A Blockchain based Cost effective Digital Voting System using SideChain and Smart Contracts

Syada Tasmia Alvi
Dept. of CSE
Jagannath University
Dhaka, Bangladesh
tasmia.rng@gmail.com

Mohammed Nasir Uddin
Dept. of CSE
Jagannath University
Dhaka, Bangladesh
nasir@cse.jnu.ac.bd

Linta Islam
Dept. of CSE
Jagannath University
Dhaka, Bangladesh
linta@cse.jnu.ac.bd

Sajib Ahamed
Dept. of CSE
Jagannath University
Dhaka, Bangladesh
sajeeb07ahamed@gmail.com

2020 11th International Conference on Electrical and Computer Engineering (ICECE) | 978-1-6654-2254-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICECE51571.2020.9393081

***Abstract*—Democracy plays a significant part in voting. If the voting process is not clear, stable and tamper proof, the integrity and legitimacy of the entire system is at risk. In recent years, neither civilians nor elected leaders have appreciated traditional ballots. Elections are surrounded by vote falsification, bribery and other voting problems. Often an individual must stand in a long line of people while casting votes and the procedure is quite lengthy. There has to be an exceptional feature of modern technologies to upgrade the existing system. Block chain provides the various features that will alter the scenario. But to implement ethereum based blockchain is expensive as for each transaction there is a computation cost. So we have used the sidechain concept to provide a cost effective blockchain based voting mechanism as sidechain extends the capabilities of blockchain by performing some operation besides it using duplicate currency and returns the result to mainchain for its use.**

***Index Terms*—Voting, Blockchain, Ethereum Smart Contracts, Sidechain**

I. Introduction

Elections seem to be a very significant occurrence in modern democracy, but vast parts of societies do not support their voting mechanism, which is a crucial issue for democracy [1]. Existing voting schemes have failed to be successful in terms of their expectations: secret ballots, the pseudo-anonymity of the electors, the lack of clarity in the number of votes, the reliance of the voting process on the central organisation [2]. These are actually the most serious concerns in current voting processes [3]. Control in the hands of central authorities plays a vital role in exploiting the alteration in the votes cast and announcing biased results [1]. To slove the aforementioned problem blockchain technology is one of the alternatives since it encompasses a shared structure and multiple people own the whole database [4]. It is possible to eliminate one of the manipulating origins of database abuse by implementing blockchain throughout the distribution of databases on voting platforms [5]. It's a highly secured technology [6] which provides both security and privacy [7]. But implementation of Ethereum blockchain voting system, computing is costly because all the peers on the Ethereum Network perform and validate transactions. Ethereum specifies a gas measurement to calculate transactions computation and storage costs. In other terms, any transaction has a charge (consumed gas) payable in the Ether by its sender. There is also a limitation on block gas specifying the maximum quantity of gas consumable from all cumulative transactions in a single block. Smart contracts cannot however contain extremely costly calculations exceeding the block gas limit [8]. To solve these issues sidechain can be used. Sidechains expand the network to make it easier to build additional functionality by preventing writing on the main blockchains and the need to create a new currency [9]. Our objective is to design a ethereum blockchain based digital voting using sidechain and smart contracts to reduce the cost consumption and extends the capabilities of mainchain. In our proposed system, there are three blockchain : Registration Chain, Voting Chain and Vote Managment Chain where Vote Managment chain is acted as Main Chain and Registration Chain and Voting Chain are used as side chain to reduce the cost of the proposed system.

The paper is organized as follows. In Section II, related works about voting based on blockchains are discussed. In Section III, general architecture of the proposed blockchain based voting election system is explained. At the following section, Section IV, Cost of proposed system is analyzed theoretically. In the final section, Section V, future work on the system is discussed and conclusions about the research have been made.

