MAT JOURNALS

Journal of Computer Science Engineering and Software Testing
e-ISSN: 2581-6969
Volume 5 Issue 3

Blockchain Based E-Voting System for India Using UIDAI's Aadhaar

Spurthi Anjan*[1], Johnson P Sequeira[2]
[1]*Assistant Professor, Department of Computer Science and Engineering, PES University, Bengaluru, Karnataka, India*
[2]*Founder, PawsNYou International B.V., Bengaluru, Karnataka, India*
***Email:** *spurtianjan16@gmail.com*
DOI:

Abstract

With the current rise in the demand and usage of the blockchain technology for a variety of purposes, ranging from finance, medical, identification amongst others, major focus has been dedicated towards its legal implications rather than leveraging on the practical applications in administration. In this paper, we discuss the concepts of blockchain and how it can be implemented as an efficient solution towards public voting while aiming to destroy the disadvantages of the current voting system in India, at the same time providing a better, more reliable, secure and transparent means of public governance. We also aim to provide an exemplified voting solution for India with the integration of the current Aadhaar identification system as implemented by UIDAI.

Keywords: *Aadhaar, blockchain, blockchain voting, decentralized, distributed ledger, e-voting, uidai*

INTRODUCTION

Voting in India has always been a topic of high controversy, whether with the initial "Balloting System", implemented in the 1951−52 General Elections or the recent "Electronic Voting Machines", implemented extensively since 1998. [1] In the balloting system, a voter casts their vote on a pre-printed ballot paper, in the presence of an appointed voting official and the cumulative votes are captured in a physical box and transported to a centralized vote counting location. The issues with this system as evident enough were mitigated by replacing them with an electronic voting system where votes are captured on an electronic balloting unit and transported across to a centralized location for calculation using the control unit. Votes cast on an EVM are assumed to be tamperproof to a great extent. However, the other obvious issues with this system were the reliance on an authority for the purpose of monitoring the voting process as well as allegations of influence by political parties to support their cause.

Apart from this, other issues concerning the current voting system in India include, amongst the least, lack of transparency, fake voter IDs, prone to political manipulation in remote locations, as well as delay in the result declaration. All these identified issues can be well resolved by replacing any current voting option with a blockchain based electronic-voting system which operates on a user level capturing the votes on a distributed interface (web/mobile).

Blockchain technologies are often implemented where there is a need for transparency or a decentralized authentication/identification of entities, whether currency, intellectual property or otherwise. This encrypted, decentralized and agile strategy for data storing lead by a government blockchain record will result in a progressively responsive and easy to use administrative cooperation. In this paper, we aim to establish the efficiency of a blockchain based digital voting system

with higher security and complete transparency integrated with UIDAI's Aadhaar identification system. The purpose of integrating UIDAI's Aadhaar with the Voter ID of citizen is to mitigate the duplicate/fake voter ID issues evident in our current infrastructure.

