International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Survey on Blockchain Based Online Student's Leader Election System Formulated by ECC And ECDSA Hashing Algorithm

Vivek Anand M [a], *Bharath Veerakumar S* [b], *Charan U A* [c], *Naveenkumar G* [d]

[a] Assistant Professor, Department of Information Technology, Kumaraguru College of Technology, Tamil Nadu, India.
[b] Student, Department of Information Technology, Kumaraguru College of Technology, Tamil Nadu, India.
[c] Student, Department of Information Technology, Kumaraguru College of Technology, Tamil Nadu, India.
[d] Student, Department of Information Technology, Kumaraguru College of Technology, Tamil Nadu, India.

ABSTRACT

The election plays an important role in governance and administration. The word VOTE means to select leader or representation. Voting is every individual's right and no one can interfere they are rights by misusing. Online voting system emerged as a current trend. The voting system in college deals with electing the representatives like leaders, president, vice president, secretary etc. This pape deals with electing the student's leader in the college. The voting system is implemented using blockchain technology.

Keywords: ECC, ECDSA.

1. Introduction

"SURVEY ON BLOCKCHAIN BASED ONLINE STUDENT'S LEADER ELECTION SYSTEM" can offer a transparent, secure and decentralized way to conduct elections and other types of voting. Here are some key points that could be included in an introduction to such a system. Online voting systems using blockchain technology can provide a more secure and transparent way to conduct elections, as all votes are recorded and stored in a tamper-proof manner on a decentralized network of computers. The use of cryptographic techniques and digital signatures helps to ensure the integrity and confidentiality of each vote, as it makes it difficult for anyone to alter or tamper with the voting data. Because all transactions on a blockchain are recorded and stored in a transparent manner, it is possible for anyone to see the entire history of a particular blockchain. This transparency helps to build trust and confidence in the system, as it allows anyone to verify the accuracy of the votes being recorded. The decentralized nature of blockchain technology makes it much more difficult for a single entity to exercise control or manipulate the system. This helps to ensure fairness and impartiality in the voting process. A college voting system using blockchain technology could bring numerous benefits to the voting process. By using a decentralized, secure ledger to record and verify votes, a college voting system using blockchain could provide election results with a tamper-proof record and high confidence in integrity of the voting process. This system could be particularly useful for colleges and universities with a large, dispersed student body, as it would allow students to cast their votes from any location.

2. Literature Survey

The previous online voting systems are nothing but a simple web application. Some minor level organizations elect their representatives through google forms, microsoft forms. The voting system is also designed using blockchain. But it was formulated by various algorithms like DSA, RSA etc.

Table 1 – Literature survey

Paper Title	Authors	Year	Inference
[1] Web-based open-audit voting	• Adida, B • Helios	2008	• Simple web application. • Easy to hack. • Less security features.

Paper Title	**Authors**	**Year**	**Inference**
[2] Scantegrity: End-to-end voter-veriable optical- scan voting	• Chaum, D. • Essex, A. • Carback • R., Clark, J. • Popoveniuc, S. • Sherman, A. • Vora, P.	2008	• First end to end verification mechanism. • Does not require manual recount. • Based on optical scan voting.
[3] Star-vote:A secure, transparent, auditable, and reliable voting system	• Bell, S., • Benaloh • Byrne • M. D., Debeauvoir • D.,Eakin, B. • Kortum • McBurnett • N., Pereira • O., Stark • P. B., Wallach • D. S., Fisher • G., Montoya, J. • Parker, M. • Winn, M	2013	• Based on Mega-star voting system. • Does not include Blockchain.
[4] A fair and robust voting system by broadcast	• Dalia, K. • Ben, R. • Peter Y. A • Feng, H	2012	• Maintaining secrecy of ballot by decisional Diffie–Hellman (DDH) assumption. • Based on DDH cryptography algorithm.
[5] Votereum: AnEthereum-based E-voting system	• Linh Vo-Cao-Thuy • Khoi Cao-Minh • Chuong Dang-Le-Baoand Tuan A. Nguyen	2019	• Implemented using Blockchain. • The proposed system is based on etherium. • It is implemented with private blockchain network, smart contract, and web service
[6] Online Voting: Voting System Using B-chain	• Vaibhav Anasune • Pradeep Choudhari • Madhura Kelapure • Pranali Shirke Prasad Halgaonkar	2019	• Distributed Ledger Technology(DLT) • Eliminates illegimate votes.
[7] Decentralized Voting Platform Based on Ethereum Blockchain	• David Khoury • Elie F. Kfoury • Ali Kassem • Hamza Harb	2018	• Etherium based voting application. • SMS authentication. • It restricts multiple votes per mobile.
[8] Survey on Blockchain Based E-Voting Recording System Design	• Bhavani . G	2018	• SHA 256 Algorithm • AES Algorithm • Includes fingerprint verification.

