International Journal of Current Engineering and Technology
©2021 **INPRESSCO**®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

E-voting using Block-Chain Technology

Ashwini S Solankar and Prof. S. B. Javheri

PG Student, Department of Computer Engineering JSPM's Rajashri Shahu College of Engineering

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

Expanding advanced innovation has revolutionalized the life of individuals. In contrast to the appointive framework, there are numerous customary employments of paper in its execution. The part of security and straightforwardness is a danger from the still across the board race with the customary framework (offline). General races still utilize an incorporated framework, wherein one association oversees it. A portion of the issues that can happen in customary discretionary frameworks is with the association that has full command over the database and framework. It is feasible to mess with the information of critical chances. Blockchain innovation is one in everything about, on the grounds that it grasps a decentralized framework and the whole database are claimed by numerous clients. Blockchain itself has been utilized in the Bitcoin framework alluded to as the redistributed Bank framework. By embracing blockchain in the circulation of databases on e-casting a ballot frameworks one can decrease the duping wellsprings of database control. This venture intends to execute casting a ballot result utilizing blockchain calculation from each place of decision. Not at all like Bitcoin with its Proof of Work, this will be a strategy dependent on a foreordained turn on the framework for every hub in the worked of the blockchain.

Keywords: *Security and Protection, Hardware, Online Information Services*

Introduction

Of late, electronic choice frameworks have started getting utilized in a few nations. Estonia was the essential inside the world to receive relate degree electronic appointive framework for its national races [1]. Before long, electronic determination was embraced by Schweiz for its state-wide races [2], and by Norway for its gathering decision [3]. For partner degree electronic appointive framework to fight with the standard ticket framework, it needs to help similar criteria the conventional framework bolsters, for example, security and secrecy. An e-Voting framework ought to have increased security so as confirm it's offered to voters anyway shielded against outside impacts dynamical votes from being produced, or shield a voter's tally from being altered. Numerous electronic choice frameworks have confidence in Tor to cover the personality of voters [4]. In any case, this framework doesn't give absolute lack of clarity or honesty since a few insight organizations round the world administration totally extraordinary parts of the net which may empower them to spot or on the other hand capture cast a ballot.[14]

Review of Literature

Progressively computerized innovation in the present helped numerous individuals lives. In contrast to the constituent framework, there are numerous customary employments of paper in its usage. The part of security and straightforwardness is a danger from still boundless decision with the ordinary framework (offline).Block chain innovation is one of arrangements, since it embracesa decentralized framework and the whole database are claimed by numerous users[1].

Bit coin presents a progressive decentralized agreement component. Be that as it may, Bit coin-inferred accord instruments connected to open square chain are insufficient for the sending situations of maturing consortium square chain. We propose another agreement calculation, Proof of Vote (POV).The previous ensures the detachment of casting a ballot right and official right, which improve the freedom of bulter's job, so does the interior control framework inside the consortium. Concerning the last mentioned, under the situation that in any event Nc/2+1 officials are working successfully, our investigation demonstrates that POV can ensure the security, transaction[2].

There is no uncertainty that the progressive idea of the blockchain, which is the hidden innovation behind the acclaimed cryptocurrencyBitcoin and its successors, is setting off the beginning of another time inside the web and along these lines the on-line administrations. In this work, we have actualized and tried an example e-casting a ballot application as a savvy contract for the Ethereum organize utilizing the Ethereum wallets and the Solidity language[3].

Square chain was first presented by Satoshi Nakamoto (a pen name) who proposed a distributed installment framework that permits money exchanges through the Internet without depending on trust or the requirement for a monetary foundation. Square chain is secure by structure, and a case of a framework with a high byzantine disappointment tolerance[4].

Evidence of stake convention of square confirmation doesn't have confidence in over the top calculations. It has been authorized for Ethereum and bound altcoins.

