Trust in Internet Election Observing the Norwegian Decryption and Counting Ceremony

Randi Markussen, Lorena Ronquillo and Carsten Schürmann
IT University of Copenhagen. Rued Langgaards Vej 7
DK-2300, Copenhagen (Denmark)
Email: {rmar, lron, carsten}@itu.dk

***Abstract*—This paper discusses the Decryption and Counting Ceremony held in conjunction with the internet voting trial on election day in the Ministry of Local Government and Regional Development of Norway in 2013. We examine the organizers' ambition of making the decryption and counting of electronic votes public in order to sustain trust in internet voting. We introduce a pragmatic approach to trust that emphasises the inseparability of truth from witnessing it. Based on this and on a description of how the event was made observable and how the complexities in the counting process were disclosed, we discuss what we term *economy of truth* from the perspective of the IT community involved in the ceremony. We claim that broadening the economy of truth by including more explicitly social and political perspectives in the ceremony, and in internet elections in general, and how witnessing is brought about, would make a more solid case for understanding how democracy is transformed.**

I. Introduction

Democratic elections in contemporary society, according to Article 21, Universal Declaration of Human Rights, shall be periodic and genuine; they shall be by universal and equal suffrage and guarantee the secrecy of the vote. Practicing elections in a manner that is compatible with these principles raises, among other things, the question of who is involved in organising, administrating and overseeing the electoral process and the voting procedures, in particular. Thus the public staging of the election, as well as public involvement in the counting, have in many countries been constitutive elements in preserving trust and legitimising a representative democracy.

Internet voting challenges these elements in a significant and profound manner, as the public engagement in counting is replaced by counting by computers that are managed by technical experts. What is rarely addressed in detail, however, is how the experts carry out their work, and how their activities may relate to the public. The internet voting trials in Norway in 2011 [2], [19], [29] and in 2013 [7], [22] stand out, as the Norwegian Ministry deliberately experimented with the idea of publicly overseeing the experts' counting activities during a public event, the so-called Decryption and Counting Ceremony. The Ministry of Local Government and Regional Development of Norway (hereafter *the Ministry*) was responsible for designing and running the ceremony. The ceremony took place on the premises of the Ministry on election day.

In this paper, we study in detail the way in which the Administration Board (employed by the Ministry) rendered the decryption and counting activities observable. The goal of the ceremony was to convince the audience that truth is produced. The Ministry argued in advance that "Observation in the *back office* combined with voter observation of return code replaces the function of the observer in the polling station" [6]. We mainly concentrate on the *back office* disclosure in order to explore how the idea of trust in this event can be addressed.

Based on a pragmatic understanding of trust in science and within science, and inspired by Shapin's framework [26, p. 6], we describe the ceremony and explore what we term *economy of truth* from the IT community's perspective. We argue that broadening the economy of truth by articulating more explicitly social and political perspectives may create a more solid understanding of how democracy is transformed. Our arguments intend to inform research communities in the area of e-governance more broadly, when trust is a key concept, as well as politicians and the public in general.

This paper is organized as follows: Section II introduces a pragmatic, philosophically motivated understanding of trust and its importance in everyday life as well as in scientific communities, and briefly presents its relevance in understanding trust in elections. Section III introduces the Decryption and Counting Ceremony and its organizational set up, including the legal bodies witnessing the event. Then, Section IV gives a high-level understanding of the decryption and counting stages of the Norwegian internet voting system as it was designed, and sketches those procedures that were executed during the actual ceremony to render parts of the system observable. The description aims by no means at being a comprehensive outline of all the details involved in the ceremony, but it serves mainly to communicate the technical complexities and challenges involved in the ceremony in a manner that is consistent with what the organizers probably intended to achieve. More technical information about the voting protocol can be found in [11]. Section V brings the insights from the various sections together by discussing the economy of truth shaped by the Decryption and Counting Ceremony from a technical perspective, as well as a social and political perspective, and finally Section VI concludes the paper.

II. How to understand trust

Over the last decades the term *trust* has received increasing academic attention. This is driven in part by our curiosity to understand how contemporary societies work, not least the role of trust in science in the making of society, as well

as the role of trust in producing knowledge within scientific communities [15], [27], [33]. Predominant perspectives tend to build on rational philosophical assumptions focusing on individual rational decision making. In contrast, pragmatic perspectives, which are the ones this paper follows, emphasize the collective aspects in the making of social orders and in knowledge production, and argue that whether actions are rational or not do not belong to the individual actor, but it also depends on how they are perceived by others [30, p. 19]. Of special interest in our context is Steven Shapin's seminal work on the origins of experimental philosophy [26]. Shapin shows that the gentlemanly culture of truth telling that Robert Boyle together with members of the Royal Society developed was consequential for trust in their new natural science. Furthermore he suggests that contemporary scientific truth claims similarly involve the witnessing by specific scientific communities [26]. In relation to elections, this argument implies that the community involved in the counting go hand in hand with the community of accounting. Where Besselaar et al. [5] argue that voters' trust in the technology is more important than the technical characteristics, we want to avoid in this paper the dichotomy between trust/subjectivity versus things/objectivity and argue that the concept of technical characteristics is closely related to the witnessing of truth claims within a specific scientific community.

