Usability and security of electronic voting systems

Safia Aouragh, Fanny Kalinowski, Karima Boudaoud

Usability and security of electronic voting systems

Safia Aouragh*, Fanny Kalinowski *, Karima Boudaoud†
*UCA,Polytech'Nice Sophia
Email: safia_aouragh@hotmail.fr, kalinowski.fanny@orange.fr
†UCA, CNRS, I3S
Email: karima.boudaoud@univ-cotedazur.fr

***Abstract*—Nowadays, the interest towards electronic voting systems is increasing. However, in the existing e-voting systems several issues need to be resolved regarding usability and security. Is an e-voting system usable? Does it guarantee security? To answer these questions, we have conducted a comparative study of a non-exhaustive list of e-voting systems with a focus on usability and security properties. We have first identified the main tasks of an e-voting system and the usability and security properties that must be provided by a e-voting system. Then, we have analyzed what are the different tasks and usability and security properties provided by the selected e-voting systems and how they have been implemented, as well as their impact on the functioning of the system. Our study highlighted the strong relationship between security and usability. More specifically, we came to the conclusion that even if a system fulfills many security properties, its security can be fully guaranteed if it is usable. Finding the good tradeoff between security and usability increases the confidence of the users in these systems, which is an essential parameter.**

I. Introduction

Currently several e-voting systems have been developed. An e-voting system is a voting system that involves the use of electronic means. In general, two main types of electronic voting can be distinguished: electronic voting supervised by the physical presence of an electoral authority, such as electronic voting machines in polling stations or municipal offices; and electronic voting under the sole influence of the voter, not physically supervised by any electoral authority. For example, voting from a personal computer via the Internet or by mobile phone, including by SMS[1].

When designing e-voting systems, generally the developers have focussed more on providing an e-voting system that fulfils the voting process and offer a secure system[1] [2][3][4][5] than on the usability aspects. Some experiments and research have been done to try to find a good compromise between usability and security [5][6][7].

The objective of this paper is to present the results of a comparative study that we have conducted on a non-exhaustive list of e-voting systems with a focus on usability and security properties. We have first analysed how the existing systems work to extract and then define the main tasks and steps necessary for a e-voting system. Then, we have identified all the usability and security properties that must be provided by a e-voting system, after identifying all the properties provided by existing systems. Noticing that these properties were not defined and not evaluated in the same way by the studied systems, we have proposed a consensual definition for each property. Finally, we have analyzed what are the different tasks and properties of usability and security provided by the selected systems, and how they have been implemented to understand their impact on the functioning of the system.

The rest of the paper is organized as follows. In Section 2, we define the main tasks of an e-voting system and describe how these tasks have been implemented by the five e-voting systems that we have selected. In Section 3, we provide the list of usability and security properties that we have identified after analysing the existing e-voting systems and give a consensual definition. In Section 4, we analyse the usability and security properties provided by the five e-voting systems. Finally, we conclude this paper and provides an outlook on future work.

II. The tasks of the e-voting processes

An e-voting process includes several tasks, where a task is an activity associated with one or more steps in achieving an objective. In this study, we have identified and defined eight tasks:

- **Documentation**: at this step, the voters gather information about the parties running in the election and the process to prepare their vote. For the election organizers, this documentation phase consists of thinking about and comparing the methods to be adopted in order to set up the vote.
- **Identification**: it is necessary for the voters to identify themselves. This task allows them to establish their identity by declaring it with a unique identifier. More simply, the voters answer the question: "Who are you?".
- **Authentification**: After declaring their identity, the voters must authenticate themselves. The double authentication allows to prove that the voter is who she/he claims to be. In a client/server relationship, authentication can work both ways. The server needs to know who is actually accessing its site or information, but the client is equally legitimate in verifying that the server is the system it claims to be.
- **Making a choice**: after the authentication phase, the voters make a choice from among those available to them, such as the parties running in the election. This decision is unique: they can choose only one option, and they will not be able to reconsider their decision.

[1]E-Voting: International Developments and Lessons Learnt

- **Validation of a choice**: at this stage, the voters validate their choice.
- **Vote verification (voter side)**: after validating their choice, the voters can check that it has been added in the ballot and has been counted. This individual verification can also take place on the content of the vote.
- **Vote verification (assessor side):** the verification task is also performed by the voting organizers. The assessors can check the votes universally to make sure that the vote was correctly cast and that the count is correct.
- **Feedback sharing**: Finally, the voters are often invited to share their feedback via questionnaires or interviews.

In our study, we have analysed the implementation of these tasks for each selected voting system.

A. Prêt à Voter

Prêt à Voter is an e-voting system that has been the subject of an experiment piloted in May 2007 at Newcastle University. 105 volunteers were invited to vote for a donation to one of the Campus' institutions: Oxfam, Barnados and UNICEF [8].

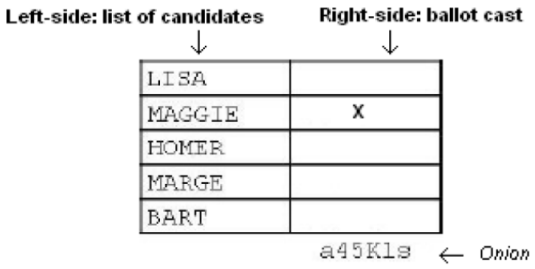

Fig. 1. System ballot of Prêt à Voter [8]

a) Documentation phase: Within the university, emails were sent to the mailing lists of each department. The volunteers present at the campus also encouraged participation in the charity vote.

b) Identification: A demographic questionnaire was distributed to each participant. Participants were asked to provide information about their age, educational background and past voting experience. This questionnaire replaced the presentation of identity document.

c) Authentication: This task was not available. This is probably due to the experimental aspect of the study.

