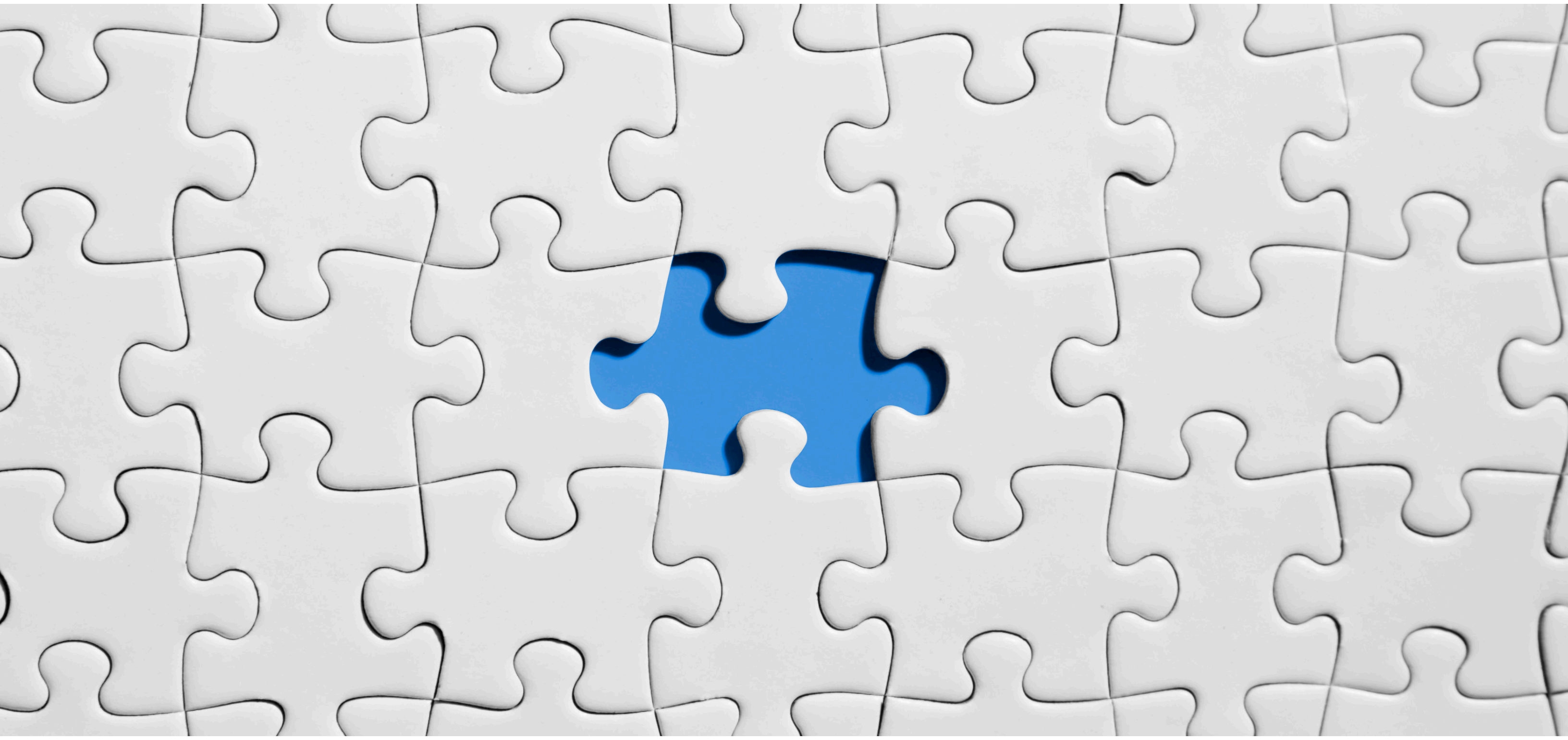
ELECTRONIC VOTING SYSTEM USING BLOCKCHAIN



Raghavendra Ganji

Consultant

Dell EMC

Raghavendra.Ganji@dell.com

Yatish BN

Consultant

Dell EMC

Yatish.Bn@emc.com

Knowledge Sharing Article

© 2018 Dell Inc. or its subsidiaries.