Rather than dissonant squares crosswise over proportionately to the relative hash rates of excavators (for example their mining influence), evidence of-stake conventions split stake squares relatively to the present abundance of excavators. The thought behind Proof of Stake is that it might be increasingly troublesome for mineworkers to procure adequately huge measure of advanced money than to gain adequately amazing processing equipment.[5]

E-casting a ballot is a potential answer for the absence of enthusiasm for casting a ballot among the youthful technically knowledgeable populace. For e-casting a ballot to end up progressively open, straightforward, and freely auditable, a potential arrangement would be base it on square chain innovation. Square chain innovation has a great deal of guarantee; notwithstanding, in its present state it probably won't achieve its full potential.[6]

Electronic casting a ballot has been utilized in fluctuating structures since 1970s with essential advantages over paper based frameworks, for example, expanded proficiency and diminished mistakes. With the remarkable development in the utilization of square chain advancements, various activities have been made to investigate the practicality of utilizing square tie to help a successful answer for e-casting a ballot. It introduced one such exertion which use advantages of square chain, for example, cryptographic establishments and straightforwardness to accomplish a successful answer for e-casting a ballot. The proposed methodology has been executed with Multichain and indepth assessment of methodology features its adequacy as for accomplishing principal necessities for an e-casting a ballot scheme.[7]

Open square chains are open for all. Anybody can go along with them to present exchanges and on take an interest in the mining and agreement procedure of adding new square of exchange to the square chain .These square chains typically utilize Proof of work (PoW) or Proof of Stake (PoS) for accord instrument. Having progressively number of members functions admirably for this model, as it further diminishes the likelihood of a 51% attack.[8]

Permissioned square chains are assembled for the most part by associations for their particular business require. Such square binds Are probably going to have interfaces with existing uses of the association. Associations may settle on consortium square chains where constrained believed individuals compulsorily need to close down an exchange. In completely private square chains, the compose authorization over the square bind is given to a focal association. The previous are alluded to as incompletely decentralized by Buterin.[9]

A conventional augmentation of square tie exchanges to exchange stuff other than digital currency is proposed by Zyskind et al. In their proposed framework, the exchanges are utilized to carry directions for putting away, lining and sharing information. With upgraded scope of versatile applications looking for complete access to client information like contacts, messages, photographs and an assortment of other individual information, Zyskind et al. have given the usage plan of a framework that utilizes square chain alongside a disconnected stockpiling component so as to oversee authorizations expressly for each detail, as opposed to giving total access consent in certainly. Disconnected capacity, for example, Level DB or any distributed storage can be utilized to restrain the measure of information put away in the square chain. This could anyway result in a restricted outsider reliance, yet makes the arrangement more scalable.[10]

Existing System

School Voting System

In Colleges or Organizations, races are directed to choose Secretary and different individuals. Hopefuls might be from various offices so along these lines it is troublesome for them to facilitate vote from that point. An internet surveying framework helps the procedure, with efforts by which they can cast a ballot secretly from any division. This Internet casting ballot framework gives great arrangements to College Voting System but it stays back in giving security and privacy for casted votes. The candidate needs to be physically present to cast the vote. These votes are collected through EVM machines in computer system and analysed through database and winner is declared.Figure below studies the existing voting system.

