International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195219

An Anonymous off Block Chain Scheme for I-Voting Using Bit Coin in the Real World

Akshaya Selva S[1], Anusuya R V[2], Dhanya N K[3], Sharmila Rani D[4]
[1-3]Department of Computer Engineering, Sri Krishna College of Technology Coimbatore, India
[4]Assistant Professor, Department of Computer Engineering, Sri Krishna College of Technology, India

ABSTRACT

Democratic voting is a crucial and serious event in a country. The most common way in a country votes through a paper based system, but is it not time to bring voting into the 21st century of modern technology Digital voting system uses electronic devices such as voting machines or an internet browser to cast votes. These are sometimes referred to as e-voting where voting use a machine in a polling station and i-voting when using a web browser. Security of digital voting is always the biggest concern to implement a digital voting system. One way the security issues can be potentially solved through the technology of block chain. Block chain technology originates from the architectural design of the cryptocurrency bitcoin. With the use of block chains a secure and robust system for 4 digital voting can be devised. The report outlines our idea of how block chain technology could be used to implement a secure digital voting system.

Keywords : Bitcoin , Blockchain, Distributed Database, Survey.

I. INTRODUCTION

A block chain is a list of records called blocks which are linked using cryptography.Each block contains a cryptographic hash of the previous block and transaction data .By design a block chain resistant to modification of the data.The block chain is typically managed by a peer-to-peer network to a protocol for inter-node communication and validating new blocks. Once recorded the data in a block cannot be altered of all subsequent blocks.Although block chain records are not unalterable, block chain may be considered secure by design and a distributed computing system. With the help of blockchain many people can enter their entries into a record of information and a community of users can control where the record of information is amended and updated. There are many features of blockchain one among is digital ledger.It is accessible across several hundreds and thousands of computer and is not bound to be kept in a single place. Blockchain has already disrupting the financial services sector and this technology which underpins the digital currency- bitcoin transaction. The technology of blockchain is a financial sector so the participants can interact directly and can make transactions across the internet without the interference of a third party. The transaction through Blockchain will never share any information regarding the participants with any other user and it creates a own transaction record by encrypting the identifying information. The most exciting feature of Blockchain is that it highly reduces the possibilities of a data breach. In contrast with the traditional processes in blockchain there are multiple shared copies of the same database which makes it challenging to wage a data breach attack or cyber-attack.Bitcoin is a cryptocurrency and it is a form of electronic cash. It is an decentralized digital

currency that can be sent from one user to another user on the peer-to-peer bitcoin network without any intermediator.Transactions are verified by the network nodes through the cryptography and recorded in a public distributed ledger called a blockchain. Bitcoin was invented and released as open-source software in 2009.Bitcoin are created as a reward for a process known as mining. Bitcoin has criticized for illegal transactions and also it is high electricity consumption and thefts from exchanges and the possibility of the bitcoin is an economic bubble.Most of the people using bitcoin for the investment in an several regular agencies .Bitcoin functions on cryptographic technology and thrives on mining an incentivized technique to generate new bitcoins. It describe the fundamentals of Bitcoin system underlying technical aspects of the network and mining process. The method of mining the concerned opportunities and implications for the benefit of potential miners have also been accessed. Furthermore, we have also provided a comparison of existing mining pools, different types of pool reward scheme and the recent innovations in the Bitcoin industry.

II. RELATED WORKS

Untangling Blockchain: A Data Processing View of Blockchain SystemSystems. Tien Tuan Anh Dinh, Rui Liu, Meihui Zhang, Member, IEEE, Gang Chen, Member, IEEE, Beng Chin Ooi, Fellow, IEEE, and Ji Wang 2018.This paper highlights the state of the art, focusing on private block chains (in which parties are authenticated). The analysis is based on both in-production and research systems in four dimensions: distributed ledger, cryptography, consensus protocol and smart contract.

On Scaling and Accelerating Decentralized Private Blockchains. Wei Xin ; Tao Zhang ; Chengjian Hu; Cong Tang ; Chao Liu ; Zhong Chen 2017. This paper highlights an architecture for distributed private blockchain. At the same time, it also proposes three strategies to improve the scalability of private block chain optimization of block construction, block size and time control optimization, and transaction security mechanism optimization.

G. Zyskind, O. Nathan, A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data", IEEE Symposium on Security and Privacy Workshops, pp. 180-184, 2015.Regarding the mining techniques reported are all less computationally-expensive alternatives to PoW.The PoW is facilitated to trusted nodes;the selection of the miner which adds the new block depends on luck and not on the computations performed by the miner;no computations are required, the miner is chosen according to the age of coin they owns; the miner is chosen according to the amount of space, and not computational capabilities.

