



BLOCKCHAIN TECHNOLOGY-BASED VOTING SYSTEM

Md. Anik Ahamed¹, Imam Hossain², Omlan Jyoti Mondal³

¹Department of CSE, Prime University

²Department of CSE, Prime University

³Department of CSE, Prime University

ABSTRACT

In a democracy, the ruler of a nation is determined by the elections. The general public use elections to express their views through a vote. For this reason, elections are very important. A faulty voting system causes most of the problems in democratic countries like Bangladesh. The existing voting systems in Bangladesh face many problems such as vote rigging, election manipulation, and polling booth capturing, and hacking of electronic voting machines. To eliminate these problems, this paper proposes a decentralized electronic voting application based on blockchain. When the voting system first began there was a concept of secret voting. In the recent past, there have been several examples where it was noted that the voting process was not completely hygienic and faced several issues including transparency and fairness, and the will of the people was not observed to be effectively quantified and translated in terms of formation of the governments. The data and the application code of a decentralized architecture are immutable. The data or the code can not be unilaterally changed by any of the blockchain nodes. Here the blocks are used to arrange the votes and a hash function is used to chain the blocks together to form a public record. Then smart contracts are used for the application function codes. In this way, the code and the data are more secure and are tamper-proof. We therefore believe that a blockchain technology-based voting system will be more suitable for the deployment of e-voting applications in Bangladesh.

KEYWORDS: Blockchain, Decentralized, Ethereum, Democracy, Non-party Caretaker Government

1.1 INTRODUCTION

In our research voter confidentiality, voter anonymity, and end-to-end verification type key issues are given focus to investigate. When a vote transaction occurs, a strong cryptographic hash is generated by the system. This process protects the integrity and anonymity of a vote. The hash that the system generates is based on specific information of a voter. The voter uses the hash to facilitate verification [5]. Usually, a central authority manages, counts, and checks votes. In a Blockchain technology-based voting system, each voter holds a copy of the voting records. So the voters will do those tasks themselves. No one will be able to change the voting records because the other voters will immediately find out about the changes [4]. There will be no third party in the blockchain to verify transactions because it is decentralized [6]. Blockchain has a predefined set of rules. By using those rules transactions can be verified independently by anyone [5]. In this paper, we have tried to implement a voting app to explore the use of blockchain technology.

1.2 MOTIVATION

Blockchain offers peer-to-peer processes where any transaction can be performed peer-to-peer and the system can not come to validate it. So we can reduce the server cost in this process and also the performances can be moderated that causing a blockage at the main server. In the blockchain, there is no main authority that maintains the voter's private information. The privacy of the transactions is helped by this mechanism to maintain up to a certain limit. In blockchain the falsification detection is easy. Because after spreading every

transaction in the network the broadcasted block will be verified by other nodes. Thus every transaction will be checked. In Bitcoin, we can find every transaction that is done so far and this helps in increasing the accessibility and transparency of any of the transactions recorded in the blockchain [13].

1.3 CHALLENGES

For this paper, we can assume that the insights for some of the challenges described below can be offered by blockchain technology [14].

1.3.1 Privacy: Cryptographic properties are leveraged by the system to ensure the privacy of voters. After the registration of a voter, the blockchain generates a voter hash that can uniquely identify a voter. The voter is protected because the cryptographic hash has the collision resistance property [5].

1.3.2 Convenience: A web-based interface is used for the implementation of the system. HTML, CSS, and JAVASCRIPT are used for the implementation of the web app. No one should delete, modify and forge the votes [5].

1.3.3 Verifiability: For casting votes, a transaction ID is given to the voters which is a hash and have cryptographic properties. This ID can be used to track votes. Unauthorized modification of the voting results should supposedly not be allowed in the system. Every vote should be counted correctly and this should be ensured by the system [5].



1.3.4 Immutability: The voters or the blockchain admins can not edit or delete data after it is written to the blockchain ledger. This is called immutability [8].

2. LITERATURE REVIEW AND HYPOTHESIS/ES DEVELOPMENT

2.1 Blockchain

Blockchain technology was designed by Satoshi Nakamoto in 2008. In his paper, he explained mining, proof-of-work, the role of hashing, and incentives. To verify the transfers a mechanism was also provided by him [7]. All transactions that are executed from the genesis block are replicated in the blockchain. The users who want to connect to the network are allowed by the blockchain. Then new transactions are sent by them. Blockchain then verifies those transactions and creates new blocks. Blockchain is a distributed decentralized public ledger. It has a complete list of constantly growing data records that are secured from revision, tempering, and unauthorized manipulation [5].