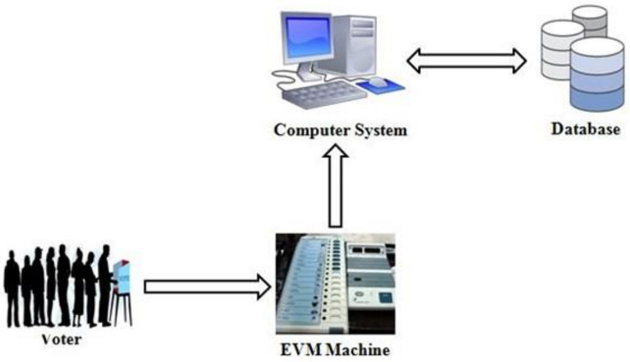


Fig. 1. Existing System Architecture

Proposed System

The square chain innovation utilized for the most part works equivalent to the blockchain innovation contained in the E-casting a ballot framework and spotlights on database recording. The hubs associated with Blockchain that have been utilized by Bitcoin are freely irregular and not tallied. Nonetheless, in this e-casting a ballot framework a blockchain authorization is utilized, for hubs to be made the inverse of the Bitcoin framework and the Node being referred to is a position of general race on the grounds that the place of races must be enrolled before the initiation of usage, it must be clear the sum and the personality. This strategy intends to keep up information honesty, which is shielded from controls that ought not occur in the decision procedure. This procedure starts when the casting a ballot procedure at every hub has been finished. Before the decision procedure starts, every hub produces a private key and an open key. Open key of every hub sent to all hubs recorded in the race procedure, so every hub has an open key rundown all things considered. At the point when the race happens, every hub accumulates the decision results from every voter. At the point when the choice procedure is finished, the hubs will hang tight to make the square. Endless supply of the square on every hub, at that point done check to decide if the square is legitimate. When substantial, at that point the database included with the information in the square. After the database refresh, the hub will check whether the hub ID that was brought as a token is his or not. In the event that the hub gets a turn, it will make and present a square that has been filled in advanced mark to communicate to all hubs by utilizing turn leads in square fasten creation to dodge impact and guarantee that all hubs into square chain. The submitted square contains the id hub, the following id hub as utilized as the token, time stamp, casting a ballot result, hash of the past hub, and the computerized mark of the node.

The square chain with the brilliant contracts,emerges as a decent contender to use in improvements of safer,cheaper, increasingly secure, progressively straightforward, and less demanding to-utilize e-casting a ballot frameworks. In the proposed framework we tackle existing after issues unravel. We require transparency,authentication and provability in the casting a ballot stage. We have to guarantee that the general population who go to the races are genuine individuals and utilize right qualifications that we know in electronic situations, and we ought to probably demonstrate that whenever, likewise we require our decisions are 100% straightforward as wanted. Along these lines, we have to accumulate and check marked and time stepped information of the decisions. Since, no one ought to most likely change the votes after they are threw. Additionally, we require singularity in races, with the goal that no one can vote in favor of another person.[16][15][13]

System Architecture

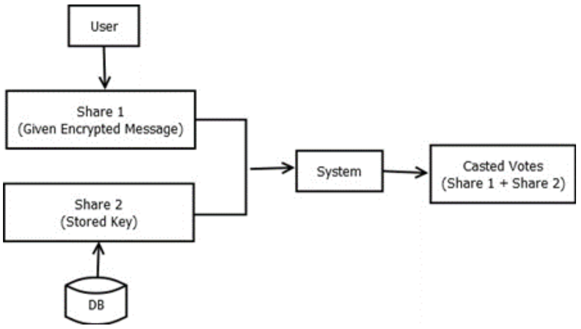


Fig. 2. System Architecture

- Admin: administrator can include competitor, voter, ward, and race. He/she can perform refresh erase task and announced outcome also.
- Visual Cryptography: Administrator (Election officer) sends share 1 to voter email id before the decision and offer 2 will be accessible in the casting a ballot framework for his login amid election. The voter will inspire the mystery secret word to make his choice by consolidating share 1 and offer 2 utilizing VC.
- User: Voter can cast a ballot just in the event that he/she signs into the framework by entering the right secret word which is produced by blending the two offers (Black & White spotted Images)using VC scheme.
- Block Chain: Blockchain is a disseminated database that stores information records that keep on developing, constrained by multiple entities. Square chain (appropriated record) is a dependable administration framework to a gathering of hubs or non-confiding in gatherings, for the most part, the square chain goes about as a solid outsider to keep things together, intervene trades, and give secure processing machines.

