ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.10

Decentralized Voting Application

Lalitha Devi[1], Devashish Kedar[2], Saurabh Kumar Malik[3], Kunal Dubey[4]
Assistant Professor (O.G)[1], B. Tech Graduate[2, 3, 4]
Department of Computer Science
SRMIST Ramapuram Campus, Chennai, India

Abstract:
In our day to day life we are using the centralized web-based services. In the centralized web the data is stored in the central server hosted by the service provider. As the number of users increases the centralized server may get lagged out. All the data is stored in one place so that if the server gets security breach, every bit of data is at compromise. This has led to development of a more efficient and secure way. The web 3.0 also known as decentralized webs is among one of the best solutions for overcoming the drawbacks of centralized web. The decentralized web is a peer to peer network of computers rather than a single/centralized server. The decentralized web is basically based on blockchain technology that provides faster data transfer, less node failure and high security of data. Building a secure electronic voting system that offers the fairness and privacy of current voting schemes, while providing the transparency and flexibility offered by electronic systems has been a challenge for a long time. In this work-in-progress paper, we evaluate an application of blockchain as a service to implement distributed electronic voting systems. The paper proposes a novel electronic voting system based on blockchain that addresses some of the limitations in existing systems and evaluates some of the popular blockchain frameworks for the purpose of constructing a blockchain-based e-voting system. In particular, we evaluate the potential of distributed ledger technologies through the description of a case study; namely, the process of an election, and the implementation of a blockchain- based application, which improves the security and decreases the cost of hosting a nationwide election

Keywords: web 3.0, decentralized web, cryptocurrency, blockchain

I. INTRODUCTION

Blockchain technologies, sensible contracts specially, square measure implausibly powerful and square measure near to disrupt several aspects of finance, business, and law. However, thanks to the settled and suburbanized nature of sensible contracts, they're unable to speak directly with valuable information sources off-chain.

An oracle provides that link by creating off-chain interactions and delivering results on-chain. Sadly, solely centralized oracles exist these days and contracts square measure forced to deem one purpose of failure that might be attacked, manipulated, or corrupted.

A suburbanized, trust less network of incentivized oracles is required to empower following generation of sensible contracts.

With the right crypto economic science at play, a statistically adequate provide of miners can, together with the staking of a token, reach a accord off-chain. Then, with efficiency inscribe the information onto the blockchain, publicly

Blockchain

It is usually one LinkedList of a block, with every block containing variety of transactions and operations to be performed. It is primarily a suburbanised web-based technology that provides an unquestionable information storage across the network of users. Assets square measure created and a typical ledger or a blacklist is maintained among its users. Trust issue is that the major and most significant issue to be thought of whereas operating with blockchain technology. The blockchain is immutable — data remains within the same state for as long because the network exists.

Decentralized Applications – DApps

Decentralized applications (dApps) square measure applications that run on a P2P network of pcs instead of one computer. dApps, have existed since the appearance of P2P networks. they're a kind of computer code program designed to exist on the net in an exceedingly manner that's not controlled by any single entity

1. Suburbanised applications essentially ought not to run on prime of a blockchain network. BitTorrent, Popcorn Time, Bit Message, Tor, square measure all ancient dApps that run on a P2P network, however not on a Blockchain (which may be a specific reasonably P2P network).

2. As critical straightforward sensible contracts, within the classic sense of Bitcoin, that sends cash from A to B, DApps have a vast range of participants on all sides of the market.

Blockchain DApps

As from the on top of rationalization it would be thought of as that it's not necessary for a dApp to be blockchain or crypto based mostly, it may be p2p affiliation however victimization the blockchain technology as its own benefits

For AN application to be thought of a dApp within the context of Blockchain, it should meet the subsequent criteria:

1. Application should be utterly ASCII text file
2. It should operate autonomously, and with no entity dominant the bulk of its tokens. the appliance might adapt its protocol in response to projected enhancements and market feedback, however the accord of its users should decide all changes.
3. Application's information and records of operation should be cryptographically hold on must be cryptographically hold on in an exceedingly public, suburbanised blockchain so as to avoid any central points of failure.
4. Application should use a cryptologic token (Bitcoin or a token native to its system) that is important for access to the appliance and any contribution important from (miners/farmers) ought to be rewarded with the application's tokens.