A cryptographic hash is assigned to each of the blocks that can be viewed as a fingerprint of the block. The hash remains valid if anyone does not alter the data of the block. If anyone does change some properties in the block, the hash also changes immediately. This type of data change can be seen as malicious activity. Blockchain has strong foundations in cryptography. For this unauthorized transactions can be mitigated. In a block, there are lots of transaction data. Each block has a hash value of the previous block and using this hash value the blocks are connected and form a valid transaction chain [8].

2.2 Miners

New blocks are created by miners after the transactions are validated using a consensus mechanism called Proof of Work (POW). If anyone has the required computing power to calculate the hashes he can create valid blocks for the blockchain. The transactions are grouped by POW and after grouping, POW broadcasts transactions to different parties [9].

2.3 Digital signature

For the verification of the integrity and authenticity of a digital message, a digital signature is used. In a cryptographic system, there are two keys: a public key and a

private key. The public key is shared widely. The owner of the private key only knows the key and he uses it to encrypt and decrypt messages.

The hash of any document can be encrypted by using a private key. Thus a digital signature is created. The signature can be decrypted by using a public key by the recipient. The result will match the hash of the document. If anyone changes the document after creating the signature the signature is invalidated. Because there will be a difference between the hash of the document and the decrypted signature. Counterfeiting a digital signature is nearly impossible because the private key can not be faked [8].

2.4 Smart Contract

A smart contract is a self-executing computer code. It can be also called an agreement and the execution of this agreement is enforceable and automated. This type of agreement can be run on a distributed ledger. For, handling common contractual conditions Smart contracts are used. The automated part is that computer code expresses through and independently executes the actual transactions among parties. No party can block this execution process. The enforceable part is that the obligations and legally binding rights of the parties that are involved are constituted by it.

The computer code and the legal prose both make smart contracts. Programmable transaction protocols are defined as computer code. The legal prose reflects that the computer code constitutes part of the binding legal agreement between the parties, and is therefore also legally binding [11].

2.5 Blockchain-based works

The evolution of blockchain-based systems largely affects business and financial services. A large number of software companies including IBM, and Microsoft introduced blockchain-based services. For improving the privacy of the Internet of Things applications blockchain is also going to use in IoT. Blockchain-based Autonomous Decentralized Peer-to-peer Telemetry has been used by IBM to construct a circulated set-up of devices. Blockchain-based apps are also used in public services to register the lands. In a reputation system, the blockchain-based apps play a significant where reputed employees are honored by some reputation currency [12].

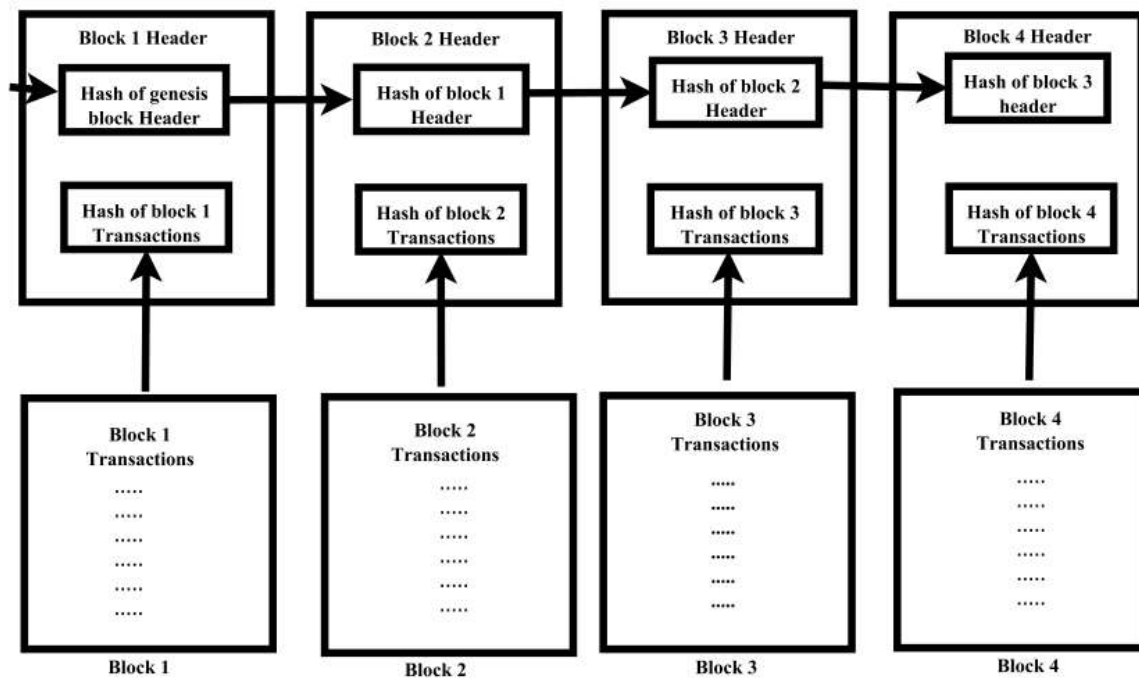


Figure-a: Blockchain

3. METHODOLOGY

A decentralized web application is presented here. This application is made for a referendum where most of the political parties of Bangladesh will participate in this referendum to choose a Non-party Caretaker Government for the upcoming 12th National Election for saving democracy.

3.1 Entities Of The system

3.1.1 Voters: Most of the political parties of Bangladesh will be the voters for this referendum.

3.1.2 Proposal: A single proposal for the referendum is, "Bangladesh needs a Non-party Caretaker Government for the 12th national election."

3.1.3 Blockchain Network: A trusted peer-to-peer network that maintains records that are accessible to all of the nodes.

3.1.4 Blockchain Admins: A team of system administrators who will start the referendum.

3.1.5 Nodes for mining: some nodes are used here for observing and verifying all referendum transactions.

3.1.6 Smart Contracts: Software codes that manage the referendum [3].

3.2 System Design

An architecture for a Blockchain-based voting application is presented here. A ledger record, smart contracts, and the user interface together make this architecture. Here blocks are used to store the votes. Then a hash function is used to chain together the blocks one after another. Thus they form a ledger. The voter interface and the admin interface together make the user interface in this architecture.

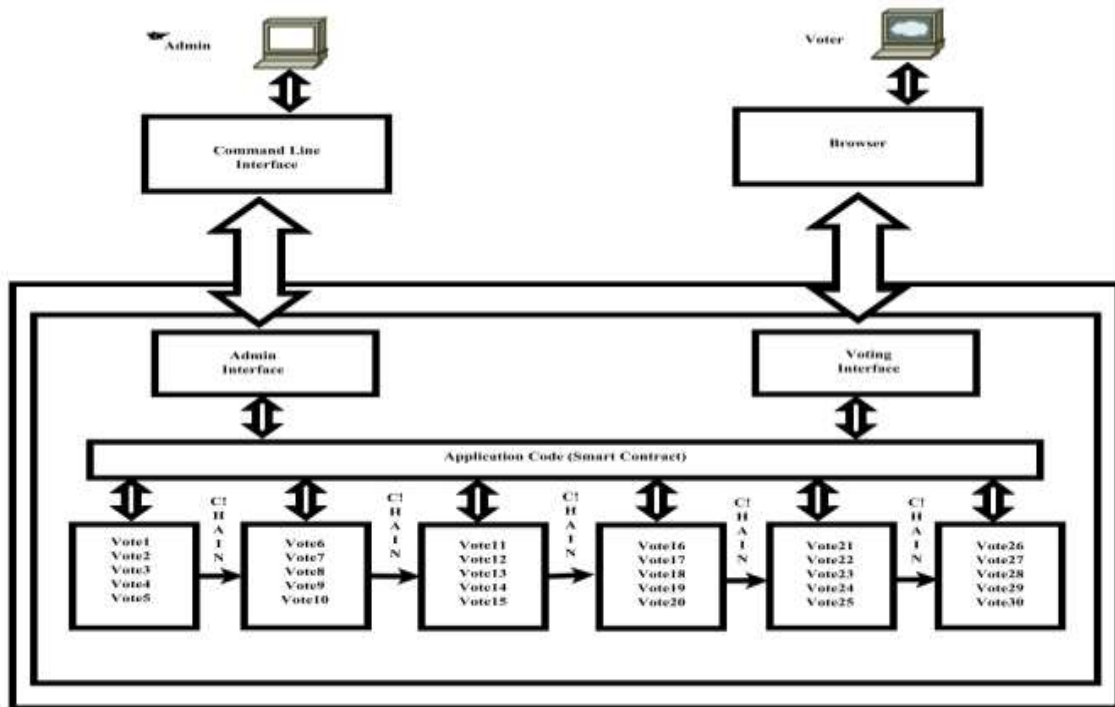


Figura-b: Architecture of the Voting Application

The same application code is run by all peer-to-peer nodes as a smart contract. We then distribute the smart contracts between the voter interface and admin interface. Remote Procedure Call is used by those interfaces to communicate with the backend. The smart contract, the ledger

record, and the user interfaces are some of the nodes of the network from the application server. Then two separate websites are used for the two interfaces [3].

3.3 Voting Algorithm

3.3.1 Admin

Step-1: Initialize the poll

Step-2: Int Total_Voter, Yes_Votes, No_Votes

Step-3: String Voter_ID, Voter_Name

Step-4: Function Add_Voters (Voter_ID, Voter_Name)

Step-5: For Loop : (I <= Total_Voter)

Step-6: Enter the Private Key of the Voter account and type the Voter name.

Step-7: Register Voter

Step-8: End For loop

Step-9: Start Voting

Step-10: Function Count_Votes (Yes_Votes, No_Votes)

Step-11: For Loop : (I<=Total_Voter)

Step-12: Count Yes_Votes and No_Votes

Step-13: End For loop

Step-14: End Voting

Step-15: Print Yes_Votes

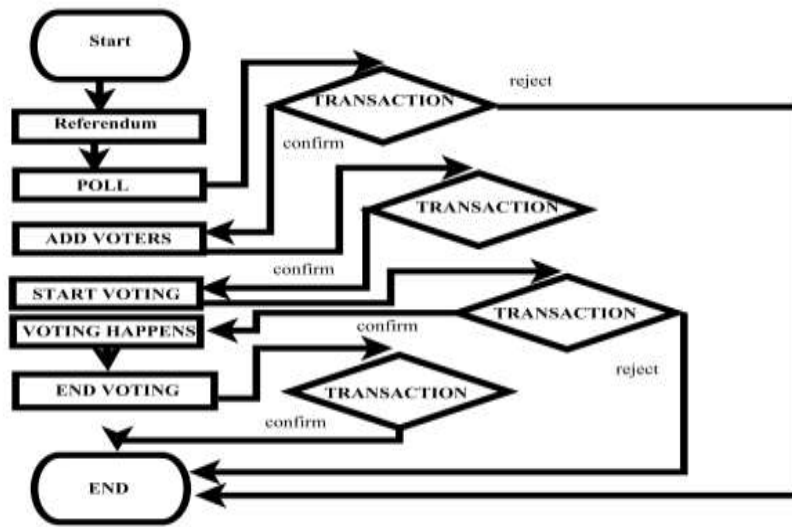


Figure-c: Flowchart For The Admin

3.3.2 Voter

Step-1: Initialize the poll

Step-2: Enter the system-generated referendum address

Step-3: Start Poll

Step-4: Enter Your Vote

Step-5: If you want the proposal

Step-6: Enter Yes

Step-7: Else Enter No

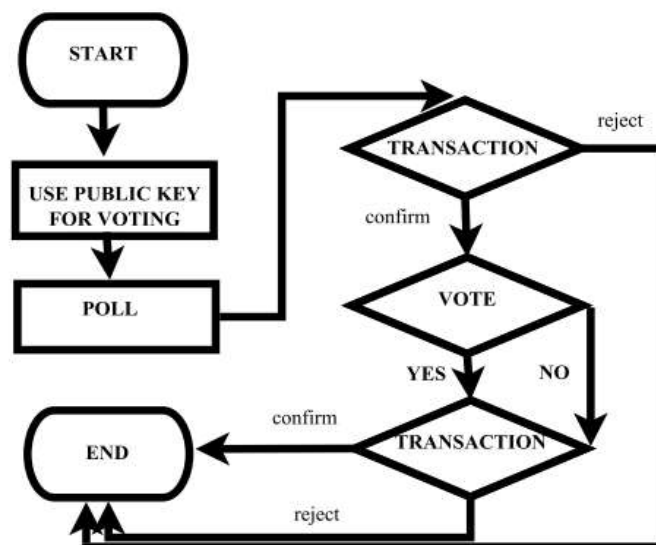


Figure-d: Flowchart For The Voters

3.4 Implementation procedure

Ethereum is an open-source blockchain that is decentralized and has smart contract functionality.[17] This platform uses Ether(ETH) for cryptocurrency. For

implementation, Ethereum Ganache is used here which is a virtual testing environment. Ganache provides us with 100 virtual blockchain nodes for testing our app. Metamask is also used here which is a browser plugin for the Ethereum wallet.

