Development of Electronic Elections Systems: A Review

Hind Salman  
Department of Computer Science, University of Technology, Baghdad, Iraq.

Dr. Rehab Hasan  
Department of Computer Science, University of Technology, Baghdad, Iraq.

Dr. Ekhlas K. Gbashi  
Department of Computer Science, University of Technology, Baghdad, Iraq.

Received September 02, 2021; Accepted December 06, 2021  
ISSN: 1735-188X  
DOI: 10.14704/WEB/V19I1/WEB19117

Abstract

Electronic voting is fast growing rapidly and offers more benefits than traditional paper voting. The use of technology in the voting process has received a lot of attention in recent years. The existing voting systems have several security flaws, and proving even basic security characteristics regarding them is challenging. E-voting system using blockchain works as a step towards creating secure and transparent environment for elections, where the users will be able to view the total votes casted in real time without having the permission to edit after elections get over.

The popularity of E-voting system is increasing in countries all over the world, for that reason this research presents a brief overview to evaluate previous national electronic voting systems in a variety of nations, how they evolved and what were their disadvantages before the appearance of blockchain technology. Then we explain the blockchain technology as well as review some of the electronic voting systems that use blockchain technology and present the strengths and weaknesses of it.

Keywords

Electronic Elections, National Elections, Blockchain.

Introduction

Elections are one of the basic pillars of a democratic society. It enables the general public to express their opinions through voting. Being so important in our society, the electoral process must be reliable to ensure the credibility of the participants; as a result, the voting method is a continuously evolving area for ensuring the security and transparency of the
system. Due to the importance of voting systems, great efforts have been made to improve the overall efficiency and flexibility of voting systems. Voter indifference has risen in recent years. As a result, the internet's growing influence challenges the voting process on a regular basis (Abdulhamid et al., 2013). Electronic voting is being pushed as a potential solution to attract young voters and also it has an important and effective role in it. A number of functional and security requirements are listed for the reliable electronic voting system, including: transparency, accuracy, audibility, system integrity, data privacy and availability, and power distribution (Liu & Wang, 2017).

E-voting has been implemented or is being considered in a number of nations throughout the world. Across Europe, a number of e-voting solutions are being developed, tested, and piloted. Outside of Europe, the United States, Brazil, Estonia and other countries have been attempting to improve and develop the electronic elections system over the recent years (Mpekoa & van Greunen, 2017).

Blockchain technology is an emerging technology with strong cryptographic foundations that enable the applications to take advantage of these capabilities in order to achieve flexible security solutions. The blockchain was created by Satoshi Nakamoto in 2008 to act as the general ledger for the cryptocurrency Bitcoin (Wisessing et al., n.d.). It is an essentially distributed decentralized database that maintains a complete list of ever-growing and ever-expanding data records which are secure from unauthorized manipulation (Patil et al., 2018). Blockchain is the greatest technology for electronic voting systems because of its inability to edit or erase information within the blocks (Ayed, 2017).

The blockchain is a continuously expanding list of documents known as blocks that are connected together via a cryptographic mechanism. Each block contains a cryptographic hash of the preceding block, a timestamp, and data (Bharadi et al., 2020). It is a secure, tamper-resistant and immutable decentralized technology. All users on the same network can be connected to each other’s and have a database that keeps all transaction records. This database is known as Ledger (Zheng et al., 2017). Before being added to the block, each transaction is validated using a consensus process based on the structure of the blockchain. As a result, this strategy ensures the integrity, reliability, and traceability of the system (Wisessing et al., n.d.).

The mission of blockchain technology is to redefine the "trust" of a system that eliminates intermediaries like governments and corporations that engineer future
generations-decentralization With blockchain. "trust" will be in the system rather than the intermediaries responsible for data privacy and security (YI & DAS, 2019).

**Review of the Electronic Election over the World Countries**

In this research, we will review electronic voting in two parts: The first part deals with some experiences of electronic elections that took place in some countries; this part is going to present some techniques that have been used and their weakness problems which they have encountered. The second part deals with electronic voting systems that have used the blockchain technology.

