MANTECH Publications
Recent Trends in Computer Science and Software Technology
Volume 7, Issue 1, January-April 2022

Research on Blockchain-based Techniques for Increasing the Security of Electronic Voting Systems

Dr. Chiranjib Nath[1], Snehanshu Singh[2]
Professor[1], Student[2]
Department of Computer Science
Dwarkadas Jivanlal Sanghvi College of Engineering
Corresponding Author's Email:- *Snehanshusingh08@gmail.com*

Abstract

In a democratic society like India (the world's largest democracy), voting is important for both selecting government people and expressing our views on how the governing body should be established. Blockchain platforms are now accessible, and several organizations have begun to use them in their operations. It can be utilized not only for commerce but also as a service, and it has the ability to make voting more accessible. Online voting is a viable alternative to both the traditional paper ballot system and the widely used electronic voting equipment (EVM). An electronic voting portal should provide security and integrity, as well as vote transparency and voter privacy. As a result, NRIs and adult internet users can vote in a couple of seconds, regardless of where they are on election day. This will be simple and secure. There is a substantial chance of fake votes and property harm with the existing system. People do not want to stand in long lines or wait for long periods of time. Also, those in charge of the election must follow an entirely different voting system, which takes longer and lacks transparency. The study also discusses the current state of certain blockchain frameworks for electronic voting. This paper provides a review of the papers and strategies that have been used to address voting issues.

Keywords: *P2P network, E-voting system, Smart Contract, Blockchain, Ethereum, decentralized, high security*

INTRODUCTION

Elections are easily controlled and rigged, especially in small towns, and can also be expanded to corrupted big cities in corrupted countries. Traditional voting requires people to be physically present in their home country. Despite the fact that the government has declared the day vacation, it is extremely difficult for individuals to remain away from their homes. E-voting can be used to solve this problem.

E-voting security concerns include security flaws, (ii) acquiring secrets (username and password), (iii) altering already cast votes, and (iv) altering future votes via hacking the voting programme [1]. In addition, any e-voting system should have the following assets. Completeness (B) Robustness (C) Privacy (D) Unrepeatable (E) Eligibility (F) Individual verifiability (A) Completeness (B) Robustness (C) Privacy (D) Unrepeatable (E) Eligibility (F) Individual verifiability [7]

Elections are institutions that are designed to help countries achieve democracy. They play an important role in the country's and citizens' lives. As a result, it is extremely important for everyone involved in these elections. Elections, regardless of the organization, must be credible. They must protect people's privacy and the security of their votes. Furthermore, the authority in charge of counting votes should not spend too much time doing so because waiting too long is inconvenient. The length of time it takes for findings to appear raises worries about results being manipulated. However, trust has been a contentious issue in each election for various reasons depending on the places where elections have been held. Because paper elections are run by a centralized authority, there is always the risk of votes and election results being tampered with. Voting is a means for a group or meeting of electorates to make a collective choice or express an opinion. Debates, discussions, and political campaigns are frequently followed by voting. The individual who is to be elected is the election candidate, and the person who casts a ballot for their preferred candidate is the voter. In most cases, the voter has the option of voting for one of the candidates on the ballot or for someone else.

So the question is, "How can we be confident that the election results are correct, and how can we find out if they are incorrect?" In paper voting, a trustworthy party is always in charge of counting the ballots, and the voters must

trust them. In this sort of election, the entire process of verifiability and counting is carried out solely by the trusted party, preventing voters from checking and verifying the accuracy of the final results. In end-to-end voting verifiable systems, the reliance on a trusted party is minimized, allowing the voter to review and verify the results to see whether they are correct.

Motivation for Blockchain Technology

The use of blockchain technology is becoming increasingly prevalent in our daily lives. Blockchain is being used by an increasing number of businesses as the underpinning network for their daily transactions. When Blockchain first gained popularity, it was mainly used to process payments using the cryptocurrency Bitcoin. However, over time, much research has been conducted, and it has begun to appear that Blockchain may be utilized in a variety of other fields. Traditionally, the database has been managed by a single entity or central authority, which has complete control over the database. It has the capacity to modify data and interfere with databases. The authority who maintains the database is usually the same one that produced it and will be using it. In these circumstances, the company has no motivation to fake or manipulate its own statistics. However, in other circumstances involving financial matters or sensitive data such as voting, it's not a good idea to allow a single authority or exclusive group management of the database.