II. Related Works

A blockchain based digital voting system using biohash and smart contract is proposed in [10]. They have generated hash value from voter registration information and used it for voter authentication. The casted vote is received by smart contract and immediately counted by it in this system. [11] proposed a decentralized electronic voting infrastructure using Ethereum Blockchain, smart contracts and homomorphic cryptography to ensure a transparent electoral mechanism using non-authority-based counting and voting data security. It is designed for using in a system of voting at university level. It is easy to configure the ballot and election system for multiple voting styles and logic-based votes. A blockchain-based e-voting scheme is proposed by Haibo Yi in [12]. In this system verification and transparency are provided using an electric curve encryption(ECC)-based user approval framework. This process takes a long time and is consequently vulnerable to quantum attacks.

978-1-6654-2254-3/20/$31.00 ©2020 IEEE

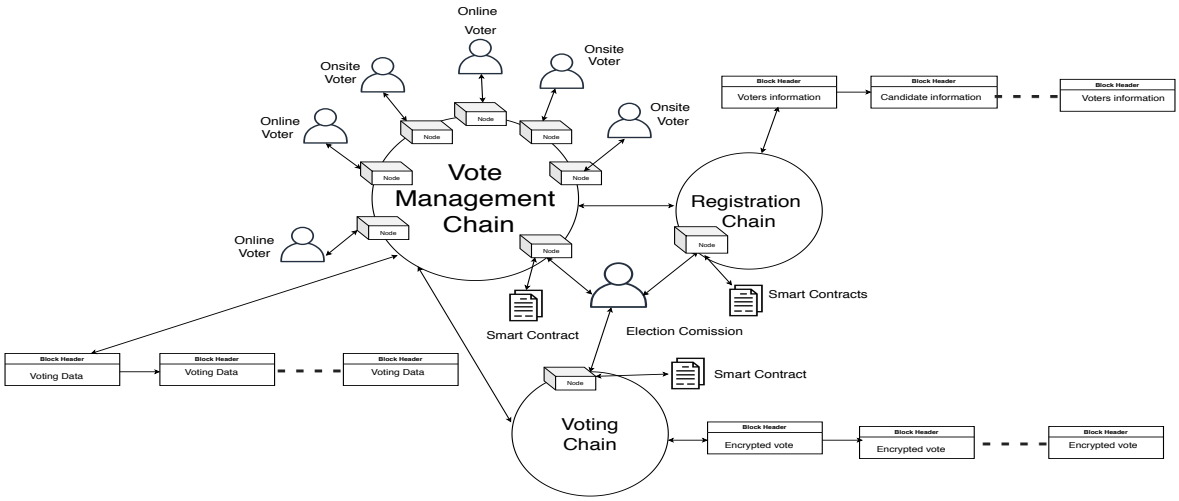

Fig. 1. Digital Voting using Sidechain and Smart Contracts

A modern e-voting method called Crypto-voting is introduced in [9]. They based this idea on the Shamirs method for hidden communication, applied using the blockchain platform. They use side chain. The proposed system manages 3 distinct phases of the voting process : preparatory activities and formation of electoral lists, management of voting , count of votes. In [13], they propose a sidechain based voting where the registration information is stored in chain through the smart contract for authentication process. After the authentication the voters can cast their vote. The voting information will be stored in main chain.

III. Proposed Voting System

To bring scalability and efficiency to the deployment of Voting Network on Ethereum, the computational and storage problems has to be solved [14]. Sidechain technolgy is used to solve these issues in this system. There are three chains named Registration Chain ,Voting Chain and Vote Management Chain Where Registration chain and Voting Chain act as Sidechain and Vote Management Chain acts as Main Chain as shown in fig 1. The details of three chains are described below :

1) Registration Chain :

There is a smart contract running in this chain named registration contract . All the information of voters are stored by the registration contract during registration process. These information are used in authentication process of voters at the time of vote casting. It also stores the candidates information in the chain. During vote casting it provides the candidate information.

2) Voting Chain :

The Voting Chain is used to record the encrypted votes of voters after performing the authentication process by registration contract. During the vote casting, voter chooses one of the candidates from the list of candidates and casts vote. The casted vote is encrypted using public key list which is provided by Election Commissioner and stored in the voting chain. After ending time of election, Election commissioner inputs all the private key in the vote counting phase. The voting contract gets all the decrypted vote one by one and then it sends all the votes to the managing contract of vote management chain.

3) Vote Management Chain :

After getting all the decrypted vote Managing contract counts all the votes and publish the result

A. Phases of Voting

The architecture of the proposed voting method is divided into four phases :

1) Registration Phase
2) Voter Authentication Phase
3) Voting Phase
4) Vote Counting Phase

1) Registration Phase

In registration phase voter and candidate registration are performed. Voter registration is important to keep an eye on the voter participation as part of the identity verification process. It is a method for monitoring the presence of non-registered individuals. The Candidate Registration process is same as like voter registration because a candidate is also a voter. After completing registration process as a voter the candidate input region, party symbol and seat number to complete registration process as a candidate. Submitted information of voters and candidates are stored by registration contract in the Registration Chain

2) Voting Authentication Phase

The voter authentication process is done by Registration contract. Voter at first sign in their wallet using their private key, Then submit the credentials for authentication. Registration contract checks the credentials to match the hash with existing hash values in the registration chain. If both hash value matches then it send the the verification result of voter.

3) Voting Phasse

A vote is represented as a transaction which contains the transaction index, timestamp and the hash of the current transaction. After performing the authentication process voter will get candidate list with party symbol. There is a list of public key from election commission. Voters can choose candidates from candidate list and cast vote. The casted vote is encrypted with the public key from the list randomly and the transaction will be added into voting chain.

4) Vote Counting Phase

The final stage of the voting protocol is the vote counting process. During the counting process Election commissionar inputs the private key of all the public key in the list. Each encrypted vote will be decrypted from voting chain and the voting contract will send the casted vote to the managing contract in vote management chain. Once the vote is sent, the vote is counted immediately by managing contract. Then the managing contract publish the result.

IV. Experimental Analysis

A. CONCUSSES IN THE BLOCKCHAIN

A issue of concussion may emerge with decentralized systems, especially with blockchain based e-voting methods. This happens as multiple electors participate at almost the same time. This is linked whenever an elector votes to create an unmistakeable or distinct line in conjunction with the last vote [15]. In case of bitcoin these types of blocks are called orphan block [16] and in case of ethereum called uncle block [17]. In the proposed system there is no concusses problem as the voting transaction is first submitted to voting contract and then vote will be added into the sidechain named voting chain. After ending time of election all the votes are unlocking in main chain and counted by the managing contract. Managing contract counts each vote and added into the vote management chain, So each block's information will be sent to the miner after a certain time interval as shown in fig.2 and there is no chance for missing any block.

B. Cost Analysis

In the Ethereum network, the currency used is called Ether (ETH). Computation within the blockchain and the EVM are repaid in ETH, while the execution charge is calculated in gas terms. Practically , one unit of gas refers to the execution of one computational phase and gas and ETH are purposely

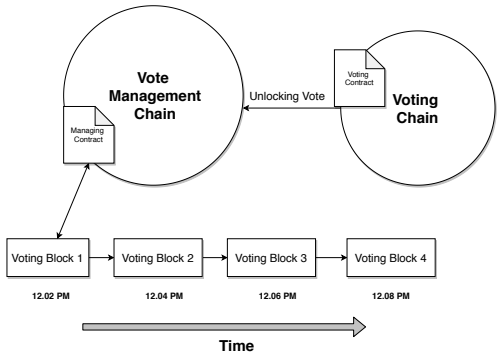

Fig. 2. Solution of Concussess

decoupled in such a manner that the fluctuation of ETH prices is induced by global market factors and the cost of gas is connected directly to the cost of computation [18]. Table 1 and Table 2 show the contract deployment and execution cost.

TABLE I
GAS COSTS FOR INITIAL CONTRACT DEPLOYMENT

Contract	Gas Cost
Registration Contract	Reg_{cost}
Managing Contract	Mng_{cost}
Voting Contract	Vt_{cost}

Total contract deployment cost is $Total_{cdcost}$,
= Reg_{cost} + Mng_{cost} + Vt_{cost}

TABLE II
EXECUTION GAS COST

Operation	Gas Cost
Registration of voter	V_{rcost}
Candidate Registration	C_{rcost}
Casted encrypted vote	$VT_{enc_{cost}}$
Vote Counting	Ct_{cost}

Execution cost of Registration Chain,
Reg_{ecost} = V_{rcost} + C_{rcost}

Execution cost of Voting Chain,

VTC_{ecost} = $VT_{enc_{cost}}$

Execution cost of Vote Management Chain,

VMC_{ecost} = Ct_{cost}

We know that, Transaction Cost is the summation of Contract Deployment Cost and Execution Cost and Sidechain creates a new currency which is the copy of mainchain to perform a particular function then returns the result to the maincahin the execution cost of sidchain is not counted. So the execution cost of registration chain and voting chain will not be counted as the transaction is done by duplicate ether

of vote management chain.

Total Transaction cost of this system is,
= $Total_{cdcost}$ + VMC_{ecost}

Saved Cost
= Reg_{ecost} + VTC_{ecost}

V. Conclusions and Future Work

Blockchain is an important and exciting option that offers data integrity and is a highly demanding subject. As the voting process should be treated with caution to prevent and proceed under exceptional situations, blockchain can minimize the limitations of manual voting and participations of third parties. But owing to cost problems of blockchain, ensuring protection in the electoral system is a significant problem for many nations. Taking this in consideration we have proposed a cost effective blockchain based voting system using sidechain and smart contracts to reduce the cost consumption. In future we will describe this voting mechanisms widely and implement it practically.

References

[1] H. Patil, M. Rathi, and M. M. V. Tribhuwan, "A study on decentralized e-voting system using blockchain technology," 2018.

[2] X. Zou, H. Li, F. Li, W. Peng, and Y. Sui, "Transparent, auditable, and stepwise verifiable online e-voting enabling an open and fair election," *Cryptography*, vol. 1, p. 13, 08 2017.

[3] D. Kumar, D. Chandini, B. Reddy, D. Bhattacharyya, and T.-h. Kim, "Secure electronic voting system using blockchain technology," *International Journal of Advanced Science and Technology*, vol. 118, pp. 13–22, 09 2018.

[4] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A decentralized patient agent controlled blockchain for remote patient monitoring," in *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 1–8, 2019.

[5] G. Bhavani, "Survey on blockchain based e-voting recording system design," 11 2018.

[6] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A patient agent to manage blockchains for remote patient monitoring," *Studies in health technology and informatics*, 10 2018.

[7] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "An efficient selective miner consensus protocol in blockchain oriented iot smart monitoring," pp. 1135–1142, 02 2019.

[8] C. Braghin, S. Cimato, E. Damiani, and M. Baronchelli, *Designing Smart-Contract Based Auctions*, pp. 54–64. 01 2020.

[9] F. Fusco, M. I. Lunesu, F. Pani, and A. Pinna, "Crypto-voting, a blockchain based e-voting system," pp. 223–227, 01 2018.

[10] S. T. Alvi, M. N. Uddin, and L. Islam, "Digital voting: A blockchain-based e-voting system using biohash and smart contract," in *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 228–233, 2020.

[11] P. Marella, M. Milojkovic, J. Mohler, and G. Dagher, *GenVote: Blockchain-Based Customizable and Secure Voting Platform*, pp. 152–171. 07 2019.

[12] H. Yi, "Securing e-voting based on blockchain in p2p network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, pp. 1–9, 2019.

[13] D. Pawade, A. Sakhapara, A. Badgujar, D. Adepu, and M. Andrade, *Secure Online Voting System Using Biometric and Blockchain*, pp. 93–110. 01 2020.

[14] M. Seifelnasr, H. S. Galal, and A. M. Youssef, "Scalable open-vote network on ethereum," *IACR Cryptology ePrint Archive*, vol. 2020, p. 33, 2020.

[15] A. B. Ayed, "A conceptual secure blockchain based electronic voting system," *International Journal of Network Security Its Applications*, vol. 9, pp. 01–09, 2017.

[16] Investopedia, "Orphan block."

[17] Investopedia, "Uncle block (cryptocurrency)."

[18] K. Patidar and S. Jain, "Decentralized e-voting portal using blockchain," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–4, 2019.