**A. Electronic Voting Systems in some Countries**

Many nations have tried to replace old paper-based voting methods with advanced election technology. The lever-arch machine was introduced in 1982, followed by optical-scan machines and punch card voting systems. Direct recording electronics (DREs), telephone, Kiosk, internet voting systems, and finally mobile voting systems. E-voting system has been used or adopted in large number of nations, but only a few have proved their effectiveness (Mpekoa & van Greunen, 2017), we will explain the experiences of some countries with electronic voting:

1. **Brazilian Electronic Elections System**

   The voting machines have been used since 1996. These machines which sometimes known as kiosks are customized computers which run with specifically created programs that store and count the amount of casted votes by using a keyboard attached to the machine. Because the source codes for the bundled software are not exposed to the public, there are serious concerns about the security of these devices. Some authorities argue that devices are safe as long as the internal software is suitable; nevertheless, if the program is compromised by external access, which may be quite easy, the results could be disastrous (Brunazo Filho & Marcacini, 2016). Since 2000, all Brazilian voters have been able to select their candidates using electronic ballot boxes. The results of the 2010 presidential election, which received over 135 million voters, were declared 75 minutes after the polls closed (Aranha & van de Graaf, 2018).

2. **Irish Electronic Elections System**

   According to reports, the Irish government employed electronic voting machines in the 2002 general election, and test projects were done in three of 42 seats during the election,
yielding 138,011 electronic votes, which were to be utilized in the 2004 European Union elections, these machines were built at a cost of €55 million. During the audit, it was determined that the machines were untrustable and that the results could not be relied upon because of the problems with the paper path and the verification system. Germany and the Netherlands have similarly chosen to prohibit voting indefinitely for similar reasons (Shahzad & Crowcroft, 2019). Due to expense of the present system and popular unhappiness of it, the environment Minister John Gormley said on April 23, 2009 that the electronic voting system would be scrapped (Keupp, 2021).

3. Indian Electronic Elections System

In the 2004 electronic general election, about 370 million Indian voters (out of a total population of 675 million) cast electronic votes, with one million electronic voting machines distributed to 800,000 polling stations (Chakrabarty & Hazra, 2016), these devices known as EVMs, have been recognized for their simple design, ease of use, and accuracy (Kumar & Begum, 2012). Despite the authorities' declaration that the elections were a big success, several key questions remained unanswered. Because the machines did not issue a receipt, the outcomes could not be traced (Oo & Aung, 2014). To reduce the risk of virus or hacking attack Gonggrijp and Hengeveld evaluated at Nedap DRE voting machines and showed software vulnerabilities based on socketed ROM chip replacement. IIT alumnus and IAS officer Omesh Saigal proved that India's 2009 elections may have been manipulated (Wolchok et al., 2010).

4. Estonian Electronic Elections system

In 2005 Estonia is the first country that its people can vote on the Internet using the national card. Voter authentication is done using national ID cards (Specter et al., 2020), as this card creates a signature using SHA1/SHA2, this card is used for the purpose of authorization, encryption and also the signature (Ayed, 2017). The card is both a standard and necessary national identity document also its a smart card that allows for safe remote authentication and legally digital signatures utilizing Estonia's public key infrastructure (Heiberg & Willemon, 2014). Between February 24 and March 2, 2011 (140,846) individuals voted online in the legislative elections. In the 2014 European Parliament elections, 31.3 % of all voters used the internet to cast their ballots. In the 2019 parliamentary elections, 43.75 % of all voters used the internet to cast their ballots (Toots & Idnurm, 2020). Despite its widespread use, the voting system still has numerous flaws, particularly when it comes to state-level attacks.
5. French Electronic Elections System

In 2007, France's UMP party held a presidential primary election employing both remote electronic voting and touch screen electronic voting over the Internet at 750 polling sites. Over 230,000 people voted in the election, accounting for over 70% of the total turnout. (Inuwa & Oye, 2015). In 2012, France's authorities permitted its people living in other countries to vote online according to a portal established by Scytl SA. The online voting operations were subsequently canceled by the National Agency for Cyber security due to the increased risk of cyber-attacks (Çabuk et al., 2020). Due to cybersecurity concerns, France declared on March 6, 2017 that Internet voting (which had previously been available to people worldwide) will not be authorized in the 2017 parliamentary elections. (Le Pennetier et al., 2017).