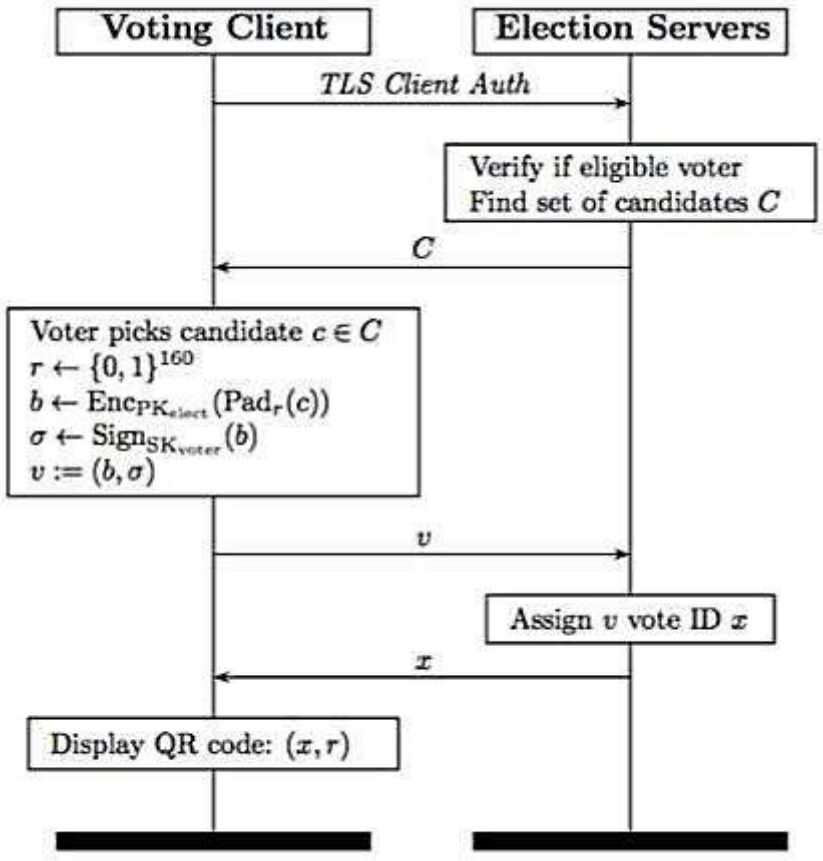
LITERATURE SURVEY

Earlier noted versions of an electronic system of voting have been attributed to David Chaum, who created a system with a public key cryptography for the purpose of vote casting, while keeping the voters anonymous, with the use of the Blind Signature Theorem. [2] Post which a lot of research has been conducted with other methods of electronic voting systems. [3−6]

Kaspersky Labs has conducted their own case-study with a blockchain secured voting system targeting proof-of-work to replace the issue of multiple voting, which is similar to "double spending" in Bitcoin. [7] With the help of unique, anonymous Bitcoin addresses, this system ensures the voting is completely transparent, while being authenticated using the U.S. based social security number. They have also created a proof-of-concept on a shared instance which can be accessible as a web application [7].

Other notable electronic/digital voting systems include the Estonian internet voting system [8].

The system was setup using the Estonian national identification card, which was used to generate a SHA1/SHA2 signature, as a private key (Fig. 1).



(a) **Vote casting process**

Figure 1: *Vote casting process in the i-voting system [8].*

Along with the election's public key, this was used to encrypt the vote and send to a private server hosted with the government. One key feature of the same was that voters were allowed to vote multiple times, while only the last vote was considered to be valid [9].

While a few nations and urban communities effectively seek after various implementations of blockchain to address their administration issues, a chosen few are wagering on blockchain for a decentralized government. For instance, the princely state of Dubai is already planning to exchange their whole legislative foundation and economy to a blockchain based system, consequently making this United Arab Emirates city one of the informal capitals of the blockchain industry.

WHAT IS BLOCKCHAIN?

A blockchain is a distributed leger of data gathered through a system that sits over the web. It is the means by which this data is recorded that gives blockchain its weighty potential. Blockchain, by itself, isn't an organization, nor is it an application, yet rather a completely different approach for archiving information on the web by means of a distributed ledger. It can be utilized to create applications, for example, for the purpose of authentication, identification, social networks, messaging, financials management, security, and on the basic level for other ledger-based implementations (Fig. 2).

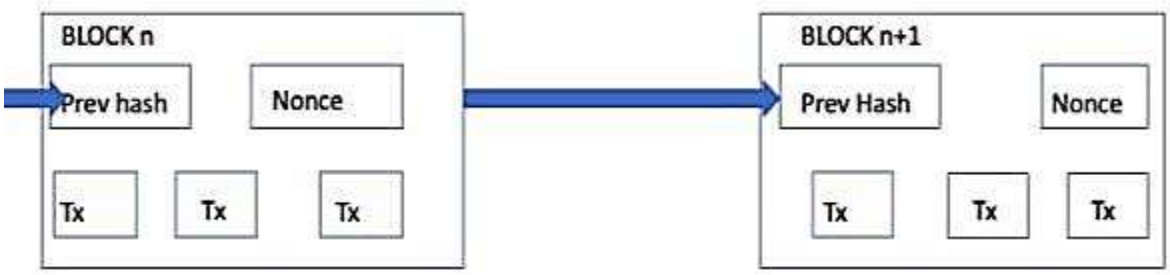


Figure 2: *Hashing of previous block in a blockchain.*

The data recorded on a block in the blockchain can take any form and a block can be used to store a transaction, entry or any other chunk of data.

HOW DOES IT WORK?

Blockchain works by means of creating blocks of data with a particular identifier, to link the current block with the previous block by means of hashing. Hashing takes an input string of varying length to output a cryptographic string of fixed length, by means of a mathematical algorithm (SHA, AES, etc.) This generated hash is then used as an identifier in the next block of the blockchain, linking it to the previous block.

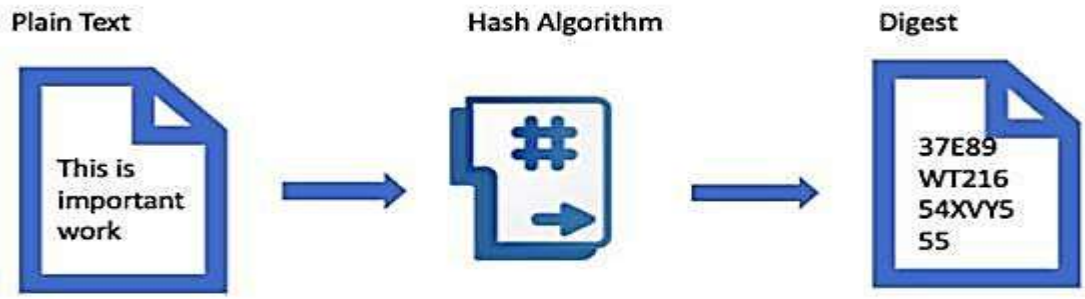


Figure 3: *Hashing process.*

Hashed data can never be traversed in the opposite direction, nor can it be decoded (Fig. 3). Also, the hash for a specific input will always remain the same, over any number of iterations.

ARCHITECTURE

In our model, we use the UIDAI's Aadhaar, which is a unique ID generated for every registered citizen of India, as a private key, along with the public key assigned to an election, to generate a digital signature for the purpose of voting. This along with the vote of the individual, is then used to generate a hash used to reserve / block the vote for that particular individual. The voting mechanism will take place over a government authorized portal (web/mobile) and the votes are captured on a tamperproof instance available openly for the public to verify and validate.

SHA-256 algorithm is used to generate the hash for the next block as well as the encryption of the user's identifiable data. The entire system rests on a standalone blockchain powered by cloud infrastructure. The proof-of-concept protocol is used for consensus of the blockchain.

METHODOLOGY

Voting UI (Web / Mobile App)

The voting UI will be designed to allow the user to authenticate themselves using their unique Aadhaar ID and then selecting the election for which they wish to cast their vote. Once the user selects the election, they can cast their vote for the desired candidate. The vote along with the Aadhaar ID (as a private key), will be used to generated a digital signature sent across to the blockchain to create a new block. This UI will be designed keeping in mind the accessibility options for the disabled (Fig. 4).