d) Making a choice: As we can see it on Fig. 1, on the left side of the ballot, the names of the charitable organizations are listed. The order in which the names appeared is random. The right side of the ballot is reserved for the voter's choice. The voters have to make a cross next to the charity their choose to support.

e) Validation of the choice: After making a choice, the left part of the ballot, containing the order of the candidates is destroyed. Voters separate the ballot in two parts and keep only the right part, containing their choice and the onion. The onion encapsulating the order of the list of candidates is encrypted on several layers with the public keys of different officials and representatives of the parties. To decrypt the onion, and thus determine the value of the vote, the officials have to collaborate. The right side of the ballot is scanned into the system by an assessor.

f) Vote verification (voter): Voters receive a receipt on which is indicated the boxes they have checked, the encrypted onion and a serial number. The receipt allows voters to ensure that the machine has recorded their choice. With the serial number, they are able to track their vote online. On the Web Bulletin Board, their number appears if the ballot has been counted.

g) Vote verification (assessor): The successive layers of encryption of the onion make the counting of the election collaborative.

h) Sharing feedback: The participant completetes a SUS questionnaire.

B. Scratch Card

Scratch Card is a variation of Prêt à Voter. [9] proposes an incremental improvement approach to the manual voting system used in the UK to ensure the secrecy of the vote with an analysis focused on the technical-social dimension.

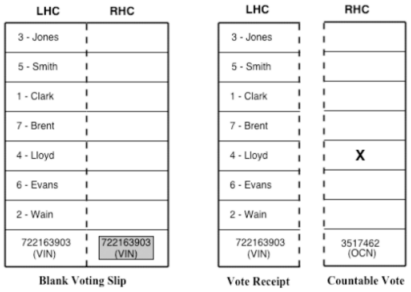

Fig. 2. Scratch Card System paper ballot before (left) and after (right) it has been counted [9]

a) Documentation phase: This phase is not specified by the authors.

b) Identification: Voters give their name and the assessor makes sure they are registered on the electoral list.

c) Authentication: This phase is not specified by the authors. Probably, the ID card is requested to prove the identity.

d) Making a choice: The ballot is similar to the *Prêt à voter* ballot (see Fig.2), except that at the bottom of each column a unique voting identification number is printed - VIN (Voting Identification Number). The voters can choose the ballot of their choice. The names of the candidates are printed on the left column (LHC), their order varies on each ballot. This portion of the ballot serves as a receipt to be kept after voting. The right-hand column (RHC) is used to collect the candidates' choice and is carried forward into the vote counting process. The RHC is actually a "scratch card" containing a small rectangle of opaque coating that initially masks a pre-printed code. This code (OCN) identifies the order in which the candidates' names were printed on the left-hand column. The VIN copy at the foot of this HCR is printed on this opaque coating.

e) Validation of the choice: Voters separate the ballot in two parts and keep only the LHC. This does not give any information about the content of the vote. Voters place the RHC in a closed box. Even before scratching the VIN on the RHC and revealing the OCN, the assessors publish the VIN at the bottom of the RHC on the web.

f) Vote verification (voter): Using the VIN on the LHC, the voters can verify that their vote has been counted on the Web Bulletin Board. The Web Bulletin Board is an online, publicly accessible display of the various registered votes that have been encrypted. The voters can verify that their VIN number is displayed. Also, the voters have the right to select any ballot. They are encouraged to select more than one, to ensure that the order of the candidates is random. Also, on the ballots having the list of candidates in the same order, the voters can scratch off the VIN on the RHC. By doing so, they can check that the OCNs are indeed identical, i.e. they do match this list order.

g) Vote verification (assessor): The counting is done by the officials at the counting center and must of course be supervised. The assessors must not count damaged ballots, i.e. ballots whose VIN has been scratched off, revealing the order of the candidates. If the ballot has not been damaged, the assessors scrape the VIN to reveal the OCN. Until the VIN is scratched off, it can be used as evidence that a vote was cast and not subsequently lost. To avoid any attempt to undermine the anonymity of the vote by recording VIN-OCN pairs, the RHCs are shuffled. Associating a sequence of OCNs with any recorded sequence of VINs that had previously obscured them is more difficult.

h) Sharing feedback: No post-vote interviews or questionnaires were conducted.

C. Code Voting

Code Voting is the subject of a study that proposes three approaches for vote registration [6]. The study involves 18 participants.

a) Documentation phase: Code Voting explores three approaches to record the vote: a manual approach, an approach using a QR-code and an approach using palpable objects. Unlike manual voting where voters enter their choice directly, here voters enter a code that represents their choice. The sheet containing voters and their associated code is distributed before the elections. The associated code is adapted to each approach. A series of numbers, a QR-code or a palpable object.

1) Manual approach:

b) Identification: A default login and password are provided on the code sheet distributed in advance. These parameters are not "specific" to the voter.

c) Authentication: Not specified by the authors. In this experiment, authentication is meaningless because voters identify themselves with default data.

d) Making a choice: Voters first enter the serial number of the code sheet. This allows matching the code number with a voter. Then, they enter the code corresponding to their choice.

e) Validation of the choice: Voters confirm their choice. Their vote is automatically sent to the electronic ballot box.

f) Vote verification (voter): The electronic ballot box sends an acknowledgement code. If this code matches the one on the code sheet, the participants have confirmation that their vote has been recorded.

g) Vote verification (assessor): This task is not specified by the authors.

h) Sharing feedback: The participants complete an SUS questionnaire and a UEQ questionnaire.

2) QR-code approach: Only the task *Making a choice* differs from the manual approach.

d) Making a choice: The voters scan the QR code which encodes the serial number of the code sheet. This allows matching the code number with the voter. Then, they scan the QR code corresponding to their choice.

