International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 24th Mar 2020. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-03

Title: **BLOCK CHAIN BASED DECENTRALIZED SECURE ELECTRONIC VOTING SYSTEM USING RSA CRYPTOGRAPHIC ALGORITHM**
Volume 09, Issue 03, Pages: 71-78.
Paper Authors

S.PHANI PRAVEEN, D.SWAPNA, A.MADHURI, S SINDHURA, T BALAMURALI KRISHNA

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

BLOCK CHAIN BASED DECENTRALIZED SECURE ELECTRONIC VOTING SYSTEM USING RSA CRYPTOGRAPHIC ALGORITHM

S.PHANI PRAVEEN, D.SWAPNA, A.MADHURI, S SINDHURA, T BALAMURALI KRISHNA

Assistant Professors[1,2,3] Dept of CSE, PVPSIT, Vijayawada.

Assistant Professors[4,5] Dept of CSE, SSIET, Nuzvid.

Abstract: The electronic voting has developed as a substitution to the paper-based democratic voting to lessen the redundancies and irregularities. The recorded point of view displayed over the most recent two decades proposes that it has not been so fruitful because of the security and protection flaws detected at that time. In recent times, researchers discover that block chain can give an option secure policy for e-casting ballot frameworks, as a result of its features of transparency and tamper resistance. This paper suggests a decentralized internet casting a ballot framework executed as a smart contract on the Ethereum block chain which ensures voter confidentiality by utilizing RSA encryption framework and stores proofs for every component of a vote.

Keywords: Decentralized voting · Ethereum block chain Smart contract

Introduction

Will of the individuals is an all around regarded wonder for portrayal of assessment in arrangement of constituent bodies. These appointive bodies shift from the school associations to the parliaments. Throughout the years, 'vote' has risen as an apparatus for speaking to the desire of the individuals when a determination is to be settled on among the accessible decisions. There are numerous types of discretionary strategies, shifting from the customary paper polling form to E-casting a ballot. The customary method for utilizing paper voting form is the most well known and least demanding to get to, nonetheless, it despite everything exists a basic issue. As indicated by the author of Follow My Vote [1]–Nathan Hourt , the respectability of the paper-put together political race despite everything depends with respect to the trust that the authorities leading their employments effectively and sincerely all through the procedure. In this way, there are chances that the outcome may have altered without individuals' awareness. That is the reason we have to wipe out the manual democratic framework. Individuals have concocted Electronic Voting Machines (EVM). The presentation of EVMs got an extraordinary leap forward in India. These EVMs require no manual voting. Voters needed to simply press the catch related with the gathering they need to cast a ballot. The presentation of EVMs has helped us to beat just the conceivable human blunders. Be that as it may, the issue with the trust of incorporated authority is left. Blockchain wipes out the need of a focal server to oversee organize and a brought together database along

these lines guaranteeing trust. It is a finished decentralized open record framework. The open record records all the votes threw and are perpetual and unchanging. It guarantees that no vote can be changed once threw. On the off chance that somebody attempts to control the record, they have to initially hack every past square before including new square, which is about outlandish as a result of accord component. Keeping up the protection and security of voters is the need for our web based democratic framework. Our proposed decentralized democratic framework utilizes the RSA calculation of the cryptographic framework makes it conceivable to count scrambled votes legitimately without unscrambling them.

Our proposed framework likewise consolidates cryptographic evidences to guarantee the honesty of the democratic procedure and to confirm the legitimacy of each vote before it is spared to the blockchain by following security prerequisites [2], for example, Eligibility of voters, Multiple-casting a ballot Detection, Privacy of voters, Integrity of ballot, Correctness of counted Result.