Algorithm

A. algorithm-I Cryptography

The purpose of network security is essential to present loss, through misuse of data. Cryptography is Greek word whose meaning is secret writing. Cryptography is process of converting text into another form that is not understandable by eve. Encryption is process of converting plaintext to cipher text using key. Decryption is process of converting cipher text to plaintext by using key which is given by sender. Encryption is done on sender side and decryption is done on receiver side.[18] Cryptography uses two types of algorithms: Symmetric key algorithm and Asymmetric key algorithm.

1. Symmetric Cryptography:

Symmetric Encryption Algorithms can be classified as stream ciphers and block ciphers. Stream ciphers encrypt one bit of image at a time. Block ciphers take a many number of bits and encrypt them as a single unit. Symmetric key algorithm uses same key for both encryption and decryption.

2.Asymmetric Cryptography (Public Key Cryptography)

Asymmetric Encryption Algorithm is also known as public key algorithm. It uses different keys for encryption and decryption. Decryption key cannot be obtained from encryption key. The secret message can be communicated securely .

B. Algorithm-II Technique Used

1. AES:

The Advanced Encryption Standard, or AES, is a symmetric block cipher to protect classified information and is implemented in system to encrypt sensitive data. AES comprises three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. The Rijndael cipher was designed to accept additional block sizes and key lengths, but for AES, those functions are not adopted.

2. Visual Cryptography:

Visual Cryptography Scheme (VCS) is a method used for protecting image-based secrets and has a computation-free decryption process. In (2, 2) VCS each secret image is divided into two shares in such a way that no information can be obtained from any single share. Transparencies are printed in each share. Two shares are stacked and secret image can be visualized by human eye without any complex cryptographic computations and this is called decryption as shown in figure below Each pixel P of the secret image is encrypted into a pair of sub-pixels in each of the two shares.[19]

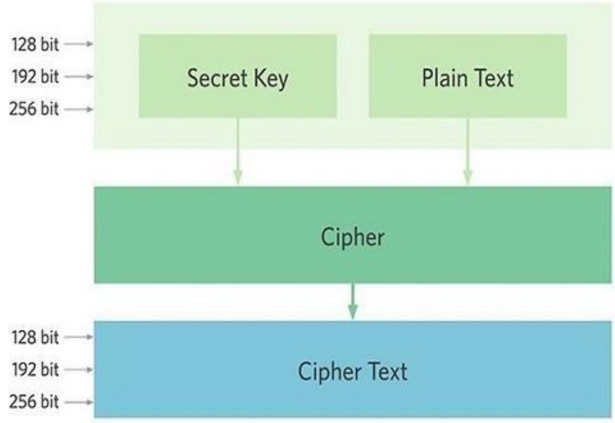


Fig. 3. AES

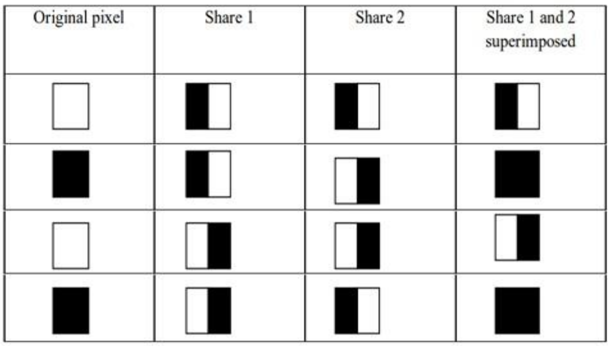


Fig. 4. Visual Cryptography Scheme

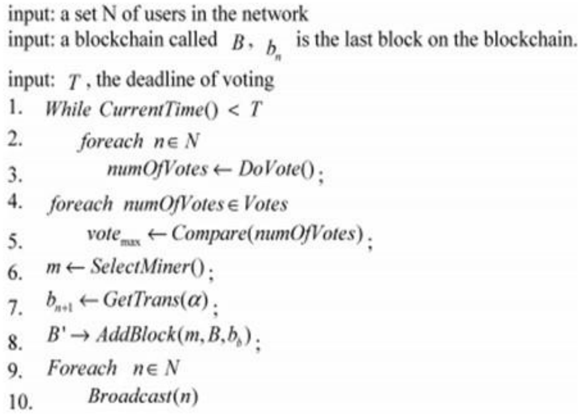
C. Algorithm-III Block chain

Algorithm in figure 5 is used to create the block embedded with voting information.AES and Visual Cryptography is applied for security.