Thus trust is involved in the dynamics in social ordering in everyday life, as well as in scientific knowledge production, as no single individual can constitute knowledge outside of a community. "Truth consists of the actions taken by practical communities to make the idea true, to make it agree with reality" [26, p. 6]. Shapin stresses that pragmatic philosophers reject a static understanding of truth, and emphasises the close connection between truth and trust by pointing to their etymological root in the Germanic word for tree: "Trust/truth is therefore, like a tree, something to be relied upon, something which is durable, which resists, and will support you." [26, p. 20]. The early pragmatist philosopher W. James compared the investment in trust to a credit system: "Our thoughts and beliefs *pass*, so long as nothing challenges them, just as bank-notes pass as long as nobody refuses them." [13, p. 88-91]. In connection to elections, this argument suggests that if people experience their government to be well working and find elections are held and have been held in a fair manner, they will continue trusting it until an event proves this wrong. The recent evaluation report of the Norwegian internet trial in 2013 [24] also makes this argument, suggesting that the slight reduction in trust in elections which was perceived in the municipalities involved in the internet election in 2011 had to do with its newness. But the moment people did not experience any major public scandals, the level of trust was reestablished [24].

This illustrates that trust not only involves routine interactions, it includes deliberate decisions on whether to trust or not, as well as distrust and scepticism. Trust but also distrust "presuppose a system of takings-for-granted which make this instance of distrust possible." [13, p. 19]. Thus computer scientists, especially cryptographers, share by training a specific way of addressing a situation and discussing the relevance of specific arguments. Hence the character of scepticism depends upon the extent and quality of trust in a given community. In a Scandinavian context it is often said that people trust their governments[1], meaning that if people express scepticism and distrust, it should be seen against a solid quality of trust as well. Scientific communities, or political communities to mention some, may cultivate specific language games, ways of making truth claims and discussing them. The opposite of trust in Shapin's account is "the public withdrawal of trust in another's access to the world and in another's moral commitment to speaking the truth about it (. . .). It is not just that we do not agree with them; it is that we have withdrawn the possibility of disagreeing with them." [26]. Thus trust, as well as distrust, are involved in making democratic societies work, and without them societies may fall apart.

We are especially interested in the metaphor of *economy of truth* that Shapin shortly introduces: "Knowledge is the result of the community's evaluations and actions, and it is entrenched through the integration of claims about the world into the community's institutionalized behavior. Since the acts of knowledge-making and knowledge protecting capture so much of communal life, communities may be effectively described through their economies of truth." [26, p. 6]. The metaphor *economy* suggests that there are interests, costs, and values involved in truth-making and hence trust-making, and that protecting certain ways of understanding the world, may be as important as producing knowledge. For instance, an economy of truth shaped by paper ballots and public involvement, is extraordinary in that it consists of all voters, including election officials who know the regulations and procedures. They perform a temporary community, distributed into several minor communities all over the countries, who have to contrive to work together locally and apply the regulations in practice. More can be said about how computers are already applied in many of their work activities. Suffice to say that the process is nonetheless in economic terms sometimes described as *people intensive* as opposed to technology intensive, following a dominant logic in our economy of replacing human labour with machines. In our context, internet voting as well as e-voting involve new scientific communities of knowledge-making and consequently other aspects of the economy of truth. Indeed, they require new equipment and machines, which in Shapin's argument, depend on specialized knowledge and a community that favours specific truth claims and ways of producing and protecting truth, as we explore in this paper. One may talk, for instance, about an economy whose monetary units includes competences, truth claims and ways of dealing with them, technologies, proofs, etc.

An important instrument for maintaining confidence in the electoral process and giving elections credibility is often expressed as transparency in every step [8], [32], meaning that the government and the organizers do not hide activities from the public. Practicing elections along these principles is a well-established habit in Norway and has no doubt inspired the Norwegian Ministry in organising the ceremony and trying to create a public space to attest to the truth produced in the counting of internet votes.

[1] According to the OECD's Better Life Index [20], 66% of people in Norway say they trust their national government, being one of the highest rates in the OECD and much higher than the OECD average of 39%.

III. The Decryption Ceremony

In June 2013 the Ministry appointed an Internet Election Committee (IEC), to ensure that the internet voting trial was conducted in accordance with the regulations, and in a manner that is open and the voters could trust [16]. The idea was to have a group of people, independent of the Ministry, to supervise the preparation, conduct verification and approve the results, besides having the authority to suspend or cancel the trial in case of irregularities. The members of this committee were also involved in the decryption event, as we will later see. The nine members covered technical and political competences, and also included a representation from the municipalities involved in the trial: one member from the Norwegian Data Protection Inspectorate, an election researcher, a cryptographer, the chairmen of the Election Boards of three of the counties, and three regular voters selected from the pilot municipalities [16]. In addition, a verification team consisting of three people with electoral and technological expertise was appointed to check the correct behaviour of the decryption and counting process [22].

