International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-1, May 2020

Citizen Identity Management using Blockchain Architecture

Aravind S, Rohini V

Abstract*: The main objective of this paper is to put forward a system for managing the identity of the citizens of a country by leveraging the power of blockchain technology. The paper illustrates how a decentralized system can help make the entire process of identity management transparent and tamper-proof at the same time. While most of the existing blockchain based solutions rely on blocks themselves, the system proposed here emphasizes on the usage of transactions. Decentralization is achieved with this system in the sense that total control over the network does not reside with a single authority, but rather is distributed among multiple authorized government entities.

***Keywords*: Blockchain, Tamper-proof, Transaction, Transparency, Identity**

I. INTRODUCTION

Blockchain technology has been making waves in the technological space in recent times. The sheer technological beauty of this has captured the imaginations of innovators around the world. The amount of possibilities that blockchain has opened up in various domains is beyond impressive. Blockchain, at its core, is a distributed ledger technology. Think of a network in which every node contains a copy of a ledger that keeps updating itself whenever there's a change. This ledger is stored in the form of blocks and records in the ledger as transactions in the block. These blocks are linked together cryptographically to form a chain. Security, transparency, and immutability are the key features of blockchain technology. Security in blockchain is ensured by using cryptographic techniques. Blockchain was initially introduced as a support system for the Bitcoin cryptocurrency network. Its main purpose was to curb the problem of double spending. Blockchain has come a long way since those days and has evolved in such a way that it is not only possible to be used for dealing with monetary transactions, but also for maintaining real-world assets and proving their validity. It is possible to run event-triggered programs in a blockchain network now. These programs, which run on previously selected nodes in the network are known as smart contracts.
Blockchains can be classified into three major kinds: public, private and permissioned. The most common and popular blockchain systems are predominantly public blockchain networks. Anyone can join the network at free will. This means that the entire data in the network is open to the public, and they're free to read, write and audit the current data in the network. These networks follow the idea that, higher the number of nodes or participants, higher will be the data integrity and security in the network. Bitcoin and Ethereum networks are prime examples of public blockchain networks. It can be said that these networks are the major reason why blockchain technology rose to fame so quickly. Corporates require their data to remain confidential and to be shared only among a select few entities. This is where the role of a private blockchain comes into picture. Private blockchains are owned and maintained by an organization or an individual. The owner has full discretion on who is to be added to or removed from the network. The data can also be altered, if needed, by the owner. A private blockchain isn't really decentralized but is rather a distributed ledger that works as a closed, secure database. These are generally tailor-made for specific needs of an organization. Permissioned blockchains are the third kind of blockchain networks in the list. These are a combination of private and public blockchain, with a lot of options for customization. One of the many real-world scenarios where all the properties of a blockchain align perfectly well with, is the management of citizen data. Citizen data is one of the most crucial and critical assets of a country and is a matter of national security. It is also one of the most tamper prone data out there. The way in which this data is stored presently is centralized. This, by itself, is prone to tampering, forgery, and single point failure. The system being proposed in this paper is a blockchain based solution for storing citizen data in a decentralized network. The key point to be noted here is that the data being talked about is non-sensitive data, that can be made public. The main purpose of this system is to curb issues that rise due to tampering of citizen information. This has the potential to eliminate the likes of fake ID cards and records. It makes the job easier for government officials to search for all sorts of government related records.

II. LITERATURE REVIEW

Satoshi Nakamoto proposed the idea of a cryptographic mechanism for storing ledger data in a peer-to-peer network of nodes, which is now referred to as blockchain, in his paper, "Bitcoin: A Peer-to-Peer Electronic Cash System" . The data is stored in the form of transactions in blocks which are chained together sequentially. Each block contains the hash value of the previous block, time-stamp, and a variable number of transactions.

