INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 3)
Available online at: www.ijariit.com

Decentralized digital voting application

Sushmitha M
sushmitham017@gmail.com
School of Engineering and Technology Jain University (SET JU), Bengaluru, Karnataka

Aishwarya H D
aishwaryahd4@gmail.com
School of Engineering and Technology Jain University (SET JU), Bengaluru, Karnataka

Madhushree M
madhushreem28@gmail.com
School of Engineering and Technology Jain University (SET JU), Bengaluru, Karnataka

Pooja P
poojagowda122@gmail.com
School of Engineering and Technology Jain University (SET JU), Bengaluru, Karnataka

Dr. Saravana Balaji
saravanabalaji.b@gmail.com
School of Engineering and Technology Jain University (SET JU), Bengaluru, Karnataka

ABSTRACT

The blockchain is a decentralized, distributed database. A decentralized application utilizing blockchain technology enables you to perform similar activities you would do today yet without a trusted outsider. It is a shared system, a peer-to-peer network. Blockchain solves primary issues like transparency, security, accessibility that are the fundamental issues in current law based races. Ethereum is a platform that can be utilized to assemble the decentralized application. The blockchain is a changeless record of exchanges (votes) that are distributed in the system. Everyone's information that is the votes is stored in blockchain as transactions. The past votes can't be changed, while the present can't be hacked, on the grounds that each exchange is checked by each and every hub in the system. What's more, any outside or inside aggressor must have control of the hubs in the system to modify the record. Along these lines, every one of the exchanges stored on the blockchain is unchanged and thus this makes the application more secure in every aspect.

Keywords: *Blockchain, Ethereum, Voting, Decentralized*

1. INTRODUCTION

Blockchain technology provides immutable transactions that is the details of the transaction cannot be altered. This opens up numerous opportunities for payment. The project comprises of an application, one way the security issues can be potentially solved is through the technology of blockchain. Blockchain technology begins from the hidden structural design of the cryptocurrency bitcoin. It is a type of distributed database where records appear as exchanges; a square is a gathering of these exchanges. With the utilization of blockchain a secure and powerful framework for advanced voting can be conceived. The report plots our concept of how blockchain technology could be utilized to implement a secure digital voting application.

2. BACKGROUND WORK

Despite blockchain being in its initial stages, a lot of applications and services are being rapidly developed. Services such as transfer of money, proof of consistency, proof of ownership, smart contracts and various other concepts. The blockchain is used for voting in the distant future. But what concerns us the most is its robustness and immutability. Upon looking up these concepts enabled us to envision the project which can be used in any institution and alleviate many difficult processes.

Blockchain is the technology used in the digital cryptocurrency known as Bitcoins. This technology was developed by a group known as Satoshi Nakamoto to solve the double spending problem which was the problem of duplication/falsification. This paved way for a transaction without a trusted authority or a central server.

Web 3.0, a term coined for the change in the protocol of the Internet. At the moment, the majority of the internet works on a centralized network where there is always a central server look after functions of the network. Since the introduction of bitcoins, the technology behind it is being applied to the web as well. Decentralization is the key word here, which tells how Web 3.0 is totally a different path from the old Web 2.0. The protocols behind the new Web are in contrast with the old version, which means many applications are to be built from a scratch.

A blockchain is intended to be accessed over a peer-to-peer network, every node/peer at that point communicates with different nodes for block and exchange transactions. When

© 2018, www.IJARIIT.com All Rights Reserved

associated with the system, peers begin sending messages about different companions on the system, this makes a decentralized strategy for peer disclosure. The motivation behind the nodes inside the system is to approve unverified exchanges and as of recently mined blocks, previously another node can begin to do this it initially needs to complete an underlying block download. The initial block download influences the new node to download and approve all blocks from block 1 to the most current blockchain, once this is done the node is viewed as synchronized.

Without the developing web numerous web applications needed to move up to the rise of the new innovation. Tech mammoths, for example, IBM, Microsoft, Amazon, Infosys and numerous more have abided profound into this technology. Blockchain as a service (BaaS) has been initiated by cloud service providers, for instance this service is available on Bluemix by IBM, Amazon web services and even Microsoft Azure. This enables developers to build, test and deploy decentralized applications.

Despite the fact that the possibility of a blockchain as a basic design is moderately new, there are ongoing advancements which propose uses of the blockchain in different domains apart from cryptocurrencies.
There are three fundamental classifications of blockchain applications:

- Currency
- Smart contracts
- Areas in government, health, science etc.

3. PROBLEM DEFINITION

Various digital voting systems are currently being used in nations around the globe. As inquired, about a portion of these frameworks to familiarize ourselves with current usage, especially Estonia. Estonia has had electronic voting since 2005 and in 2007 was the primary nation on the planet to permit internet voting. In the 2015 parliamentary election 30.5% of all votes were made in the country's i-voting framework.