The composition of the new legal institutions is noteworthy, as it suggests that political and social competences are also important in accounting for the event, besides only technical expertise. At the same time, the internet voting technology in use is based on a specialized discourse of advanced mathematics, including cryptography, and its own system of takings-for-granted, assumptions and technical challenges. Opening this black-box to convince the technically savvy audience that the system performs as expected is one thing. However, making specialized concepts such as encryption and decryption keys, secret-sharing and zero-knowledge proofs comprehensible, and therefore relevant, to a public in general that does not necessarily share this discourse, is another.

As already mentioned, many internet voting technologies are based on cryptography, and so is the Norwegian that uses, in particular, asymmetric key cryptography. During the course of the election a public and a private keys are created and used. The public key is known by everyone and used by the voter to encrypt his/her vote and make it unreadable[2], while the private key allows to decrypt the encrypted vote and hence recover the original vote. Clearly, the election private key is of special importance in the voting system when securing the privacy of votes, thus in the Norwegian context the IEC members were assigned the authority to safeguard that key. At the beginning of the election, during the so-called Key Generation Ceremony, the election keys were created and each IEC member was given a smartcard containing a unique share of the private key. Their task consisted of keeping these shares safe until the Decryption and Counting Ceremony, at the end of the election, where by putting at least 6 out of the 9 shares together [14], the key would be reconstructed and used to decrypt the electronic votes.

The Decryption and Counting Ceremony took place in an auditorium in the Ministry, two hours before the election closed. As the design of the auditorium suggests, it creates a room for an audience to watch a performance. In this context, the stage (see Fig. 1) allowed for several computers, a safety deposit box, a blender (used to destroy physical storage media) and some screens, as well as the people responsible for the internet voting system. Besides the IEC and the verifier team, the audience included election observers such as representatives from the OSCE, the Carter Center, as well as from other countries, and also the company that had built the system.

Fig. 1. The setup and the agenda [17].

The term *ceremony* underlines the formal character of a public event, and stresses the serious challenges involved in developing ways of making decryption visible, even to a mixed audience, including anybody interested in watching the online broadcast of the event [17]. However, what is shown in the ceremony is not the final counting of the election results, but a preliminary counting. As mentioned by the main spokesperson, the ceremony works as a *guided tour*, a demonstration of the virtual procedures that describe the internet counting, at the same time as the audience is invited to stay and review the final count later on.

Norway is not the only country in the world having engaged in internet elections. In Estonia, internet voting has been used for binding political elections since 2005, both local and nationwide, and other countries like Canada and Switzerland from 2003, and Australia from 2011 [2], [4] have also used it for some municipalities. However, to our knowledge, the decryption events of these elections, if any, have mostly gone unnoticed in the literature. In the case of Norway, recent reports from International Election Observation Bodies [7], [22] mention the Counting and Decryption Ceremony just as one more step taken by the Norwegian Ministry in order to make the system transparent, but do not seem to have looked into the event as such. In Estonia, Alvarez et al. [1] mention that the decryption and counting of internet votes in the election of 2007 took place before the election closed, and in order to ensure that none of the results from the internet vote tabulation could be broadcast to the media, candidates, or parties until the polls had closed, all communication devices of observers were confiscated, the doors of the room sealed, and security guards posted at the doors, while the authors do not mention any online broadcast of the event. According to the OSCE/ODIHR [21], the counting of internet votes in the Estonian parliamentary elections of March 2011 was done in the presence of the National Electoral Committee members and domestic as well as international observers, but no ceremony, as in the case of Norway, is mentioned either. In the local

[2]This encrypted vote is unreadable under certain assumptions well-known within the cryptographic community but out of the scope of this paper.

elections of October 2013, however, Halderman et al. [12] do mention in passing that the encrypted votes were decrypted and counted at an event that resembles somewhat the Norwegian Decryption and Counting Ceremony, in that there was an audience witnessing the process in a room of the Estonian Parliament building, and the event was also made available online [10]. As for other countries like Canada, Switzerland, and Australia, to our knowledge, the opening of the electronic ballot box and decryption of internet votes was not witnessed by the public, but by scrutineers and sometimes also the police, as in the case of Geneva, Switzerland.

IV. Decryption and counting

This section briefly describes the main characteristics of the Norwegian internet voting system, paying special attention to the decryption and counting stages, and then reviews some of the procedures we observed about the system working during the public ceremony.

The Norwegian internet voting system is conceived as a supplement of the traditional paper-based voting. In order to mitigate the risk of voter coercion or vote buying inherent to internet voting, and given that voters were able to vote electronically during an advance voting period of roughly one month, the system supports *repeat voting*, by which voters are able to vote multiple times, but in such a manner that only one vote will be counted. Thus if a voter casts multiple electronic ballots, the last cast ballot is the one counted, while any vote cast on paper is final and overrides previous electronic votes [11].

The system also uses return-codes, a mechanism that allows voters verify that their vote has been correctly received by the voting server and thus provides individual verifiability, usually referred to as *cast-as-intended*. This feature is not discussed further in this paper.

