INNOVA Research Journal, ISSN 2477-9024
(Enero, 2018). Vol. 3, No.1 pp. 55-70
DOI: https://doi.org/10.33890/innova.v3.n1.2018.338
URL: http://revistas.uide.edu.ec/index.php/innova/index
Correo: innova@uide.edu.ec

Debilidades en los protocolos de votación por Internet centralizados y descentralizados

Weaknesses in centralized and decentralized internet voting protocols

Ricardo Chica
Universidad Laica Eloy Alfaro de Manabí, Ecuador
PhD. Student Universitá di Pisa,Italia

Autor para correspondencia: r.chicacepeda@studenti.unipi.it
Fecha de recepción: 27 de Julio 2017 - Fecha de aceptación: 15 de Enero de 2018

Resumen
El presente documento analiza las debilidades de los protocolos relativos a los sistemas de votación por Internet, ya sean centralizados o descentralizados, como una tecnología utilizada en muchos países del mundo que puede aumentar significativamente el número de electores, ofrece transparencia, entrega de resultados y reduce la costos de todo el proceso electoral, permitiendo una forma auditable para el ciudadano y las entidades públicas. El uso de Sistemas de votación electrónica remota (REV) había abierto una nueva vía para los servicios de gobierno electrónico, brindando a la comunidad otras herramientas para fines electorales, y al mismo tiempo creó una larga lista de desafíos de valores que han permitido el desarrollo de nuevos sistemas de votación I, entre las comunidades que se centran en la investigación de diferentes maneras de minimizar los riesgos de este proceso.

Palabras clave: elecciones; protocolos; descentralizados; centralizados; e-democracia; REV

Abstract
The present document analyzes the weaknesses of the protocols regarding internet voting systems, either centralized or decentralized one, as a technology used for many countries around the world that may significantly increase the numbers of electors, offers transparency, delivery of results and reduces the costs of the whole electoral process, allowing an auditable way either for the citizen and public entities. The use of Remote Electronic Voting Systems (REV), had been opening a new way for e-government services, giving the community other tools for electoral purposes, and at the same time had create a long list of securities challenges which have allowed the development of new I-voting systems, among communities that focus on the research of different ways to minimize the risks of this process.

Key words: elections; protocols; decentralized; centralized; e-democracy; REV

Introduction

The constant growth and development of information technology in all fields of society have enabled a substantial improvement in activities related to the electronic government and the way in which the public sector connects with the citizens and improves its own services.

Voting is the basis of any democratic system, either to elect representatives, to take decisions (referendum) or to reach a large-scale agreement. REV permits the voters to record a vote without having to be physically present in a supervise polling station, like traditional election do; instead of that, the citizens will have the possibility with the use of electronic devices like personal computers or smartphones connected to the internet, to record and transmit their votes during a specific time, set by the authorities of the election.

The daily activities, the geography and the disposition of the resources used for traditional voting, make that in the majority of cases, the eligible citizens do not participate in the elections, which is harmful to democracy and in some cases, affect the results when not counting with the minimum number of participants, cases like Colombian referendum that was made in 2016, to approved or deny the negotiation between the government and the guerillas group known as FARC, to end a fifty years arm conflict had a 62% of abstention (Mundo), or in 2016 the United Kingdom Brexit election, which decided if the country should remain or leave the European Union, had more than 28% of abstention as well. (Results, 2016)

Most of the countries in the last decades have opted for government systems, where the legal age citizens making use of the vote, elects its rulers to represent them before the different instances of power (President, Congress, assembly, etc). Each nation has adopted its own mechanisms that allow an optimal, safe, fast and verifiable electoral process, for that reason we have seen the use of ballots, marking cards, color inks and electronic devices like DRE, among others many mechanisms that have marked the history of our countries.

With the rise and massification of information and communication technologies, new forms have been developed in recent years to improve electoral processes, including internet voting, which has already been carried out in countries such as Estonia and Switzerland on a large scale, and some North American and Latin American cities as Santa Catarina Brazil and Santo Domingo de Los Colorados in Ecuador, as a pilot test.

This paper discusses the weaknesses in centralized and decentralized internet voting protocols that will allow deepening in more robust security mechanisms for this type of technology, which has grown significantly in the last decade and will undoubtedly make the difference compared to traditional voting mechanisms. Also, analyze the cases of Estonia 2013 election and de pilot election carry out by the Washington D.C. District in 2010.