Table of Contents

Disclaimer: The views, processes or methodologies published in this article are those of the authors. They do not necessarily reflect Dell EMC's views, processes or methodologies.

Abstract

Cryptocurrencies are being used widely and gaining popularity. The main theme of all cryptocurrencies are a transfer of value between two peers without needing a central authority, such as a bank or financial institution; it is distributed and decentralized. Blockchain is a technology behind all cryptocurrencies. It’s a constantly growing ledger that keeps a permanent record of all the transactions that have taken place, in a secure, chronological and immutable way that makes peer to peer value transfer possible. Value can be anything. In the case of cryptocurrencies, it takes the meaning of money. Whereas in gaming it can take the form of points.

In electoral voting, the value can take the form of a vote. In this paper, we will show how blockchain can be used to transfer votes between two peers. In our case, one peer is the voter and the other is the candidate who receives the vote. We will explain how blockchain can be employed in mass electoral voting procedures in a more secure way without needing a central authority body. We will explain a voting system using blockchain that is more robust, tamper-proof (immutable to voting changes either by the voter or by any other third parties) and cost-effective. We have reviewed various blockchain technologies, i.e. Ethereum, Multichain, available today to use in our voting system. Also, we will elaborate on the architecture, design and design constraints and implementation implications of such a voting mechanism in our society.

Introduction

Extensive research has been done on electronic voting systems that enable voters to vote at their convenience using a mobile phone, computer or any other electronic device. Still, none of these technologies have been incorporated on a larger scale due to inherent security threats/concerns that these systems might pose to the integrity of the voting process.

In this paper, we discuss electronic voting system using blockchain [1], a secure and robust system that ensures anonymity of the voter, transparency in the process, and robust functioning.

Blockchain

The blockchain is a digital platform for digital assets. It consists of a continuously growing list of records known as blocks that are linked and secured using cryptography. Major usage of Blockchain has been in all cryptocurrency transactions, mainly Bitcoin [2]. However, they are increasingly being used in a number of other applications because of their inherent resistance to modification to the transaction/block/whole distributed ledger - Blockchain. One such application is Electronic Voting. We will review some of the variety of blockchain technologies that are usable, scalable and secure, fit for Electronic Voting Application.

Ethereum

Ethereum [3] is an open Blockchain platform that lets anyone build and use decentralized applications that leverage Ethereum Platform. Ethereum community support is very active. It can be used as Public or Private Network. We need the Ethers (Ethereum Cryptocurrency) in order to transact on Public Ethereum Platform. Ethereum supports the concept of smart contracts which is a code of business logic which can be deployed inside Blockchain network. An advantage of using Ethereum for Voting application is that we can use the Smart contract to validate and store voting count states in the Blockchain. However, it comes at the cost of transacting in public network. Also, mining computation is heavy in the case of Ethereum Public or Private Platform to give consensus to blocks.

Multichain

Multichain [4] is a platform for the creation and deployment of private Blockchain. This can be more secure as it will be built on a private network and only peers inside the network can send transactions. This has medium community support but it is improving. It supports Python, C#, and JavaScript to interact with the platform. Advantages of Multichain is that it has an auto mining option which will mine blocks at less computation power and it is a free for transacting on the private network. Multichain supports asset management, which is unique in that one can define an Asset and issue Units of assets in the network. This is the feature we have explored in our use case. We have assigned “Vote” as an asset. Each registered voter will be assigned with exactly one vote during the registration process. In this paper, we propose Electronic Voting Application using Multichain.

Our solution

In ideal conditions as occurs with paper ballot voting, information about whom the voter voted is kept secret. This information is not even known to the Election commission. This security aspect is very central to the electronic voting system. The system should be secure enough that no one should be able to know whom the voter voted for and tamper with it at later stages. Also, there should be efforts to ensure the anonymity of the voter. To maintain voting data confidentiality, Trusted Third Party (TTP) can be used. TTP acts as an agent between the voter and the Election Commission to authenticate the voter to vote during elections. Without TTP, it is difficult to incorporate security and data confidentiality.