Related Work

Right now, have examined the foundation of the blockchain innovation and other related terms, which is help to us to structure an increasingly secure and powerful electronic democratic framework. Cryptography is basically the act of scrambling certain information or data with the goal that it tends to be stayed quiet from outsiders. Cryptography has been used for everything from the Allied forces sending military messages forward and backward during World War 2 to Julius Ceaser using figures to send mixed messages to his officials during old events. There are different ways that cryptography may be applied to a small piece of data[8][9]. At present, the letters in a message are developed by utilizing transposition figures. This is an essential use of the possibility of cryptography.The techniques for actualizing cryptography to information have gotten essentially increasingly mind boggling. Presently, unfathomably complex PC and numerical innovation can be utilized to scramble information in more confused manners than any time in recent memory before. No matter how entangled the cryptography is, it generally chips away at a similar fundamental rule; encode information and conceal its actual importance so just an individual with consent can decode it. In 2014, in Russia, the city of Moscow's Active Citizen program was propelled [3]. Numerous surveys had been directed from that point forward on assorted subjects like what ought to be the shade of seats in another games field, and so on [4]. In 2017, in South Korea a brilliant agreement based blockchain empowered democratic framework was utilized [5]. All the significant information like votes and results was put away on a blockchain. There was no association of any focal position or the board all the while. As of late, Yu et al. [6] proposed a stage autonomous e-casting a ballot scheme based on block chain, which suggests that adjustments in the basic block chain protocols would not influence the democratic framework. Nonetheless, in their plan, there is a amazing "casting a ballot overseer", who creates general society and mystery keys for ballot

encryption and unscrambling so he can know the between time result easily. Thus, if the executive connives with one of the applicants, the candidates can alter his/her technique in time as indicated by the break result. In 2017, McCorry et al. [7] proposed a decentralized and self-counting e-voting protocol utilizing blockchain without a counting authority, called open vote network. It accomplishes a decent security and obscurity. Notwithstanding, the calculation overhead is huge. It requires O(n) augmentation activities for a voter to process a public parameter (the recreated key), where n is the complete number of voters. If utilizing the calculation to the chain, for example utilizing shrewd agreement, it would cost a lot of blockchain calculation asset and just backings all things considered 50voters' remade enters in one Ethereum exchange, as a result of the gas limit of Ethereum, which restricts the quantity of voters .At this moment, am going to cover a secure E-Voting structure show using open key cryptography. This show is consolidated in three techniques, at first find a good pace which incorporates the ID and confirmation stages for the applied occupants. In addition, the majority rule methodology which will be done by calculating the voter information using open key encryption cryptosystem (RSA), to be submitted over a temperamental framework to the predefined government political race server. Finally, the political choice server supervisor will sort the indisputable result by deciphering the received mixed information using RSA private key. Taking everything into account, this E-Voting show is more capable than others E-Voting shows since the voter can cast a polling form from his/her own one of a kind (PC) with no extra cost and effort. The RSA open key encryption system ensures the security of the proposed show. In any case, to thwart a savage force ambush, the choice of the key size gets fundamental.

Public-Key Encryption:

The open key cryptosystem thought was made by Diffie-Hellman in 1976. The RSA figuring is the essential encryption show subject to the open key thought, which was appropriated by Revist, Shamir and Adleman in 1978. In RSA, one key is known to open (recipient's open key), and is used to scramble the information by the sender. The other key is known as a private key, and it is used to unscramble the encoded data got by the gatherer (beneficiary's private key).Only two or three open key counts are both secure and sensible. Among these, some are suitable for encryption. While the others are only sensible for electronic signatures. Some of the counts are Integer Factorization, Discrete Logarithm issue, Probabilistic system, Elliptic bend.RSA Public-key Encryption Protocol: The RSA convention is the most broadly utilized open key encryption calculation. It might be utilized to give both mystery and advanced marks. The RSA security depends on the recalcitrance of the whole number factorization issue. Notwithstanding, there are three numbers e, d and n utilized in the encryption and unscrambling calculation, where $n = p \times q$, with p and q being enormous primes..