An important cryptographic component of the Norwegian internet voting system are *zero-knowledge proofs*, i.e. methods by which a verifier can be convinced (with negligible amounts of doubt) that a particular statement is true without learning anything else apart from the fact that the statement is true. In the case of voting, for instance, zero-knowledge proofs allow verifiers to check, among other things, that the votes have been correctly decrypted without the private key being revealed to them.

The electronic ballot box contains all internet ballots encrypted [9] and also digitally signed by the corresponding voter [11]. Once the voting phase is over, this ballot box is taken offline and handled on air gapped servers, i.e. physically isolated and not connected to the internet. The decryption and counting of internet votes thus takes place in three phases. The first phase, called *cleansing*, identifies the ballots that will be counted according to the repeat voting policy, and disregards the rest. The signature of the resulting ballots is also checked during this phase. The second phase is called *mixing*, which cryptographically anonymizes the cleansed ballots so as to prevent tracing them back to the voters who cast them. This means that the ballots are shuffled and re-encrypted at each mix-net node, so that they end up in a different order and also look different (yet still encrypt the same votes). In the final phase, the *e-counting*, the decryption key is recovered from the shares of the smartcards of the IEC [25]. The mixed ballots are then decrypted, tallied, and the electronic vote count is finally submitted to the central election administration system (EVA[3]).

In addition, every phase of the decryption and counting process generates zero-knowledge proofs showing, respectively, that the cleansing of ballots was done properly, the mix-net nodes behaved correctly and actually shuffled and re-encrypted the ballots, and that the decrypted votes accurately reflect the encrypted votes.

A. Making the decryption and counting visible

In what follows we review some of the relevant procedures we observed, carried out by the Administration Board (hereafter *the organizers*) at the Decryption and Counting Ceremony.

On the auditorium stage there is a table with three laptops, a safety deposit box, a blender and three overhead displays, showing the screen content of the laptop in use, as well as some explanatory slides giving details about what is happening during each phase. Two of the organizers are seated at the table. They will be the ones running a number of commands on the laptop corresponding to the respective phase, while a third, the spokesperson, is standing up and guides the event. In a corner of the room, a group of verifiers with a computer connected to their own big screen are sitting and waiting to come into play (see Fig. 1). Among the audience, the nine members of the IEC, equipped with their smartcards, also observe the event, awaiting to be called upon during the e-counting phase to insert their smartcards into a smartcard reader, used to reconstruct the election private key.

According to the organizers, the electronic ballot box that is about to be decrypted and counted as part of the ceremony was retrieved from the central database server some time before the ceremony in the presence of the verification team and the observers. Starting with a memory stick containing the electronic ballot box, a second one containing the electoral roll, and a third one with some other election data, the process goes through the cleansing, mixing and e-counting phases. At the same time, the overhead screens show the commands running each phase. Most of these commands are standard Linux commands, and no user interface is used but the terminal. By doing this, the organizers deliberately give the audience a glimpse into the inner details of the decryption and counting process like, for instance, which folders are being accessed at any time, what is their content, etc.

The three laptops on the table are color-coded and each connected to different servers through a cable of the same color. The audience is informed that each laptop runs one of the three phases of the decryption and counting process, thus the colors identify the components that are in use during each phase, and illustrate that the servers are apparently not connected to each other and therefore are air gapped. To confirm the latter, whenever some data (the processed ballot box) needs to be transferred from one phase to the next one, it is physically moved from one laptop to the one running the next phase by means of a new and recently unsealed memory

[3]Elektronisk Valgadministrasjonssystem.

Fig. 2. A member of the verification team taking a picture of the hash value shown in one of the big screens [17].

stick. These memory sticks are taken from the safety deposit box, for which the verifier team has the key. The organizers also show that the memory sticks are new by showing each time that they are empty. In addition, the main table of the auditorium is *kept tidy* at all times which is achieved by extracting the memory stick from the respective laptop whenever the organizers finish working with it. This aims to help the verification team and the audience to understand the movement of the data throughout the three phases. Furthermore, in order to show that the cleansed ballot box and the mixed ballot box remain unchanged when transferred from one phase to the other, and no process injects new votes into the ballot box, a well-known cryptographic tool known as *hash function* is used. The output of a hash function is unique (at least for our purposes it may be considered as such), thus it is used here to prove the equality of two files located in different machines. In the context of the ceremony, the hash value of the file to be transferred is shown both before being copied to the memory stick, and after being copied to the next machine. This enables the verifier team, as well as anyone among the audience, to take a picture of the first hash value and compare it to the second one for equality (see Fig. 2).

Because of the sensitive nature of the data contained in the two memory sticks used between the cleansing and the mixing phases, and between the mixing and the e-counting phases, as well as to illustrate that the ballots in these memory sticks should never be recovered, these memory sticks are immediately destroyed in a blender after use.

Once the mixing phase is completed, the verifier team is given two memory sticks containing, respectively, the mixed ballot box and the zero-knowledge proofs generated in the mixing phase, to check that the mixing has been conducted correctly. Later on in the ceremony, the verifiers inform that the checking has been successful. Next, as part of the e-counting phase, the organizers take a top hat in which, prior to the ceremony, they have put the name of the IEC members in small pieces of paper. One by one, the members are named at random to bring their smartcards and enter their parts of the key into the system [25], until the election private key can be recovered and finally used to decrypt the internet ballots and obtain the preliminary results. These results are then copied to a memory stick, and transferred to EVA after the public ceremony.