Blockchain Technology Based Voting System

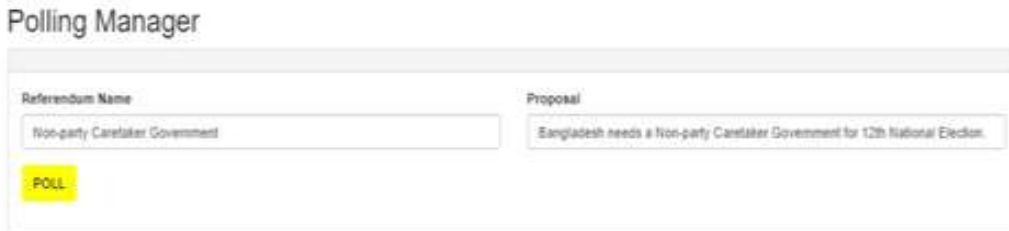


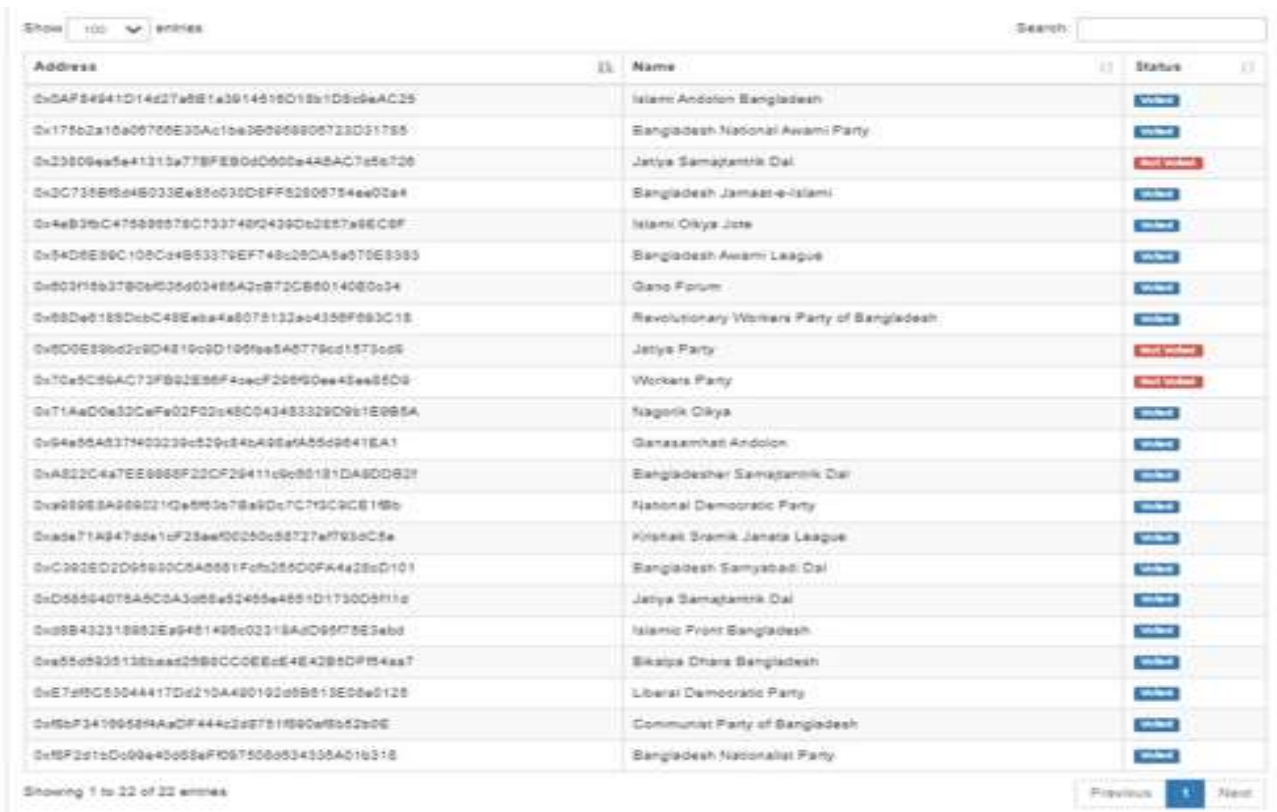
Figure-e: Admin Webpage Part-1



Figure-f: Admin Webpage Part-2 (Voter Registration)

Using Ganache we can set our local blockchain network. After that, the ganache needs to be connected with the Metamask. For every successful transaction, some gas fees

need to be paid. So for testing every smart contract we need to always pay transaction fees.



Address	Name	Status
0x5AF94941D1427a8E1a3914510D15b1D5c9eAC25	Islami Andolon Bangladesh	Voted
0x175b2a10a00766E30Ac1ba3B9968906723D31755	Bangladesh National Awami Party	Voted
0x33809ee5e41315a778FE80d000c448AC7e5e720	Jatiya Samajtantrik Dal	Not Voted
0x2C738B5d4B033E4850030C8FF82808754e02a4	Bangladesh Jamaat-e-Islami	Voted
0x4eB3bC475898579C733748D439Dc2857a8EC8F	Islami Oikya Jote	Voted
0x34D8E90C10Dc44B53379E7F48c28DA5e070E9385	Bangladesh Awami League	Voted
0x8031f8b3780e53603485A2c872CB80140E0c34	Gano Forum	Voted
0x88Dd0188DcbC48E8ba4a8078133ac4358F883C1E	Revolutionary Womens Party of Bangladesh	Voted
0x8D0E88bd2c9D4819c9D195fa5A8778cd1573cd8	Jatiya Party	Not Voted
0x70e5C86AC73F892E38F4ccF2089D9e4Eee85D8	Workers Party	Not Voted
0x71AaD0e32CafE02F02a48C043483329D961E885A	Nagorik Oikya	Voted
0x94e55A837403239c529c84a08a9A55c9641EA1	Ganasamhati Andolon	Voted
0xAS22C4a7EE888F22CF26411c988181DA8DD83F	Bangladesher Samajtantrik Dal	Voted
0xa8888A8880210e888e78a8d7C79C9CE198b	National Democratic Party	Voted
0xade71A8478de1cF23ae50250c88727a793cC8e	Krishak Shramik Janata League	Voted
0xC992ED2D99930C8A8881Fcb285D0FA428cD101	Bangladesh Samyabadi Dal	Voted
0xD588e4075A5CCa3c88a52455e4881D173009f11e	Jatiya Samajtantrik Dal	Voted
0x988432318882E99481488c02318A0D95F78E3abd	Islamic Front Bangladesh	Voted
0xe55c9351388a82888CC0EEe4E4285DF84aa7	Bikrpa Dhara Bangladesh	Voted
0xE729C85044417Dd210A480192d88813E08e0128	Liberal Democratic Party	Voted
0x5bP34199588AaCF44c2a8781889c8f852a0E	Communist Party of Bangladesh	Voted
0x5F2d1cD09e48088F087508934355A010318	Bangladesh Nationalist Party	Voted

Figure-g: Admin Webpage Part-3 (Parties who have participated in this referendum)