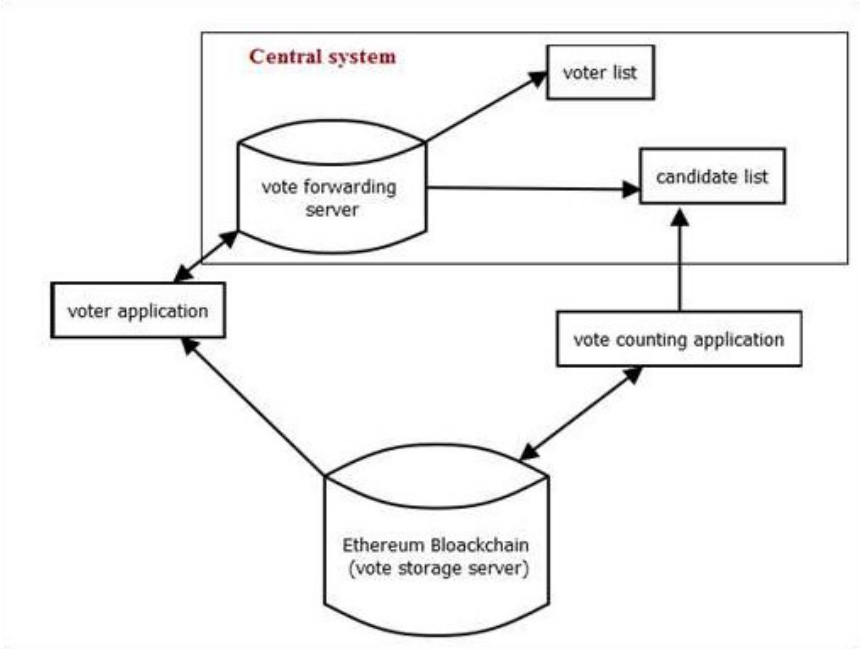

Fig. 1 Example of e-voting diagram

Even if the business guarantees that no fraudulent changes will be made to the database, hackers will find it easier to manipulate a central database. To circumvent this, Blockchain makes the database public, allowing anyone to store an individual copy of the database that can be compared at any time to check for modifications. Individual copies, on the other hand, must be updated on a regular basis to ensure consistency. Blockchain uses a consensus process to keep a decentralized database consistent.

DApps will, as a result, have the following Blockchain features: 1) Data integrity is essential. 2) Consensus techniques provide decentralized control and validation. 3) A run-time environment that is transparent. 4) In the run-time context, public business rules are active. 5) A high level of availability.

Smart contract

These are similar to traditional commercial contracts that are used for two parties to agree on a code of conduct. When the defined criteria are met, the smart contracts are automatically executed. Smart contracts allow untrustworthy or unknown parties to carry out agreements and transactions in a trusted manner without the need for a central authority. A smart contract is an account with its own code that controls it. It is the basic basis and main building block of any DApp, and it is considered an independent agent operated by the EVM (Ethereum Virtual Machine). The EVM will take care of running this code after it is deployed on the Blockchain as long as the conditions are met. It's worth noting that, once deployed to the Blockchain network, smart contracts can be visited and viewed publicly via their address, together with all of its associated transactions (to address, from address, timestamp, etc...). Any account can perform smart contract triggering functions as long as the following two conditions are met: 1) The smart contract's address is known; 2) The function caller has enough Ether to trigger the smart contract. Smart Contract Determinism The first problem to solve is to ensure that smart contracts are deterministic. To ensure that every stage of voting, validating, and tabulation is done under the consensus of all voters, we hope that the entire voting flow can be driven by smart contracts. Because a smart contract is executed by all peers in a network, its behaviour must be deterministic to ensure that various executions always produce the same result.

DApp(DECENTRALIZED APPLICATION)

DApp is a web application that is "blockchain-enabled" and runs on a peer-to-peer computer network rather than a single server. It has both a front end and a back end, and it runs on all nodes separately. The front-end interface is typically created using the same technologies as other applications. The only significant distinction is the use of a smart contract to connect the app to a blockchain network. [18] DApps intends to solve these problems by distributing important components such as data storage and infrastructure components among multiple peers or nodes. As a result, security, affordability, and usability features should all be considered while creating a DApp. Some features are essential in DApp apps. For example, [10] Improved performance (low latency, fast throughput), Reasonably cheap transaction price Maintainability that is flexible User data should not be stored or replicated in DApps.