Paper Title	Authors	Year	Inference
[9] Blockchain-Based E-Voting System	• Friðrik Þ. Hjálmarsson • Gunnlaugur K. Hreiðarsson,	2018	• Based on Distributed Ledger Technology. • Improved security by implementing blockchain. • Smart contract based on Go-Etherium (Geth)
[10] Blockchain Based E-Voting Recording System Design	• Rifa Hanifatunnisa • Budi Rahardjo	2017	• Stimulation done using Pycharm. • Using digital signatures to make legitimate block.

3. Scope and features

3.1 Scope

The proposed system is implemented in a private organization where the representatives or leaders elected through the online voting. The proposed system has strong security aspects because it was implemented using Blockchain technology, signature generation through ECC algorithm and hashing using ECDSA algorithm. The system has a wide scope that can be implemented in various organizations like public and private communities, government, industries and various associations where election plays a major role to select their representatives.

3.2 Features

- Highly secured
- Transparent
- No third party influence
- Very tough to hack
- Ensuring the privacy of the voters
- Avoid tedious paper filtering method
- No illegitimate votes

4. Methodology

4.1 ECC algorithm

ECC is abbreviated as Elliptic Curve Cryptography. It is one of public-key cryptography. It is based on the algebraic structure of elliptic curves. It is commonly used in blockchain and other applications to provide secure communication and protect against cyber attacks. In ECC, encryption and decryption of messages are done or happens through public key and private key. The private key works or acts like a secret key for the owner, while the public key, other users can be used to verify the authenticity. ECC algorithm provide high level of security compared to other algorithms, but with smaller key sizes. This makes it more efficient and faster to use, especially in applications with limited computational resources, such as mobile devices or IoT (Internet of Things) devices. ECC is also resistant to certain types of attacks, such as the attack on the discrete logarithm problem, which makes it a secure choice for use in blockchain and other applications. Overall, ECC is an important cryptographic algorithm that is widely used in blockchain and other applications to provide secure communication and protect against cyber attacks.

4.2 ECDSA algorithm

ECDSA is abbreviated as Elliptic Curve Digital Signature Algorithm. It is commonly used in blockchain and other applications to provide a secure, digital way to sign messages and documents. In ECDSA, encryption and decryption of messages are done or happens through public key and private key. The private key works or acts like a secret key for the owner, while the public key, other users can be used to verify the authenticity. One of the main advantages of ECDSA is that it provides a high level of security and is resistant to certain types of attacks, such as the attack on the discrete logarithm problem. It is also more efficient and faster to use than other signature algorithms, making it a popular choice for use in blockchain and other applications.

In a blockchain, ECDSA is typically used to sign transactions, which the integrity and authenticity of the transaction data is ensured. It is also used to generate and verify digital signatures for smart contracts and other types of blockchain-based applications. Overall, ECDSA is an important cryptographic algorithm that is widely used in blockchain and other applications to provide secure, digital signatures and help to ensure the authenticity and integrity of messages and transactions.

5. System Requirements

5.1 Hardware requirements

Processor	:	i3 or above
Ram	:	2 GB or above

5.2 Software requirements

Database	:	MySQL Server
Operating System	:	Windows 7 or above
Language	:	Java
IDE	:	NetBeans 8.1
Front End	:	JSP
Back End	:	Java Servlet

Implementation

The proposed system consists of the user interface and admin interface. The admin interface contains modules like candidate registration module, user registration module, declaration of the voting day, maintaining the process and declaring the results. The users interface contains the login page, homepage, they can see the candidates to whom they should vote. The candidate registration is done by the admin the admin verify is the Identity of the candidate and examination the profile of the candidate by verifying there Adhar card, college ID card and gather the personal details like their name and their date of birth, academic well behavior. Those details are stored in database. Only liable candidates can able to participate in the election or contest in the election. Now the user registration phase takes place. The admin collects the personal information of the uses such as full name sir name email id, password, branch, contact number, date of birth, gender, roll number department etc. The login credentials for every user are provided by the admin. Every user has a unique login credentials. If the user shares their login credentials, the person whom they shared their login credentials can misuse their vote. When I use enters the portal throw their login credentials, it shows the homepage about the basic information of the college and the voting system. At the time of voting the voters can see the finalized candidates and their designation for which they are contesting during voting. The voters can poll their vote to their likely candidates. The duty of each water is completed by polling their vote to their candidates. Here comes the blockchain technology. Every voter is given by a secret key. The candidate also provided with the secret key after their registration. The secret key generation is done by using ECC algorithm. ECC algorithm is abbreviated as elliptic curve cryptography algorithm. Just imagine the following situation, the voter X polled their vote to the candidate A, it looks like the secret key X polled their vote to the secret key A. Here the admin or the management or the third party people or the candidates cannot check the voting flow like who voted to whom. The privacy of the voters is ensured by ECC algorithm. The polled votes are hashed and stored in blocks by using ECDSA algorithm. It is abbreviated as elliptic curve digital signature algorithm. After the voting process was completed the admin can declare the result on the result day. The winners are calculated based on securing the higher number of votes.