5. Application should generate tokens according to a regular cryptologic formula acting as a symptom of the worth, nodes square measure causative to the appliance (Bitcoin uses the Proof of labor Algorithm).

II. DAPP DEVELOPMENT PROCESS

The subsequent is that the common procedure for launching a d-apps

Whitepaper

A whitepaper is printed describing the dApp and its options. This whitepaper will define the thought for dApp development however additionally entail an operating paradigm.

Token Sale

Initial tokens sale is ready up

ICO – Initial Coin Offering

The possession stake of the dApp is unfold

Implementation & Launch

Funds square measure invested with into building the dApp and deploying it. Apart from this, it takes plenty of your time to make a cryptocurrency and to circulate it, so we tend to square measure victimization the Ethereum because the base cryptocurrency for the event method.

III. CHARACTERISTICS OF DAPPS

Distributed information:

Data printed on a blockchain exists as a shared and ceaselessly reconciled-database. The blockchain information isn't hold on in central location that makes the record actually public and simply verifiable. Since there's no central copy of the date, there's no scope for hackers to corrupt the information. The information is hosted by legion computers at the same time that is accessible to anyone on the network

Durability and robustness:

Lustiness is an intrinsic characteristic of the blockchain technology like the net. By storing blocks of knowledge that square measure identical across its network, the blockchain will neither be controlled by any single entity nor has no single purpose of failure. the net has displayed its sturdiness for nearly 3 decades. it's an affidavit that augurs well for blockchain technology because it continues to advance.

Transparent and incorruptible:

The blockchain network lives in an exceedingly state of accord, one that mechanically updates all the transactions each 10 minutes. Every cluster of those transactions is stated as a "block". the 2 vital properties that result from this square measure transparency i.e. the information out there on the network is public which might be accessed by anyone, and honestness i.e. the information is hold on the network. Dynamic the information on the network would on paper mean victimization tremendous quantity of process power and much not possible.

Network of nodes:

Blockchain may be a network of computers. every pc inside the network that contributes to the process power of the network is termed a node. In essence, the blockchain interprets to a network that possesses super-computing power.

Decentralization:

The blockchain is meant to perform as a suburbanized technology. Something that happens on that may be a perform of the network as a full. Some vital implications stem from this. Decentralization implies that the network operates on a peer-to-peer basis. This characteristic has been working out to the conception of distributed ledger technology. A distributed ledger may be a style of information that's distributed across participants on the network. All of the participants on the distributed ledger will read all of the records in question. The technology provides a verifiable and auditable history of all data hold on on a specific dataset.

IV. BLOCKCHAINS BASED E-VOTING SYSTEM

This section proposes a new e-voting system based on the identified voting requirements and blockchain as a service. We explain the setup of the blockchain, define the smart contract for e-voting that will be deployed on the blockchain and show how the proposed system satisfies the envisioned voting requirements.

Blockchain setup

In order to satisfy the privacy and security requirements for e-voting, and to ensure that the election system should not enable coerced voting, voters will have to vote in a supervised environment. In our work, we setup a Go-Ethereum permissioned Proof-of-Authority (POA) blockchain to achieve these goals. POA uses an algorithm that delivers comparatively fast transactions through a consensus mechanism based on identity as a stake. The reason for using Go-Ethereum for the blockchain infrastructure is explained in sub-section C. The structure of the blockchain is illustrated in Figure 1 and mainly consists of two types of nodes.

(i) District node: Represent each voting district. Each district node has a software agent that autonomously interacts with the "bootnode" and manages the life cycle of the smart contract on that node. When the election administrator (see smart contract section) creates an election, a ballot smart contract is distributed and deployed onto its corresponding district node. When the ballot smart contracts are created, each of the corresponding district nodes is given permission to interact with their corresponding contract. When an individual voter casts her vote from her corresponding smart contract, the vote data is verified by the majority of the corresponding district nodes and every vote they agree on is appended onto the blockchain.