The essence of Blockchain security is that there is no single point of failure. Users should use the programme to manage their independent and unique identities as the sole administrator. It lessens reliance on the government. The application should not be overly sophisticated and have a straightforward user interface. Unnecessary coding should be avoided because it raises costs and exposes security vulnerabilities.

Fig. 2Decentralized Application diagram

Challenges of voting

1. Election Privacy: There will be no third-party interference of any type in the election. Only the voter has access to his or her personal information and the people for whom he or she voted. The only information about the election that has been made public is the total number of votes cast for each candidate, as well as the total number of votes cast for the entire election.
2. Lack of Evidence: Although anonymity and privacy can protect against electoral fraud. There is no way to know if ballots were cast under the influence of bribes or other forms of election fraud. This problem has been present since the beginning.
3. Anti-fraud: Each qualified voter should only be allowed to vote once, and no one else should be allowed to vote. The system must authenticate each possible voter's identification and ascertain their status, but this information must not be linked to their vote.
4. Ease of Use: Elections must be accessible to the general public. It must be designed in such a way that it can be utilized with only a little training and technical knowledge.
5. Scalable: Elections are a way to reach a huge number of people. It must also be adaptable enough to work on a wide scale.
6. Speed: In this computer-driven era, results must be announced within a few hours of the election procedure ending.
7. Low Cost: One of the most important aspects of any system design is the cost. The system should be cost-effective, efficient, and require as little maintenance as feasible.

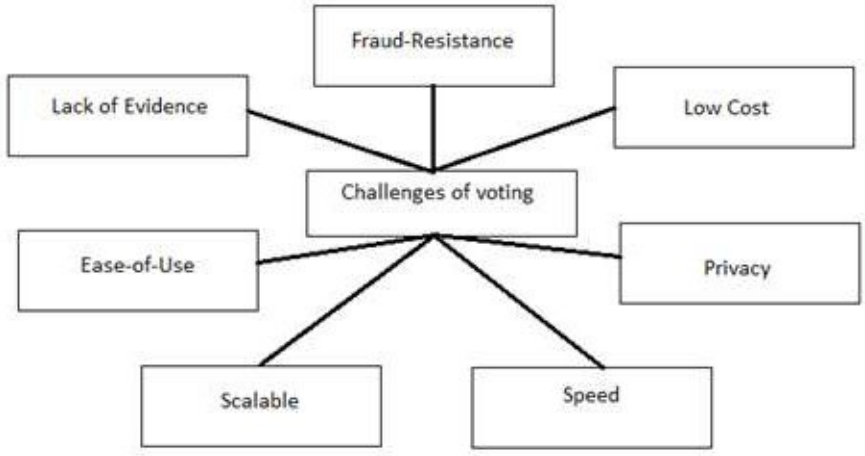

Fig. 3 challenges of e-voting system diagram

Why Ethereum

Ethereum leads in terms of usability, scalability, support, and development, and it has its own set of quirks in terms of development, security, and currency, with the exception of flexibility, which isn't really a concern because development isn't entirely focused. Ethereum is additionally supported by the fact that it employs cutting-edge encryption technology such as SHA 3[4] and keys created using the elliptic curve[4]. Solidity, the Ethereum programming language, is user-friendly since it is a blend of C++ and Javascript. Every week, millions of transactions are committed by the Ethereum community. The community's assistance is extremely valuable to new developers. Ethereum's method of operation is permissionless, and it may operate in both private and public modes, which is useful for testing.

P2P Network

The systems are connected via a peer-to-peer network when one system communicates with another over a peer-to-peer network. To improve the security of e-voting, use Blockchain in a peer-to-peer network. To prevent vote faking, we first create a synchronized model of voting records based on distributed ledger technology (DLT). Second, to offer authentication and non-repudiation, we create a user credential model based on elliptic curve encryption. For the essential requirements of the e-voting process, a peer-to-peer network is recommended. A blockchain-based e-voting system for numerous candidates has been built on Linux systems in the P2P network to prove and verify the scheme.