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Key generation	n = P * Q d * e = 1mod Φ(n)
Encryption	c = m^e mod n Public Key(n,e)
Decryption	m = c^d mod n private key (d)

Human Unreliability in Cryptographic Protocols:

Non-programming designing specialists have a limited appreciation of PC security thoughts and how to use its applications. Additionally, the International Journal of Network Security and Its Applications (IJNSA), past law based shows are mentioning that the inhabitants become pros in a cryptographic show too in the quick narrative electronic (DRE) throwing a polling form machine. In any case, the security in DRE machine relies upon how the voters will choose their decisions, the associations between the DRE and voter, and the warily checking for the DRE's yield. Ethereum gives a characteristic stage to our distributed casting a ballot framework, in that it gives a decentralized "open notice board" to bolster coordination among voters. The execution of the political race procedure is upheld by similar accord components that make sure about the Blockchain. The smart contract code is put away on the Blockchain and executed by all friends to reach accord on its output. We present a basic democratic agreement written in Ethereum's Solidity language.

Proposed Methodology

Right now present our proposed decentralized, self-counting, positioned choice,smart contract-based democratic framework. The essential thought is as per the following: Numerous past examinations on E-Voting strategy have been done and centred on encouraging the E-Voting technique. These strategies are experiencing different shortcomings, for example, voters' weariness, the necessary equipment cost, and the required surveying places. Right now, proposed strategy depends on the examination of the different variables that assume a huge job in the past E-Voting strategies. In this manner the proposed convention is limiting the voters' depletion since the voters can cast a ballot by utilizing his/her own PC and the necessary time to gather and break down the conclusive outcomes. In any case, the proposed convention depends on RSA open key encryption convention. Whereby, the RSA is utilized to ensure data it is open just to approve elements and is distant to other people. Too RSA is utilized likewise to ensure data stays unaltered from the source substance to the goal element. For the most part, the proposed technique portrays three stages for electronic democratic framework by utilizing the open key E-Voting convention. These means are: the framework get to control process that is to confirm the voter on the political race server, the democratic procedure, and gathering information process.

System Access Control Process:

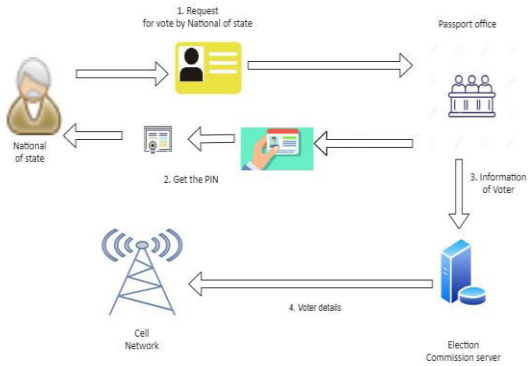
System Access Control Process is one of the cryptographic organizations, which is used to approve the voter in the

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

organization political choice server. This methodology is the underlying stage in the proposed E-Voting system that prepares the voter to be affirmed in the impelled E-Voting process. In like manner, the system finds a good pace Identification phase and Authentication period.

a.) Identification stage:

At the present time, Department of Civil Status and Passports expect the essential employment, whereby it watches that the occupant can cast a polling form legally. The inhabitant should visit the Department of Civil Status and Passports to affirm his/her information to get the political race right. At the point when the occupant enrolled in the Department of Civil Status and Passports, the inhabitant becomes asserted voter. The voter data will be saved in the predefined political race server and a while later went to PDA Company for advance technique.



b) Verification stage:

The variables that are required to direct the E-Voting process are the product and equipment related elements. Right now, voter can get to the democratic procedure just by utilizing his/her PC. The voter login to the E-Voting site by using his/her national_ID and PIN numbers as in International Journal of Network Security and Its Applications (IJNSA). At the point when the voter set apart to the political race website, the political race cut off will deliver a prepared RSA open key. This open key will be then prompt passed by convenient association as a short adaptable message (sms) to the voter. Note that, the tolerant of the open key shows that the voters are set up for throwing a polling form system immediately.

To caste the vote voter will sign in into the Electronic-voting website by using Registered ID and Personal Identification Numbers. After signing in RSA key will be generated and sent as SMS to the specified phone of the voter. After the voter enters the sent key then they are eligible to poll a vote from the system.