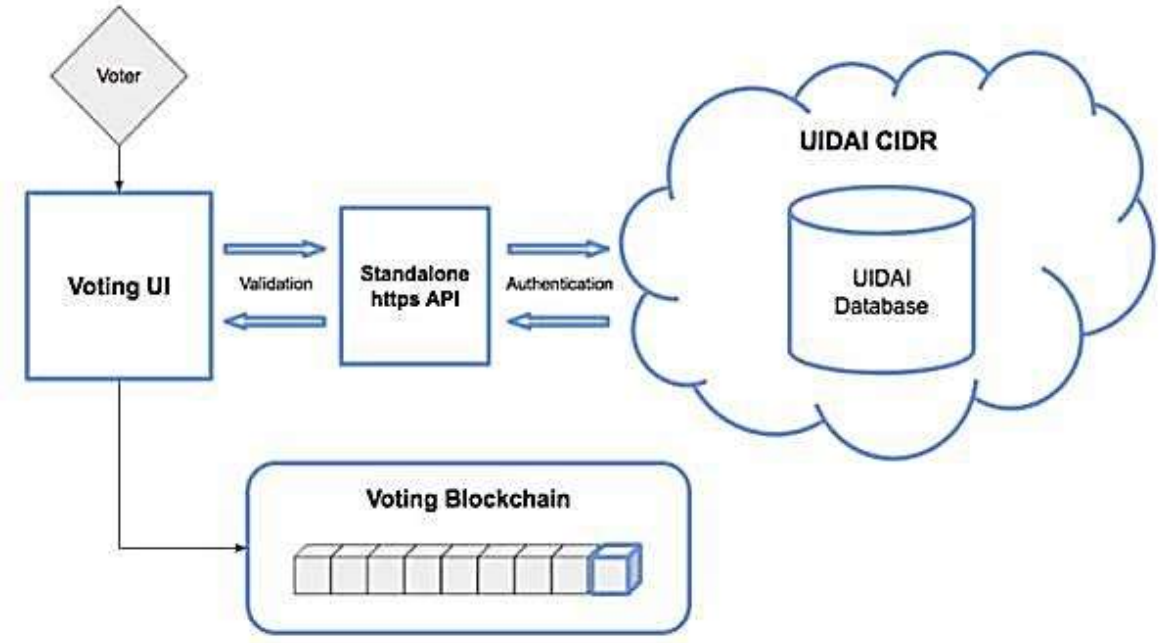
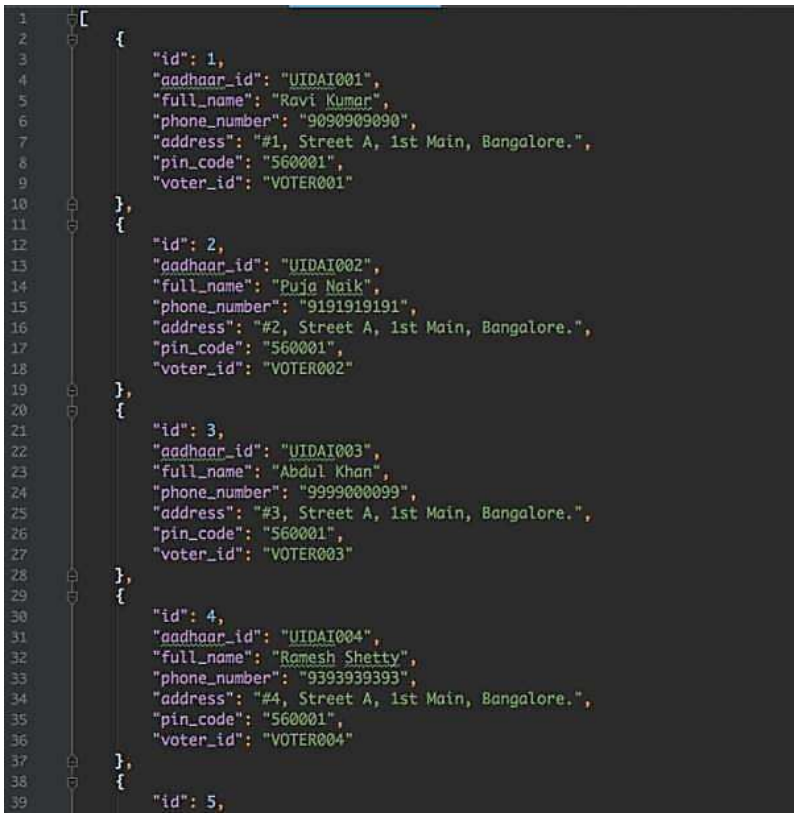


Figure 4: *System architecture.*

Accessing Aadhaar API

The UIDAI's Aadhaar API will be accessed using a standalone API from the voting UI validating the current user as a valid / invalid voter for the given election. Standard Aadhaar authentication using OTP/biometrics as available within the voting UI will be used to authenticate the user (Fig. 5) [10].



```
[
    {
        "id": 1,
        "aadhaar_id": "UIDAI001",
        "full_name": "Ravi Kumar",
        "phone_number": "9090909090",
        "address": "#1, Street A, 1st Main, Bangalore.",
        "pin_code": "560001",
        "voter_id": "VOTER001"
    },
    {
        "id": 2,
        "aadhaar_id": "UIDAI002",
        "full_name": "Puja Naik",
        "phone_number": "9191919191",
        "address": "#2, Street A, 1st Main, Bangalore.",
        "pin_code": "560001",
        "voter_id": "VOTER002"
    },
    {
        "id": 3,
        "aadhaar_id": "UIDAI003",
        "full_name": "Abdul Khan",
        "phone_number": "9999000099",
        "address": "#3, Street A, 1st Main, Bangalore.",
        "pin_code": "560001",
        "voter_id": "VOTER003"
    },
    {
        "id": 4,
        "aadhaar_id": "UIDAI004",
        "full_name": "Ramesh Shetty",
        "phone_number": "9393939393",
        "address": "#4, Street A, 1st Main, Bangalore.",
        "pin_code": "560001",
        "voter_id": "VOTER004"
    },
    {
        "id": 5,
```