The bases of this framework are the national ID card that every single Estonian individual are given. These cards contain scrambled records that distinguish the proprietor and enables the proprietor to complete various on the web and electronic exercises including internet managing an account administrations, carefully marking archives, get to their data on government databases and I-voting. (Electronic ID card, no date) Keeping in mind the end goal to vote, the voter must enter their card into a card reader and later get to the voting site on the associated PC. Then at that point they enter their PIN number and a check is made to check whether they are qualified to vote. On successful confirmation, they can cast/switch their vote up until four days before Election Day.

The voter may likewise utilize a cell phone to recognize themselves for I-voting in the event if they don't have a card reader for their PC. Be that as it may, this procedure requires a specific SIM card for the mobile. At the point when a voter presents their vote, the vote is gone through the openly available vote sending server to the vote stockpiling server where it is scrambled and put away until the point when the web-based voting period is finished. At that point the vote has all distinguishing data cleaned from it and is exchanged by DVD to a vote checking server which is detached from all systems. This server decodes and checks the votes and after that yields the outcomes.

Each phase of this procedure is logged and examined. Amid the 2013 Local Election, analysts watched and considered the I-voting process and featured various potential security dangers with the framework. One such risk is the possibility of malware on the customer side machine that screens the client putting their vote and after that later changing their vote to an alternate applicant. Another conceivable risk is for an attacker to specifically taint the servers however malware being put on the DVDs used to set up the servers and exchange the votes.

4. IMPLEMENTATION

A. Architecture

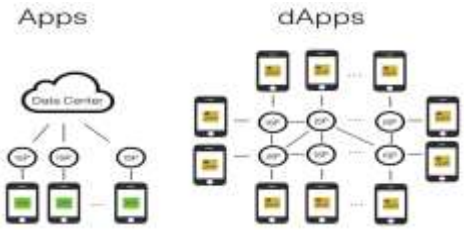

Fig 4.1: Difference between an app and a Dapp

The proposed system which is discussed is not a centralized web application but a decentralised one. The figure above shows the difference between a centralised application and a decentralised one. DApps are applications that utilise the concept of Blockchain which was discussed earlier. ISPs do not locate in to a single server which is the core of the network. In this type of application there is no central server, the data is distributed across various ledgers and the network must work through all the required ledgers that lead to the final one. Below we discuss on how the Dapp's architecture is constructed.

The Fig 4.2 describes the system architecture of the proposed system. In this architecture the client uses a Blockchain client interface for Ethereum or any lightweight client in the front end of the web application. The front end also comprises of web application which is run on Node JS as the server environment. The intermediate section utilizes the web3.js library and its APIs. These APIs are used to interact with the smart contracts which are written for the backend of the application. Finally the backend consists of the blockchain which is embedded with a smart contract. These contracts are invoked when a certain event occurs or is called by the middleware APIs. After invoking these contracts a certain computation is performed on the blockchain. Either a data is posted into the blockchain or retrieved from it. In this case the hash is received and verified.

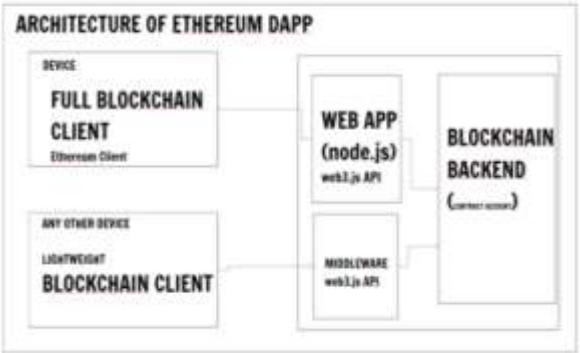

Fig. 4.2: Architecture of proposed system

© 2018, www.IJARIIT.com All Rights Reserved

B. Test network

There are several networks present on Ethereum. The main network is the network where real transactions of ethers take place. In a development environment, paying actual money is not feasible because of the reiterations of the transactions. The other three development test networks are Rinkeby, Kovan and Ropsten. One of these networks had to be chosen for the development test network. Rinkeby was chosen because it provided an environment close to the main network with the Proof of Work consensus algorithm.

C. **Solidity smart contracts**

Initially before constructing the server framework of the application, we first design the interactions of the code with the blockchain. Solidity is statically typed language, meaning type checking is done at compile time over runtime. In the development of this application we require it to perform the necessary interactions with blockchain. These interactions include setting maximum gas limits, setting the amount of ether for the transaction, input the data such as the hash into the blockchain. The coding of the smart contract in the Remix IDE provided by Ethereum. This allows the contract to be deployed onto the blockchain using the Web3.js injection and Metamask.

D. Nodes

With basic foundation to the HTML and CSS of the front end of the application, that is the creation of forms and input fields, the server side of the application was coded in NodeJs. Providing multiple pages of HTML and redirecting/rendering the templates was the task of this framework. Node Js is used to control the flow of the application, meaning upon an event, to which template must the server redirect to and also is used for error validation.

