Aadhaar security through blockchain

Venkatasubramanian S, Swarnakamali V, Kaviya J, Vigneshwar A,
Computer Science Engineering,
Saranathan College of Engineering,
Trichy, India.

Abstract

Blockchain technologies are gaining massive momentum in the last few years. A blockchain is a shared database, consisting of a ledger of transactions. Blockchains eliminate the problem of trust that affect other databases. It enables full decentralization and independent verification. Data stored in blockchain is tamper proof. So we can store confidential data by creating private blockchain network. In this paper, we will see how to provide security for aadhaar card data.

Keywords—blockchain; ethereum; aadhar card; smart contract; security;

I. INTRODUCTION

Aadhaar is a 12-digit unique identity number that can be obtained by residents of India, based on their biometric and demographic data. The data is collected by a statutory authority, the Unique Identification Authority of India (UIDAI). Aadhaar is the world's largest biometric ID system. The detailed personal information being collected is of extremely high importance to an individual. Major financial transactions are linked with information collected in Aadhaar. Data leaks are a gold mine for criminals. The UIDAI confirms more than 200 government websites were publicly displaying confidential Aadhaar data; though removed now, the data leaked cannot be scrubbed from hackers' databases.

Those confidential aadhaar details are stored in a single database and it is maintained by UIDAI. Since the database is centralized there are so many disadvantages. The main disadvantage is that the security threat. If those data are stored in blockchain, data vulnerability will be reduced.

II. SOLUTION USING BLOCKCHAIN

Each block contains a unique block number, the data, previous hash value and hash value of its own block. Thus it contains two hash value. The hash values are computed from the data and the previous hash value by performing SHA-256 algorithm and so it is of 64 bit length. Blockchain uses hash tables as data structures which are implemented on timestamp servers and each transaction on the timestamp service is verified using the Proof of Work [3]methodology. A timestamp server works by taking a hash of a block of items to be time stamped and widely publishing the hash, such as in a newspaper or Usenet post. The timestamp proves that the data must have existed at the time in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it [16]. The blockchain structure is described in Fig.1. below[2].

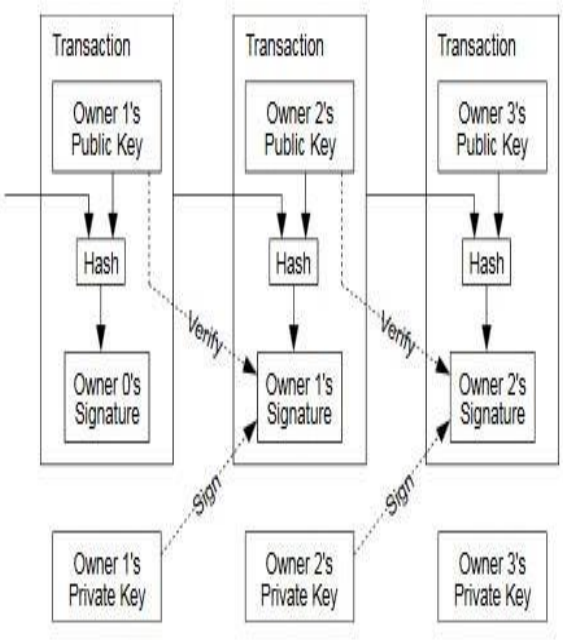

Fig 1: Structure of blockchain

The most relative and well understood use-case of the blockchain technology is bitcoin[4]. Through a clever combination of cryptography and game theory, the Bitcoin 'blockchain' – a distributed, public transaction ledger – could be used by any participant in the network to cheaply verify and settle transactions in the cryptocurrency.

Blockchain technology has been applied in the domains of healthcare, electronics, manufacturing, education, economics, social networking, etc. [5]

III. RELATED WORKS

Blockchain gives an opportunity to radically transform the way we do things by providing a standard architecture to address different business and

organizational problems. With blockchain, various digital challenges like transparency, integrity, immutability, security, customer centricity etc can be addressed. In [5], a blockchain based smart collaboration mechanism has been described in which each collaboration is encoded as a transaction message.

In [6], blockchain has been used to overcome some problems on energy internet like data creditability, trading model changes etc and some problems on Internet of Things like IoT node legal identity certification, IoT data security and privacy issues, IoT upgrading issues etc and some problems on big data like data center anti-attack pressure, data storage costs, data center maintenance overhead, privacy and security issues.

IV. SMART CONTRACT

Smart contracts have gained recently attention, especially in the context of the blockchain technology. A smart contract is a contract that can verify its correctness and enforce predefined rules, thus, smart contracts are self-executing and self-enforcing. However, a smart contract without a proper infrastructure is not ”smart” at all, because it needs such an infrastructure to run, execute, and verify these contracts. A blockchain is such an infrastructure for smart contracts that can operate in a fully autonomous and decentralized manner. Smart contracts can be used for financial services (e.g., Bitcoin) or they can be used for general services e.g., (Ethereum). A blockchain executes, verifies, and collects and stores smart contracts in blocks.[7]

The main benefit of using a blockchain with smart contracts is that these contracts can be evaluated automatically. Current solutions produce a PDF that needs to be verified manually. Using smart contracts, the temperatures can be assessed automatically and notify sender and recipient. Furthermore, the stored data is tamper-proof and can be used for audits by external parties. With Ethereum, such a tamper-proof fully decentralized system can be used at a low cost and on a per contract and per-byte basis. [7]

V. PROPOSED MODEL

Here the main idea is to decentralize the aadhaar database. We can decentralize it in blockchain network by making the exact copies of the entire database and store it in the decentralized blockchain node. The biggest problem in storing the data in blockchain is the amount of data you can store. The amount of data we can store is quite limited. We can circumvent that limitation by the following ways.

A. Data chunks

We can split the large database into many small chunks. That would allow us to store larger files/data but also would significantly increase our costs. It costs because the amount of data you store has to be stored by other nodes.

B. Storing hashes

One way of getting the benefits of blockchain is only storing the hash of the data in the blockchain**.** A hash is a generated string. As I mentioned earlier, it is computed from our input data. With the same input, the output hash will always be the same. Other input does result in another hash. In comparison to our data, the hash is very small so the cost of a transaction is relatively low. The raw data can be stored in any way we want. For example, we could use a relational database or just a file system. We should assign the hash of the blockchain transaction to our raw data. In a relational database we would add another column to store the transaction id. In this way, we can utilize the advantages of traditional storage mechanisms (like queries) while still getting the tamper-evidence of the blockchain.

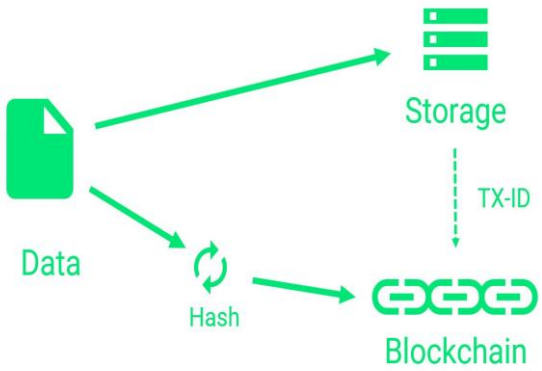

Fig 2: Storing hashes in blockchain

C. Storing subsets

Another way is to store the hash of the data and parts of the data on the blockchain. We can store the data in any distributed file systems like ipc. In this method transparency and decentralization is enhanced to greater extent.

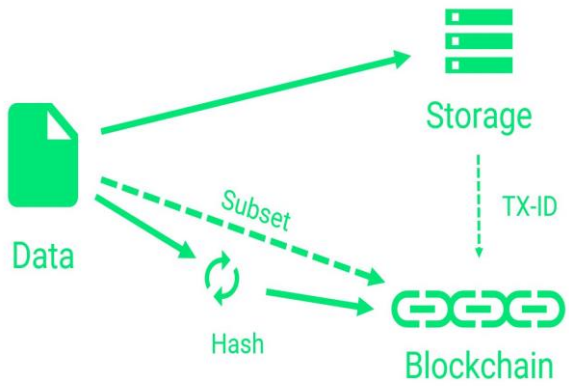

Fig 3: Storing hashes and data subset in blockchain

VI.DATA CHUNK CREATION

The centralized aadhaar database is made into smaller data chunks and stored in ethereum blockchain environment. Ethereum is a blockchain that allows you to run programs in its trusted environment. This contrasts with the Bitcoin blockchain, which only allows you to manage cryptocurrency. Metamask is used to manage the Ethereum accounts and private keys. It is a browser extension for Chrome and Firefox. We use smart contracts which are a code that runs on the EVM. Smart contracts can accept and store ether, data, or a combination of both. We use Web.js to communicate between the smart contract and ethereum network.

T

VII. ADVANTAGES

The most dangerous single point of failure threat of centralized database system will be minimized by this decentralized blockchain network. When hackers try to attack this decentralized blockchain data blocks, they cannot gain control over the entire database. Moreover, to add or decrypt, hacker must control atleast 51% of the nodes which is very tedious. Thus security is highly guaranteed. There will be multiple UIDAI trusted nodes and only those trusted nodes can append block in blockchain. Every node have full copy of the blockchain. So one or few node failure is not an issue. Updation will be visible to all without any intermediary. If someone tries to cheat the system, other record keepers can detect it. Data in blockchain are securely encoded. No plain data can be retrieved from underlying ledger until the user has permission and entitlements to get data.

VIII. CONCLUSION AND FUTURE WORK

Many government, non-government, financial and non-financial organizations are looking into blockchain-based solutions in order to reduce the master-slave strategy and to improve security. The success rate of blockchain in both private and public application domain tells that those technically available characteristics and advantages can be practically exploited efficiently. In this paper, a novel application of the blockchain has been proposed.

REFERENCES

[1] Tien Tuan Anh Dinh, Rui Liu, Meihui Zhang , Member, IEEE, Gang Chen, Member, IEEE, Beng Chin Ooi, Fellow, IEEE, and Ji Wang Untangling Blockchain: A Data Processing View of Blockchain Systems

[2] Yi Liu, Ruilin Li, Xingtong Liu, Jian Wang, Chaojing Tang and Hongyan Kang, “Enhancing Anonymity of Bitcoin Based on Ring Signature Algorithm”, 2017 13th International Conference on Computational Intelligence and Security

[3] Catalini C, Gans JS, “Some simple economics of the blockchain”, National Bureau of Economic Research; 2016

[4] Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system.

[5] Rajvardhan Oak, Karanveer Singh Jhala, Mrunmayee Khare “Smart Collaboration Mechanism using Blockchain Technology” 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud

[6] Li Shuling, “Application of Blockchain Technology in Smart City Infrastructure, 2018 IEEE International Conference on Smart Internet of Things

[7 [7] Thomas Bocek, Bruno B. Rodrigues, Tim Strasser, Burkhard Stiller “Blockchains Everywhere - A Use-case of Blockchains in the Pharma Supply-Chain