6. Norwegian Electronic Election System

In 2011, Ten cities in Norway participated in the first local election over the Internet. A remote voting system developed by the e-voting vendor scytl was used for national elections. During the 2013 parliamentary election, a second trial was performed in 12 towns. In 2013, more than 250,000 eligible voters had the chance to vote over the Internet (Volkamer et al., 2011). In 2014 the work with Scytl's Internet Voting initiative stopped due to security flaws, low turnout, and expensive price (Saglie & Segaard, 2016).

<table>
<thead>
<tr>
<th>Country</th>
<th>Year introduced</th>
<th>Technique Used</th>
<th>No. of voters</th>
<th>Voting Population</th>
<th>weakness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil</td>
<td>1996</td>
<td>kiosks</td>
<td>32 million (65%)</td>
<td>48 million</td>
<td>The machines, according to analysts, are open to hacking and other sorts of manipulation.</td>
</tr>
<tr>
<td>Ireland</td>
<td>2002</td>
<td>Irish EVM</td>
<td>24841 (18%)</td>
<td>138011</td>
<td>the machines were untrustable and that the results could not be relied upon because of problems with the paper path and the verification system</td>
</tr>
<tr>
<td>India</td>
<td>2004</td>
<td>EVMs</td>
<td>370 million (54%)</td>
<td>675 million</td>
<td>Scientists evaluated the voting machines and showed software vulnerabilities based on socketed ROM chip replacement, as well as the problems of security attacks</td>
</tr>
<tr>
<td>Estonia</td>
<td>2005</td>
<td>national ID cards</td>
<td>9,317 (0.7%)</td>
<td>1.3 million</td>
<td>Despite its widespread use, the voting system still has numerous problems, particularly when it comes to state-level attacks.</td>
</tr>
<tr>
<td>French</td>
<td>2007</td>
<td>touch screen for E-voting</td>
<td>230000 (70%)</td>
<td>328670</td>
<td>The National Agency for Cyber Security later stopped the online voting operations owing to the elevated danger of cyber-attacks.</td>
</tr>
<tr>
<td>Norway</td>
<td>2013</td>
<td>e-voting vendor scytl</td>
<td>70000 (38%)</td>
<td>250000</td>
<td>Due to security problems, low turnout, and expensive price, Norway abandoned Scytl's Internet Voting initiative in 2014.</td>
</tr>
</tbody>
</table>
Table 2 Comparison between Manual and Automatic Election

<table>
<thead>
<tr>
<th></th>
<th><strong>Manual Election</strong></th>
<th><strong>Automatic Election</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>compliant with the principle of</td>
<td>It is not possessed by all citizens.</td>
</tr>
<tr>
<td>2</td>
<td>The system provides no security, neither</td>
<td>The biometric characteristic of voters is verified between the control and ballot units</td>
</tr>
<tr>
<td></td>
<td>during polling nor voting.</td>
<td>during polling. Allow just the authorized individual to vote.</td>
</tr>
<tr>
<td>3</td>
<td>error prone</td>
<td>There are Fewer error than manual election</td>
</tr>
<tr>
<td>4</td>
<td>Time consuming</td>
<td>It takes very little time at all.</td>
</tr>
<tr>
<td>5</td>
<td>The voter's identity is known.</td>
<td>Neither the PC of the electoral committee nor the electoral register knows the voter’s identity</td>
</tr>
<tr>
<td>6</td>
<td>No e-election automation exists</td>
<td>All e-election processes are automated</td>
</tr>
<tr>
<td>7</td>
<td>Ballot paper is issued by Electoral officer on which voter could cast his vote</td>
<td>Ballot is issued by Electoral officer by pressing a button on the control unit</td>
</tr>
<tr>
<td>8</td>
<td>No digital signature possibilities</td>
<td>Voting may be done from anywhere with a digital signature.</td>
</tr>
<tr>
<td>9</td>
<td>Officials will have to check the ballots manually, which will be a lengthy and time-consuming procedure. Due to human mistake, the data is inaccurate.</td>
<td>The control unit records the number of votes cast for each candidate, whereas the voting unit does not save anything.</td>
</tr>
</tbody>
</table>

B. Electronic Elections Systems based on Blockchain Technology

1. Electronic Elections Systems Based on Blockchain in some Countries

i. Electronic Elections in Moscow

This election proposed a pilot project based on the Ethereum smart contracts platform to integrate blockchain into its electronic voting system. The Russian capital's local administration claims it will be the first city in the world to use blockchain in e-voting on such a large scale (Andoni et al., 2019).