Here different political parties such as Gano Forum, Communist Party of Bangladesh, Bangladesh Nationalist Party, Revolutionary Workers Party of Bangladesh, Nagorik Oikya, Ganasamhati Andolon, Bangladesh Jamaat-e-Islami, Islami Oikya Jote, Islamic Front Bangladesh, Islami Andolon Bangladesh, Krishak Sramik Janata League, Liberal Democratic Party, Bikalpa Dhara Bangladesh, National Democratic Party, Bangladesh National Awami Party, Bangladesh Samyabadi Dal, Jatiya Samajtantrik Dal, Bangladesher Samajtantrik Dal, Bangladesh Awami League, Jatiya Samajtantrik Dal, Workers Party, Jatiya Party are used as blockchain nodes who are the voters for this referendum. We use the private keys from ganache to import these voter accounts into MetaMask. There is a single proposal for this referendum and that is “Bangladesh needs a Non-party Caretaker Government for the 12th National Election.” Two separate web pages have been created one for the blockchain admin and the other for the voters. The admin goes to the specific website (<https://btbvs.000webhostapp.com/>) built for voting to start. There the blockchain admin starts the poll for

this referendum. This referendum is written in a smart contract. When the admin starts this poll a transaction needs to be confirmed for the payment of the gas fees. After the confirmation of the transaction, a new smart contract is created. In this contract, the system generates a public key for the referendum address. Every voter uses this public key for the voting process. Now the admin registers the voters using their ganache accounts public key and name. With every registration, a transaction occurs and the admin has to pay some of the gas fees. After the successful completion of the registration process, the admin starts the voting. The voters go to a specific web address

(<https://btbvs.000webhostapp.com/vote.html>) that has been given to them. There they use the public key of the referendum. The voters log in to their Ethereum account via MetaMask. Then with the help of the public key of the referendum, the voters give their votes. For every vote, a transaction occurs and a voter needs to pay some of the gas fees. After the successful completion of the referendum, the admin ends the voting. Then the results are published.



Figure-h: Admin Webpage Part-4 (The voting has ended)

4. RESULTS AND DISCUSSION

4.1 Result

In this web-based blockchain voting system, a scenario is presented where 22 political parties have participated as voters.

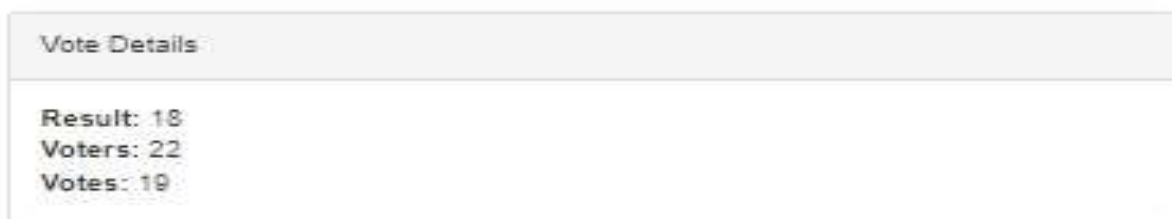


Figure-i: Admin Webpage Part-5 (Only Yes votes are displayed)



Figure-j: Voter Webpage Part-1 (Voters will put the referendum address here for voting to start)



Figure-k: Voter Webpage Part-2 (Voters will give Yes or No Vote for the referendum)

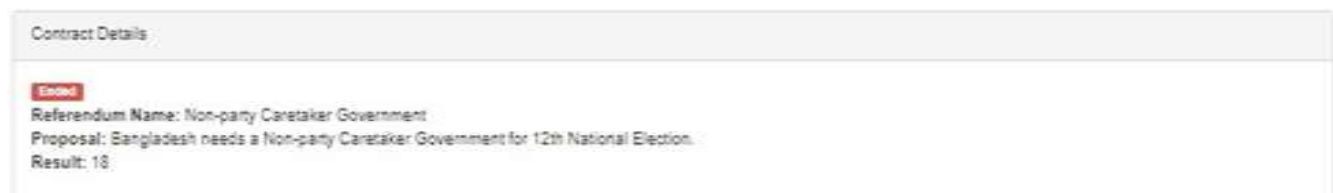


Figure-l: Voter Webpage Part-3 (Results from the Voter webpage)

Of the 22 parties, 19 political parties participate in this referendum, and from them, 18 political parties give “YES” votes for the proposal, “Bangladesh needs a Nonparty Caretaker Government for the 12th National Election.” Three political parties do not participate in this election. Only one political party “Bangladesh Awami League” gives a “No” vote for the proposal. So the result is that 18 political parties want a Non-party Caretaker Government for the upcoming 12th general election in Bangladesh.