The following are the components involved in the electronic voting system.

A. **Authentication Organization**

This is the entity that holds voter information. It is something similar to Election Commission in India. During electronic voting, this organization should determine voter validity. At the same time, it should not expose the voter information to any other party.

B. **Trusted Third Party**

We introduced this additional entity that can be a private organization helps in validating the voters during voting. TTP acts as an agent between election commission and voter. This helps keep voter information anonymous to the Authentication Organization. Otherwise, Authentication organization can know who the voter is and potentially manipulate the votes.

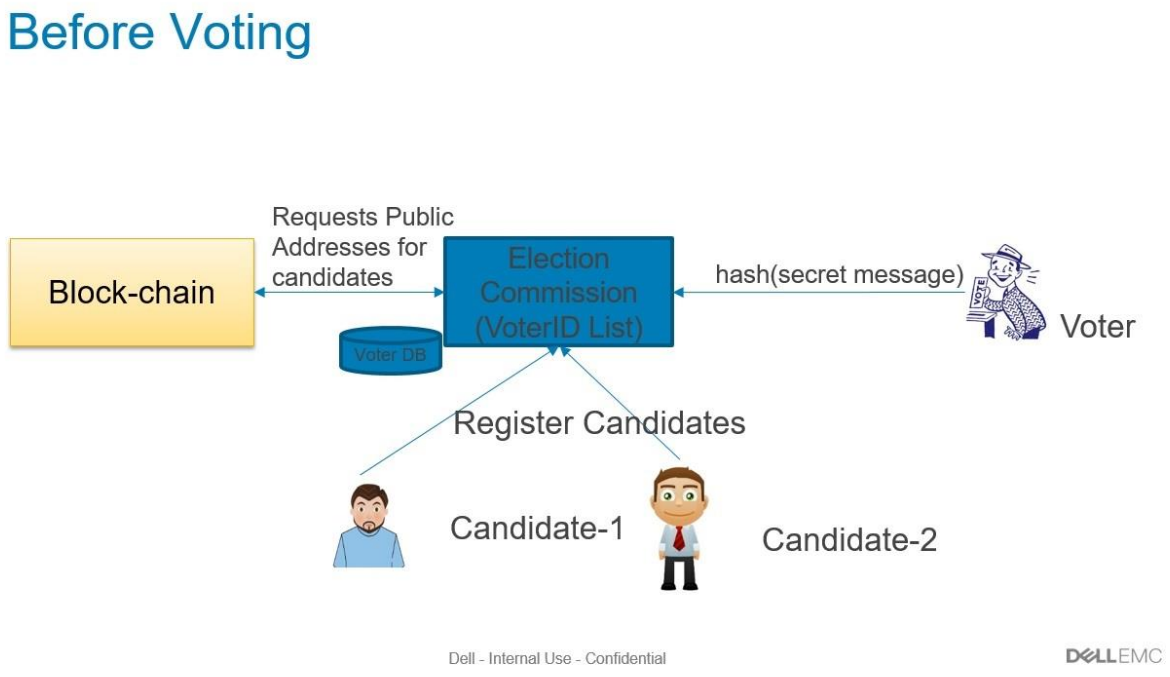
C. **Multi-chain**

Blockchain is the backbone of the electronic voting system. We have used multi-chain in demonstrating voting application. Once TTP authorizes voters to vote, the voter can choose whom he wants to vote for within his constituency. Each vote is conceptually equivalent to the asset in multi-chain and the transaction happens between voter and candidate. By restricting the multi-chain asset to a process maximum of one transaction between parties, the system is capable of restricting either multiple votes sent to the same candidate or voting for multiple contenders.

The following sections describe the voting process and the components involved.