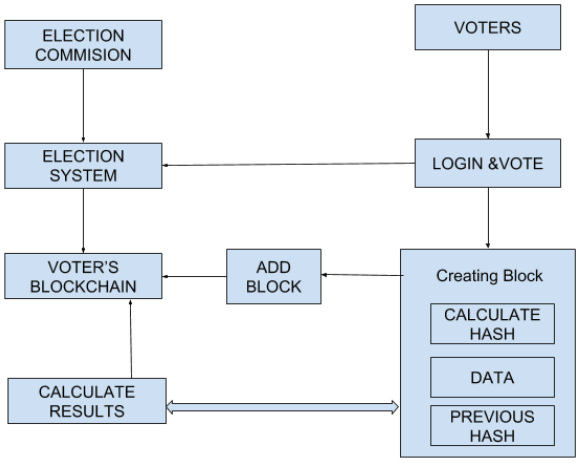
SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies Joseph Bonneau ; Andrew Miller ; Jeremy Clark ; Arvind Narayanan ; Joshua A. Kroll ; Edward W. Felten 2010 .Bit coin has grown to comprise billions of dollars of economic value despite only cursory analysis of the system's design. Since then a growing demand has identified hidden but imminent properties of the system, discovered attacks, proposed alternatives, and singled out difficult future challenges.A large and vibrant open-source community has also proposed and deployed numerous modifications and extensions. This paper provides the first systematic exposition Bit coin and the many related crypto currencies or 'bitcoins.' Drawing from a scattered body of knowledge, three key components of Bit coin's design that can be decoupled have been identified.

III. PROPOSED SYSTEM

The proposed system makes use of SHA 256 (secure hashing algorithm) . There are many cryptographic algorithms that we can choose from, however SHA

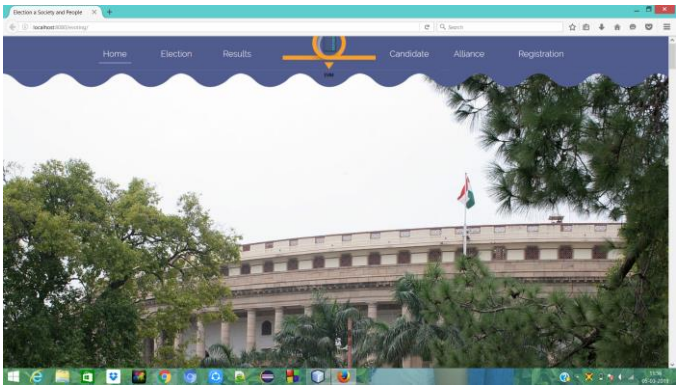
256 fits just fine for this example. java. security. Message Digest is imported to get access to the SHA 256 algorithm. Each block doesn't just contain the hash of the block before it, but its own hash is in part which refers to the digital signature, calculated from the previous hash. If the previous block's data is changed then the previous block's hash will change (since it is calculated in part, by the data) in turn affecting all the hashes of the blocks there after. The hashes are calculated and compared which allows us to see if a blockchain is invalid.

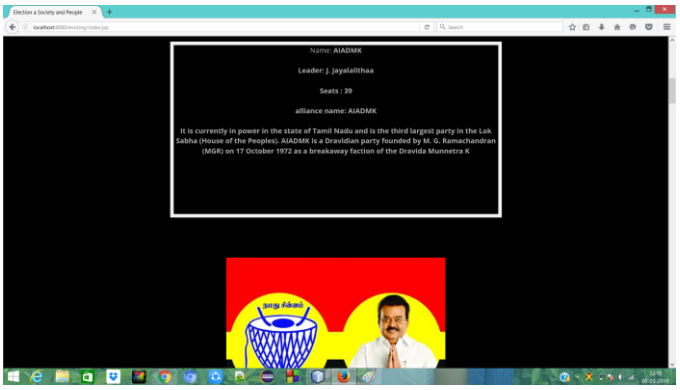
By casting votes as transactions, a blockchain can be created which keeps track of the tallies of the votes.Everyone can agree on the final count because they can count the votes themselves. With the help of the blockchain audit trail we can verify that no votes were changed or removed, and no illegitimate votes were added.