Finally, the verifier team is given the memory sticks containing the mixed ballot box and the zero-knowledge proofs generated in the e-counting phase, to check the decryption. The result of this check, however, is not given during the ceremony because of timing constraints.

V. Discussion

The Decryption and Counting Ceremony demonstrates that the truth in the processes involved in counting electronic votes, when internet is used to cast votes and cryptography is a prime warrantor of both the secrecy of these votes and the election's integrity, is produced very differently from the counting of paper ballots. The sketch in Section IV-A, done primarily with an eye on what we think the intention of the organizers was, points to the event as a spectacle where various elements are visualised in order to make the procedures transparent and observable to the audience and some sort of public. Following Shapin's argument that truth and trust are closely related to the witnessing of an event, we discuss the economy of truth and the ambition of accounting for the decryption to the public in various perspectives on the event.

A. The economy of truth in the IT community's perspective

Trust in the internet election, and in e-voting more generally, is mostly addressed as a question of citizens' trust. Thus the Norwegian evaluation reports of the internet voting trial in 2011 [23, p. 63] and in 2013 [24] measure the degree to which citizens trusted the technology without addressing more explicitly the ceremony and the Ministry's communication efforts as such. More broadly, the field of *e-governance* is engaged in suggesting and defining measures that should be in place for a specific technological solution to be considered trustworthy by the IT community and consequently, as we tend to hope, also by the public. E-governance also focuses on aspects that are relevant to internet voting, such as transparency, evaluation according to international standards, separation of duty, verifiability, vote updating, etc. to establish trust among the public [28], [31].

The Norwegian Decryption and Counting Ceremony adds an important element to this context, however, by opening the black-box of how decryption works, and highlighting that trust as understood by Shapin is an element within the IT community as well. As mentioned in Section II, the IT community shares a system of takings-for-granted that makes them expect certain things to take place, and this in turn makes specific ways of distrusting possible. Indeed, distrust is a hallmark of IT security with its focus on defining adversary models and estimating what might go wrong. As Shapin suggests [26], distrust is crucial in many kinds of knowledge production, and in our view the ceremony points to important aspects of the economy of truth within the IT community. Most importantly, it bears witness to the technical complexity of the Norwegian internet voting system. The IT community seems to agree that this complexity inevitably makes the system prone to risk and failures, as also mentioned in the Carter Center report [7], but it also recognises the efforts made by the organizers in managing the complexity by encouraging transparency and inviting peers to give feedback and witness the ceremony.

The ceremony attests to the idea that IT is not so much an autonomous object as a socio-technical learning process.

However, not everything that the IT community would have liked to observe, could be made visible at the ceremony. For instance, the audience could not check, and therefore needs to trust, that the correct electronic ballot box was the one used for the ceremony, or that the actual preliminary results, and no others, were transferred to EVA. While disclosing these steps could have helped in making the process more transparent, they were only shown to the verifier team. In addition to this, given that the decryption key was recovered from the IEC members during the preliminary count and before the final count, the audience has again to trust the organizers to have safeguarded and not misused it during this (even if short) period of time.

There are some other aspects in which the ceremony, probably due to time or space constraints, did not succeed in making the process more visible from a technical point of view. For instance, the use of standard Linux commands might not have given enough confidence to an IT literate about what the programs were actually doing, since it is possible to override these commands to perform a completely different task. We suspect that before the ceremony started and in front of the verifier team and the observers the organizers demonstrated the robustness of the Linux platform and that they had the right implementation of the hash function. Regarding the zero-knowledge proofs, the public has to trust the verifiers to use reliable software to check these proofs and complete checking those proofs that were not checked by the end of the ceremony. And ultimately, taking into account that what was covered by the ceremony was just a preliminary count, one wonders how the audience can be sure that the final count was indeed done in a manner similar to the simulation just observed. Besides these questions closely related to the system of takings-for-granted in the IT community, one can add the trust in the wider infrastructure in which the internet election and the ceremony depend on. Perhaps not intended as such, but to us, the top hat pointed to the ambiguities involved in keeping some things secret while making others visible, suggesting that the boundaries between science and fiction may not be necessarily as robust as we tend to think.

The organizers took also some other precautions to make the system more transparent, such as, for example, publishing the source code and the system documents in advance. This allowed for independent reviews and assessments and thus contributed to the IT community's trust in the system. The Decryption and Counting Ceremony did this to a much lesser extent because, we suspect, of those aspects that could not made visible during the event, as we have discussed above. More importantly, while the ambition to create transparency is one of the goals of the ceremony, we observe that it is reduced to trusting the work of the verification team that is responsible for approving the final result. Their position in the room as partly on the scene when checking the hashes and equipped with their own computer, and partly in the audience when they sit back and watch together with the rest of the audience, points to their role as what is increasingly termed a *proxy* in the election observation community: a stand in for the audience and the public, as the IEC appointed them. Thus the ceremony makes obvious that trust in that the votes are counted correctly ultimately is about trust in the verifiers, as well as the organizers. In this respect the ceremony relates to the idea of replacing the function of the observer in the polling station in democratic elections.

B. The economy of truth in a social and political perspective

While the ceremony makes it possible for the IT community to discuss and form an opinion on the quality of the counting of votes, it is less obvious, however, to what extent the fact of replacing the observer in the polling station is meant to be an explicit part of the ceremony. One might expect that the IEC was assigned the task to try to address questions relating to democratic legitimacy and political and social aspects of the ceremony and the internet voting trial. But their role in the decryption ceremony was apparently to focus on controlling the access to the election private key, and thus attesting to the correctness of a central albeit small part of the ceremony. They seem to fulfill the expected performance during the ceremony, but to our knowledge they have not documented their work or reflections in a publicly available form. The OSCE report points to the vague definition of their tasks and argue that "the IEC met rarely and its role appeared largely formalistic. Most IEC members with whom the OSCE/ODIHR EAM [4] met were not conversant with the system and relied entirely on the MLGRD[5]'s guidance and advice. This called into question the IEC's competence and its effectiveness as an oversight body." [22, p. 8]. It is noteworthy that this criticism stays within a technical framing of the event and the system of takings-for-granted within the IT community, which only a few members of the IEC share. However, the OSCE report does not mention the possibility of discussing the ceremony more explicitly in social and political terms, and thereby providing the politicians and the public with other kinds of arguments.

As mentioned in Section II, the term economy of truth emphasises that "Knowledge is the result of the community's evaluations and actions, and it is entrenched through the integration of claims about the world into the community's institutionalized behaviour. Since the acts of knowledge-making and knowledge protecting capture so much of communal life, communities may be effectively described through their economies of truth." [26, p. 6]. The above suggests that for the Norwegian trial, technologists did not include discussions about the witnessing and its quality in their economy of truth. They also did not consider other public aspects of the event, e.g. in what respect is the aforementioned replacement useful, desirable or promising. But then we beg the question why the organizers bothered to organize the Decryption and Counting Ceremony in the observed form and to make it public, if only computer scientists and other experts are considered reliable observers if not to speak of reliable witnesses? We feel strongly that it is prudent to start considering witnessing and observing as part of the economy of truth for any internet voting platform and respective ceremonies, in particular.

In broader terms, if we compare the ceremony to the democratic paper-based election in Norway, there are noteworthy differences in the kind of public that the various processes allow for. In Norway as well as in many other countries, the paper-based enactment does not only give the public the opportunity to observe the election, as the organizers of the Decryption and Counting Ceremony mention, but they are allowed to participate in the counting as volunteer election officials. If we take the distributed nature of the counting

[4]Election Assessment Mission.

[5]Ministry of Local Government and Regional Development.

process across numerous municipalities into account as well, it demonstrates the involvement of any voter who cares to participate, as well as it presumes that voters are able to count and understand the event. This means that they are accountable witnesses in the particular part of the event they take responsibility for, and it signifies a shared responsibility in terms of trusting/distrusting the counting of one's fellow citizens as the results are finally brought together in the Ministry.

The Decryption and Counting Ceremony, on the other hand, involves only computer scientists as reliable witnesses in the legitimate audience. However, there were also others in the audience, e.g. peers from the e-voting community, observers from various organizations, or representatives from other governments who want to know about the technology, and vendors. At the same time, anyone from anywhere in the world is, in principle, invited to take part via the online broadcasting. This position is strikingly different from the involvement in the local paper-based election process. The role of the audience may be described as attestive spectators[6] as opposed to active participants. Attestive spectators hardly qualify as witnesses in the way Shapin understands it, as they are not explicitly involved and accountable for the ceremony and the performance they attest to. In this respect, the verifier team is the only community that qualifies as a reliable witness. To what extent it is possible as well as acknowledged that spectators of different professional trainings may contribute to a debate is not clear. This is not so much meant as a criticism, but also as a way of exploring possible ways of making the event legible in broader terms. We believe that ordinary citizens may hardly choose to watch the online performance for entertainment, or even as a citizen duty, but perhaps engaged teachers might want to use the broadcasting in discussing democracy and technology for educational purposes. We do not know to what extent the event has had an impact for instance on politicians and their decision making, but obviously one can argue that the ceremony and the way it was presented makes it difficult for people outside of the community engaged in internet election to make sense of the performance.

J. Barrat i Esteve et al. raised the following concerns: "Internet voting was in its infancy when the Council of Europe Recommendations were written. We know now that e-enabled elections are far more complex than previously thought, not only technically, but also legally and from the procedural point of view. Yet, the recommendations say little on the legal basis, trying, on the contrary, to cover every possible situation in a technically neutral way" [3, p. 8]. The idea that internet voting can be understood in a technically neutral way, which we see as another way of putting that it is exclusively about counting and not accounting, as if counting votes efficiently without taking the dimensions and the quality of the witnessing into account was possible, brings with it major political consequences. One of them is that when Election Observation Bodies approve of election results, for instance on the basis of the Council of Europe's Recommendation on legal, operational and technical standards for e-voting, or on the basis of the Decryption and Counting Ceremony, they implicitly also approve of the radical changes in the way witnessing takes place, but without addressing this explicitly.

[6]We owe this expression to Ingvar Tjøstheim, personal communication.

As it is well known by now, the Norwegian government decided to stop the internet trials [18], based on the arguments that the parliament disagreed on the subject, and this subject was considered too important to allow for disagreement. Besides this, they stressed that ordinary voters do not understand the mechanisms involved in internet voting [18]. This is, of course, a perfectly legitimate way of expressing a political standpoint. We do not know whether the experiences of the politicians involved in the ceremony have had a say in this argument, but common experience as well as analyses such as the OSCE report [22] certainly support the idea that ordinary citizens do not usually understand this voting mode. These arguments are indeed important from a democratic point of view. But in addition, we would like to argue that an analysis of the economy of truth that takes the new conditions of witnessing into account would provide critics, as in this case the government, with additional arguments. These arguments would in turn point to some of the conditions internet voting depends on, by opening the back-box of how the counting, and hence the accounting, take place. It would eventually make the radical changes in the way democracy is understood more obvious in terms of public involvement. The point we want to make, based on the guidelines that Shapin's idea of trust and the economy of truth provide, is that it is possible to explore political and social aspects in the process as well as sketch what the IT community is doing, and what ordinary people arguably do not understand. The argument does not so much point to missing competences among the voters, but informs about the process and the kind of public involved in the internet voting experiment. Seeing is not necessarily believing, trust and distrust go hand in hand according to Shapin, and we may reject the idea of trusting people and arrangements, if we do not know how to relate to them. The argument also suggests proponents of internet voting to be explicit about the vision of democracy that they carry with them in terms of witnessing, among other things. Currently it seems that the idea of proxy is well accepted in the community of observers, as a logical consequence of the competences and complexities involved in internet elections and deciding about the efficiency in counting votes, but less discussed within a political context: Is this what people and their representatives in Norway or elsewhere want?

VI. Concluding Remarks

The Ministry of Local Government and Regional Development of Norway organized on election day a Decryption and Counting Ceremony in the internet voting trials of 2011 and 2013. Starting from the organizers' declared perception of the ceremony in 2013, as an effort to sustain trust in internet voting, we have introduced a pragmatic approach to trust, that underlines the inseparability of truth from the witnessing of how it is brought about. We have suggested that academic or political communities can also shape the economy of truth, including their systems of takings-for-granted in how they view the world. Based on this approach as well as a description of how the event is organized in terms of an overseeing body, the IEC, and a group of appointed verifiers, this paper has examined how the organizers made the event observable to the audience and emphasised the complexities in decrypting and counting votes as well as the specific framing of the event by the IT community.

We have also discussed the limits in trying to make sense

of the event exclusively from a technical counting perspective, and explored a broader understanding of truth-making and trust-making by including a discussion of the witnessing process and the idea of making it public. We have suggested that exploring a pragmatic approach to truth and trust may be helpful in the e-governance community, as well as in other communities engaged in the idea of trust in technology. More specifically, we believe that any government considering to adopt internet voting may benefit from taking on the job of articulating social and political perspectives on internet voting. This will bring two advantages. First, it will help with refining the requirements of the internet voting architecture, by creating a space for discussing how to improve the technical performance, by mechanisms other than zero-knowledge proofs, for example advanced logging infrastructures, time stamping, distribution, redundancy, and risk-limiting audits. Second, and just as importantly, it should articulate explicitly how witnessing is brought about, to what extent a public can take shape and how those processes transform the basis for representative democracy.

ACKNOWLEDGMENT

The authors were supported in part by the DemTech grant 10-092309 from the Danish Council for Strategic Research, Program Commission on Strategic Growth Technologies. The authors would also like to thank the anonymous reviewers for their helpful comments and suggestions.

REFERENCES

[1] R.M. Alvarez, T.E. Hall, A.H. Trechsel. *Internet Voting in Comparative Perspective: The Case of Estonia*. Political Science and Politics, 42, pp. 497–505, 2009.

[2] J. Barrat i Esteve, B. Goldsmith, N. Turner. *International Experience with e-voting: Norwegian E-Vote Project*. IFES, June 2012.

[3] J. Barrat i Esteve, B. Goldsmith. *Compliance with International Standards: Norwegian E-Vote Project*. Washington, DC: IFES, 2012.

[4] C. Barry, I. Brightwell, L. Franklin. *iVote, Technology Assisted Voting*. Electoral Commission of New South Wales, November 2013.

[5] P.V.D. Besselaar, A. Oostveen, F.D. Cindio, D. Ferrazzi. *Experiments with E-Voting Technology: Experiences and Lessons*. Building the Knowledge Economy: Issues, Applications, Case Studies, IOS Press, 2003.

[6] C. Bull. *Safety first! Verifiability in the Norwegian e-voting System*. Seminar on Internet Voting, Norway, September 8, 2013.

[7] Expert Study Mission Report, *Internet Voting Pilot: Norway's 2013 Parliamentary Elections*. The Carter Center, March 19, 2014.

[8] The Electoral Knowledge Network. *Elections and Technology, Guiding principles*. aceproject.org/main/english/et/et20.htm (accessed 4 August 2014)

[9] T. ElGamal. *A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*. IEEE Trans. on Inf. Th., 31 (4), pp. 469–472, 1985.

[10] Estonian Internet Voting Committee, videos (in Estonian). www.youtube.com/channel/UCTv2y5BPOo-ZSVdTg0CDIbQ/videos (accessed 4 August 2014)

[11] K. Gjøsteen. *The Norwegian Internet Voting Protocol*. IACR Cryptology ePrint Archive 2013, 473.

[12] J.A. Halderman, H. Hursti, J. Kitcat, M. MacAlpine, T. Finkenauer, D. Springall. *Security Analysis of the Estonian Internet Voting System*. Technical report, May 2014. estoniaevoting.org/wp-content/uploads/2014/05/IVotingReport.pdf (accessed 4 August 2014)

[13] W. James. *Pragmatism*. Buffalo, N.Y., Prometheus Books, pp. 88–91, (1907) 1991.

[14] Kommunal og Regionaldepartamentet. *Regulations Relating to Trial Internet Voting During Advance Voting and Use of Electronic Electoral Rolls at Polling Stations on Election Day During the 2013 Parliamentary Election in Selected Municipalities*. June 19, 2013.

[15] D. MacKenzie. *Mechanizing Proof: Computing, Risk, and Trust*, MIT Press, 2001.

[16] Ministry of Local Government and Regional Development. *Internettvalstyret er oppnemnd*. Press release. June 20, 2013. (in Norwegian) www.regjeringen.no/en/archive/Stoltenbergs-2nd-Government/Ministry-of-Local-Government-and-Regiona/Nyheter-og-pressemeldinger/pressemeldinger/2013/internettvalstyret-er-oppnemnd-.html?id=731211 (accessed 26 May 2014)

[17] Ministry of Local Government and Regional Development. *Decryption and counting ceremony of the Internet votes, video.* (English language). www.regjeringen.no/en/dep/krd/Whats-new/news/2013/dekryptering--og-opptelling-av-internett.html?id=735379 (accessed 26 May 2014).

[18] Ministry of Local Government and Regional Development. *Ikke flere forsøk med stemmegivning over Internett*. Press release. June 23, 2014. (in Norwegian) www.regjeringen.no/nb/dep/kmd/pressesenter/pressemeldinger/2014/Ikke-flere-forsok-med-stemmegivning-over-Internett-.html?id=764300 (accessed 4 August 2014)

[19] News about the Norwegian e-voting trial in 2011 (in Norwegian). www.regjeringen.no/nb/dep/kmd/prosjekter/e-valg-2011-prosjektet/nyttomevalg/nytt-om-e-valg/2011.html?id=631622 (accessed 27 May 2014).

[20] OECD's Better Life Index. oecdbetterlifeindex.org/countries/norway (accessed 31 July 2014)

[21] OSCE/ODIHR, *Estonia: Parliamentary Elections 6 March 2011*. Election Assessment Mission Report. May 16, 2011.

[22] OSCE/ODIHR, *Norway: Parliamentary Elections 9 September 2013*. Election Assessment Mission Final Report. December 16, 2013.

[23] S.B. Segaard, H. Baldersheim, J. Saglie. *E-valg i et demokratisk perspektiv* Rapport (2012:005) Institutt for samfunnsforskning, Oslo, 2012.

[24] S.B. Segaard, D.A. Christensen, B. Folkestad, J. Saglie. *Internettvalg, hva gjør og mener velgerne?*, Rapport 2014:07, Institutt for samfunnforskning, Oslo, 2014.

[25] A. Shamir. *How to share a secret*. Communications of ACM 22, November 11, pp. 612–613, 1979.

[26] S. Shapin. *The Social History of Truth. Civility and Science in Seventeenth-Century England*. The University of Chicago Press, USA, 1994.

[27] J. Simon. *Trust*. Oxford Bibliographies in Philosophy, Oxford University Press, New York, 2013. www.oxfordbibliographies.com/view/document/obo-9780195396577/obo-9780195396577-0157.xml (accessed 4 August 2014)

[28] O. Spycher, M. Volkamer, R. Koenig. *Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting*. VoteID'11, Tallin, Estonia, 2011.

[29] I.G. Stenerud, C. Bull. *When Reality Comes Knocking: Norwegian Experiences with Verifiable Electronic Voting*. Proceedings of EVOTE2012, LNI GI Series, Bonn.

[30] A.L. Strauss. *Continual Permutations of Action*. New York, Aldine de Gruyter, 1993.

[31] M. Volkamer, O. Spycher, E. Dubuis. *Measures to Establish Trust in Internet Voting*. ICEGOV'11, Tallin, Estonia, 2011.

[32] K. Vollan. *Final Verification Report from the Voting Card Printing and the Secure Handling of Cryptographic Keys*, Version 0.1 DRAFT. The Internet Voting Board Representative: Internet Voting Trial 2013, August 26, 2013.

[33] M. E. Warren. *Democracy and Trust*, Cambridge University Press, 1999.