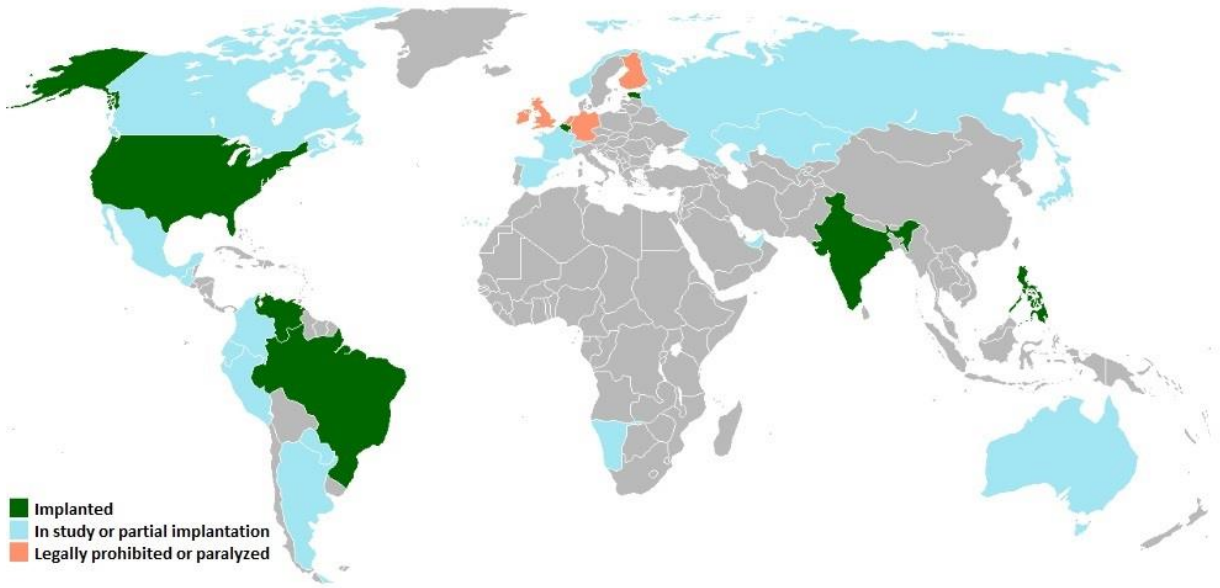

Figure 1. Implementation degree of E- voting system around the world (Dirección de Régimen Jurídico, 2016)

I-Voting:

I-voting is a technology where eligible citizens can vote using electronic devices such a laptop or smartphone, through internet connection, while ensuring privacy and integrity of the results in a way to improve accessibility, as well as alternative method to traditional on-site elections, without losing sight of the main fundamental objectives:

- Ensure universal, free, equal, secret and direct vote.
- Achieve greater citizen participation.
- Ensure the transparency of the electoral process

There are two types of internet voting: On-site, which is conducted at controlled places, where election officials can authenticate eligible voters and the electronic infrastructure that must be used. The second type allows voters to transmit their votes from any internet connection to which they have access using a computer or smartphone.

When casting votes, the system gives a unique digital identification number (PIN) to the citizens that allow them to access the screens where the choice is made. Once the voter enters the site he can select the candidate of his preference and send the choice instantly. Voting is transmitted through a network of communications, either in a Centralized or decentralized protocol, from the place where it has been issued up to a remote digital urn or central server.

Internet Protocols:

All the voting protocols tend to meet the same set of security requirements, the privacy of all the voters is the principal security requirement, the result must be totally secret until the

election is completed and verifiable. That provides the user the confidence that their votes had been treated correctly.

Table 1. General Security requirement for electronic voting protocols

Security Requirement	Description
Privacy	Is not revealed to anyone the way an eligible user voted
Authentication of voter's	To ensure that only eligible voters can vote and only one vote per person is counted.
Accuracy	Valid votes cannot be removed or manipulated. No invalid votes can be added
Secrecy of intermediate results	All results are kept secret until the election is completed.
No-coercion	The system must not enable the selling of votes or the coercion of voters.
Verifiability	Voters must be assured of the correct treatment of their votes, and have means to irrefutably prove of any fraud.

Features and functionalities of remote electronic voting system:

For a basic understanding of what can be achieved with electronic voting systems, it is useful to consider the security and the end-user functionalities that these systems can offer for both voters and election officials. (Paper, 2011)

Regarding legal principles, the system most meet the following requirements:

- **Universal:** The voting system must be available for all eligible voters, without requiring special knowledge, and be easy to navigate, including graphics and sounds mechanism for people with disabilities.

- **Availability:** Must never enter an undefined state, and have a backup mechanism to recover the system in case of an emergency.

- **Free:** Voters should make their choice without any interference or influence of anybody, as well they must not be paid or get paid for it.

- **Equal:** Voters should authenticate themselves to prevent unauthorized access, and each person can only vote once, each ballot is counted exactly once within the result. All ballots have the same influence on the result.