E. Web3.js

Web3.js is a Javascript library which is used to interact with the smart contract which is deployed in the blockchain. web3.js is not only used to help create instances of the smart contract in the application but also to detect the presence of a valid account in the plugin. This helped in validating if the user is valid and has an account or not. It is used to retrieve the transaction id or the hash of the transaction. web3.js is included after the preparation of the basic skeleton of the application.

F. Etherscan API

Etherscan provide APIs to query some of the transactional data on the blockchain. Etherscan also provide APIs for test networks such as Ropstenas well. Using Postman API along with API key provided, the queries were made. This enabled to return a JSON file which comprises of most of the transaction data of the address. Despite these API's being in beta (providing up to 1000 transactions only), the data provide was enough for testing. Retrieval of transaction hash of the address was made possible by parsing through the JSON file and can be compared with the entered hash by the user

5. RESULTS

Fig. 5.1: Organization login

Fig. 5.2: Creation of a ballot

On successful login by the user, he/she can create a ballot by providing the necessary credentials.

Fig. 5.3: Deploy to blockchain

Once the ballot is created, the election is deployed to blockchain to send the unique code (public key) to the voter.

Fig. 5.4: Voter page

The voter casts the vote by entering the unique key.

Fig. 5.5: Cast a vote for a candidate

© 2018, www.IJARIIT.com All Rights Reserved

Fig. 5.6: Acknowledgment of voting

Fig. 5.7: Overview of the transaction

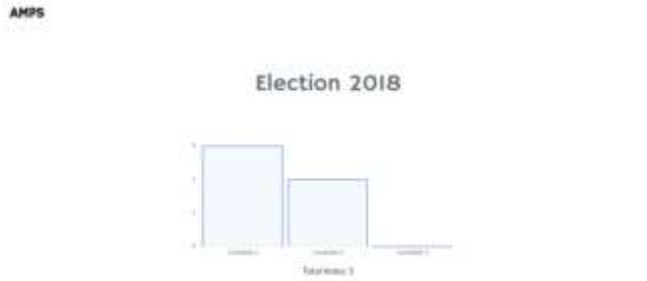

Fig. 5.8: Result page

6. CONCLUSION AND FUTURE WORK

To conclude, our implementation the blockchain containing information of who has registered to vote also allows our service to ensure each voter in unique and as described in section. Once registered you are then allocated to vote after verification of your details has been completed. To ensure these registered voters are who they are, when voting begins the code is verified.

The blockchain in its basic form can be viewed as the decentralized, transparent and chronological database of transactions, at times likewise called the record. The system in which a blockchain fills in as the database includes nodes or laborers. These specialists are in charge of appending new blocks to the blockchain.

Further when the user enters the code before the ballot starts; it informs the user about the timings of the election. And also when he/she tries to cast their votes multiple times it prompts that the votes is already casted and recorded in the blockchain. The user can also verify if the votes is stored in the blockchain. Once after the election ends the result is displayed to the user using the same unique code.

The present system provides single authentication process, where in future an advancement of multi factor authentication can be provided to the users. The present system is used only by the private organizations; an advance step for this process would be by gathering all the government data where the verification can be done by those identities.

7. REFERENCES

[1] Dawes, Sharon S. "Stewardship and usefulness: Policy principles for information-based transparency." Government Information Quarterly 27.4 (2010): 377-383

[2] Christensen, Clayton M. (2003). The innovator's solution: creating and sustaining successful growth. Harvard Business Press. ISBN 978-1-57851-852-4.

[3] Consensys (2015). uPort: The Wallet is the new browser. Available at: https://media.consensys.net/uport-the-wallet-is-the-new-browser-b133a83fe73

[4] Dawes, Sharon S. "Stewardship and usefulness: Policy principles for information-based transparency." Government Information Quarterly 27.4 (2010): 377-383.

[5] Gibson, D., Ostashewski, N., Flintoff, K., Grant, S., & Knight, E. (2015). Digital badges in education. Education and Information Technologies, 20(2), 403-410.

[6] Hanson, R.T., Staples, M. (2017). Distributed Ledgers, Scenarios for the Australian economy over the coming decades. Canberra. Commonwealth Scientific and Industrial Research Organisation.

[7] Jentzsch, C. (2016). Decentralised autonomous organisation to automate governance. Retrieved from https://download.slock.it/public/DAO/WhitePaper.pdf

[8] MIT Media Lab (2016). What we learned from designing an academic certificates system on the Blockchain. Available at: https://medium.com/mit-media-lab/what-we-learnedfrom-designing-an-academic-certificates-system-on-the-Blockchain-34ba5874f196

[9] Smolenski, N. (2016a). Academic Credentials in an era of digital decentralisation. Learning Machine Research.

[10] Vigna, J. and Casey, M.J. (2016). The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order. Picador.

© 2018, www.IJARIIT.com All Rights Reserved