A. **Before Voting**

Figure 1 depicts voter and contestant registration process with the authentication organization.


Before Voting

Dell - Internal Use - Confidential

Figure 1: Before Voting

Election commission maintains data related to voters and contestants. Before voting, registered voters have to prove their intention to vote and contestants should file nomination forms.

1) **Intent to vote by voters**

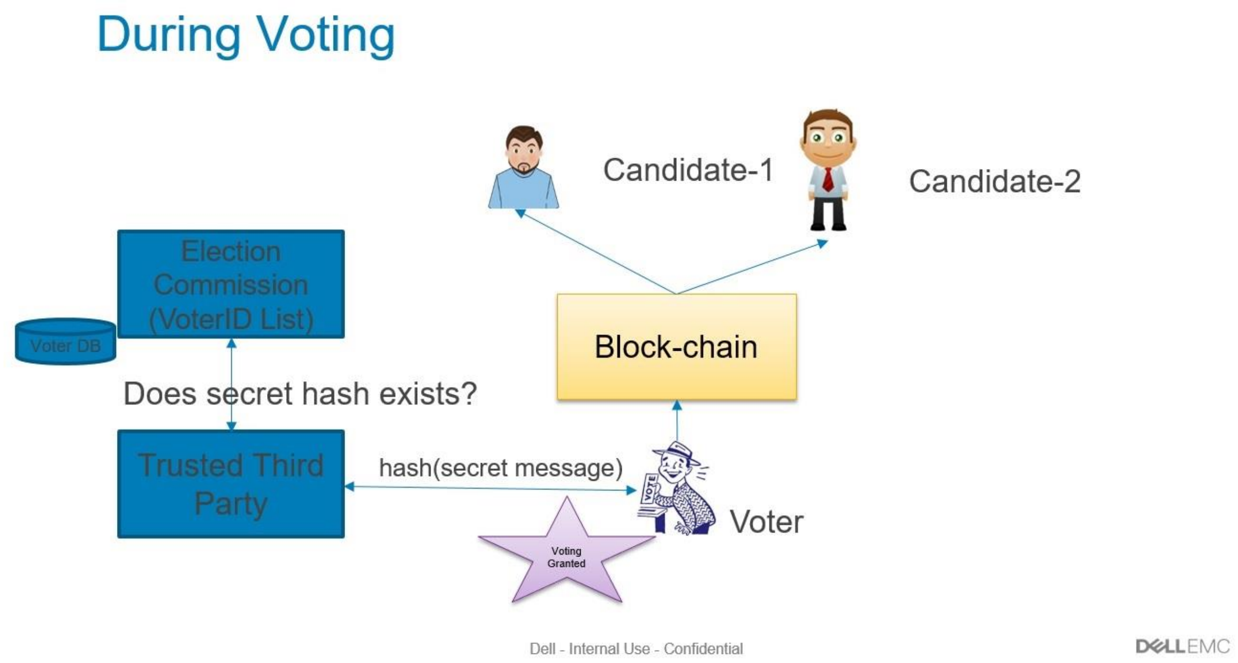
The Election Commission should provide a user interface to the voter to express his intention for voting. The voter can be identified with any of the unique identification numbers assigned by the Election Commission. This identification number must be used consistently throughout the process. Otherwise, there could be chances that the same voter can register multiple times with different identities and then vote multiple times. In the registration process, the voter submits a secret message. As a response to the secret message, the client-side web page generates a unique random reference number to the voter which has to be noted for future reference during voting. An internally hashed secret message and reference number is generated and stored in the Election Commission database. It’s important that the voter not share this secret message and reference number with the Election Commission. Otherwise, the Election commission might get to know who voted for whom and potentially manipulate the whole voting process at later stages of voting.

2) Filing nomination by contestants

The contestant can be any valid voter who intends to contest an election. Such candidates have to file for nomination with the Election Commission. In the nomination process, the candidate registers intention to participate in the election as a contestant by submitting their voter ID. The Election Commission will generate a public address in the multi-chain network and stores it against the candidate. Later, during voting, this public address will be made visible to the voters to vote for candidates.