Manuscript received on April 30, 2020.
Revised Manuscript received on May 06, 2020.
Manuscript published on May 30, 2020.
* Correspondence Author
Aravind S*, Department of Computer Science, CHRIST (Deemed to be University), Bangalore, India. Email: aravind.s@mca.christuniversity.in
Dr. Rohini V, Department of Computer Science, CHRIST (Deemed to be University), Bangalore, India. Email: rohini.v@christuniversity.in

This allows for the data to be secure and tamper-proof. The system aims to provide a decentralized environment that makes it possible to transact digital money without the intervention of a third-party. A consensus algorithm by the name Proof of Work (PoW) was devised in order to make decisions in the network. The major flaw of this system lies in PoW itself; which is that a lot of computational power is wasted in the process of mining. [1]

A new kind of blockchain network is proposed in the paper, "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform", by Vitalik Buterin. This takes the application of blockchain beyond just monetary transactions. This is mainly achieved by introducing a mechanism known as a smart contract. A smart contract is a program that is executed on all nodes in the Ethereum network and are triggered based on pre-defined events. Ethereum builds on top of Bitcoin on the fact that it can not only do monetary transactions, but also do transactions of anything that holds value in the real world. Unlike the Bitcoin network, the network proposed in this paper makes use of a consensus algorithm that goes by the name Proof of Stake. [2]

The solution proposed by Rahul Acharya and Sumitra Binu in "Blockchain based examination system for effective evaluation and maintenance of examination records", is through the implementation of a peer-to-peer network. Questions can be submitted by each node participating in the system, and are allowed to vote for and verify the authenticity of the questions. This allows for a very reliable and unbiased system where question papers can be truly random and still maintain the level of quality expected. [3]

"Logchain: Blockchain-assisted Log Storage" proposes a solution to the issues found in traditional cloud-based logging systems, in the form of a framework called "LogChain as a Service" (LCaaS). William Pourmajidi and Andryi Miranskyy explain this as a hierarchical blockchain framework that overcomes the limitations of current consensus algorithms by segmenting a portion of a blockchain and locking-it-down in a block of a higher-level blockchain. This system allows for tamper-proofing logs, making it more secure than the cloud-based solutions that already exist. [4]

Antra Gupta and Deepa V. Jose aim to provide a more secure, fool-proof, and trustless solution to the current FIR system that is prevalent in this day and age, with their paper "A Method to Secure FIR System using Blockchain". The system makes use of the immutable and cryptographic nature of blockchain technology to achieve this. Whenever a complaint is registered, it is given a cryptographic hash and a time-stamped FIR is associated with it. The complainer, suspect, witness, and the officers are considered as individual users. The officers update the ledger as the investigation progresses based on the information provided by the complainer and the witness. The identity of the officers in charge aren't revealed during the process. This helps in making the whole process corruption-free and smooth. [5]

Elli Androulaki et. al. introduces an entirely novel system in this paper called "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchain", which is quite contrasting to the existing blockchain systems. Fabric is a modular system for deploying and operating permissioned blockchains. The system is capable of running distributed applications written in general purpose programming languages, and does not rely on a cryptocurrency to operate. It also supports modular consensus models allowing for the system to be tailormade for particular use-cases and trust models. [6]

Hashcash was initially proposed as a mechanism to curb systematic abuse of un-metered internet such as email, and anonymous remailers in May 1997. Adam Beck explores the various applications, proposes suggestions, and describes the initial experience of experimenting with Hashcash in his paper "Hashcash – A Denial of Service Counter-Measure". The cost function that Hashcash uses computes a token which can be used as a proof-of-work. [7]

Eric Harris-Braun et al. propose a new scalable, agent-centric distributed computing platform with his paper "Holochain". The benefits of shifting from a data-centric model to an agent-centric model are demonstrated extensively in this paper. The popular version control system git is taken as an example and compared with Bitcoin to demonstrate the differences between agent-centric and data-centric models throughout. The paper addresses the root data-centric assumptions of the blockchain approach in order to achieve the proposed system. [8]

"Majority is not Enough: Bitcoin Mining is Vulnerable" is a paper by Ittay Eyal and Emin G¨un Sirer that claims that the mining in Bitcoin is vulnerable, and its security can be compromised. They do this by proving that Bitcoin mining protocol is not incentive-compatible. This is achieved by introducing an attack on the Bitcoin network that can get colluding miners a revenue much higher than their fair share. The resulting consequences can prove disastrous as rational miners would prefer to join selfish miners, rendering the entire network to be decentralized in a matter of some time. [9]

A new random probability distribution network model for a blockchain system is described by Aditya Goyal et al. in their paper "Stability and Scalability of Blockchain". The authors identified a structural property known as "one-endedness" which is desirable in any blockchain system. They prove in this paper that whenever a blockchain network is stochastically stable, it is "one-ended". The au1thors also test the scalability and stability of blockchain systems on large peer-to-peer networks with the help of this model. The data from the Bitcoin network, as well as synthetic data was used to test their insights. [10]

III. METHODOLOGY

Blockchain, as it is known, emphasizes on blocks for storing data. The idea explained here is to store the data of every citizen of a country in a single chain. In order to achieve this, the data is stored in the form of transactions, and not blocks as such. Each transaction contains a certain kind of data belonging to a certain individual, in JSON format. Along with the data, the transaction ID of the previous transaction related to the current one will be attached (Fig 1). When a data is to be added, that data along with the current transaction ID will be stored as a transaction. This new transaction ID will serve as the identifier for the user. This means that every individual can be referred using the transaction ID of the latest transaction that had been made related to them. Note that the emphasis is on transactions, and not blocks as such.

Since the system proposed here deals with government related information of an individual, the nodes participating in the network are government bodies. Transactions can be made only by a government body. Transactions must be approved by other government bodies in the network, hence bringing consensus to the equation. The previous transaction ID corresponding to the transaction of that citizen is stored as part of the current transaction in order to enable traversal.

The latest transaction ID will be used as the identifier for a user. Using this transaction ID, the chain can be traversed for the entire data of that particular user. An external database is used for storing off-chain data to map a user's latest transaction ID and initial transaction ID with their unique ID.

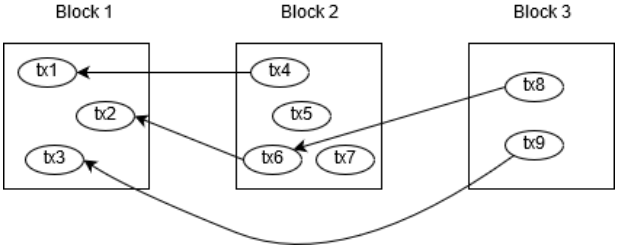

Fig 1. Linking transactions based on previous transaction ID

There are various types of entries that can be made, which is specified in the beginning of each transaction. These can vary from initial, criminal, property etc. The very first transaction of every individual is marked as "initial". The data fields that are included in the transaction are dependent on the type specified. The fields that are common for all transactions are "type", "previous transaction ID", "initial transaction ID", "transaction ID", "timestamp", "node ID" (Fig 2).

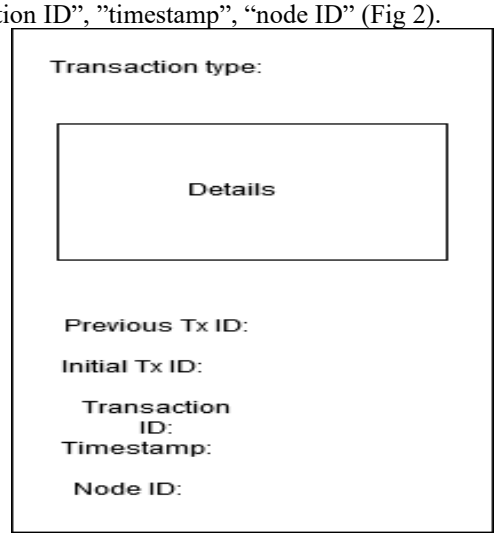

Fig 2. Structure of a transaction

Previous Tx ID: ID of the previous transaction corresponding to the individual.