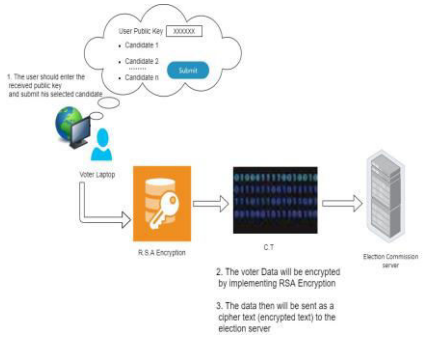
c) Casting a ballot Process:

Normally, the democratic procedure is exceptionally basic since the voter can't logout subsequent to accepting the open key. In any case, the voter is presently ready to choose his/her up-and-comers from the political decision site. As will to upgrade the speed of the democratic procedure, the political decision site will just show the names of competitors as the voter certain division.

In the wake of choosing the applicants and embedding's the got open key through the political decision site, the voter should tap on the submit catch to send his/her choice to the political decision server. Along these lines, the RSA encryption calculation is executed to encode the voter data which will be then sent as a cipher text (scrambled content) to the administration political race server. As will as, toward the finish of the booked time of casting a ballot, the gathering information procedure

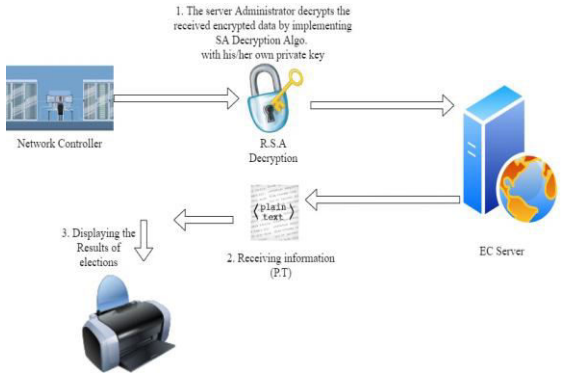
International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

will be enacted for tallying votes and affirm the conclusive outcomes.



d) Collecting Data Process:

The third step in the proposed technique is that the collector (server Administrator) utilizes the determined RSA private key to decode the external scrambled data. At long last, the Administrator will report the democratic outcome to general society.



Results Analysis

This segment talks about the presentation of our proposed casting a ballot framework. The investigation depends on the calculation time of each handling step, isolated into 4 stages, identification, verification, casting ballot, collecting data. In our proposed convention, each vote is encoded twice utilizing various keys (normal key of political race manager and mystery key of the voter,). All tests were performed utilizing a 512-piece key (pis512-bit), which gives a higher security level than one-time encryption utilizing a 1024-piece key. We tried our proposed convention utilizing an elite execution of libgmp by means of the gmpy2 python module, on a PC with the accompanying determinations: 2.8 GHz quad-center Intel Core i7 with 6 MB shared L3 store and with 16 GB of 1600 MHz DDR3Lon-board memory.

The performance can be analysed for the following aspects:

Total Computation Time: we use T_{voter} to denote the total time spent before submission (including the proof generation time), where

$T_{voter} = (t_E*n_c+t*n_c)+ (3*n_c*t) + (3*t)=(6n_c+3)t$

In this experiment, we tested T_{voter} in five rounds, varying the number of candidates (n_c =3,5,10,15,20). The result is shown in (a) Fig.1. From the results in (a) Fig.1, we can see the time cost for casting a vote is less than 12ms even if there are 20 candidates to be ranked.

Total Submission Size: We assume the size of digital signature is 1024-bit and we use S_{vote} to denote the total submission size for a voter.

