Decentralized Voting System : A Solution To Save Democracy Not Only In Bangladesh Also The World

Md. Meharab Latif

Department of CSE, National University

Abstract:

If we look at the history people was always the most important part of Democracy. But when the population got increase very rapidly and the method/technology was not suitable to engage in Democracy then the society have no option but to be semi-centralized. In centralized environments, the results of voting events have always been questionable and perceived differently by voters. Most existing E-Voting systems are based on centralized servers where the voters must trust the organizing authority for the integrity of the results. In this paper i propose a novel approach for a decentralized trustless voting platform that relies on Blockchain technology to solve the trust issues. The main features of this system include ensuring data integrity and transparency, and enforcing one vote per national identification number for every poll with ensured privacy. To accomplish this, the Ethereum Virtual Machine (EVM) is used as the Blockchain runtime environment, on which transparent, consistent and deterministic smart contracts will be deployed by organizers for each voting event to run the voting rules. Users are authenticated through their NID and Birth certificate serial number. Results showed that the system is feasible and may offer a step towards ideal environments for such experience.

Problem Statement:

Bangladesh's 29 December 2008 general election is expected to end a two-year military-enforced state of emergency and return the country to democratic governance. While an end to emergency rule and elections do not equal democracy, both are necessary preconditions for the country's stability. Through peaceful dialogue – an important achievement in its own right – the army-backed

caretaker government (CTG) and the country's main political parties have reached agreements on many issues that could derail the elections. However, there are no guarantees that the election will take place on time, that all the major parties will participate, or that all of them will accept the results.

Above statement is covered by a international news organization called Crisis.org Since then there are not a single election held that satisfied all parties. Even a neutral election commission has been created but then the accusation came that the election commission is biased or corrupted. So, the results of all the problems are

1. Voters cannot provide vote to their desired candidate.
2. Vote is not count properly
3. Fake vote is massively conducted
4. Cost of election is massive (corruption excluded)
5. Lack of Safety for the voters
6. Takes a long time to perform the whole procedure
7. Vote damages.

Etc.

বাংলাদেশ নির্বাচন কমিশন: সংশোধিত বাজেট ও ব্যয় (২০০৮-০৯ - ২০১২-১৩ অর্থবছর) (অংকসমূহ হাজার টাকায়)

বিবরণ	২০০৮-০৯		২০০৯-১০		২০১০-১১		২০১১-১২		২০১২-১৩	
	সংশোধিত বাজেট	ব্যয়	সংশোধিত বাজেট	ব্যয়	সংশোধিত বাজেট	ব্যয়	সংশোধিত বাজেট	ব্যয়	সংশোধিত বাজেট	ব্যয়
সচিবালয়	১৫,৭৬,৬১	১৪,১৩,০৩	২৭,০৬,৬৮	২৫,৭৯,৮৭	২৮,৮৮,৮৯	৯,৬৯,১০	২১,৪১,২৯		৭৫,৪৯,১৬	
নির্বাচনী প্রশিক্ষণ ইনস্টিটিউট	৭০,০৫	৫৯,৫৫	৮৯,৮০	৭৪,৬৬	৯০,২৪	৮১,৪৬	৪,৯৫,২৩		৮,৯৭,৭৯	
মাঠ পর্যায়ের কার্যালয়	২৬,৭৪,৪৭	২৩,২৫,১১	২৯,২৩,৪২	২৬,৭৯,৩৫	৩৪,২৬,২৬	২৯,১৩,৭৬	৪১,৪১,৩৭		৪৫,৫৬,৮৫	
আন্তর্জাতিক প্রতিষ্ঠানের চাঁদা	০	০	০	০	৭০	৭৩	১০০		১০০	
মোট (প্রশাসন)	৪৩,২১,১৩	৩৭,৯৭,৪৯	৫৭,১৯,৯০	৫৩,৩৩,৮৮	৬৪,৯৬,৩৩	৩৯,৬৫,০৫	৬৭,৭৮,৮৯		১৩০,০৪,৮০	
নির্বাচন ব্যয়	৪১৯,০০,০০	১৯৫,১২,৩৮	৩০০,০০,০০	৩,৯০,৭৭	১৫০,০০,০০	১৩৮,৮১,৩৩	১২৩,০০,০০		৮৩,৩৫,০০	
মোট	৪৬২,২১,১৩	৩৩৩,০৯,৮৭	৩৫৭,১৯,৯০	৫৭,২৪,৩৫	৩১২,২৯,৩৪	২৭৮,৪৬,৩৮	১৯০,৭৮,৮৯		২১৩,৩৯,৮০	