3) Approach with palpable object: Only the task *Making a choice* differs from the manual approach.

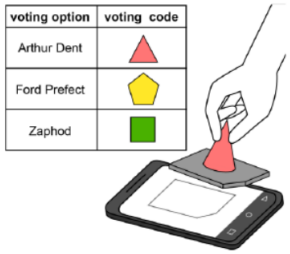

Fig. 3. Modality of palpable object approach of the Code Voting system [6]

d) Making a choice: Voters place first the item corresponding to the serial number of the code card on a touch screen (see Fig. 3). The system detects it and decodes the serial number. Then, voters put the item corresponding to their choice on the touch screen. The system detects it, decodes the choice and records it.

D. Blockchain-based e-voting system

We have also studied a fully decentralized e-voting system based on Blockchain and using smart contracts to address security aspects [5].

a) Documentation phase: The list of voters contains at least their name, their national identification number and their fingerprint. Alternatives to fingerprinting exist: sending a pin code to the voter's number and the voter must provide the pin code to verify themselves, or using a grooming finger if the person does not have a thumb.

As input of the genesis block (parent block of the first block of the chain), the organizers provide the list of eligible voters consisting of the fingerprint and an associated binary value, candidates, date and time of the beginning of the vote, date and time of the end of the vote. The role of the organizer stops here. The program code is previously integrated into the blockchain according to the concept of smart contract. When the starting date and time are reached, a function is called

invoking the election procedure to begin and the corresponding activities are performed.

Based on the number of voters, they are grouped randomly. Each group has a separate schedule, with a starting and ending dates and times for voting. Voting duration (represented by a boolean flag) is adjusted so that no voter suffers from a network slowdown or failure. Each group is notified by message and email. Once the time is up, the voters of the group can no longer access the vote.

b) Identification: Voters give their public key. The program checks whether the voter is part of the group whose turn is to vote (flag = true), and is present on the eligibility list.

c) Authentication: Voters give their private key, which is their own fingerprint. The program converts it into binary and checks if it matches with the list of the genesis block. The SHA-256 hash of this binary value is used as the only representation of the voter in the block.

d) Making a choice: The list of candidates is represented as logos associated with binary values. Once the candidate is chosen, the ballot is created and contains the hash of the binary fingerprint and the choice string. The choice string consists of the candidate's choice hidden in other randomly generated values. The random string consists of randomly generated 0/1 values. A block is created containing the ballot, and another sibling block is created that consists of the voters hash (binary fingerprint), the reference number of the broadcast block, its own reference number, and the opening value of the choice.

e) Validation of the choice: When voters validate their choice, they broadcast the block that contains the bulletin in the chain.

f) Vote Verification (voter): Once all voters voted, all sibling blocks are broadcasted one by one sequentially. The even-numbered nodes start calculating the result by referring to the blocks and extract the candidate's choice for each block. Here, all nodes are expected to get the same result, as no blocks are discarded unnecessarily in between and the blockchain does not support any changes.

g) Vote Verification (assessor): After validation, the peer nodes begin the proof of work on the sister block. The peer that wins the proof of work will be the first to verify that the voter did not vote earlier and that the ballot is in the correct format. After all the checks, the block containing the ballot is added to the blockchain and other peer nodes check and update their chains. The majority is taken into account. If the majority does not agree, the block is rejected.

h) Sharing feedback: No post-vote interviews or questionnaires were conducted.

E. Benaloh Challenge

The Benaloh Challenge is not a voting system but a technique to support the verification of voting intention which is widely implemented in e-voting systems. The experiment chosen [7] presents a realistic scenario. It has been used for the elections of the Federal Parliament of Germany in 2017.

The purpose of this experiment is to verify the usability of the verification process. To do this, the screens are recorded. An intention card, indicating for whom to vote is given to voters, to preserve their privacy and avoid revealing real voting intentions. They will be then able to verifiy if the recorded vote corresponds to the intention on the card, using the site or the mobile. Three verification approaches are proposed: manual, automatic and mobile.

a) Documentation phase: When starting the users are informed about the purpose of the study and that their actions will be recorded. They are asked to sign a consent form. Then, they are asked to fill out a demographic questionnaire: age, gender, occupation, previous voting experience. If the individual is under the age of majority, she/he must provide permission from a legal guardian to participate.

b) Identification: Before starting the experiment, the participants received the information and materials necessary to conduct the verification approach. All the participants had a falsified letter sent by the election authority containing login credentials and a blank space to use for writing down the verification code. The mobile outreach group received a slightly different version mentioning the verification device. In addition, a smartphone was provided with the application pre-installed.

c) Authentication: Not specified by the authors. In this experiment, authentication is meaningless since the credentials are false.

d) Making a choice: Participants select an option and send to the system, which encrypts it. During the encryption, the system generates a random value that acts as a salt to individualize each vote. This avoids that two identical information provide the same fingerprint when hashed. A verification code is generated from the hash of the customer's choice and the salt. At this stage, the participants can either vote by validating the encrypted vote or proceed to a verification. As the verification supported by the Benaloh Challenge is not compatible with the secrecy of the vote, the verified vote cannot be taken into account and must therefore be discarded.

e) Validation of the choice (voter): The participants validate their encrypted choice.

f) Validation of the choice (assessor): The verification is done with the help of a verifier, which is a software that is either present on the voting device (for the manual and automatic approach) or on an auxiliary device like a smartphone (for the mobile approach).

