016.On the security and scalability of bitcoin's blockchain. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, Vienna, Austria, October 24–28.