সূত্র: নির্বাচন কমিশন থেকে প্রাপ্ত তথ্য অনুযায়ী, আগস্ট ২০১৩।

figure: Budget and cost of election

So we can see that there is a massive inconsistency cost raise during every election. Every year the participant of voter is exponentially decreasing. And there are many complaints came from the voter that votes are purchased by money or they are being threaten to vote a particular candidate.

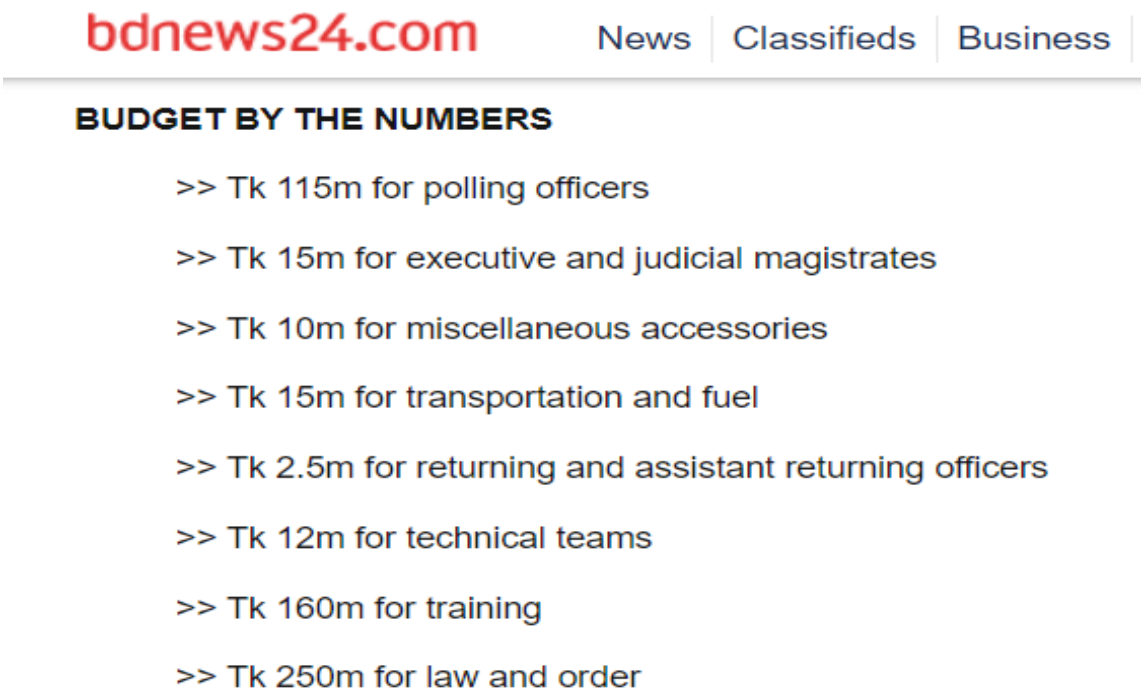

Figure: Budget distribution

Solution:

The solution to this problem has to meet the following criteria

1. All the voter will have opportunity to vote to their desire candidate
2. Vote have to count properly
3. A voter cannot give more than one vote
4. Cost will be less
5. Identity of voter will not be reviled
6. Have to take short amount of time
7. The whole process should be transparent

If the Blockchain is applied then it will cover all the criteria that is stated above. More specifically if Ethereum is used as a platform to deploy the Dapp, it will ensure the above criteria stated above. The Ethereum is suitable for this service because it provides EVM (Ethereum Virtual Machine) services and the mining time is comparably low.

In my solution I will use 2 server , a centralized server and blockchain.

The centralized server will used to store voters necessary information and the blockchain will used to process voting transactions.so the Dapp process will go as follows

Step 1: first a voter has to provide his NID, NAME as in NID, and Birth Certificate number to log into the app.

Step 2: then the voter will provide a 64bit long private key which will be led him to a digital wallet.