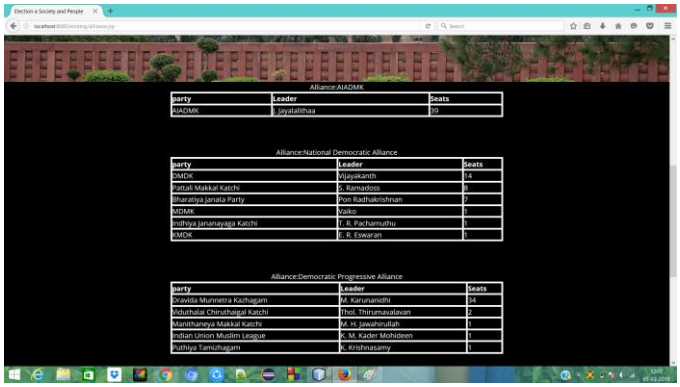


CREATING ELECTION SYSTEM :

The online Election System consists of a candidate registration, admin login which will be handled by the Election Commission .The admin uses the admin login in order to create an election and mention the candidates.The candidate gets into the voting platform using the candidate login.







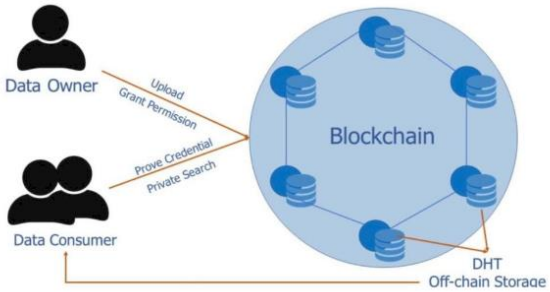
CANDIDATE REGISTRATION & LOGIN :

The voters must first register themselves in the website using their details.Then the voters can log in to cast their votes with their correct username and password.After the validation of the user id and password,an OTP will be sent to the user's mail.The voter is expected to enter the correct OTP before starting to vote.

CREATING BLOCKCHAIN:

Design the Blocks for the Blockchain. Basically, a block contains the following information :

- Timestamp to store the creation date of the Block.
- Hash of the previous Block.
- Vote stored in the Block.
- Hash of the current Block to ensure integrity of its content.



CHECKING THE RESULTS:

The block chains which are created keeps track of the tallies of the votes.The election admin will be able to see the results.

IV. RESULT & DISCUSSION

The i-voting system is implemented using blockchain and bitcoin in order to enhance the security of the voting process. Each voter logs in using a unique user id and password. After the validation, the user will be able to access the election data such as about the candidates, constituencies and voters.

Whenever a user logs in, each one is provided with a bitcoin. When the user votes for a particular candidate, then the number of bitcoin in the user's account decreases by 1 and becomes 0.A blockchain is created for every voter so that all the votes are stored in blocks.

The user cannot vote more than once because everyone is provided with only one bitcoin. The casted votes cannot be changed by any means because it is encrypted using blockchain. Hence it greatly helps in improving the accuracy and efficiency of the system.

V. CONCLUSION & FUTURE SCOPE

- Helps to remove the discrepancies in the already existing e-voting.
- Can be used by voters who live far away from the voting venues.
- In future,it can replace the conventional voting methods such as ballot voting and e-voting.
- Modifications can be done to receive the OTP in user mobile phones.

VI. REFERENCES

[1]. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system,"2008.

[2]. Q. Lin, P. Chang, G. Chen, B. C. Ooi, K. Tan, and Z. Wang, "Towards a non-2pc transaction management in distributed database systems," in Proceedings of ACM International Conference on Management of Data (SIGMOD), San Francisco, CA, USA, 2016, pp. 1659–1674.

[3]. A. Thomson, T. Diamond, S. Weng, K. Ren, P. Shao, and D. J. Abadi, "Calvin: fast distributed transactions for partitioned database systems," in Proceedings of ACM International Conference on Management of Data (SIGMOD), Scottsdale, AZ, USA, 2012, pp.1–12.

[4]. P. Bailis, A. Fekete, M. J. Franklin, A. Ghodsi, J. M. Hellerstein, and I. Stoica, "Coordination avoidance in database systems," PVLDB, vol. 8, no. 3, pp. 185–196, 2014.

[5]. "Ethereum blockchain app platform," https://www.ethereum.org/.

[6]. Ripple, "Ripple," https://ripple.com.

[7]. Melonport, "Blockchain software for asset management," http://melonport.com.

[8]. J. Morgan and O. Wyman, "Unlocking economic advantage with blockchain. a guide for asset managers." 2016.

[9]. Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183-187.

[10]. Deshpande, V., Badis, H., & George, L. (2018, September). BTCmap: Mapping Bitcoin Peer-to-Peer Network Topology. In 2018 IFIP/IEEE International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN) (pp. 1-6). IEEE.

[11]. Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. IEEE Software, 35(4), 95-99.

Cite this article as :

Akshaya Selva S, Anusuya R V, Dhanya N K, Sharmila Rani D, "An Anonymous off Block Chain Scheme for I-Voting Using Bit Coin in the Real World", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 2, pp. 210-214, March-April 2019. Available at doi : https://doi.org/10.32628/CSEIT195219 Journal URL : http://ijsrcseit.com/CSEIT195219