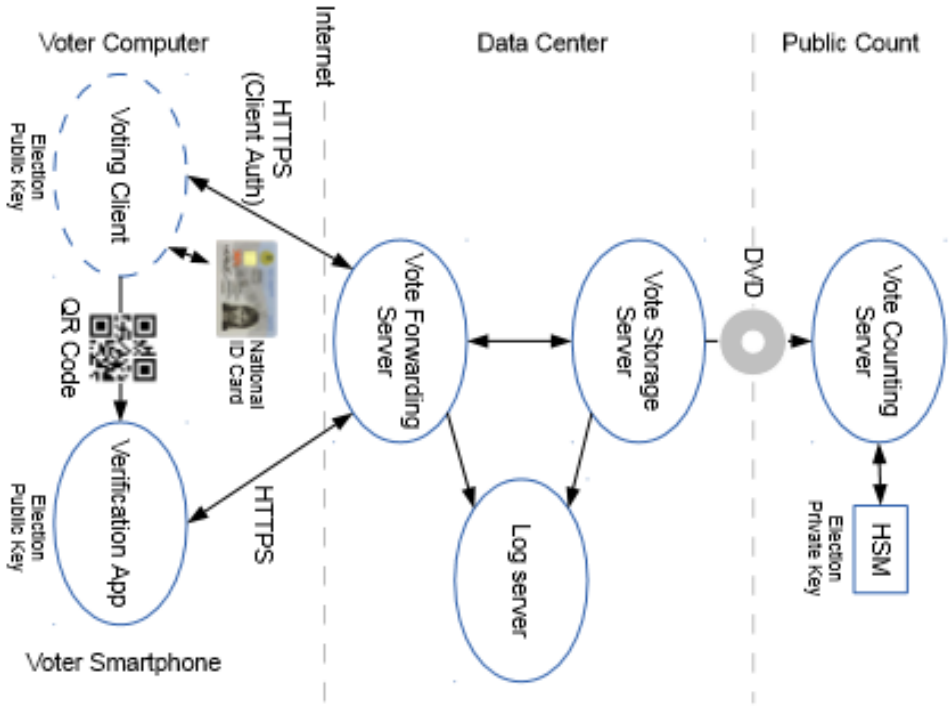

Figure. 2: I-voting system overview

Basic software components:

- **I-voting client application.** This user-friendly application allows voters to cast i-votes from a wide range of platforms. It can be customized to support any kind of election.

- **I-voting system.** It is comprised of a group of protected servers that collect, store, tabulate votes and create reports for election management. All these servers are controlled by the election commission.

- **I-voting verification application.** Because every voter should be certain that their vote is counted as intended, this mobile app allows voters to confirm that their vote was registered appropriately. (Smartmatic, Estonia Election)

Centralized Protocol:

The most common electronic schemes in centralized protocol required the uses of a very trusted counting server as a third party, which makes the security of this third party extremely critical for the voting system.

The internet architecture for this protocol uses three layers (Web–Application-Database) on which the system executes an "applet" in the browser and establishes a secure connection (HTTPS) for authentication, selection of options and registration of the vote.

All the processing is controlled in a central location using a server to collect and save the ballots by a Serie of steps described in the following graphic. (OEA, 2014)

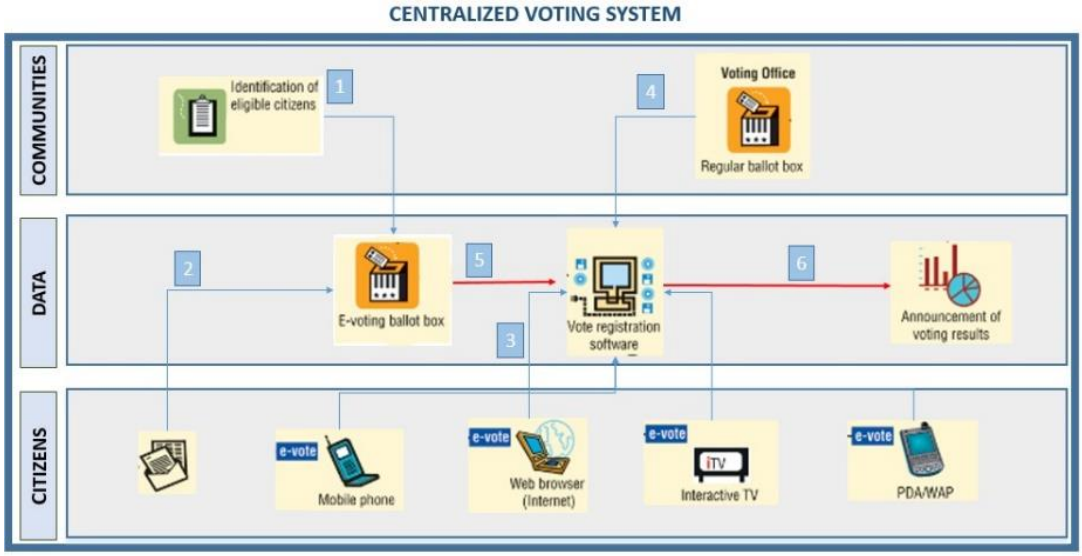

Figure 4. Centralized Voting System

Decentralized Protocol:

One of the newest cryptographic decentralized voting protocols is the blockchain, which is a distributed database that maintains a continuously-growing list of ordered records called *blocks*. Each block contains a timestamp and a link to a previous block, by design blockchain are inherently resistant to modification of the data, once recorded, and the data in a block cannot be altered retroactively.

A blockchain is an audit trail for a database which is managed by a network of computers where no single computer is responsible for storing or maintaining the database, and any computer may enter or leave this network at any time without jeopardizing the integrity or availability of the database. Any computer can rebuild the database from scratch by downloading the blockchain and processing the audit trail.

The most obvious way to ensure that no single entity can manipulate the database is to make the database public, and allow anyone to store a redundant copy of the database. In this way, everyone can be assured that their copy of the database is intact, simply by comparing it with everyone else's. (Followmyvote, n.d.)

Taking in count that in a decentralized protocol there are no authorities or trusted parties – all voters operate independently with equal mutual suspicion. All traffic is performed on regular communication channels. The protocol is also accurate in that cheating is discovered immediately and in some cases, the perpetrator may be identified.

The system used in DP based on blockchain offers a transparent public ledger which is a collection of accounting entries that is not centrally controlled by and individual or organization

and the ledger entries only get confirmed as correct and officially enter into the ledger once they have been mathematically verified by the blockchain. At the same time, the ledger is completely public.

The most prominent concern about an implementation of Blockchain voting system is the lack of experimental evidence that such a system could hold up in a large-scale use, for example in a national election. Another important issue is regarding the use of cryptographic key in which a verified voter can cast their ballot, and in some cases, can be difficult to deal with this aspect as well making the attackers to compromising the voter's key instead of the system. (Francesca Caiazzo, 2016)

Blockchain uses security methods like asymmetric cryptographic keys, which are two types of keys, the first one is the public key that may be disseminated widely, and private key which is known only by the owner, this accomplishes two functions: Authentication when the public key is used to verify that a holder of the paired private cast the vote, and encryption, whereby only the holder of the paired private key can decrypt the message encrypted with the public key.

When a legitimate user cast his vote, what the system does is broadcast a transaction to all the nodes that compromise the peer–to–peer network.

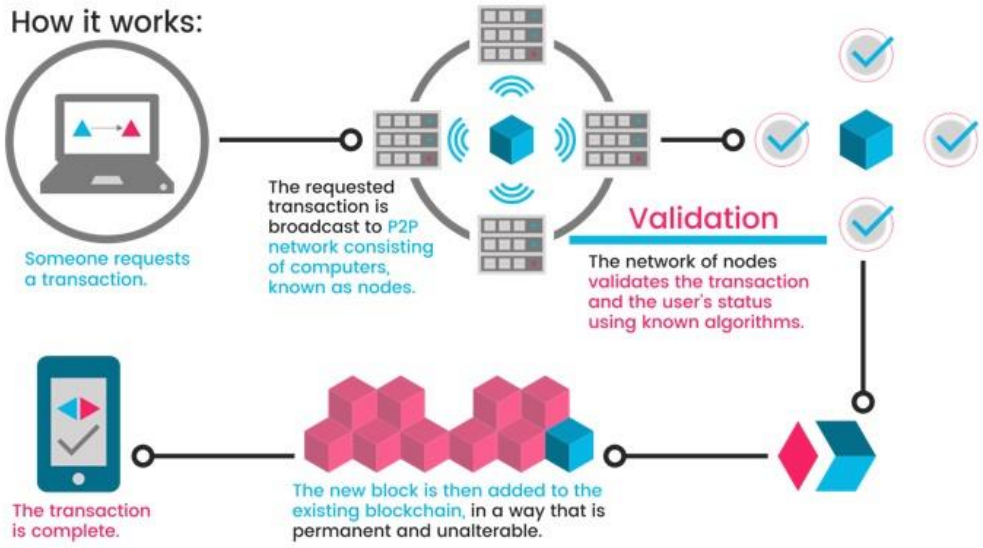

Figure 5. Blockchain Working Scheme. (Blockgeeks, n.d.)

Giving that a variety of users are broadcasting the transaction to the network, the nodes must agree on exactly which transaction was broadcast and the order in which these transactions happened. This will result in a single, global ledger for the system.

So, at any given point, all the nodes in the peer- to- peer network have a ledger consisting of a sequence of blocks, each containing a list of transactions, that they've reached consensus on (Arvind Narayanan, 2016)

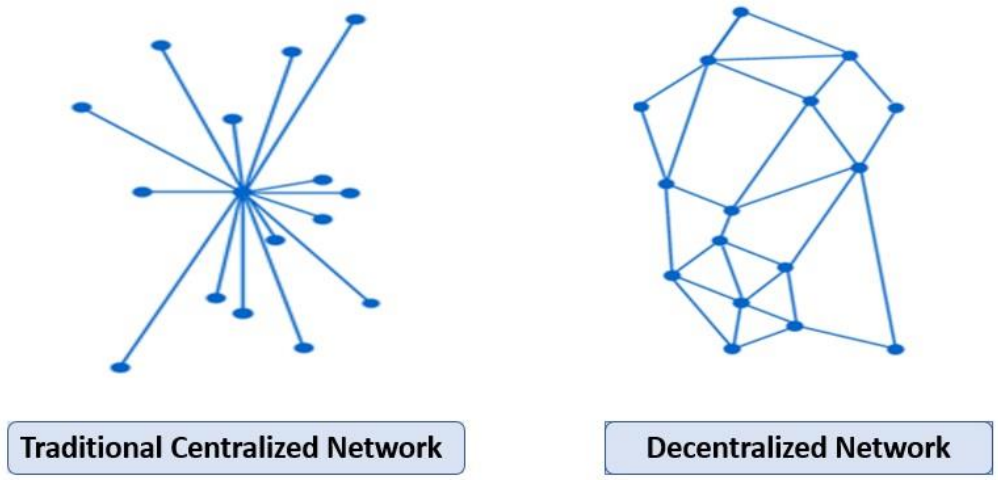

Figure 6. Centralized and decentralized network. (https://followmyvote.com/, n.d.)

Security Risk Analysis:

Election		
	Authentication	- There is not a physical probe that the person voting is really the authorized voter. - Possibility of stolen voter packages or identification cards - Misuse of elector's ID card and personal information voting by others without the knowledge of the elector
	Voting	- Unable access to election website - Network Saturation - Internet signal cut off - Dissociation of the instructions for user verification and voting options - Phishing - Malware
	Validation	- Internet signal cut off - Attacking the web application
	Storage	- Hacker - Manipulation of the algorithm of the voting counting program in the server (*The company that installed can decide also who win*) - Replacement of the voting counting software
	Decryption	- Remove or replace de cryptography parameters

Threats In Centralized And Decentralized Protocol:

Threat	Centralized Protocol	Decentralized Protocol
Denial of Service	Common	Uncommon
Trojan horse spyware to change or monitor votes	High probability	Low probability
Automated vote buying	High probability	Low probability
Insider attack on voting system	Common	Common
Virus-specific to Internet voting system	Common	Common
Spoofing	High probability	Low probability

Vulnerabilities In Centralized And Decentralized Protocol:

	Centralized Protocol		Decentralized Protocol	
	Threats	**Vulnerabilities**	**Threats**	**Vulnerabilities**
Voter Station	Electronic device as client PC or smartphone can be located in voter´s home, public or commercial places. These devices could be infected with malware.	Excessive privileges Confusing or unclear information for voters	Offline Messaging Bootstrapping Keystroke Logging	Excessive privileges. Confusing or unclear information for voters.
Vote Collection Server	Backdoor, Trojan horses, Hacking, worms	Storage media Exposure Misconfigured database	Decentralized protocol does not use a single server DDoS, hacking	
Administration System	Malware Phishing Spyware Trojan horses Time jacking	Limited security expertise	Malware. Pharming. Phishing Ransomware, Trojan horses. WIFI eavesdropping. spyware Sybil attack Time jacking	Remote denial of service. The issue is triggered during the handling of a specially crafted signature alert. This may allow a remote attacker to cause a consumption of CPU or RAM resources, which will crash the system
Transmition Data	TCP connections attack, Volumetric Attacks DNS Reflection Break Cryptography	Connection failure Break Cryptography Consensus	TCP connections attack Volumetric Attacks DNS Reflection Break Cryptography	Connection failure Overflow condition. The program fails to properly sanitize user-supplied input resulting in an integer overflow.

Comparative Specifications Between Centralized And Decentralized Protocols:

Main Issues	Centralized Protocol	Decentralized Protocol
Voter can verify if vote is cast as intended	✓	✓
Voter can verify if the casting vote is recorded	✓	✓
Voter can verify if votes are tallied as recorded	✓	✓
Assurance on tallying integrity when TAs are all corrupted	✓	✓
Suitable election (Small and large scale)	✓	✓
Faster counting and tabulation		✓

Greater accuracy in results		✓
Comfort for voters	✓	✓
Increased participation in electoral process	✓	✓
Costs	✓	✓
Prevention of fraud		✓
Greater accessibility	✓	✓
Communication in several languages	✓	✓
Flexibility to make changes, handling deadlines	✓	
Risk of manipulation by external agents	✓	✓
Risk of manipulation by agents	✓	
Internal		
Infrastructure	✓	✓
Supplier dependency	✓	✓

Estonia Internet Voting System Weaknesses:

The 2013 Estonia local election used REV and there were identified many potential security risks, like malware on the client side machine, that monitors the user while placing his vote and then later changing the vote to a different candidate. Another weakness was regarding the HTTP. If a client sends a request containing unexpected header fields, the server logs the field names to disk, by sending many specially crafted requests containing fields with very long names, an attacker can exhaust the server's log storage, after which it will fail to accept any new votes.

Also, there was a vulnerability with the shell-injection in a server-side user interface that was intended to allow operators to perform pre-determined administrative tasks. The vulnerability would allow such an operator to execute arbitrary shell commands on the election servers with root privileges.

The encrypted ballots are separated from the signatures and copied to an isolated machine before being decrypted and counted, an attacker who can smuggle this information out through a covert channel can compromise every voter's secret ballot.

The counting server malware can sort the encrypted ballots and leak the voter choices corresponding to each as a sequence of integers in the same order.

Another possible risk has infected the server through malware being placed on the DVD´s used to set up the servers and transfer the votes. (Andrew Barnes)

Estonia's system also fails to provide compelling proof that election outcomes were correct. The tabulation process at the end of the election was also concerning, because after the votes were decrypted on the counting server, an unknown technical glitch prevented workers from writing the official counts and log files on a server DVD, and transfer them to a computer where they sign the results officially, instead the electoral authorities decided to use a regular personal USB to transfer those files, that might add a multiple potential attack vectors. (Drew Springall)

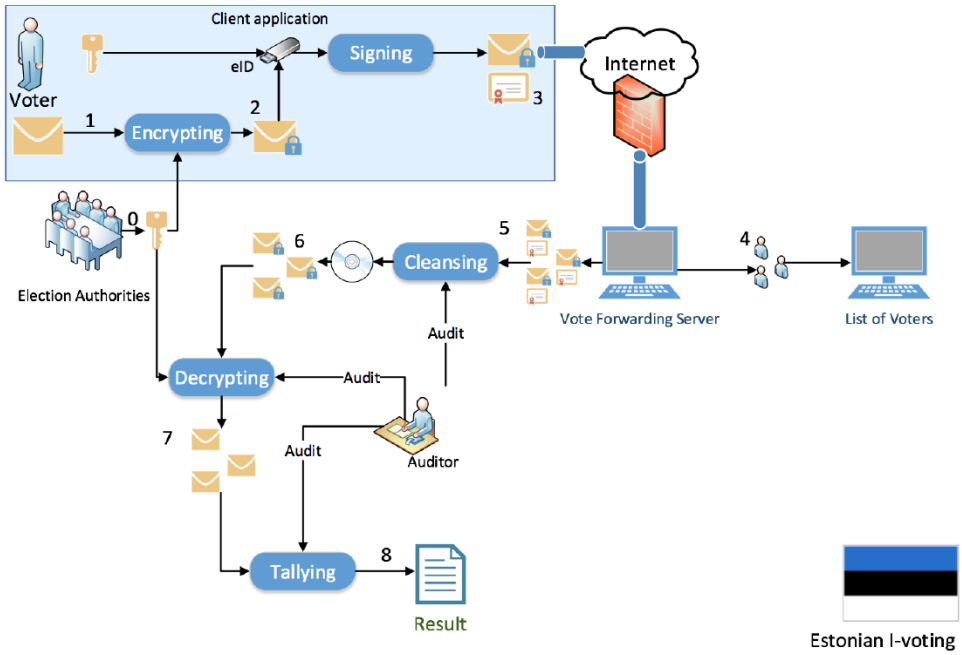

Figure 8. Estonian Digital Voting System (Source: R. Verbij. "Dutch e-voting opportunities." Master thesis, University of Twente, 2014)

Washington D.C. Internet Voting System Weaknesses:

In 2010, Washington, D.C. developed and internet voting Pilot project that was intended to allow voters to cast their ballot using a website, prior to election the district made a public trial and invited to test the system or attempt to compromise its security, a team of student from the University of Michigan with Professor Alex Haldeman were able to break into the system and they found the next Vulnerabilities: (Scott Wolchok, Attacking The Washington, D.C. Internet Voting System, 2012)

- Web Application: The application was open source and it was possible for the team to hack the voter login, ballot, database communication, and network activity.
- Shell-injection vulnerability. Was located in the code for encrypting voted ballots uploaded by users.
- Network Infrastructure: Using Nmap's OS it was possible for the team to access the router, the gateway and the network webcams and the terminal server.
- Stealing Secrets: Retrieved several cryptographic secrets from the application server that includes the public key used for encrypting ballots, which allows attackers to substitute arbitrary ballots in place of actual cast ballots.

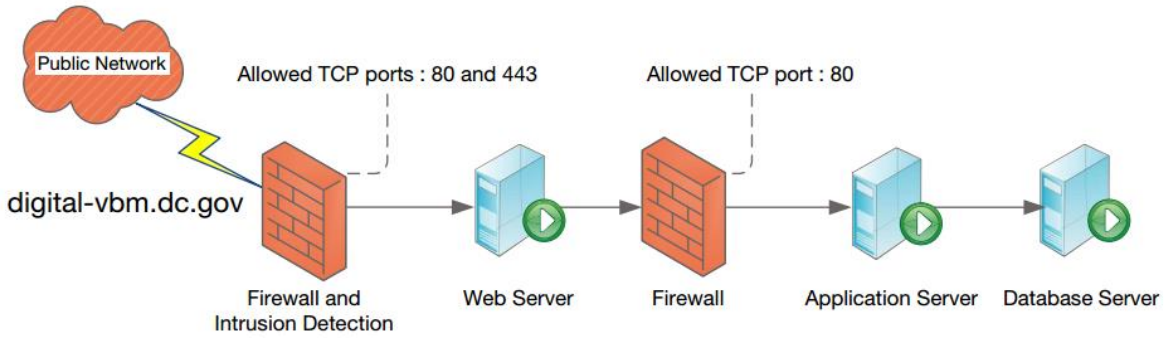

Figure 9. Network Architecture – Washington D.C. Internet Voting System (Scott Wolchok, Attacking The Washington, D.C. Internet Voting System, 2012)

Challenges Of Internet Voting Protocols.

- Either for centralized or decentralize protocols, the identification of eligible voters is a great challenge, or it's been solved using a unique voter id and digital signatures as well public and private keys. However, if the voter information is stolen, that person can place a legitim vote in that voter's name.
- The insecurity of the user's device that could record a voter's private key and pin, and then submits unauthorized votes in the client's name.
- In centralized protocol's the Vote Collection Server (VFS), and the vote counting machine presents the most attractive targets for adversaries since they must be connected to the internet and be exposed from all over the world.
- Bugs in software either client or server side, that might expose voter's ballots to the public and violate the secrecy.
- Undetectability of attacks, in 2010 attack on Washington D.C system, researchers had full access to the central server for many days, before official discover their presence. (Wolchok S, 2012)
- Raise consciousness in the community about the benefits and comfort of the internet use for electoral purposes, mainly to those related to security issues, ease of access and results delivery in less time than traditional ways.

Future Perspective Of IVP.

The most important gap found in traditional protocols system are those especially regarding security issues, and can be minimized by the use of the Blockchain technology, which had shown us the many uses like Cryptocurrency as the Bitcoin or Ethereum, where this kind of technology gives many benefits.

1. **Disintermediation and trustless Exchange:** Two or more parties can make and exchange without the oversight or intermediation of a third party, reducing the counterparty risk, and generating more trust to those involved.

For electoral purposes, this technology will help the voters to secure cast their votes and let everybody in the network know it, and will not need any other entity to validate it.

1. **Empowered users:** Users control of all their information and transaction
2. **High-quality data:** Blockchain data is complete, consistent, timely, accurate, and widely available.
3. **Durability, reliability, and longevity:** Due to the decentralized networks, blockchain does not have a central point of failure and is better able to withstand malicious attacks.
4. **Process integrity:** Users can trust that transactions will be executed exactly as the protocol commands removing the need for a trusted third party.
5. **Transparency and immutability:** Changes to public Blockchains are publicly viewable by all parties creating transparency, and all transactions are immutable, meaning they cannot be altered or deleted.
6. **Ecosystem simplification:** With all transactions being added to a single public ledger, it reduces the clutter and complications of multiple ledgers.
7. **Faster transactions:** Traditional transactions can potentially take days for clearing and final settlement, especially. Blockchain transactions can reduce transaction times to minutes and are processed 24/7.
8. **Lower transaction costs:** By eliminating third party intermediaries and overhead costs for exchanging assets, blockchains have the potential to greatly reduce transaction fees. (Deloitte)

In a constantly growing society, the globalization and a strong democracy are the keys for an accurately use of Information technology and at the same time can lead us to better results on electoral process. Governments most implement new mechanism that increases the participation of electoral users, given results in less amount of time, as well offering to society security measures that guaranty those results.

Conclusions

Since decentralized protocol, do not share a single copy in a specific server of the information, then there is no single entity that can manipulate the database, that allows the voters to store a redundant copy of this database and everyone can be assuring that their copy is intact by just comparing it to everyone else´s.

In a DP, the nodes in the network use consensus mechanism, this might involve significant back-and-forth communication and/or deal with forks and their consequent rollbacks. While it's true that centralized protocols must also contend with conflicting and aborted transactions, these are far less likely where transactions are processed in a single location.

Centralized Protocol process transactions once, in a decentralized one those must be processed independently by every node in the network, making that more work must be done for the same result.

In CP two parties can make an exchange without the oversight or intermediation of a third party, strongly reducing or even eliminating counterparty risk.

With all transactions being added to a single public ledger, it reduces the clutter and complications of multiple ledgers.

In CP, a single small mistake during the configuration or implementation of the voting server or its network infrastructure can compromise the legitimacy of the entire election

By eliminating third party intermediaries and overhead costs for exchanging assets, DP has the potential to greatly reduce transaction fees.

Bibliografía

Ammar Alkassar, M. V. (2007). *www.download.springer.com.* Obtenido de http://link.springer.com/chapter/10.1007/978-3-540-77493-8_1

Andrew Barnes, C. B. (s.f.). *Digital Voting with the use of Blockchain Technology*. Team Plymouth Pioneers – Plymouth University.

Arvind Narayanan, J. B. (02 de 2016). *Bitcoin and Cryptocurrency Technologies.* Obtenido de https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1

Bitcoinwiki. (s.f.). *Bitcoinwiki*. Obtenido de https://en.bitcoin.it/wiki/Weaknesses

Blockgeeks. (s.f.). Obtenido de http://blockgeeks.com/guides/what-is-blockchain-technology

Commission, U. E. (2016). *The electoral Commission.* Obtenido de http://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/upcoming-elections-and-referendums/eu-referendum/electorate-and-count-information

Deloitte. (s.f.). *Deloitte.* Obtenido de Blockchain Technology: 9 Benefits and 7 Chalenges: https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/blockchain-technology-9-benefits-and-7-challenges.html

Dirección de Régimen Jurídico, S. y. (03 de 05 de 2016). *http://www.euskadi.eus.* Obtenido de http://www.euskadi.eus/botoelek/otros_paises/ve_mundo_impl_c.htm

Drew Springall, T. F. (s.f.). *Security Analysis of the Estonian Internet Voting System.* Obtenido de https://jhalderm.com: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

Followmyvote. (s.f.). *Online Voting Technology*. Obtenido de https://followmyvote.com/online-voting-technology/blockchain-technology/

Francesca Caiazzo. (14 de 12 de 2016). *The Benefits and Risks of Block-Chain Voting.* Obtenido de http://www.cs.tufts.edu: http://www.cs.tufts.edu/comp/116/archive/fall2016/fcaiazzo.pdf

Gritzalis, D. A. (s.f.). *http://www.instore.gr*. Obtenido de http://www.instore.gr/evote/evote_end/htm/3public/doc3/public/aegean/paper7.pdf

Gritzalis, P. D. (septiembre de 2002). *Secure Electronic Voting System*. Obtenido de https://www.terena.org/activities/tf-csirt/meeting7/gritzalis-electronic-voting.pdf
https://followmyvote.com/. (s.f.). *https://followmyvote.com/* . Obtenido de https://followmyvote.com/

Inteco. (s.f.). *BITCOIN Una moneda criptografica*. Obtenido de Instituto Nacional de Tecnologias de la Comunicación: https://www.certsi.es/sites/default/files/contenidos/estudios/doc/int_bitcoin.pdf

Lauer, T. W. (2004). The Risk of E-voting. *Electronic Journal of e-government Volumen 2 Issue 3*.

Melanie Volkamer, D. H. (s.f.). From Legal Principles to an Internet Voting System. *German Research Center for Artificial Intelligence GmbH* .

Mundo, B. (s.f.). *bbc.com*. Obtenido de http://www.bbc.com/mundo/noticias-america-latina-37539590

OEA, S. d. (08 de 2014). *"TECNOLOGÍAS APLICADAS AL CICLO ELECTORA.* Obtenido de http://www.oas.org/en/: https://www.oas.org/es/sap/docs/deco/Tecnologias_s.pdf

Paper, P. (Diciembre de 2011). *Introducing Electronic Voting - Esential Considerations*. Obtenido de International Idea: http://www.eods.eu/library/IDEA.Introducing-Electronic-Voting-Essential-Considerations.pdf

Pomares, J. P. (August de 2016). *www.springer.com.* Obtenido de http://link.springer.com/article/10.1007/s12243-016-0525-8

Project, E.-V. (s.f.). *The Future of Voting*. Obtenido de https://www.usvotefoundation.org/E2E-VIV

Results, E. R. (2016). *Electoral Commission.* Obtenido de http://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/eu-referendum/electorate-and-count-information

Scott Wolchok, E. W. (2012). *Attacking the Washington, D.C. Internet Voting System.* Obtenido de https://jhalderm.com: https://jhalderm.com/pub/papers/dcvoting-fc12.pdf

Scott Wolchok, E. W. (02 de 2012). *Attacking The Washington, D.C. Internet Voting System.* Obtenido de https://jhalderm.com/pub/papers/dcvoting-fc12.pdf

Smartmatic. (s.f.). *Estonia Election.* Obtenido de Smartmatic.com: http://www.smartmatic.com/uploads/tx_news/CS_Estonia_elections_2014_2015.pdf

Smartmatic. (s.f.). *Estonia Elections 2014 - 2015: Technology Case Studie* . Obtenido de Smartmatic.com: http://www.smartmatic.com/case-studies/article/estonian-elections-2004-2015-technology/

Technologies, E. V. (s.f.). *Electronic Votes Pros and Contra*. Obtenido de http://www.bravenewballot.org/

The Hebrew University of Jerusalem, I. (2002). *Electronic Voting Protocols and Schemes*. Obtenido de http://www.cs.huji.ac.il/~ns/Voting2.pdf

Volkamer, A. A. (2007). *springer.com.* Obtenido de https://link.springer.com/book/10.1007/978-3-540-77493-8

Wikipedia. (s.f.). *Wikipedia*. Obtenido de https://en.wikipedia.org/wiki/Blockchain_(database)

Wolchok S, W. E. (2012). *Attacking the Washington, D.C. Internet Voting System.* Obtenido de https://paperpile.com/c/XmUfWx/e6X3