Step 3: the voter have to copy the private key and have to have one of the following

- A crypto wallet extension in his browser e.g., metamask
- A legacy browser (it has built-in wallet)
- A crypto wallet app in his system

Step 4: the voter has to import the account using private key which will contain limited amount of currency to provide Gas price for 1 vote

Step 5: then the voter has to go to next page by pressing next button to enter digital ballot paper page

Step 6: in the digital ballot paper page the voter will see candidates' names and their photos and a button for vote for each candidate. This data will provide by smart contract

Step 7: the voter will have to vote either one of candidate. The vote cannot vote more than one because the smart contract will not allow this and he will not have enough gas to pay.

After voting the voting button will disappear and the voter can see real time voting update.

There are no need for 3rd party to handle the process. But an admin is need to deploy the smart contract and shut down the smart contract. There will not need for particular admin page. The smart contract will be active when the admin lunch the app and the admin will see the additional shutdown button in his digital ballot paper page.

When the admin shutdown the smart contract the contract will be destroyed and immediately the result will reveal.

Vision & Mission:

"Keep Democracy Alive & Decentralized"

Our vision is to create a system that is very easy to use for every level of user and also decentralized.

Voting is first and the most important right of a citizen. Because of massive population and the cost is very high to arrange an election, so it is not possible for a government to arrange an election for every matter in a state. So, we cannot practice democracy in proper way. So, our mission is

1. Reducing the cost of election.
2. Make the election so reliable that every aspect of citizen can participate.
3. Keep voting practice available in every aspect of our daily life. No matter how little or big it is.

Service:

Our service is to the end users are

1. Maintain anonymous/privacy
2. Very easy interface
3. Not very time consuming
4. Live vote update
5. Less technical problem
6. Lightweight app
7. Cross platform app

This are the basic services that every user wants.

Legal Issue:

We all concern about the law of Bangladesh government that state " Financial institutions are not allowed to facilitate bitcoin transactions." In September 2014, Bangladesh Bank said that "anybody caught using the virtual currency could be jailed under the country's strict anti-money laundering laws". So, in this Dapp the

Bangladesh government have to provide the crypto currency or the whole process will be illegal by the law.

Technology:

There are two different approaches in voting system

1. The paper based approached
2. EVM (Electronic Voting Machine)

Problems with paper based approached are

1. Vote could be damage
2. Fake vote can be supplied by intruder
3. Very lengthy process
4. Vote have to count by hand
5. Very costly process
6. Need 3rd party to execute the whole process
7. Not transparent

Problems with EVM (Electronic Voting Machine) are

1. Lack of transparency
2. Still a costly process
3. Still need 3rd party to execute the whole process
4. Still a lengthy process
5. Centralized database is not secured
6. Voter's privacy is not covered by the system
7. Database & EVM (Electronic Voting Machine) both are damageable

Reasons because the blockchain is the better choice are

1. Blockchain provides a distributed and decentralized platform where every node is synced with each other. So, even if a few nodes got down but it will not affect the network. So, data will be safe.
2. Because of the chain of hashing block of blockchain system, it will be impossible to hack to change the data. So, blockchain is almost unbackable. Hacker will need 1/3 of computational power of the world to hack bitcoin blockchain.
3. In blockchain network everything is transparent. So, any node tries to manipulate the data other nodes will know because of hashing mechanism.

4. Voter's privacy or anonymity will not be compromised because of the transparency. Because in blockchain everything processes as n-bit hash address.
5. Voting process will be fast because the server will not be down because of over hitting.
6. Using blockchain as a database and a platform, it will reduce the cost enormously.
7. If blockchain is used, there will not need for any 3rd party because there are a service called smart contract which will automate the process and also will count and show data in real time.

Reasons behind choosing Ethereum as a platform for voting Dapp application are

The Ethereum network currently dominates Dapp development for several reasons. Ethereum implements a development interface that reduces programming time and helps quickly launch projects. Beyond this, the Ethereum developer community has grown remarkably since the platform's launch. And Ethereum retains formidable network effects from its global coalition of technologists who remain committed to maintaining the network and actively developing user resources that drive adoption. Further, the ability to adequately monetize Dapp projects incentivizes others to partake in the Ethereum ecosystem. Other tools

- **Front-End** : HTML, CSS, JavaScript
- **Front-End Frameworks** : Sublime, Bootstrap, jQuery
- **Back-End** : JavaScript, PHP, Solidity
- **Back-End Frameworks** : Node.js, Xampp, Remix, Express.js
- **Blockchain** : Ethereum
- **Blockchain Interaction Frameworks** : web3.js, metamax, ganache