Initial Tx ID: ID of the first transaction of the individual.

Transaction ID: ID of the current transaction.

Timestamp: The time at which the transaction was verified.

Node ID: The ID of the node that initiated the transaction.

It is not necessary for the data of a single citizen to be stored in subsequent transactions. Each time a new transaction is done on behalf of an individual, their latest transaction ID will get updated to that of the transaction.

Looking from a layman's perspective, this system can simplify the process of document submission. The user can be provided with a QR code that redirects to a webpage that displays their latest transaction ID. What this means is that a lot of paperwork can be saved. If the user wants to apply for something documents and certificates are to be submitted, the user can just provide their corresponding QR code, and from the latest transaction ID, the concerned party can traverse through the entire history of the person. This also makes it hard for someone to hide their criminal track records, if any.

IV. RESULT

The idea being proposed in this paper introduces a decentralized way of storing citizen data. The aim of this is to make the system tamper-proof and traceable. By leveraging the power of blockchain, the system is being made more reliable, secure, decentralized, and transparent, which helps in keeping corruption driven data manipulation at bay.

V. CONCLUSION

With the system, the objective is to make the lives of citizens easier and traceable, helping to avoid a lot of unnecessary hassles while introducing a new level of trust over the existing system. Since this novel system is dealing with only a limited number of authorities who have the right to control the network, the possibility of this system failing in the event of these authorities being compromised cannot be denied. This limitation and implementation of this system shall be addressed in a future paper.

REFERENCES

1. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," www.bitcoin.org, p. 9, 2008.
2. B. V. Buterin, "A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM", www.ethereum.org, January, pp. 1–36, 2009.
3. R. Acharya and S. Binu, "Blockchain based examination system for effective evaluation and maintenance of examination records", International Journal of Engineering & Technology, vol. 7, pp. 269–274, 2018.
4. Pourmajidi, William & Miranskyy, Andriy. (2018). "Logchain: Blockchain-Assisted Log Storage". 978-982. 10.1109/CLOUD.2018.00150.
5. G. Antra and V. J. Deepa, "A Method to Secure FIR System using Blockchain", International Journal of Recent Technology and Engineering (IJRTE) vol. 8. p. 626-629, May 2019
6. Androulaki, Elli & Barger, Artem & Bortnikov, Vita & Cachin, Christian & Christidis, Konstantinos & Caro, Angelo & Enyeart, David & Ferris, Christopher & Laventman, Gennady & Manevich, Yacov & Muralidharan, Srinivasan & Murthy, Chet & Nguyen, Binh & Sethi, Manish & Singh, Gari & Smith, Keith & Sorniotti, Alessandro & Stathakopoulou, Chrysoula & Vukolic, Marko & Yellick, Jason. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains.
7. Adam Beck, "Hashcash – A Denial of Service Counter-Measure", www.hashcash.org, August 2002
8. Eric Harris-Braun, Nicolas Luck, Arthur Brock, "Holochain", www.holochain.org, May 2018
9. Eyal, Ittay & Sirer, Emin. (2013). "Majority Is Not Enough: Bitcoin Mining Is Vulnerable". 8437. 10.1007/978-3-662-45472-5_28.
10. Gopalan, Aditya & Sankararaman, Abishek & Walid, Anwar & Vishwanath, Sriram. (2020). "Stability and Scalability of Blockchain Systems". arXiv:2002.02567

AUTHORS PROFILE

Aravind S is pursuing his degree in Master of Computer Applications from the Department of Computer Science, CHRIST (Deemed to be University). His areas of interest include data structures, blockchain and network security.
aravind.s@mca.christuniversity.in

Dr. Rohini V is a faculty in the Department of Computer Science, CHRIST (Deemed to be University). Her areas of interests include generic algorithm, machine learning and natural language processing.
rohini.v@christuniversity.in