System Requirements

A. Software Requirement

In this project software technology used Java, Tools JDK 1.8, IDE Netbeans 8.2 and operating system windows 7 or above.



```
input: a set N of users in the network
input: a blockchain called $B$, $b_n$ is the last block on the blockchain.
input: $T$, the deadline of voting
While $CurrentTime() < T$
    foreach $n \in N$
        $numOfVotes \leftarrow DoVote()$;
foreach $numOfVotes \in Votes$
        $vote_{max} \leftarrow Compare(numOfVotes)$;
$m \leftarrow SelectMiner()$;
$b_{n+1} \leftarrow GetTrans(\alpha)$;
$B' \rightarrow AddBlock(m, B, b_b)$;
Foreach $n \in N$
        $Broadcast(n)$
```

Fig. 5. Algorithm

B. Hardware Requirement

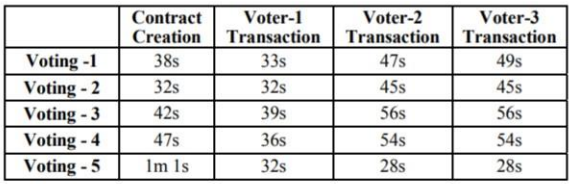
The hardware requirements is hard disk 80GB, RAM 2GB or above, Processor Intel Pentium 4 and above.

Advantages

1) The main advantage of the system is secure voting system.
2) The proposed system is user friendly.[17]

Result and Discussions

In Table I, 5 test ballots are presented. We calculated the time spent in each vote for all voters. Voter 1 is the one who creates the test-election, and has the right to vote initially, but other voters do not have this right to vote, therefore we should give them the voting permit.Voting permit or verfication is done with help of OTP .It usually adds one block creation time to their voting time. As can be seen in the table, generally voter 1 is faster than others during casting their votes. All transactions can be run asynchronously, so voter 3 doesn't have to wait others. The cause of the time variation in experiment is the block creation and workload in the Rinkeby network. But, it never exceeds one minute.



	Contract Creation	Voter-1 Transaction	Voter-2 Transaction	Voter-3 Transaction
Voting -1	38s	33s	47s	49s
Voting - 2	32s	32s	45s	45s
Voting - 3	42s	39s	56s	56s
Voting - 4	47s	36s	54s	54s
Voting - 5	1m 1s	32s	28s	28s

Fig. 6. Experimental Analysis Table

In this system, our scope is limited for small-scale polls and elections. A larger voting with millions of voters may have different problems to address. The Ethereum network's scalability is still unknown and needs further research, that's why we cannot suggest use of these contracts for nation-wide elections, at least for now. Our contracts are executed in the Ethereum block chain, so wherever Ethereum wallet can be run (location, platform, device, etc.), our voting application can be used, too. Right now, the Ethereum wallet is supported in Linux, OS X, and Windows platforms.

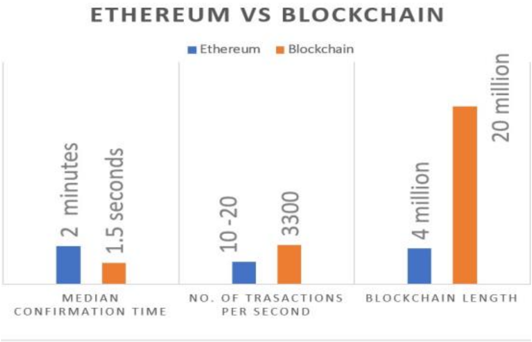


Fig. 7. Comparison of Blockchain and Ethereum

Also, a person who will vote should have a small amount of Ethereum coins, to be able to execute the voting application and to cast a vote. A fundamental problem of block chain based e-voting systems is to provide anonymity for voters without compromising the transparency of the general voting process. While both Bitcoin and Ethereum are powered by the principle of distributed ledgers and cryptography, the two differ in many technical ways.