2) Voting transaction: Each voter interacts with a ballot smart contract for her corresponding voting district. This smart contract interacts with the blockchain via the corresponding district node, which appends the vote to the blockchain. Each a deterministic list of eligible voters. This might require a component for a government identity verification service to securely authenticate and authorize eligible individuals. Using such a service is necessary to satisfy the requirement of secure authentication as this is not guaranteed, by default, when using a blockchain infrastructure. In our work, for each eligible voter, a corresponding identity wallet would be generated. A unique wallet is generated for each voter for each election that the voter is eligible to participate in.

3) Tallying results the tallying of the election is done on the fly in the smart contracts. Each ballot smart contract does their own tally for their corresponding location in its own storage. (iv) Verifying votes in the voting transaction, each voter receives the transaction ID of his vote. In our e-voting system, voters can use this transaction ID and go to an official election site (or authority) using a blockchain explorer and (after authenticating themselves using their electronic identification) locate the transaction with the corresponding transaction ID on the blockchain. Voters can, therefore, see their votes on the

blockchain, and verify that the votes were listed and counted correctly. This type of verification satisfies the transparency requirements while preventing traceability of votes.
An individual voter receives the transaction ID for their vote for verification purposes. Every vote that is agreed upon, by the majority of the corresponding district nodes, is recorded as a transaction and then appended on the blockchain. Figure 2 is a visual representation of this process. A transaction in our proposed system (see Table I) has information on i) the transaction ID, ii) the block which the transaction is located at, iii) to which smart contract the transaction was sent - which indicates from which voting district the vote was cast, and iv) the value of the transaction, i.e. the vote, indicating which entity (party) the voter voted for. A voting transaction in our system, therefore, reveals no information about the individual voter who cast any particular vote.

The title and author data are in one-column format, while the rest of the paper is in two-column format. To accomplish this, *Word* has section break commands that will separate the one and two-column format. There are two ways to setup this format: 1) Use this template as a guide, 2) make your own formatted template.

To make your own template, open a new document and begin by inserting the title and author information in the standard one-column format. After you type in your title and your author information, double space. Click the Insert menu, select Break, then select Section Break—Continuous. This will set your paper up in sections so you can now proceed to a two-column section for the body of your paper.
If you are creating your own template, you will then set upthe two-column format. Click the Format menu, and select Columns. This option will open the Columns window. In the number of columns input box, enter 2. Select equal column width. In the spacing input box, enter 0.2. If you have the margin widths set correctly, the width of the column should display as 3.40". If column width is not 3.40, you'll need to correctly set your margins. To do so, go to the Format menu, select Document, select margins, input .75 for left and right margins, and 1.0 for top and bottom margins This will create correct margins and columns throughout the paper.

V. REFERENCES

[1] Marco Conoscenti ,Antonio Vetrò,Juan Carlos De Martin, "Peer to Peer for Privacy and Decentralization in the Internet of Things",2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C),INSPEC Accession Number: 17011290,03 July 2017,

[2] Bogdan Cristian Florea, "Blockchain and Internet of Things data provider for smart applications",2018 7th Mediterranean Conference on Embedded Computing (MECO),INSPEC Accession Number: 17914987,09 July 2018

[3] Friðrik Þ. Hjálmarsson ; Gunnlaugur K. Hreiðarsson; Mohammad Hamdaqa; Gísli Hjálmtýsson "Blockchain-Based E-Voting System", 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), INSPEC Accession Number: 18079263, 10 September 2018

[4] Florian Wessling ; Volker Gruhn, "Engineering Software Architectures of Blockchain-Oriented Applications",2018 IEEE International Conference on Software Architecture Companion (ICSA-C),INSPEC Accession Number: 18007913,13 August 2018