$S_{vote} = (1024*n_c)+ (2048*n_c)+ (2048+512+2*n_c*512)+(1024) = 4096*n_c +3584$

The total result is shown in Fig.2 based in different numbers of candidates (n_c=3,5,10,15,20). From the result of Fig. 2, we found the submission size of one vote is less than 11KB even for a 20 candidate ballot.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

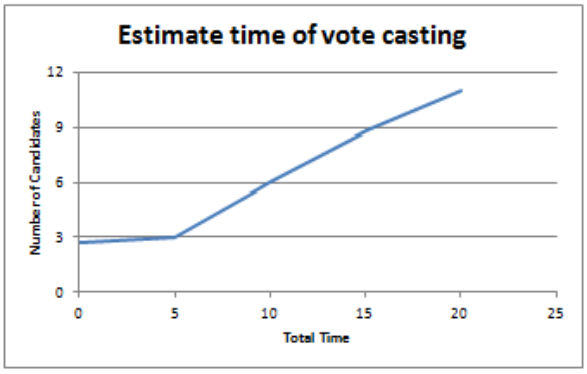


Fig1: Estimate time of vote casting

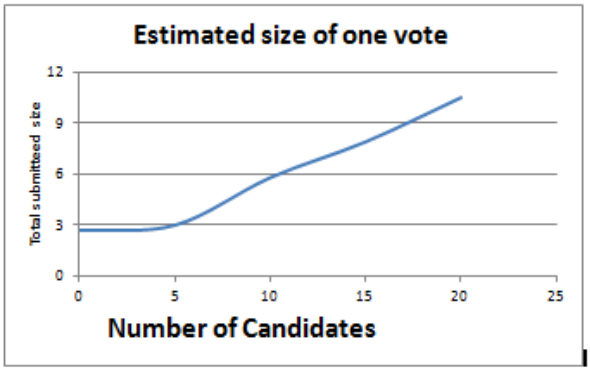


Fig2: Total submission size

Conclusion

The security of the proposed E-Voting relies upon RSA open key encryption convention. The convention we talked about is more productive than the other E-Voting conventions. It permits the voter to cast a ballot from his/her very own (PC) with no additional expense and exertion.

As new innovation for electronic democratic convention, this convention is proposed to supplant the questionable past democratic framework, since voters feel reasonably certain that their votes will be checked. Just as, the proposed convention needs just the essential necessities, for example, PC, web association, casting a ballot site and standard cell phone.

References

1) Followmyvote.com. Introducing a secure and transparent online voting solution for the modern age: Follow My Vote (2016).
2) Yang, X., Yi, X., Nepal, S., Kelarev, A., Han, F.: A secure verifiable ranked choiceonline voting system based on homomorphic encryption. IEEE Access (2018)
3) M. Hochstein, "Moscow's Blockchain Voting Platform Adds Service for High-Rise Neighbors," CoinDesk, 15 Mar. 2018; https://www.coindesk.com/moscows-blockchain-voting-platformadds-service-for-high-rise-neighbors, 2018.
4) M.D. Castillo, "Russia Is Leading the Push for Blockchain Democracy," CoinDesk, 2018; https://www .coindesk.com/russiascapital - leading-charge-blockchain– democracy, 2018.
5) "South Korea Uses Blockchain Technology for Elections," KryptoMoney, https://kryptomoney.com/south-korea-usesblockchain-technology-for-elections, 2017.
6) Yu, B., et al.: Platform-independent secure blockchain-based voting system. In:Chen, L., Manulis, M., Schneider, S. (eds.) ISC 2018. LNCS, vol. 11060, pp. 369–386. Springer, Cham (2018).https://doi.org/10.1007/978-3-319-99136-820
7) McCorry, P., Shahandashti, S.F., Hao, F.: A smart contract for boardroom votingwith maximum voter privacy. In: Kiayias, A. (ed.) FC 2017. LNCS, vol. 10322, pp.357–375. Springer, Cham

(2017).https://doi.org/10.1007/978-3-319-70972-720.

8) Swapna D., Praveen S.P. (2020) An Exploration of Distributed Access Control Mechanism Using BlockChain. In: Satapathy S., Bhateja V., Mohanty J., Udgata S. (eds) Smart Intelligent Computing and Applications. Smart Innovation, Systems and Technologies, vol 160. Springer, Singapore.
9) Swapna, D., Praveen, S.P.: Enhanced block chain-based electronic voting system. JARDCS Special Issue **10**(7) (2018). ISSN: 1943-023X.