Conclusion

A country with less casting a ballot rate will battle to create as picking a correct pioneer for the country is exceptionally fundamental. Our proposed framework intended to give safe information and a reliable E-casting a ballot among the general population of the majority rules system. Square chain itself has been utilized in the Bitcoin framework known as the decentralized Bank framework. By embracing square chain in the dispersion of databases on e-casting ballot frameworks one can diminish the deceiving wellsprings of database control. This task plans to execute casting a ballot result utilizing square chain calculation from each place of race. The objective of the system is to provide a flexibility to allow casting vote from any remote place and provide security measures by visual cryptography.

References

[1]. Ahmed Ben Ayed,"A Conceptual Secure Block Chain-Based Electronic Voting System",2017 IEEE International Journal of network & Its Applications(IJNSA),03 May 2017.

[2]. Budi Rahardjo, "Blockchain Based E-Voting Recording System Design", IEEE 2017.

[3]. Yongle Chen, "Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain", IEEE 3rd International Conference on Data Science and Systems.

[4]. EmreYavuz, "Towards Secure E-Voting Using Ethereum

[5]. Blockchain",2018 IEEE.Vrushali Kulkarni, "Blockchain and Its Applications – A Detailed Survey", International Journal of Computer Applications 2017.

[6]. Konstantinos Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy",IEEE 2018,03 July 2018.

[7]. Junaid Arshad, Muhammad Mubashir Khan, "Secure Digital Voting System based on Blockchain Technology", IEEE 2017.

[8]. Huaiqing Wang, Kun Chen and DongmingXu. 2016. A maturity model for blockchain adoption.

[9]. Buterin, Vitalik. 2015, On Public and Private Blockchains.

[10]. Zyskindet. al. 2015. Decentralizing Privacy: Using Block chain to Protect Personal Data, 2015 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, July 2015.

[11]. Gallup, "Trust in Government," Gallup, 30 September 2015. [Online]. Available: http:// www.gallup.com /poll/ 5392 /trust-government.aspx. [Accessed 28 Septmeber 2016].

[12]. Wikipedia, "List of controversial elections," 20 September 2016. [Online]. Available: https: // en.wikipedia.org /wiki /List-of-controversialelections. [Accessed 27 September 2016].

[13]. R. Skudnov, "Bitcoin Clients," Turku University of Applied Sciences, Turku, 2012.

[14]. Affectiva, "Affective Product Overview," 15 January 2016. [Online]. Available: http:// www.affectiva.com /wp-content /uploads/2014 /11/Affectiva Product Overview.pdf. [Accessed 28 September 2016].

[15]. P. Noizat, "Blockchain Electronic Vote," in handbook of digital Currency, Paris, Elsevier Inc., 2015, pp. 453-461.

[16]. The electoral knowledge network, "Cost of Registration and Elections," ACE Project, 15 Jan 2016. [Online]. Available: http://aceproject.org /aceen /focus/core /crb/crb03. [Accessed 28 September 2016].

[17]. N. Uribe, "10 Benefits of Electronic Voting," 01 August 2016.

[18]. [Online]. Available: http://www.fobsoftware.com/ blog/10-benefits-ofelectronic-voting-for-home-ownerassociations. [Accessed 28 September 2016].

[19]. G. Schryen, "Security Aspects of Internet Voting," in IEEE, Hawaii, 2004.

[20]. Ambritha,T Sri, J Jebarani, J Selvarani, Pradhiba. (2016). Comparative Study of Various Visual Cryptography Techniques to Analyze the Quality of Reconstruction. International Journal for Research in Applied Science and Engineering Technology. 4. 800-806.