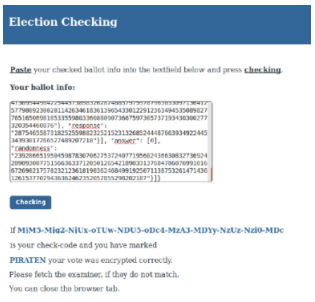

Fig. 4. Manual approach to verification in the Benaloh challenge [7]

1) Manual and automatic approaches: The system generates the data to be checked (option + random value). The participant clicks on the option *Check* (See Fig. 4 and 5.) and chooses the verification entity from a list. The data to be checked is automatically sent to the verification entity. The verification entity compiles a new verification code from the *hash* of the sent data and displays it. The participant compares the original verification code, written on her/his letter, with the newly created one. If the two codes match, the participant has confirmation that her/his choice was correctly encrypted.

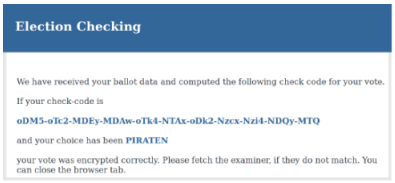

Fig. 5. Automatic approach to verification in the Benaloh challenge [7]

2) Mobile Approach: Instead of writing the verification code on a paper, the participant scans a QR-code that represents the verification code, using a mobile device such as a smartphone. The verification code is then transfered to the mobile device. By clicking on *Verify*, the participant is redirected to a second QR-code, which contains the verification data. She/he scans this QR-code and the mobile device uses the data to recalculate a verification code. This verification code is then automatically compared to the previously scanned code. Even, if participants do not have to compare the two results, they must verify that the mobile has encrypted the right choice. The mobile device displays the name of the candidate and participants must confirm that they have voted for the displayed candidate. (See Fig. 6.) If this is the case, participants have the confirmation that their choice has been correctly encrypted.

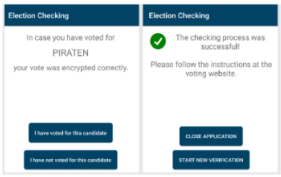

Fig. 6. Mobile approach to verification in the Benaloh challenge [7]

g) Vote Verification (assessor): Not specified by the authors.

h) Sharing feedback: Once the participants declare that they have finished, they are asked to complete the SUS questionnaire. Open-ended questions are included to collect their impressions on the different approaches (problems at the verification phase, whether they were really going to use it, how often). Each question has a space to allow the participants to justify their answers. The participant can also ask questions at the end of the questionnaire.

III. Properties

We have identified all the usability and security properties characterizing the e-voting systems that we have studied. When studying these systems, we have seen that the definitions vary according to the articles (i.e. authors), the e-voting systems and the evaluation methods. A same property can be defined and evaluated differently. Therefore, we had to propose a unified definition for each property and discuss the evaluation methods. In a way, we wanted to create our reference document (i.e. a kind of repository) regarding the usability and security properties cahracterizing e-voting systems. This repository takes into account the sub-properties and adjacent properties. The definitions provided are based on what we found in the litterature.

After definig the usability and security properties, we could conduct the comparative analysis of the e-voting systems.

A. Usability

According to ISO 9241-11[2], usability is the degree to which a system, product or service can be used by specified users to achieve defined goals with effectiveness (performance), efficiency (utility) and satisfaction, in a specified context of use. Usability is thus declined according to three properties, namely:

- **Utility or efficiency:** Is the task feasible? With what means? The interface must meet the needs of the users. Usefulness can be evaluated by doing a task analysis.
- **Performance or efficiency** : Performance is related to the efficiency property defined as the accuracy and degree of completion with which the user achieves specified objectives. Thus, the error rate also impacts the performance property.
- **Satisfaction** : The degree to which the user's physical, cognitive, and emotional reactions resulting from the use of a system, product, or service meet the user's needs and expectations. Although subjective, satisfaction can be evaluated based on user feedback. Different evaluation methods exist, such as the SUS (System Usability Scale) test, the implementation of the Thinking Out Loud protocol and behavioral observation.

Depending on the objectives of the analysis, usability is evaluated according to several evaluation methods, namely:

- *Inspection:* heuristic evaluation allows, through usability guidelines, such as those defined by Nielsen, to find and solve interface problems. The inspection can also be done through the verification of compliance with usability rules and recommendations. ISO standards can be used for standardized inspections.
- *User tests:* The Thinking Aloud protocol asks participants to say anything that comes to their mind as they complete a task. This may include what they are looking at,

[2]https://www.iso.org/obp/ui/#iso:std:iso:9241:-210:ed-2:v1:fr

thinking, doing, and feeling. Observers are asked to take notes on what participants say and do, without attempting to interpret their actions and words. In particular, they should note where they are having difficulty. The test sessions are mostly recorded on audio and video. This observation phase allows the developers to analyze afterwards what the participants did and how they reacted.
- *The survey:* The demographic questionnaire (age, past experience, social category, etc.) allows to target the groups of users to be tested. Coupled or not with a pre-interview, the participants' background sheds light on the way they will apprehend and use the system. The SUS (Brooke's System Usability Scale) questionnaire is used to measure usability[10]. The SUS uses a Likert scale ranging from "strongly disagree" to "strongly agree" to allow the participants to assess the usability of the system they have tested. The participants must respond quickly to capture the feeling, and if they do not know what to answer, they must respond in the middle of the scale. Although subjective, the SUS score can show extreme correlations or disagreements. The UEQ (User Experience Questionnaire, Laugwitz et al) test measures user experience.

B. Acceptability

Nielsen [11] distinguishes between practical acceptability and social acceptability. Practical acceptability emphasizes the relationship between the proposed functionalities and the ease of use. It therefore includes usability, ergonomic criteria and the interaction model. Social acceptability includes the users' impressions, attitudes and social and normative constraints leading to the choice or support of the use of a given technology.

C. Trust

According to ISO/IEC 10181-1:1996[3], Entity X is said to trust Entity Y for a set of activities if and only if Entity X assumes that Entity Y will behave in a certain way with respect to the activities. In the context of e-voting, the degree of trust is based on security, accuracy, privacy and verifiability. This property is considered critical because it can influence the intention to vote.

D. Consistency

According to Schneiderman, consistency occurs when consistent sequences of actions are required in similar situations[4]. Nielsen adds that users should not have to wonder if different words, situations, or actions mean the same thing[5]. In security terms, consistency would be the fact that for the same sample to be analyzed, the same result is obtained.

E. Accuracy

ISO 5725-1:1994[6] defines accuracy as the correctness and precision of measurement results and methods. All votes cast must be counted.

F. User experience

For Donald Norman, the user experience (UX) is "the responses and perceptions of a person that result from using or anticipating the use of a product, service or system"[7]. In the selected e-voting systems, three properties emerged:

- **Stimulation:** is a hedonic attribute of a product, which can lead to new impressions, opportunities and ideas.
- **Attractiveness :** the Magnus Revang's User Experience wheel[8] presents attractiveness as the combination of several design elements (interface and graphics). Attractiveness in the user experience would then depend on the placement of elements, typography, colors and contrasts, media used and graphic elements.
- **The novelty :** it is estimated to be a period of three months. In this temporary range, the user shows curiosity and discovers the environment.

G. Security

The main security properties are:

- **Integrity :** guarantees that the elements considered are accurate and complete. Integrity guarantees the accuracy of the information. This property ensures that the content of the vote has not been altered from its original intent, nor destroyed in an unauthorized manner (either incidentally or intentionally). We have identified two sub-properties of integrity. Namely:
  - **Transparency :** e-voting systems are often compared to "black boxes". However, it must be possible to audit them (thanks to an analysis conducted by experts and with the release of the source code for example). According to a BeVoting study, a system is transparent if there are audit possibilities adapted to any voter. Everyone must be able to verify that the election was conducted correctly. This audit must allow voters to determine how their vote was composed, and how this vote will be taken into account in the election result.
  - **Verification :** According to He [12] and Riera [13], a system is verifiable if each voter can ensure that her/his vote was included in the final tally. Sako [14] distinguishes between individual and universal verification. In individual verification, the participants must be able to verify whether or not their message reached its destination, but cannot determine whether this is true for other voters. In universal verification, everyone can independently verify that all votes

[3]https://urlz.fr/eVqV
[4]https://bit.ly/3EFmHll
[5]https://www.nngroup.com/articles/ten-usability-heuristics/
[6]https://urlz.fr/eVsd
[7]https://www.usabilis.com/definition-ux-experience-utilisateur-user-experience/
[8]Magnus Revang's User Experience wheel: https://urlz.fr/eVpO

have been correctly counted. We would add that the verification process must ensure that the system has encrypted the vote according to the voter's intent. In this way, no one can falsify the result of the vote [15].

- **Confidentiality :** only authorized persons have access to the elements considered. Confidentiality ensures secrecy. In this context, no one should be able to link a voter to a vote, and the audit should not alter the secrecy of the vote. The privacy of the vote must be preserved during the election as well as afterwards, and over a long period of time. We have identified two sub-properties of confidentiality. Namely:
  - **Privacy :** It is a multidisciplinary concept, with multiple perspectives depending on the type of actors. Westin [16] defines it as the control of the communication of personal data, Altman [17] as the control of interpersonal boundaries. The CNIL defines personal data as "any information relating to a natural person who can be identified, directly or indirectly"[9]. According to this definition, the vote is a personal data, and must therefore remain secret.
  - **Anonymity:** excluding the identity of the voter.

- **Availability:** it is a question of guaranteeing access to a service or a resource. The system must be able to perform a function under predefined conditions of time or performance. An underlying property has been defined, namely :
  - **Scalability :** The ability of an IT device to adapt to demand. It must be able to maintain its functionality and performance in case of high demand.

- **Non repudiation :** it guarantees that a transaction cannot be denied. One sub-property has been identified, namely:
  - **Tracability:** guarantees that accesses and attempts to access the elements considered are traced and that these traces are kept and exploitable. Everything must be recorded in the activity logs, so that it can be traced back in a history.

- **Authentication :** guarantees the origin of an element. This property allows to be sure that the sender is the real one. It ensures the identity of a user. An underlying property has been identified, namely :
  - **Unicity :** each voter has a unique identifier that she/he can attest by authenticating herself/himself. This property guarantees that the voters can vote only once and the ballot is valid only once.

[9]https://www.cnil.fr/fr/definition/donnee-personnelle

IV. Analysis of the voting systems from the repository

A. *Prêt à Voter*

Prêt à voter was developed to enable vote verification and election audits. It combines a paper trail (for recount) and a sophisticated cryptographic process to ensure secrecy and verification. Usability was evaluated using the SUS questionnaire. Among the 105 voting participants, 70 completed the SUS test.

In terms of effectiveness, 75.8% of participants understood the voting instructions. Only half of the participants understood the value of discarding the left side of the ballot, which contains the list of candidates. Those who did not discard the left side of the ballot may have jeopardized the secrecy of their vote, and therefore their privacy. Indeed, if an individual recovers the left part and attaches the right part kept by the candidate before the latter scans it, she/he can reconstitute the ballot. It is interesting to note that voters did not have much difficulty using the Web Bulletin Board, despite the fact that verification was a completely new experience for them. So when the usability guide is clear, security is enhanced.

The scan that records the content of the vote can be compromised by the behavior of the participants. If the participant withdraws the ballot too soon, the system may incorrectly record the check mark and/or the onion containing the order of the list of candidates. An incorrectly scanned onion renders the ballot null and void because if no match is found, it cannot be deciphered and therefore the order of the candidates is lost. Also, if the cross on the ballot is misshapen, or the expected time during the scan is not considered by the voter, the system may misinterpret its intent. It would undermine the integrity of the vote, against the will of the system.

The SUS score was 68.5. 63.3% of participants were reassured that the marks on the receipt matched those on their report card. This verification step not only provided security, but also improved participant comfort. 40.5% of participants felt confident using the voting procedure. The authors acknowledge that the usability of the *Prêt a voter* is lower than comparable voting systems in the United States. As a complement to the SUS test, the UTAUT model was used to assess acceptability and confidence. Among the 105 voting participants, 53 responded to this survey. 36.2% of participants would agree to use *Prêt a voter* in national or local elections, but 56.9% would prefer to use it for other types of elections. Acceptance is therefore above average when the stakes are lower. To explain this, the authors found a positive correlation between the average value of acceptance and security. In terms of safety, opinions are very divided. 41.5% think the system is vulnerable or very vulnerable to attack, 41.5% think it is somewhat not vulnerable and 17% think it is not vulnerable.

Considering the misunderstanding problems encountered, usability and security could be significantly improved by adding information on the voting procedure.

B. Scratch Card

One of the major challenges of e-voting systems is their adoption by the general public. Indeed, despite the benefits of e-voting systems, the confidence is these systems is decisive for their acceptability. In order to understand what is behind the already established trust in manual voting systems in the UK, the authors analyzed several elements. These include the close supervision of voting and counting by the electoral authorities, the fact that the system is based on physical evidence, kept under seal with the possibility of re-examination, and the simplicity of the process and its steps, enhanced by the several years of experience. The reticence towards e-voting systems is understandable, as thanks to the electronic devices the authorities do not have to supervise the election process, the votes are recorded in a dematerialized way and it is possible to transmit the votes and access to them remotely. The process and its steps are becoming more complex, the volatility of digital data is feared and the verification tasks are being rushed. These changes and new methods obscure the perception of e-voting systems, impede their acceptability and hinder their usability. The ability to review votes in the event of allegations of irregularity in the UK represents a privacy vulnerability as ballots are stamped with a discrete identification code linked to the polling station. What might be perceived as a problem is in fact known but generally accepted. The assumption made in the face of this paradox is that linking a code to an individual is a manually non-trivial task. This paradox shows the importance of the belief in the non-subversive character and the robustness of the system. This is possible only through the trust and transparency of the e-voting system. Thus, it seems crucial to the authors to tend towards these two essential characteristics - the non-subversive aspect and a degree of comprehension accessible to the larger number of users - while preserving usability.

The design of Scratch Card is part of an incremental improvement approach to the manual voting system used in the UK. Partially automated, the e-voting systems are, according to the authors, likely to preserve and/or gain the level of trust already given to manual voting systems. Thus, the use of paper ballots as the norm is retained. In particular, the authors aim to improve the secrecy of the vote, the accuracy and the overall efficiency of the system, rather than innovating the voting medium.

The secrecy of the vote is preserved, until the counting of the votes is done by the scratch card. The scratch card system is a widespread system and the general public is generally familiar with it. Since the secrecy of the vote is ensured, the properties of privacy and resistance to coercion are also enhanced.

Various aspects of the system are being changed and can be automated to speed up the voting process and improve the efficiency of the system. The use of voting machines to record and/or count votes is being considered, due to the large number of votes. To maintain and preserve the confidence of this proposal, two schemes are considered. In the first case, a single voting machine would be present at the counting center. The ballots would be transported in paper format to the counting center where they would be scratched before being scanned for counting by the voting machine. In the second case, each voting center would have a voting machine that would electronically transmit the counts to the counting center. Automated vote counting would eliminate human errors and thus increase the accuracy of the system. In addition, if the recording of the votes is entrusted to a machine, voters would be able to verify that their vote has been counted.

C. Code Voting

Code Voting [6] is the subject of a study that proposes 3 approaches to experiment different ways of recording a vote. This study focused on usability only, security was not addressed. Usability was evaluated through a SUS questionnaire.

All the participants were able to successfully register their vote. The level of efficiency is therefore 100 percent. Although the study sample is not representative of a population with only 18 participants, this indicator is promising for the usability of the three approaches. The QR-code approach had the highest SUS score (84.02), followed by the palpable object approach (78.61) and the manual approach (61.25). To understand the reasons of this score, the authors conducted a UEQ test where the allocation of points ranged from -3 to +3 depending on whether the property was rated as very poor or very good. The following properties were assessed: novelty, stimulation, dependence, reliability, effectiveness, clarity and attraction.

The manual approach had the lowest scores. The evaluation of its innovative character was negative. Its attraction and stimulation score was relatively low, and can be explained by its daunting nature. The participant had to enter multiple codes by hand. 5.5% of the participants were in favour of this approach. They felt it was safer because they were in control.

In contrast, the palpable object approach was recognized for its innovation and stimulation. 38.8% of participants were in favor of this approach. 4 people appreciated its intuitive nature and 3 felt pleasure in voting. Palpable objects are seen as a good alternative to the manual and QR-code for the elderly and visually impaired. Nevertheless, the study was not conducted on such profiles. Therefore, usability needs to be evaluated in more detail on these groups.

Overall, the QR-code approach was evaluated positively. Its clarity and effectiveness received the highest scores of the three approaches. 55.5% of participants were in favor of this approach. The familiarity of the QR-code allowed them to quickly get the hang of the system, and to feel relatively comfortable. 5 people justified this choice by the fact that the objects have a more important manufacturing and distribution cost than the QR-Code. Indeed, the devices must be custom-made for the election. To be recognized on touch screens, a particular recognition technology must be developed in a conductive material. As a result, it will be more difficult to implement this approach on a large scale. The scalability of this approach is compromised.

D. Blockchain

The blockchain [5] is a distributed database. It is public, meaning that all peer nodes in the network can access it. The records ensure traceability. Also, each node has the same data records. This is called consistency. Each activity is transparent; peer nodes can verify and validate it. Each transaction or activity in a block is verified. If the majority of peer nodes do not approve it, the action will not be entered into the registry. Thus, there is both individual and universal verification. Since all nodes have the same records, they must provide the same result as to the outcome of the vote. Non-repudiation is enforced. The majority of the group takes precedence over the individuality of the results. It is also a protection against DoS (Denial Of Service) attacks: all nodes have copies, there is no loss of information.

The blockchain is decentralized. The reduction of the third party is an interesting avenue as the participation of the third party can have a vulnerable effect on the procedure. The smart contract, in the form of code, is executed automatically. It establishes the terms of the contract between the two parties. During the execution of the smart contract, all validation steps are recorded in order to secure all data. This prevents the data from being modified or deleted afterwards. Once a data has been inserted, it is very difficult to falsify it. Dishonest miners must modify the previously broadcast block to insert themselves into the chain, and these modifications must be approved by the other miners on the network. The integrity of the vote is then preserved. Also, attempts to "double spend" are difficult. Proof of work requires a lot of computing power and energy to generate fingerprints that uniquely identify the blocks. If a node tries to vote twice, its second vote will be rejected as its fingerprint already exists in the booklet.

Finally, the blockchain guarantees confidentiality. The identity of the voter is recorded by the system as the hash of the fingerprint converted into binary. Privacy is preserved, in the sense that personal information is not broadcasted on the network. The voter is anonymous and her/his hashed public key is broadcasted and attests her/his identity. The voting slot is randomly generated and then allocated to groups when needed. It is more difficult to plan blackmail attacks or to try to manipulate intentions. Attackers do not know which individuals make up the next group to vote, nor when they will vote.

E. Benaloh challenge

The Benaloh challenge study explores three approaches to conduct a voting intention audit [7]. Since the voter is particularly active in this challenge, usability is a crucial parameter. In fact, the usability of the manual, automatic and mobile approaches was evaluated. Overall, the majority of participants were able to successfully verify their vote. 61.3% successfully completed the manual verification. The automatic and mobile approach had the same completion score of 81.25%. However, the experience of 5 participants was not included in the post-vote analysis either because they dropped out of the experiment or because they encountered technical difficulties preventing the necessary data collection.

The results of the study have shown that the automatic approach was not more effective than the mobile approach, and vice versa. In the manual approach, participants reported difficulties in understanding what they had to copy and paste and what verification data was displayed. Either they misunderstood the instruction and thought they had to copy and paste the verification code, or they did not understand what to copy and paste at all. The interface lacked some information: the status of the verification was not indicated, the instructions were not clear, and error handling was not taken into account. Several readings were required to understand the instructions, resulting in wrong actions that were not detected by the system.

The time required for a successful verification was recorded, with a starting time defined as t when the participant were pressing the verification button, and the ending time defined as t' when the participant were redirected to the system.

On average, the manual approach took three times longer than the automatic approach. Those who did the check with a smartphone were on average twice as fast as those in the manual approach. However, the mobile approach took a little longer, as the user had more actions to satisfy. QR-code scanning time was characterized by wide variations, ranging from 2 to 15 seconds per QR-code. Some participants found this waiting time too long, others gave up. A common usability issue highlighted by the authors was participants' motivation to verify the voting system. Those who thought the verification was too complex to understand or too time consuming did not want to proceed with the verification. There was a counter-intuitive aspect, participants were checking the voting system and not their personal vote which had to remain secret. If we want to check the voting system efficiently, we need to be able to test it several times and quickly. This is why the speed of execution is also important.

Regarding satisfaction, the automatic approach obtained the highest SUS score with 79.4 points. The mobile and manual approach had a similar score, respectively 75.8 and 75.4. In both the manual and automatic approach, usability issues related to the verification code were reported. Consisting of 43 characters, including both numbers and letters, the sequence was time consuming to copy and compare. It was easy to see that verification errors could occur. If the participants do not notice a mismatch, they may believe that their vote did not derive from the original intention and miss a fraud, or conversely, think that they vote was manipulated. The security of the vote is then compromised, and more particularly its integrity. A careless mistake done by the participant compromises the accuracy of the information. Moreover, QR-codes are limited in terms of character capacity. Thus, the encrypted voting data, too important, cannot be satisfied with a single QR-code. To facilitate the usability of the mobile approach, it would be relevant to consider reducing the number of characters to be able to use a single QR-code. On the other hand, since security also depends on the size of the verification

data sequence, this option must be subject to a risk analysis. Indeed, if the size of the sequence is reduced, brute force attacks aiming at establishing a correspondence between the vote and its verification code will be faster and have more chances to succeed. It would be interesting to analyze the size of the verification data sequence in such a way that the risk of compromising the security is acceptable. This problem is an example of the importance of having a trade-off between security and usability. An alternative to this scalability problem is the one used in Estonia, where the QR-code redirects to a link where the verification data are located.

V. Conclusion

End-to-end verifiable e-voting systems facilitate the verification of the integrity of individual votes during the election process. More specifically, end-to-end verification methods allow voters to confirm that their votes have not been manipulated by the client. Verification can be done in two ways.

- Verification based on the vote cast; ensuring that the voting system has encrypted the vote corresponding to the voter's intention.
- Verification based on the recorded vote; ensuring that the vote recorded by the voting system corresponds to the vote cast, and that it is correctly included in the election result

The common finding of the e-voting system experiments studied is that the approaches using QR-code are the most successful. To explain this, we hypothesize that the widespread use of this technology makes it more acceptable and usable. In the Benaloh Challenge [7], we saw that human errors in verifying the verification code is aborted, as the integrity of the vote is checked by the system. Unlike manual approaches, QR-code technology offloads the user by automating a few steps that seem burdensome, whether in terms of time, comprehension, or stimulation. While trusting this technology is a lead for usability, QR-code technology is limited in terms of security. Blockchain [5], on the other hand, appears to address many of the trust issues with e-voting systems identified by the authors of the Scratch Card study [9]. Although there is no physical evidence in blockchain, this distributed database concept in which all nodes have a copy of the information prevents information loss. Better yet, blockchain provides the traceability property that is essential to ensure non-repudiation. However, blockchain is still an abstract concept. In terms of usability, this can be problematic as it contributes to the obscure perception of the cryptography supported by e-voting system technologies. In addition, traditional voting systems were usually delegating the responsibility of managing the vote to an election authority whereas blockchain proposes a system that is decentralized. This can be not well perceived by the users and potential voters who can have a certain reluctance since the responsibility of the good functionning of the vote is no longer delegated to a single entity (to a trusted third party) but to individuals.

To increase the adoption of electronic voting systems, it is important to take into account both usability and security and find the best compromise between them. As future work, we plan to improve an existing e-voting system focussing on providing the best tradeoff between usability and security based on the properties and tasks that we have defined in the context of this study.

Through our analysis we have also identified a third inextricably linked criterion related to voter education. Indeed, voters' perception regarding the act and process of voting, as well as the relationship to electoral participation or democracy is considerable in the adoption of a new system. We believe that this is an area that should be explored in future work.

References

[1] Ameen, Zinah J Mohammed. Secure Electronic Voting Application Based on Face recognition and Ciphering. Journal of Computer Science Applications and Information Technology, s. d., 2018

[2] Adida, Ben, et Ronald L. Rivest. Scratch Vote: Self-Contained Paper-Based Cryptographic Voting. In Proceedings of the 5th ACM Workshop on Privacy in Electronic Society - WPES '06, 29. Alexandria, Virginia, USA: ACM Press, 2006. https://doi.org/10.1145/1179601.1179607.

[3] Chaum, D. Secret-Ballot Receipts: True Voter-Verifiable Elections . IEEE Security Privacy Magazine 2, no 1 (janvier 2004): 38-47. https://doi.org/10.1109/MSECP.2004.1264852.

[4] Weldemariam, Komminist, Adolfo Villafiorita, et Andrea Mattioli. Assessing Procedural Risks and Threats in E-Voting: Challenges and an Approach. In E-Voting and Identity, edited by Ammar Alkassar and Melanie Volkamer, 4896:38-49. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007. https://doi.org/10.1007/978-3-540-77493-8_4.

[5] Sadia, Kazi, Md. Masuduzzaman, Rajib Kumar Paul, et Anik Islam. Blockchain-Based Secure E-Voting with the Assistance of Smart Contract. In Proceedings of the IETE International Conference on Blockchain Technology (IC-BCT 2019) Blockchain Technologies. Mumbai, India, 2020. https://doi.org/10.1007/978-981-15-4542-9_14.

[6] Marky, Karola, Martin Schmitz, Felix Lange, et Max Mühlhäuser. Usability of Code Voting Modalities . In Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, 1-6. Glasgow Scotland Uk: ACM, 2019. https://doi.org/10.1145/3290607.3312971.

[7] Marky, Karola, Oksana Kulyk, Karen Renaud, et Melanie Volkamer. What Did I Really Vote For? On the Usability of Verifiable E-Voting Schemes . In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18, 1-13. Montreal QC, Canada: ACM Press, 2018. https://doi.org/10.1145/3173574.3173750.

[8] Marco Winckler, Regina Bernhaupt, Philippe Palanque, David Lundin, Kieran Leach, Peter Ryan, Eugneio Alberdi, Lorenzo Strigini. Assessing the usability of open verifiable e-voting systems: a trial with the system Prêt à Voter . https://www.researchgate.net/publication/228559244_Assessing_the_usability_of_open_verifiable_e-voting_systems_A_trial_with_the_system_Pret_a_Voter

[9] Randell, Brian, et Peter Y A Ryan. Voting Technologies and Trust. In Proceedings of the Formal Aspects in Security and Trust, Third International Workshop, FAST 2005, Newcastle upon Tyne, UK, July 18-19, 2005

[10] Brooke, John. SUS - A Quick and Dirty Usability Scale , s. d., 7.

[11] Nielsen, J. (1993) Usability Engineering. Academic Press, Inc., Harcourt Brace Company, San Diego, USA.

[12] He Q., Su Z. (1998) “A New Practical Secure e-Voting Scheme”, IFIP/SEC’98, Austrian Computer Society, Austria, pp. 196-205.

[13] Riera A., Borrell J., Rifa J. (1998) “An Uncoercible Verifiable Electronic Voting Protocol”, IFIP/SEC’98, Austrian Computer Society, Austria, pp. 206-215.

[14] Sako K., Kilian J. (1995) “Receipt-Free Mix-Type Voting Scheme: A Practical Solution to the Implementation of A Voting Booth”, EUROCRYPT’95, Malo, France, pp. 393-403.

[15] Fujioka, Atsushi, Tatsuaki Okamoto, and Kazuo Ohta, *A Practical Secret Voting Scheme for Large Scale Elections*, s. d., 2.

[16] Westin Alan F. Privacy and Freedom. New York: Atheneum Press, 1967

[17] Altman, I. The environment and social behavior: Privacy, personal space, territoryand crowding. Monterey, CA.: Brooks/Cole, 1975.