In September 2019, The Internet voting technique based on blockchain was authorized to be utilized by voters in the city of Moscow's Parliament election. The encryption employed in this system is a variation of ElGamal over finite fields, and the key sizes utilized are too small. Using available resources, it is possible to extract the private keys from the public keys in a short amount of time. (Enikolopov et al., 2013).
ii. Electronic Elections in West Virginia State

During the 2018 midterm elections, West Virginia became the first state in the US to enable selected voters to use a program called "Voatz" to cast their ballot on a mobile phone, using a permissioned blockchain, biometrics, a mixnet, and hardware-backed key storage modules on the user's device. Researchers from the Massachusetts of technological institute discovered that Voatz's reliance on a third-party vendor to authenticate its users' identities poses possible privacy concerns that could jeopardize the anonymity of ballots, Voatz claims its technology provides Secure digital voting system using blockchain technology (Specter et al., 2020).

General Researches for Electronic Elections Systems

During recent years, a lot of researches and studies have been conducted to implement safe and transparent systems for the electronic voting process using the blockchain technology. The results were good but there were a number of weaknesses. We will review some of the researches.


This research presents an attempt to take the blockchain advantages such as the encryption and transparency basics to achieve an effective scheme for electronic voting. The details of the proposed electronic voting plan were implemented by using the multichain platform.

The system is implemented in a controlled environment with a web-based application, implemented by Java EE within the Netbeans platform using a Glassfish server native. The application uses mysql as a database. Researchers used the multichain platform as it was suitable for cryptocurrency.

The procedure is as follows:

1. The first transaction added to the block must represent the candidate.
2. When a transaction is made, the candidate's name should be included as the foundation block, with each vote placed above the indicated nomination.
3. It doesn't sound like it's exclusively under the candidate's name, unlike the rest of the Transaction Foundation. Our electronic voting system will allow for a protest vote
whereby the voter can send a blank vote to show dissatisfaction with all candidates or reject the current political system.

4. Every time someone votes, the transaction will be registered and the blockchain will be updated.

5. To guarantee that the system is secure, the prior voter's information must be included. Because all of the blocks are connected, it will be easy to determine whether any of them has been hacked.

6. The real vote takes place on the blockchain. The user's vote is delivered to one of the system's nodes, which records it on the blockchain.

7. The voting system has a node in each region to ensure that the system is decentralized.

8. The researcher provides a solution to vibration in the case of presenting more than one block at one time to the blockchain, which is the use of the longest chain rule which was used by Bitcoin to solve the same problem.

**Weakness**

- The researchers assume that the voters should use a secure device to transmit their votes even if the system is secure. Hackers have the ability to change or modify the votes by using the malicious SW installed on the voters' device.

- This system does not contain the ability to change the voice in case of user error, as he can broadcast his voice only once.


In this research, researcher designed a synchronous model for voting records based on the distributed ledger techniques, and designed a model for the user’s encoded data by using the elliptic curve to provide authentication and non-repudiation and also allow voters to change their votes before a previously set deadline. The system used a Linux (Ubuntu) implementation platform. Each block contains the voter ID, the vote, the new voter’s signature, the timestamp, and the previous block hash.

In combination with other voting systems, it is more secure and anonymous, as each user uses an identifier instead of his true identity and also the decentralization is implemented without the presence of a third party. The results show that the system is safe, practical and it solves the problem of voting fraud during electronic voting.
Weakness

This technique has several drawbacks, because that the malicious software can be placed on the device which will be used to broadcast votes.

3. Oleksandr Kurbatov, Pavel Kravchenko, Oleksiy Shapoval, Nikolay Poluyanenko, Mariana Malchyk, Alina Sakun and Vladyslav Kevtun “Anonymous Decentralized E voting system” (Kurbatov et al., 2019).

This research employs the ring structure to secure voter’s anonymity, as well as the blockchain technology to assure integrity and transparency. To generate the signature, the user must utilize his private key safely and enter the public keys of the other members in the ring for the input algorithm. The number of keys picked is determined by the voter's level of anonymity. If the chosen group is tiny, the chances of concealing the voter's identity are substantially higher.

Some of the advantages of this method include the ability to assess the voter's rights and anonymity, as well as the voter's ability to verify the authenticity of his vote.