Figure 5: *Mock UIDAI database used.*

The Aadhaar API will validate the user and return the basic information of the user including their name, address, photograph and validity for voting (Fig. 6).

```
validateVoter: function (req, res) {
    let _aadhaar_id = req.body.aadhaar_id;
    let _unique_aadhaar_token = req.body._unique_aadhaar_token;

    // Calling UIDAI Aadhaar API with the user valid id
    function validateUser(_aadhaar_id, _unique_aadhaar_token) {
        // Function to mock UIDAI Aadhaar OTP verification behavior
        // This function call will be replaced with the actual
        return {
            status: true,
            full_name: _full_name,
            phone_number: _phone_number,
            address: _address,
            voter_id: _voter_id
        };
    }

    let response = validateUser(_aadhaar_id, _unique_aadhaar_token);

    if (response.status) {
        // Success, Valid voter
        res.status(200).json({
            message: "User is allowed to vote.",
            data: {
                full_name: response.full_name,
                phone_number: response.phone_number,
                address: response.address,
                voter_id: response.voter_id
            }
        });
    } else {
        // Failure, Invalid voter
        res.status(400).json({
            message: "User not a valid voter."
        });
    }
```

Figure 6: *Validate voter API endpoint.*

E-voting Blockchain

The blockchain will be setup on a standalone instance available publicly for validating the vote count as well as adding votes.

For the purpose of adding the vote, a private function add Vote is called from the Voting UI. The function creates a new block with the supplied data, and with a SHA256 generated hash of the user's data in the current block and the SHA256 generated hash of the previous block in the header of the current block. This completed block is then verified and added to the chain. Since the hashing process is a one-way transaction, no one will be able to reverse it. This will ensure that there is no way the user's identity is revealed, although the vote count is available publicly. For the purpose of vote count, a private function display Vote Count can be called from the voting UI or from any authorized implementation of this publicly available endpoint. The function returns of the full details of vote count along with party wise breakdown and can be further modified to provide location wise breakdown as well.

Since blockchain works on a broadcast mechanism, as opposed to traditional databases, the authenticity of votes captured is always ensured. As long as a particular block is valid, it is authentic. Additionally, instead of being a completely decentralized blockchain voting platform, this model incorporates the advantages of blockchain by having the nodes authenticate using a centralized permission (private key) for every node and then approving the addition of the block to the chain.

CONCLUSION

At the current rate of development our country is going through, it is imperative that traditional methods of administration must be replaced with newer more advanced alternatives. At the same time ensuring that our efforts are applied in the direction of added user flexibility, security and complete transparency. This model of electronic voting system ensures the same while adding further benefits of instant electoral count, transparent and open-source voting platforms, while also providing the user the flexibility to vote from their convenience. The Election commission of India reportedly spent INR 35000 crores in polling for the 2014 Lok Sabha Elections [11]. A major chunk of this amount is spent in arranging and setup of the voting booths across all locations in the country. With a digital implementation of the voting system, a huge amount of the taxpayer's money can be saved, which can then be utilized for other welfare projects.

REFERENCES

1. Election Commission of India, *https://eci.gov.in/*.
2. DL Chaum (1981), "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communication of the ACM*, Volume 24, Issue 2.
3. T ElGamal (1985), "A public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *IEEE Trans. Info. Theory*, Volume 31.
4. S Ibrahim, M Kamat, M Salleh, SR A, Aziz (14−15 January, 2003), "Secure E-Voting with Blind Signature", *Proceeding of the 4th National Conference of Communication Technology*, Johor, Malaysia.
5. J Jan, Y Chen, Y Lin (16−19 October, 2001), "The Design of Protocol for e-Voting on the Internet", *Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology*, London, England.
6. DL Dill, AD Rubin (2004), "E-Voting Security", *Security and Privacy Magazine*, Volume 2, Issue 1.
7. Kaspersky, Eugene (2016), "Cyber Security Case Study Competition-Kaspersky", *The Economist*, Volume

15, Accessed on December 14. 2016. *http://www.economist.com/sites/default/files/drexel.pdf.*

8 D Springall, T Finkenauer, Z Durumeric, J Kitcat, H Hursti, M MacAlpine, JA Halderman (2014), "Security Analysis of the Estonian Internet Voting System", *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.*

9 Trueb Baltic, "Estonian Electronic ID – Card Application Specification Prerequisites to the Smart Card Differentiation to previous Version of EstEID Card Application", Available From *http://www.id.ee/public/TBSPEC-EstEID-Chip-App-v3_5-20140327.pdf.*

10 UIDAI Aadhaar API, Available From *https://uidai.gov.in/images/FrontPageUpdates/aadhaar_authentication_api_2_0.pdf.*

11 Bloomberg, "Why India's election is among the world's most expensive", *The Economic Times,* Accessed on Apr 7 2019, Available From *https://economictimes.indiatimes.com/news/elections /lok-sabha/india/why-indias-election-is-among-the-worlds-most-expensive/articleshow/68367262.cms.*

Cite this article as: