



## Blockchain Interfaced Secure E-Voting System

**Raj Shrestha, Rajiv Sah, Sabin Shrestha, Shailja Sarawagi, Nanda Bikram Adhikari<sup>1</sup>**

Department of Electronics and Computer Engineering, Pulchowk Campus  
Institute of Engineering, Tribhuvan University, Nepal

<sup>1</sup>Corresponding author: [adhikari@ioe.edu.np](mailto:adhikari@ioe.edu.np); [071bct528@pcampus.edu.np](mailto:071bct528@pcampus.edu.np)

**Received:** Nov 3, 2018

**Revised:** Dec 25, 2018

**Accepted:** Dec 28, 2018

---

**Abstract:** National elections are a big deal which has a major role in the development and progress of a country. The security of an election is in fact the matter of national security. Current voting systems in the context of Nepal and other parts of the world are still traditional and insecure. From the dawn of democracy, elections are still based on pen and papers. While there are new electronic voting machines, these systems have a high risk of rigging and are prone to failure, crashes, and attacks from intruders. The stated problems can be addressed through the implementation of new technology namely Blockchain for a transparent and reliable voting process. A blockchain based voting platform has been built to make the voting process digital, secure, reliable and intuitive. The votes casted by voters are stored in the blockchain, thus making it immutable and secure. The system can be scaled based on the requirements of an election. Voters can login to the system with the help of encrypted identification. This encrypted identification will lead to secure voting process. A separate portal for both voters and the election commission reduces the election hassle and time. So, in this system, it is demonstrated how the use of blockchain platform could contribute to modern elections using Ethereum, smart contracts and distributed systems to provide voters with secure, transparent and reliable voting platform.

**Keywords:** Blockchain voting system, smart contracts, blockchain, ethereum, decentralization.

---

### 1. Introduction

Voting is an important part of choosing a rightful candidate through the democratic process and hence is a crucial process for any country. Among different vote collection methods, a paper-based method is widely adopted one. In this method, the voter selects the preferred candidate or party by marking the corresponding symbol or letter. In the context of Nepal too, the paper-based method is practiced for the process of election. With the advancement of technology all around the world, isn't it high time that we modernize the voting process? The use of machines at the polling centers or casting vote directly from home via the internet can digitize the voting process. It would be wonderful if the voting is carried out through a platform that is secure enough and provides transparency into result of the election. The places like Estonia, Norway, and Australia have already conducted online voting process. There are several challenges that we have to face to create this online platform. Digitizing the voting process may upsurge different security issues. The weakness in the architecture of the system can lead to manipulation of the election result. Vote-fraud due to attacks from the intruders may manipulate the result or may result in the loss

of the data which is totally unacceptable in a democratic process like the election and the election process cannot be rerun. One of the best potential solutions is to use the blockchain technology.

## **2. Problem Statement**

Electronic Voting is not a new concept, in fact it was first-ever introduced in 1986. David Shagum was first to introduce the first-ever electronic voting system which was based on a public key cryptography [3]. Keeping no connection between voters and ballots, a secure country election was conducted. Electronic voting machines have been viewed vulnerable, based on physical security concerns. These machines can be sabotaged by anyone who has physical access to it, thus affecting all votes casted on the machine. The major vulnerability is the centralized database where election's data are stored. This vulnerability could be a single point of failure. However, integrating blockchain technology on the aforementioned machine can take the entire voting system to the whole new level. Blockchain-based election was held for the first time in Sierra Leone, country of Western Africa. Blockchain is a distributed, immutable public ledger introduced in 2008 by Satoshi Nakamoto in form of creation of the first cryptocurrency, called Bitcoin. The Bitcoin blockchain uses a decentralized public ledger with POW (Proof-of-Work) consensus protocol [1]. The chain of the blocks in the blockchain is cloned, cryptographically signed and verified publicly at every transaction so that no one can meddle the data once written on the blockchain [2]. Due to its immutable property and decentralized architecture, it can carry out elections in a more transparent and secure way. Blockchain E-Voting System comprising of blockchain where votes casted are recorded, smart contract handling overall election processes, private nodes providing consensus and the voter portal accessible to the voters can guarantee the security, integrity and transparency of the casted votes including the anonymity of the voters avoiding the single point of failure as compared to the traditional centralized e-voting system. The smart contract can be taken as an election, transaction as a ballot-paper and blockchain as a ballot-box. This blockchain is accessible to the general public to make the election more transparent.

## **3. Methods**

The voting process is conducted in three different phases.

### **3.1 Pre-Voting Phase**

The pre-voting phase is generally concerned with the preliminary data collection, registration and creation process. Voters are registered on respective constituencies during the election campaign. The system handles all the registration procedures and stores the data in election commission's database server. Later this data is used for the pre-validation of voters during voting phase. Voters are also registered on the smart contract on the blockchain network. Only the voters registered on the smart contract are eligible to cast their votes. Smart contract maintains the integrity of the voters data in the blockchain network. It discards the votes from fraud voters. After the registration process, voters are provided with their respective encrypted identification which is embedded on their new voting cards as QR Code. This identification gives access to their respective wallets in blockchain network. Figure 2 represents the detail activity diagram for the voter registration process. Each voter has a predefined number of tokens in his/her wallet. During the voting process, these tokens are transferred to selected candidates wallet. The token in the voter's wallet is a token created in a smart contract. This token cannot be replicated or created. So there are fix number of tokens issued to the voter. Similar to voter, candidates are also registered on the system and smart contract with their corresponding wallets.

### 3.2 Voting Phase

The voting phase is the most critical phase as it deals with hundreds or thousands of transactions at a single point of time. Voting booths are distributed at different locations and the voters who are assigned to their booth centers have to visit the respective booths strictly in order to cast their votes. Each booth is

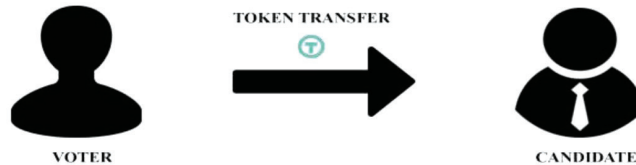


Fig. 1: Voter-to-candidate token transfer process

provided with several dedicated voting devices. Each of these devices are loaded with the voting application which is managed by respective booth admin. The system maintains the log of all activities on voting devices. Voters can cast their votes using their encrypted QR Code. The voting application has a scanner which scans and authorizes the voters. If the voters are authorized to use the device, the system starts the voting process. The system displays different ballot paper depending upon the type of election. Voter can select their desired candidate with an interactive touch screen or input device. After submitting the ballot paper, the election device makes a procedure call to API Server to transfer the tokens from voter's address to candidate address. Once the token has been transferred, the voters wallet will be empty. Fig. 1 depicts the token transfer process from voter to client. The system can assure the security of the casted votes as it is almost impossible to manipulate information stored on the blockchain.

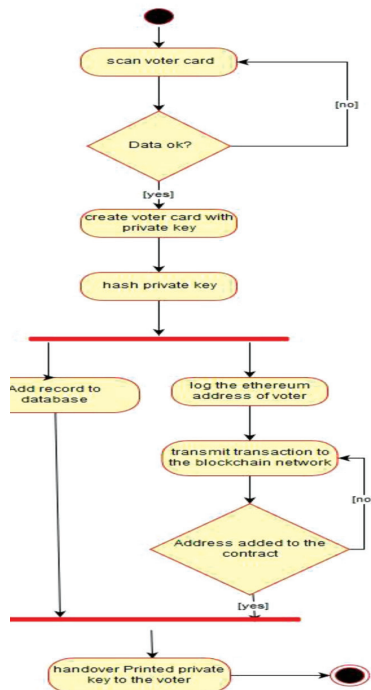


Fig. 2: Activity diagram for the voter registration

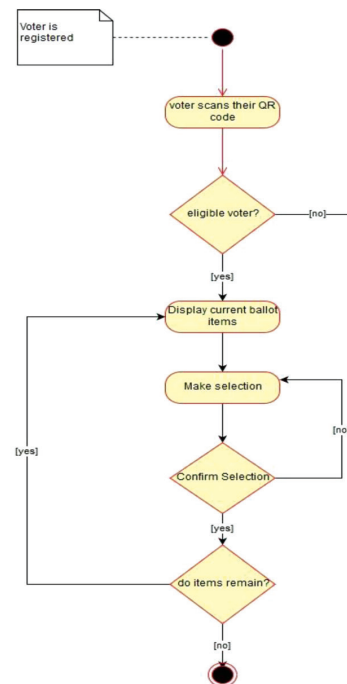


Fig. 3: Activity diagram for the voting process

### 3.3 Post-Voting Phase

Post-voting phase is another crucial phase of the election. This phase includes vote counting tasks, analyzing the results and finally declaring the winners. Traditional systems can take significant amount of time to count the votes. Counting phase is the most vulnerable phase in the voting process. The voting results can be manipulated according to interest during counting process. The system secures casted votes by storing it in the blockchain. The voting results are published by counting the number of tokens transferred to candidate's wallet. Voters can assure the legitimacy of the result by viewing their transaction history. Fig. 3 shows the block diagram of the system as of its architecture.

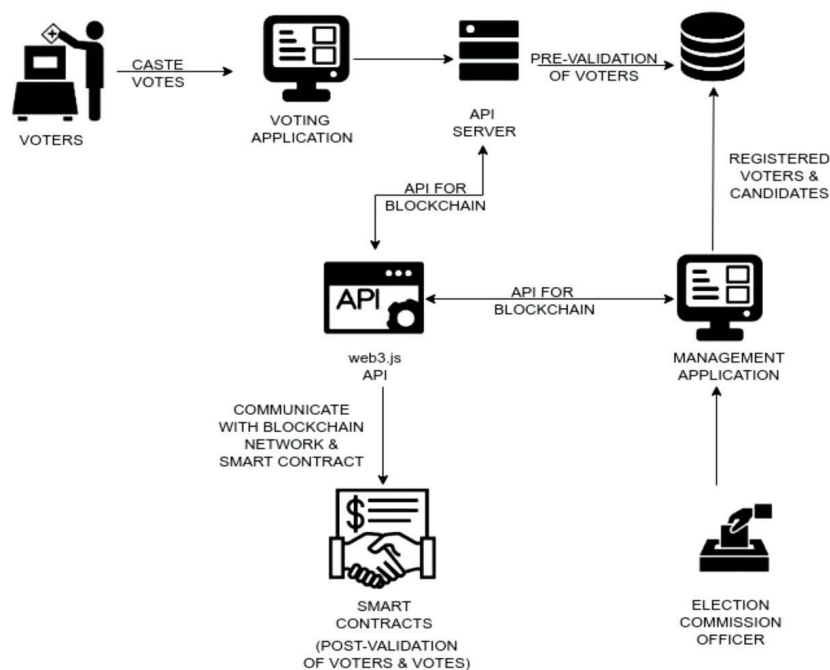


Fig. 4: System architecture

## 4. Results and Discussion

The work on the described concept can be utilized in the development of a fully functional voting system over a blockchain network. With the immutability property and decentralized architecture of blockchain, properly implemented in the case of e-voting platform, the wrangling around the voting process can be lessened tremendously. On the one hand, the inclusion of cryptography in the core architecture of blockchain the critical information of the voter and candidates results in the maintenance of the anonymity while on the other hand, the public distributed ledger can be viewed by anyone on the system to verify the aftermath of the election.

A blockchain-based electronic voting system has been implemented that utilizes smart contracts to enable secure and cost-effective election while ensuring voter's privacy. The system architecture and the design have been outlined. Comparing to the naïve electronic voting system, it has been shown that blockchain technology has tremendous potential for democratic countries to advance from pen and paper scheme, to a more cost-effective and time-efficient election scheme and offer

new possibilities of transparency. The major stages of the system, Voter Login, Voting, Voting Confirmation and Election Result respectively are shown in Fig. 4.

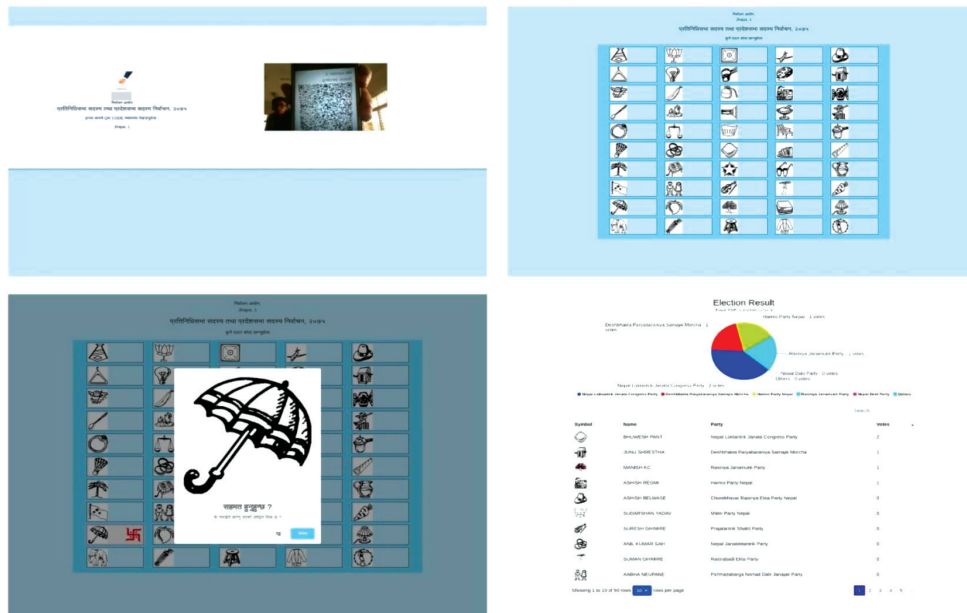


Fig. 5: Screenshots of voting system outcomes

## 5. Conclusion

The concept of digital voting systems to make the electoral process cheaper, faster, transparent and reliable, is fascinating in modern society. Each vote is important and should be registered as one vote can determine the fate of the election. Besides, paper voting system results in multiple invalid votes. The e-voting system can also be one of the viable solution to the problem of declining interest among the youth to participate in the election. Hence, to maintain the fairness, privacy, verifiability in election, blockchain has been implemented as the potential solution.

## References

- [1] Bashir I (2017), *Mastering Blockchain*, Packt Publishing, Mumbai, India.
- [2] Chase J (2017), *Distributed Systems, Failures and Consensus*, Duke University, USA.
- [3] Schaupp LC and Carter L (2005), E-voting: from apathy to adoption, *Journal of Enterprise Information Management*, **18(5)**: 586–601.