Architecture of voting Dapp

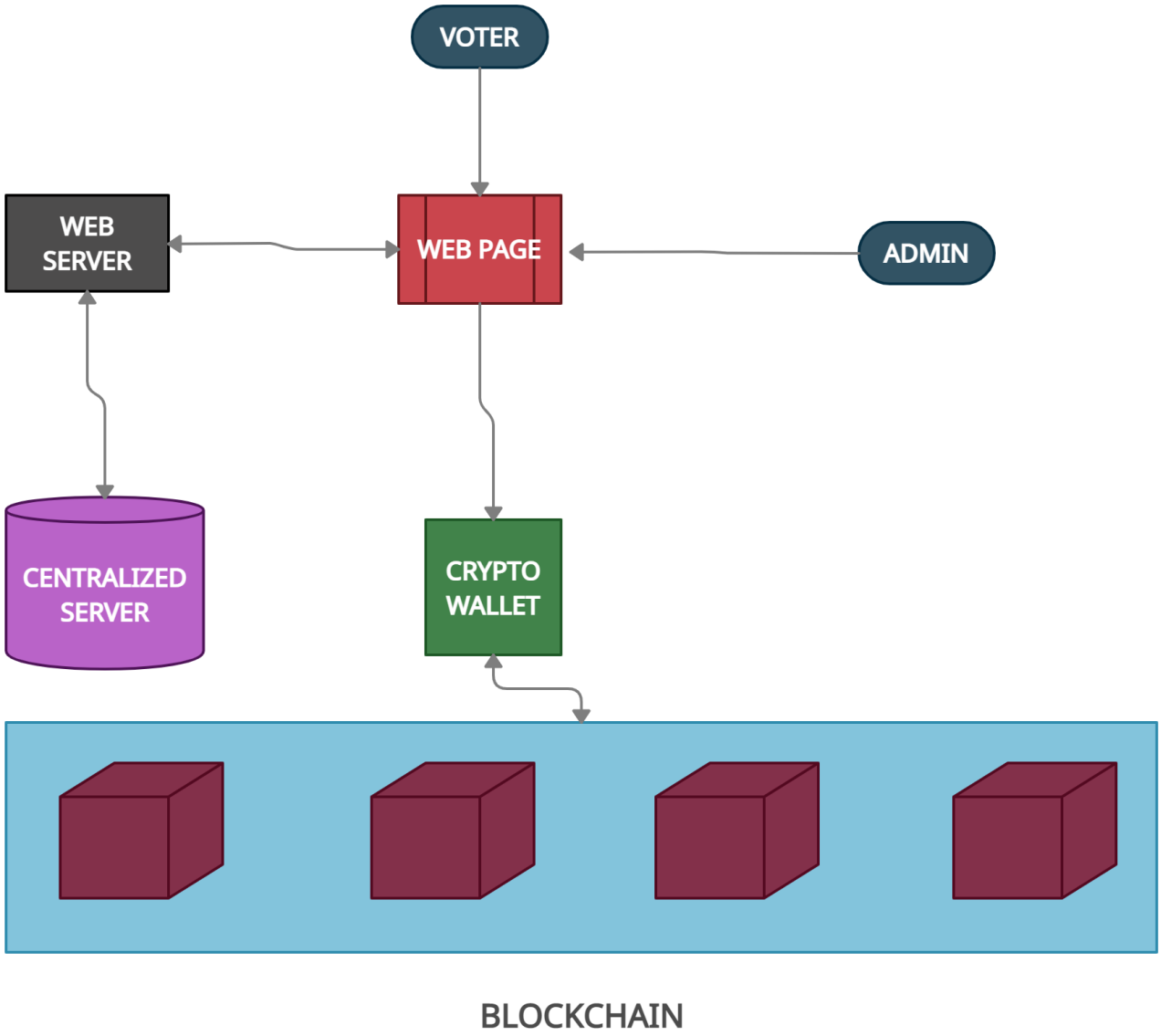

Figure: integration of different tools and frameworks for voting Dapp

Operational Procedure:

The step-by-step operational procedure of developing a voting Dapp are

1. Strategy
2. Analysis and Planning
3. UI / UX Design
    - Information Architecture & Workflows
    - Wireframes
    - Style Guide

- Mockups
- Prototype

4. App Development
    - Back-End/Server Technology
    - Blockchain
    - API
    - Web App Front-End
5. Testing
    - User Experience Testing
    - Functional Testing
    - Performance Testing
    - Security Testing
    - Device and Platform Testing
    - Smart Contract Testing
6. Deployment & Support

Cost:

There are basically two types of cost

1. Fixed Cost
2. Variable Cost

Fixed cost is the multiplication of gas price and number of voters. And adding the gas price of deployment and destroying the smart contract. Mathematically,

Fixed cost = (Gas Price * Number of voters)
+ (Gas Price of Deployment of Smart-contract)
+ (Gas Price of Destroying the Smart-contract)

Variable cost depends on the following

1. Salaries of Engineers for creating the architecture and product
2. Salaries of Developers for maintenance of the whole system
3. Web hosting price
4. Gas price
5. Server/cloud price

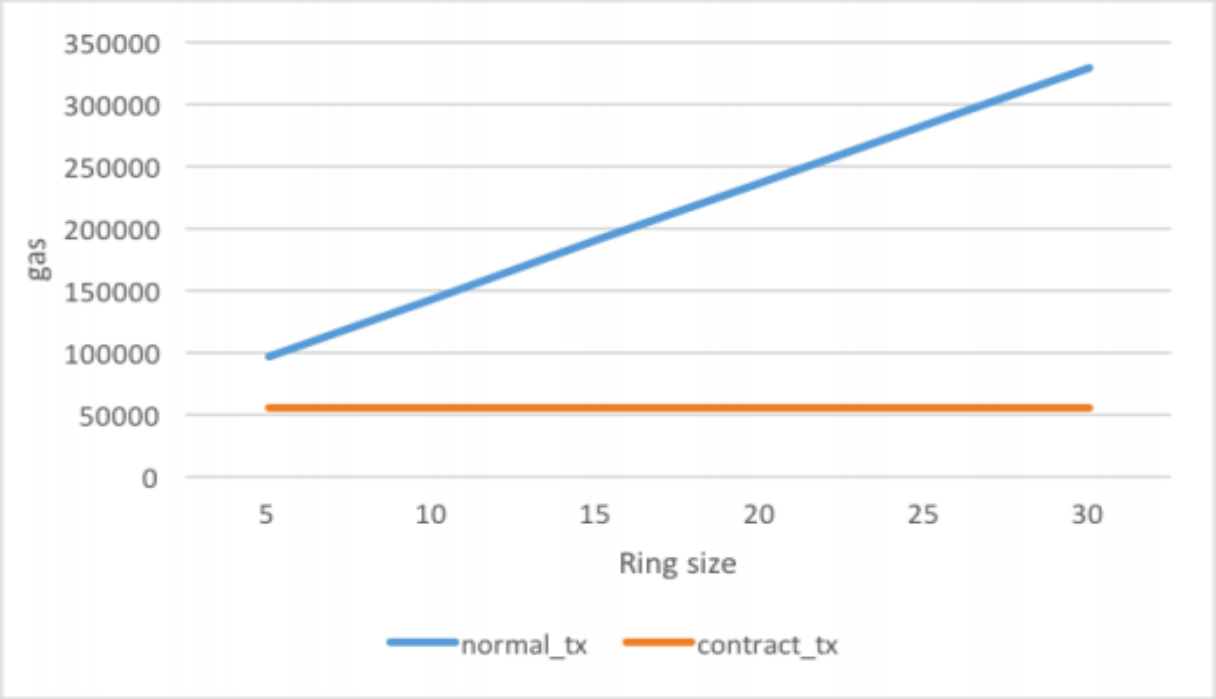

Fig2. Gas cost per ballot on Ethereum

Conclusion:

Blockchain is an emergent technology that is evolving on a daily basis. Similarly, to other new technologies, blockchain adoption by organizations will evolve step by step, through small efforts, some failures, many successes and, hopefully, widespread adoption. So, we proposed a decentralized anonymous voting system which only requires minimal trust in others and gas cost per voter. By putting all the information on Ethereum network, we make the whole election transparent and all participants have identical information. Since the tally phase could speed up via parallel computation, the system is also suitable for large-scale voting.