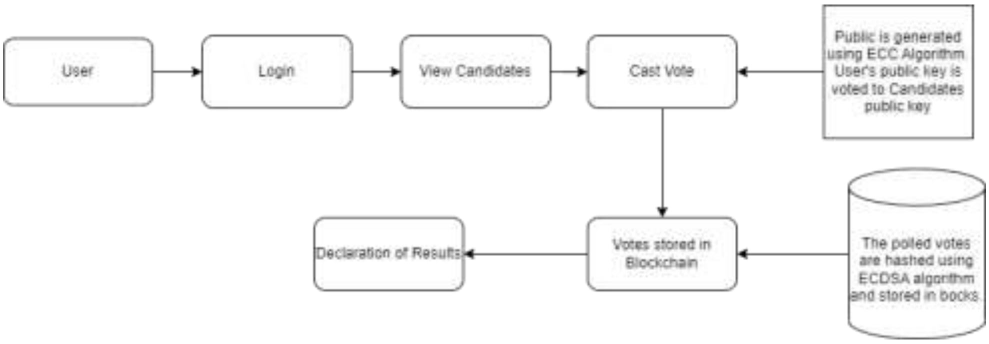
User
Login
View Candidates
Cast Vote
Public is generated using ECC Algorithm User's public key is voted to Candidates public key
Declaration of Results
Votes stored in Blockchain
The polled votes are hashed using ECDSA algorithm and stored in bocks.

Fig. 1 -Voting flow diagram.

Conclusion

A college voting system using blockchain technology and the ECC (Elliptic Curve Cryptography) algorithm can provide a secure, transparent, and decentralized way to conduct elections and other types of voting on a college campus. The use of ECC helps to ensure the privacy of each vote, as it makes it difficult for anyone to alter or tamper with the voting data. The decentralized nature of blockchain technology also makes it much more difficult for a single entity to exercise control or manipulate the system, helping to ensure fairness and impartiality in the voting process. The transparency of blockchain technology allows anyone to see and verify the accuracy of the votes being recorded, which can help to build trust and confidence in the system. Overall, "SURVEY ON BLOCKCHAIN BASED ONLINE STUDENT'S LEADER ELECTION SYSTEM" has the potential to revolutionize the way colleges and universities conduct elections and other types of voting, and it can be used widely including student government elections, club elections, and even faculty votes.

References

[1]. Adida, B., Helios (2008).“Web-based open-audit voting.”, in Proceedings of the 17th Conference on Security Symposium, ser. SS’08. Berkeley, CA, USA: USENIX Association,(2008).

[2]. Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008).“Scantegrity: End-to-end voter-veriable optical- scan voting.", IEEE Security Privacy, vol. 6, no. 3, pp. 40-46 (May 2008).

[3]. Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D.,Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013).“Star-vote: A secure, transparent, auditable, and reliable voting system.”, in 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13). Washington, D.C.: USENIX Association, 2013.

[4]. Dalia, K., Ben, R. , Peter Y. A, and Feng, H. (2012). “A fair and robust voting system by broadcast.”, 5th International Conference on E-voting (2012).

[5]. A Votereum: An Ethereum-based E-voting system : Linh Vo-Cao-Thuy, Khoi Cao-Minh, Chuong Dang-Le-BaoandTuanA.Nguyen (2019),“Votereum:AnEthereum-based E-voting system”,University of Information Technology Vietnam National University HCMC, Vietnam.

[6]. OnlineVoting:Voting SystemUsing Blockchain: Vaibhav Anasune, Pradeep Choudhari, Madhura Kelapure and Pranali Shirke Prasad Halgaonkar,“Online Voting: Voting System Using B-chain”(2019).

[7]. Decentralized Voting Platform Based on Ethereum Blockchain: David Khoury,Elie F. Kfoury, Ali Kassem and Hamza Harb (2018) “Decentralized Voting Platform Based on Ethereum Blockchain”.

[8] Survey on Blockchain Based E-Voting Recording System Design: G Bhavan,i“Survey on Blockchain Based E-Voting Recording System Design” (2018) .

[9] Blockchain-Based E-Voting System:Friðrik Þ. Hjálmarsson , Gunnlaugur K . Hreiðarsson, “Blockchain-Based E-Voting System” (2018) ,School of Computer Science Reykjavik University, Iceland.

[10] Blockchain Based E-Voting Recording System Design:Rifa Hanifatunnisa and Budi Rahardjo (2017),“Blockchain Based E-Voting Recording System Design