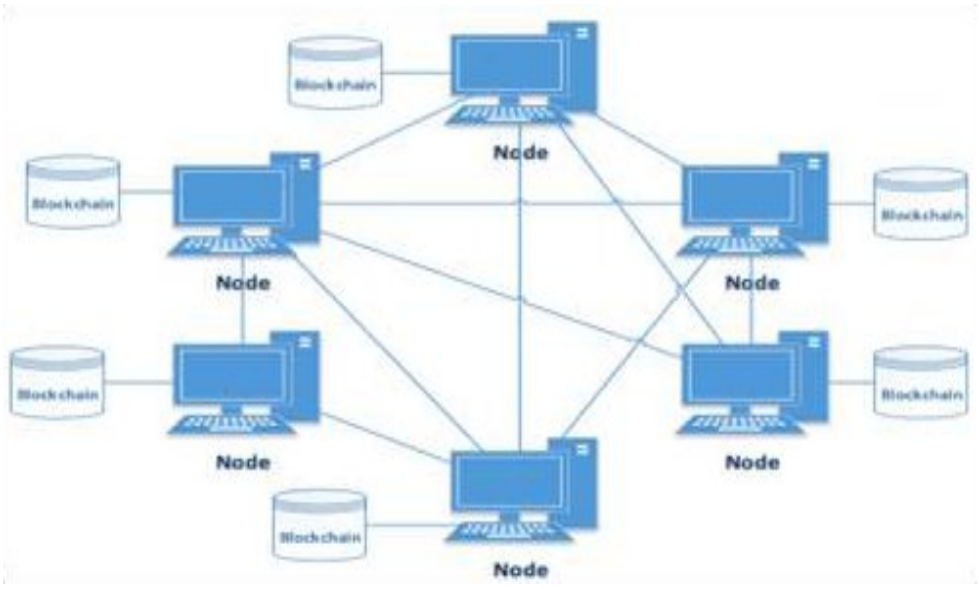

Fig. 4 Peer-to-Peer network Diagram

OVERVIEW OF METHODOLOGY

Table 1 Overview of Methodology

No.	Methodology/ Tools/ Techniques used	Define	Advantages	Disadvantages/ Limitation
1.	Solidity	Solidity is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms, most notably Ethereum.[31]	• including multiple level inheritance • **Application Binary Interface**	• **Transactional Operation** • **Limited expressiveness**
2.	Truffle	Truffle is a development environment, testing framework, and asset pipeline all rolled into one.[33]	• support for compiling, deploying and linking • automated contract testing	• The only "limitation" would simply be the features they may not have added yet.(means no right now)
3.	Ganache	Ganache is a personal blockchain for rapid Ethereum, and Corda distributed application development.[34]	• supporting both Ethereum and Corda technology. • graphical user interface	• grab the private key, not the public key
4.	Metamask	*MetaMask is a bridge that allows you to visit the distributed web of tomorrow in your browser today. It allows you to run EthereumdApps right in your browser without running a full Ethereum*	• the security level is quite good	• Still, not so easy and requires good knowledge of ETH network(meta mask)

		node.[34]		
5.	Smart contracts	Smart contracts are lines of code that are stored on a blockchain and automatically execute when predetermined terms and conditions are met.[38]	• time-saving • safety • precision • Accuracy • Transparency	• Data quality And mistakes
6.	Hyperledger Fabric	Hyperledger Fabric is a modular blockchain framework that acts as a foundation for developing blockchain-based products, solutions, and applications using plug-and-play components that are aimed for use within private enterprises.[37]	• improvises the level of trust • very flexible and scalable • a high degree of privacy • multilateral transactions	• not a Network fault-tolerant • got minimum APIs and SDKs.
7.	Homomorphic encryption	Homomorphic encryption is a method that computes encrypted data. it uses proxy re-encryption technology to protect the selected ciphertext from being attacked.[39]	• a higher standard of data security	• incredibly slow and non-performant
8.	RabbitMQ	RabbitMQ is a messaging broker. It gives your applications a common platform to send and receive messages and your messages a safe place to live until received.	• Approximately 75% of the time Redis takes in accepting messages. • RabbitMQ's queues are fastest when they're empty.	• RabbitMQ is probably not aware of the feature of lazy queues.
9.	Linkable ring signature	A linkable ring signature allows one person in the group to sign on behalf of the group but has the	• Privacy protection	• **Signature verification is a hard process**

		addition of a tag so that an external verifier can know that the signature has been produced by a defined signer, but where they cannot tell who the signer is.[35]		
10.	Distributed Ledger	Distributed ledgers use independent computers (referred to as nodes) to record, share and synchronize transactions in their respective electronic ledgers.[32]	• highly secure, transparent, immutable and tamper-proof	• Low speed in the process • Difficult to scale or to work with on a much larger scale.
11.	Biometric system	Biometrics are physical or behavioural human characteristics that can be used to digitally identify a person to grant access to systems, devices or data	• High security and assurance • User Experience • Non-transferrable	• **Costs** • **Data breaches** • **Tracking and data** • **False positives, bias and inaccuracy**

PROPOSED METHODOLOGY

It is necessary to ensure perfect election anonymity by removing any correlations between voters and votes without the added storage and computational complexity of separate blockchains for voter and vote data. Several existing designs for blockchain-based e-voting systems include the ability for the election administration to query the Blockchain during the election process to see if the voter ID of the current voting block already exists in the Blockchain, which introduces the risk of inequitable misuse by gaining access to vote count information during the election. This jeopardizes the democratic values and beliefs of a free and fair election and so must be addressed through better blockchain implementation design. Furthermore, present system designs employ techniques such as digital signatures and encryption to assure system stability but do not consider scalability when making design decisions. The suggested method tries to address these challenges in a Hyper ledger Sawtooth framework implementation, ensuring

scalability through parallel transaction processing and ensuring anonymity and fairness in the voting process by using two separate divisions in a single blockchain.

CONCLUSIONS AND FUTURE DIRECTIONS

We proposed a blockchain-based e-voting system since e-voting systems must be extremely safe. We were also able to eliminate the disadvantages of time and location constraints by allowing users to vote at their leisure from their own blockchain nodes. The entire vote-counting process is accessible to everybody to observe, limiting the possibility of vote-rigging, and the results are visible in real-time. Want to improve the established programme for scalability issues while adhering to well-accepted security criteria in the e-voting area? This paper provides information on several blockchain techniques as well as the work that has been done on blockchain techniques to date.

REFERENCES

1. JiazhuoLyu, Zoe L. Jiang, Xuan Wang, ZhenhaoNong ,Man Ho Au ,Junbin Fang "A Secure Decentralized Trustless E-Voting System Based on Smart Contract" IEEE 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering(2019)

2. Y. Liu, Q. Wang, An evoting protocol based on Blockchain, Department of Computer Science and Engineering, Southern University of Science and Technology, Shenzhen, China(2018)

3. F.Hao,P.Y. A. Ryan, "Real-world electronic voting:" Design, analysis and, pp deployment (CRC Press,(2017)

4. F. S. Hardwick, A. Gioulis, R. N. Akram, K. Markantonakis, "E-voting with Blockchain: An e-voting protocol with decentralization and voter privacy"International Conference on Computing and Communication Technologies.(2017)

5. M. Pilkington, "11 blockchain technology: principles and applications," Research handbook on digital transformations,(2016).

6. R. Hanifatunnisa and B. Rahardjo, "Blockchain-based e-voting recording system design," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, (2017).

7. KristianKost'al, RastislavBencel, Michal Ries, Ivan Kotuliak "Blockchain E-Voting Done Right: Privacy and Transparency with Public Blockchain"IEEE10th International Conference on Software Engineering and Service Science (ICSESS) (2019)

8. Linh Vo-Cao-Thuy, Khoi Cao-Minh, Chuong Dang-Le-Bao, Tuan A. Nguyen "Votereum: An Ethereum-based E-voting system" IEEE RIVF International Conference on Computing and Communication Technologies (RIVF)(2019)

9. Wei-Jr Lai, Yung-chen Hsieh, Chih-Wen Hsueh, Ja-Ling Wu "DATE: A Decentralized, Anonymous, and Transparent E-voting System" IEEE International Conference on Hot Information-Centric Networking (HotICN)(2018)

10. K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, "Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab," in International Conference on Financial Cryptography and Data Security. Springer, (2016)

11. ShitangYu,KunLu,ZhouShao,YingchengGou,BoZhang"A High Performance Blockchain Platform for Intelligent Devi" IEEE International Conference on Hot Information-Centric Networking(2018).

12. KritiPatidar, Dr. Swapnil Jain "Decentralized E-Voting Portal Using Blockchain" IEEE 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)(2019)

13. NirKshetri ; Jeffrey Voas-2018 "Blockchain-Enabled E-Voting", IEEE Software (2018)

14. M. Wohrer and U. Zdun, "Design Patterns for Smart Contracts in the

Ethereum Ecosystem", 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Canada, (2018).

15. A. Marathe, K. Narayanan, A. Gupta, and M. Pr, "DInEMMo: Decentralized incentivization for enterprise marketplace models," 2018 IEEE 25th International Conference on High-Performance Computing Workshops (HiPCW)(2018)

16. A. B. Kurtulmus and K. Daniel, "Trustless machine learning contracts; evaluating and exchanging machine learning models on the Ethereum blockchain," IEEE 25th International Conference on High-Performance Computing Workshops (2018).

17. F. Daniel, P. Kucherbaev, C. Cappiello, B. Benatallah, and M. Allahbakhsh, "Quality control in crowdsourcing: A survey of quality attributes, assessment techniques and assurance actions," CoRR,(2018).

18. Hiren M Patel, Milin M Patel, Tejas Bhatt, "Election Voting Using BlockChain Technology", International Journal of Scientific Research and Review, (2019).

19. Bin Yu, Joseph K. Liu, Amin Sakzad, Surya Nepal, Ron Steinfeld, Paul Rimba, and Man Ho Au. Platform-independent secure blockchain-based voting system. In Information Security: 21st International Conference,(2018).

20. Patrick McCorry, Siamak F Shahandashti, and FengHao. A smart contract for boardroom voting with maximum voter privacy. In International Conference on Financial Cryptography and Data Security,(2017).

21. M. Pawlak, J. Guziur, and A. Poniszewska-Maranda, "Voting Process with Blockchain Technology: Auditable Blockchain Voting System," inLecture Notes on Data Engineering and

Communications Technologies,(2019).

22. P. McCorry, S. F. Shahandashti, and F. Hao, "A Smart Contract forBoardroom Voting with Maximum Voter Privacy," inLecture Notes inComputer Science, (2017).

23. "DAO soft fork voting on Ethpool&Ethermine", forum.ethereum.org/discussion/7796/dao-soft-fork-voting-on-ethpoolethermine(2017)

24. Abhishek Kaudare, d Milan Hazra, AnuragShelar, ManojSabnis "Implementing Electronic Voting System With Blockchain Technology" IEEE International Conference for Emerging Technology (INCET)(2020)

25. Yuxian Zhang , Yi Li , Li Fang , Ping Chen , Xinghua Dong "Privacy-protected Electronic Voting System Based on Blockchin and Trusted Execution Environment" IEEE 5th International Conference on Compute (2019)

26. David Khoury, Elie F. Kfoury, Ali Kassem, HamzaHarb "Decentralized Voting Platform Based on EthereumBlockchain" IEEE International Multidisciplinary Conference on Engineering Technology (IMCET).(2018)

27. P. Zhang, J. White, D. C. Schmidt, and G. Lenz, "Design of Blockchain-Based Apps Using Familiar Software Patterns to Address Interoperability Challenges in Healthcare", the 24th Pattern Languages of Programming conference, Canada, (2017).

28. V. Buterin, "Ethereum white paper: a next generation smart contract & decentralized application platform," [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper, (2013).

29. Tutorials for the solidity https://www.dappuniversity.com/articles/solidity

30. Tutorials for the blockchain https://www.dappuniversity.com/articles/blockchain-app-tutorial

31. Truffle : https://truffleframework.com

32. Ganache: https://truffleframework.com/ganach

33. E-Voting, GitHub :https://github.com/topics/e-voting

34. Ethereum project: https://ethereum.org

35. HyperledgerFabric. www.hyperledger.org/projects/fabric

36. Ethererum. www.ethereum.org.

37. R. Aroul Canessane, N.Srinivasan, AbinashBeuria, Ashwini Singh, B. Muthu Kumar" Decentralized Applications Using Ethereum Blockchain" IEEE 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)(2019)

38. Nodejs, [Online]. Available: https://nodejs.org/en/, 2019

39. "What is a Digital Signature? - Definition from WhatIs.com." SearchSecurity. Accessed September 11, 2019. https://searchsecurity.techtarget.com/definition/digital-signature

40. Wenbin Zhang, Sheng Huang, Yuan Yuan , Yanyan Hu, Shaohua Huang, Shengjiao Cao, Anuj Chopra "A Privacy-Preserving Voting Protocol on Blockchain" IEEE 11th International Conference on Cloud Computing.(2018)