4.2 DISCUSSION

An important question that can arise is why most of the political parties (18 parties from 19) of Bangladesh want a Non-party Caretaker Government so badly. Because in the parliamentary framework, after the dissolution of the existing ministry, the practice of establishing a Non-party Caretaker Government for organizing general elections has been observed. During the period, the Non-party Caretaker Government maintains neutral status for ensuring free, fair, genuine, and internationally acceptable general elections. Non-party Caretaker Government conducted general elections in 1996, 2001, and 2008 that were mostly seen as free, fair, and genuine by international observers. But the Non-party Caretaker Government was abolished from Bangladesh by the ruling Bangladesh Awami League through the 15th amendment of the constitution, passed by the National Parliament. After that, all parliamentary elections were held under the existing parliament. The 11th National Parliamentary election of Bangladesh was held under the ruling government Bangladesh Awami League [16]. Bangladesh Awami League secured power for the third consecutive term while most of the parties boycotted the elections demanding elections under a Non-party Caretaker Government. Because the elections were highly controversial. Most of the opposition parties not taking part in an election have obvious effects on upholding a

democracy. For this reason, the 18 political parties gave “Yes” votes for the referendum.

For saving democracy for the upcoming 12th general election in Bangladesh most of the political parties participated in this referendum and the, 18 political parties presented their eagerness to a Non-party Caretaker Government for a free, fair, genuine, and internationally acceptable election. It is a successful implementation of a blockchain-based app.

5. CONCLUSION

Here blockchain technology-based voting system has been implemented in a limited area. The blockchain-based voting system will be more secure than existing voting systems. The implementation of this kind of system in our national election will reduce the election cost dramatically. Vote rigging, hacking of electronic machines, and election manipulation can also be eliminated. Numerous experts believe that blockchain may be one of the best solutions for a decentralized electronic voting system.

REFERENCES

1. *Blockchain-based E-voting System*
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3648870
2. *Blockchain for Electronic Voting System—Review and Open Research Challenges*
<http://web.archive.org/web/20220209103237/https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614>
3. *SEVA_A_Smart_Electronic_Voting_Application_Using_Blockchain_Technology*
https://kclpure.kcl.ac.uk/portal/files/165304527/SEVA_A_Smart_Electronic_Voting_Application_Using_Blockchain_Technology.pdf
4. *Securing the vote*
<http://web.archive.org/web/20161220213615/http://www.itsecurityguru.org/2016/12/19/securing-the-vote>



5. *Secure Digital Voting System based on Blockchain Technology*
<https://core.ac.uk/download/pdf/155779036.pdf>
6. *Blockchain Technology*
<https://www.developers.dev/tech-talk/blockchain-technology/how-long-does-it-take-to-go-live-with-a-blockchain-development-project.html>
7. *Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System*
<https://digital.sandiego.edu/cgi/viewcontent.cgi?article=1032&context=sdlr>
8. *Blockchain Byte*
<https://www.slideshare.net/SamKurtis/emily-rutland-blockchain>
9. *What is the distinction between a blockchain and a distributed ledger?*
https://www.finra.org/sites/default/files/2017_BC_Byte.pdf
10. *Trustworthy Electronic Voting Using Adjusted Blockchain Technology*
<https://ieeexplore.ieee.org/document/8651451>
11. *What is a smart contract?*
<https://www.r3.com/blog/what-is-a-smart-contract>
12. *Cloud-Based Commissioning of Constrained Devices using Permissioned Blockchains*
https://www.researchgate.net/publication/303515409_Cloud-Based_Commissioning_of_Constrained_Devices_using_Permissioned_Blockchains
13. *A Study on Blockchain Technology: Application and Future Trends*
https://www.researchgate.net/publication/347192831_A_Study_on_Blockchain_Technology_Application_and_Future_Trends
14. *A Decentralized Voting System*
<https://odr.chalmers.se/bitstream/20.500.12380/301905/1/DATX02-19-85%20Uppladdad%20i%20360.pdf>
15. *Blockchain-Based Online Voting System Using RSA Algorithm*
<https://easychair.org/publications/preprint/42hD>
16. *CPD Annual Report 2018*
<https://www.slideshare.net/CPDBD/cpd-annual-report-2018>
17. *Implementation of Decentralized Blockchain E-voting*
https://www.researchgate.net/publication/341890257_Implementation_of_Decentralized_Blockchain_E-voting