Weakness

It's possible that the user will be able to alter his vote. In this situation, the last transaction added to the blockchain will be counted, rather than a single transaction, for that reason security measures must be developed and implemented to avoid spam attacks and other attacks that could damage system performance, as well as data saved in the chain.


This research introduces the concept of block creation and block sealing. Its utility is to make the blockchain customizable; it was suggested by using the consortium blockchain.

Weakness

The use of the private blockchain has bad aspects, which is that only the authority in this type can access the data, and this leads to the possibility of changing the votes for the benefit of some parties.
### Table 3 Several Researches of E-Voting systems based on the Blockchain Technology

<table>
<thead>
<tr>
<th>Research Name</th>
<th>Author</th>
<th>Blockchain type</th>
<th>method</th>
<th>Programming language</th>
<th>Cryptographic algorithms</th>
<th>Advantage</th>
<th>Year</th>
<th>Ref no.</th>
</tr>
</thead>
<tbody>
<tr>
<td>An E-voting System based on Blockchain and Ring Signature</td>
<td>Yifan Wu</td>
<td>public</td>
<td>Ring structure</td>
<td>PHP</td>
<td>RSA</td>
<td>guarantee the authenticity of electronic voting</td>
<td>2017</td>
<td>(Wu, 2017)</td>
</tr>
<tr>
<td>Blockchain-Based E-Voting System</td>
<td>Hjálmarsson, Fridrik Þ Hreïka, Sigurður E. í Glaðskópur, Gisli</td>
<td>private</td>
<td>Exonum</td>
<td>Rust</td>
<td>Byzantine</td>
<td>Private blockchains solve many of today’s security problems using strong cryptography features and the limited access to the ledger, without negating the transparency aspect the blockchain technology offers.</td>
<td>2018</td>
<td>(Hjálmarsson et al., 2018)</td>
</tr>
<tr>
<td>BroncoVote: Secure Voting System using Ethereum’s Blockchain</td>
<td>Dagher, Gaby GMarella, Praneeth Babu Milojkovic, Matea Mohler, Jordan</td>
<td>private</td>
<td>Smart Contract</td>
<td>Solidity</td>
<td>homomorphic encryption</td>
<td></td>
<td>2018</td>
<td>(Dagher et al., 2018)</td>
</tr>
<tr>
<td>Secure E-Voting System using Blockchain Technology</td>
<td>Komal Agrawal, Shivali Gupta, Reetika R. Baberwal, Mukta Dhiman</td>
<td>public</td>
<td>Smart Contract</td>
<td>Solidity</td>
<td>ECC</td>
<td>Single voter can’t vote twice using the same account. No single entity on the network can manipulate the code and the votes</td>
<td>2019</td>
<td>(Agrawal et al., n.d.)</td>
</tr>
<tr>
<td>Securing e-voting based on blockchain in P2P network</td>
<td>Haibo Yi</td>
<td>public</td>
<td>DLT</td>
<td>Ubuntu</td>
<td>ECC</td>
<td>improve the security of e-voting by design a synchronized model of voting records based on DLT to avoid forgery of votes.</td>
<td>2019</td>
<td>(Yi, 2019)</td>
</tr>
<tr>
<td>Anonymous Decentralized E-Voting System</td>
<td>Md. Shahriare Arnob, Niloy Sarker, Md. Inzamam-Ul Haque, Mohammed Golam Sarwar Bhuiyan</td>
<td>public</td>
<td>Ring Structure</td>
<td>Java</td>
<td>SHA-256</td>
<td>the ability to verify voter permissions ; the ability of the voter to verify the correctness of his vote; anonymity</td>
<td>2020</td>
<td>(Kurbatov et al., 2019)</td>
</tr>
</tbody>
</table>

### Conclusion

Our research presents various studies to show and study the advantages and disadvantages of both the traditional and blockchain E-voting systems, the analysis and the final results of our study show that the government’s decision-makers and major election stakeholders don’t have the adequate information to hold a successful E-voting system in the national...
elections. This research demonstrates the experiences of some national elections in many major countries, and how they suffered from problems and the failure of their experiments. Then the blockchain technology appeared, which is the new solution to the problems of electronic voting systems, and there are many experiments conducted by researchers on the blockchain technology at the national and individual levels. The results showed satisfactory, although they have certain security and privacy flaws.

References