B. **During Voting**

In the real world, voting happens during the stipulated period. The same procedure is followed here. However, the duration of the voting can be extended. During voting, the voter has to submit the same secret message and reference number that has been generated during voter registration to the trusted third party. Trusted third party sends the message hash to the election commission to verify that the voter is a valid voter. Upon verification, Election commission returns validity of the voter to trusted third party. A voter identified as valid will be taken to the voting page. There, a list of candidates will be shown based on constituency. During this process, trusted third party generates a public key for the voter using the multi-chain network and stores this information against the hash of the secret message and reference number of the voter. The same is depicted in Figure 2. There are cases where a voter might try to vote multiple times for the same contestant or vote for multiple contestants. In either case the system guards against such malicious voting. This safeguarding is made possible in multi-chain by restricting the number of transactions between two parties to one. Hence, even if the voter does more than one transaction/votes, those will be invalidated by multi-chain.



During Voting

Dell - Internal Use - Confidential

DELL EMC

Figure 2 Voting process

C. **After Voting**

Since its an electronic voting system, reports can be generated in real-time. However, the real-time report of who is leading and who is lagging should not be made public as it might affect public sentiment and could bias to a particular party or candidate.

After the voting completes, detailed reports about a candidate's results, party-wise results, constituency results, etc. can be easily prepared using any BI tool by combining data from multi-chain and data stored in Election Commission records.

Voting example

In this section, we describe the whole process of voting with an example. John and Eric are two voters who intend to vote. John's records are present in Election Commission whereas Eric's are not. John is able to register for the upcoming election using his voter ID. He will declare using the Election Commission web portal. John will submit voter ID to the Election Commission. If John is eligible for voting, he will be asked to submit a secret message. Once submitting a secret message, John will receive a unique reference number along with the secret message. In the process, John should not reveal the secret message or reference number to anyone. Eric also tries to register for voting. Since his records are not present in Election Commission, he will be denied voting. Hence, the system will not take his secret message hash and a unique reference number will not be generated.

During voting, John visits Trusted Third Party website and shares his secret message and reference number to vote. Trusted third party determines if the hash of the secret message and the reference number is present in Election Commission database. Upon confirmation, John is allowed to navigate to the next page where he can vote for contestants that belong to his constituency. During this phase, trusted third party generates a public address for John in multi-chain and stores this against the voter public address in its database.

John can then select any of the listed candidates to vote for and then click on the Submit button. Once his vote is submitted, the system will transfer one vote/asset from John's account to the contestant John has voted for. If John tries to vote for the same candidate or any other candidate by entering his secret message and reference number, trusted third party will check if voter IDash is already present in its database. If it's present, it means that John is trying to vote for the second time and the system will prevent that.

Auditing

In this electronic voting system, we have introduced many parties that work independently of each other. It's important for these parties to adhere to rules and regulations for the system to work seamlessly to ensure data integrity, data confidentiality, anonymity, and reliability. Auditing can be employed to make sure that these multiple parties are adhering to the voting rules.

Conclusion

In this paper, we proposed an electronic voting system using multi-chain. We showed how multi-chain can be configured to restrict transactions to only one vote between voter and contestant. A new entity – trusted third party – was introduced to keep the voting secret. Without this organization, it's not possible to maintain voter anonymity and whom the voter votes for. This is also necessary to avoid forgery of votes by either the Election Commission or trusted hird party. We stablished a workflow between authentication organization, trusted third party and multi-chain ledger. In the end, we showed how auditing can ensure authenticity of the entire system.

References

1. Kibin Lee, Korea University et al, Electronic Voting Service using Block-chain
2. BitCoin, https://blockchain.info/
3. Ethereum, https://www.ethereum.org/
4. Multichain, https://www.multichain.com/

Dell EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” DELL EMC MAKES NO RESPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying and distribution of any Dell EMC software described in this publication requires an applicable software license.

Dell, EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries.