Stéphane Frénot, Stéphane Grumbach, Damien Reimert (2014):
E-Voting, the Case for Decentralised Systems.
In Olav W Bertelsen, Susanne Bødker, Fiorella de Cindio, Volkmar Pipek (Eds.), International Reports on Socio-Informatics (IRSI),
Proceedings of the COOP 2014 Workshop on Collaborative Technologies in Democratic Processes
(Vol. 11, Iss. 1, pp. 82-84)

E-Voting, the Case for Decentralised Systems[1]

Stéphane Frénot, Stéphane Grumbach, Damien Reimert
INRIA
firstname.lastnam@inria.fr

Abstract. Despite serious concerns about their robustness, e-voting systems have started to be adopted by some countries to support political elections. These systems essentially offer electronic solutions to support existing election paradigms. Social media though radically change the ways citizens can interact with political powers, by allowing in particular a more continuous form of participation. New possibilities permitted by digital technologies should be investigated, to extend these interactions and support new election capacities beyond legacy protocols. Two principles seem of uttermost importance to us. First, the {\it freedom of election}, that is the capacity not only to participate to an election, but to launch an election and invite people to participate to it. Second, the {\it control of election}, that is the capacity for the people to control the election process and the computation of its tally. We claim that to satisfy these two principles, decentralised protocols, with no trusted third party control, are of great help, if not necessary.

E-voting systems have been adopted in various countries. Cryptographic means are used to ensure some reasonable level of confidence. Nevertheless, most protocols have been shown to be vulnerable to attacks, thus impeding their widespread adoption. We propose a radically different approach. While elections are traditionally based on a central authority, collecting the votes and computing the tally, we propose to use decentralised protocols, leaving control and tally to the voters themselves.

[1] Work supported by INRIA ADT Brow2brow as well as ANR C3PO projects.

We claim that decentralised protocols might allow to improve classical properties by not relying only on cryptography to guarantee them. More importantly, they can ensure new properties and support new forms of elections. Liquid Feedback offers the possibility to freely organise elections, by using its open source software. Nevertheless the control stays in the hand of the organisers around centralised structures.

The fundamental property we want to ensure, that is the basis of the two principles we propose, is the property of *no concentration of knowledge*, which can be stated as follows:

> *The amount of data accumulated by each participant during an election, that includes ballot casting and computation of tally is logarithmic in the number of eligible voters.*

The amount of data participants are able to accumulate is an indication of the level of control they have over the process. Decentralising the control, means distributing the data evenly between participants.

Such principles have demonstrated their efficiency. For popular decentralised protocols, the control is not ensured by a trusted third party, but by the participants themselves. It is the case for BitTorrent, used by hundreds of million of users for file sharing, as well as for Bitcoin, used for electronic currency. The confidence in these systems, of particular importance for Bitcoin, relies on a *trust by computation*.

Since in centralised systems, one authority concentrates all the knowledge of the election, it will always be a challenge to trust this authority, and ensure differential privacy for instance, and be confident that the ballots of voters cannot be recovered using additional data. If the control is shared by participants, and they can accumulate at most a *logarithmic amount* of encrypted data about the tally computation, trust is greatly increased, since leaks and corruption are severely restricted.

Moreover, in such decentralised systems, nobody can interrupt the election process without hijacking the network. The freedom to organise elections cannot be contested by force.

We have developed such a system for electronic voting, which relies on a decentralised protocol. The proposed system, BitBallot, which departs from legacy systems, does not require a central authority to control and certify the correction of the processes. Instead, BitBallot, strongly inspired by decentralised

systems such as BitTorrent or Bitcoin, performs complex tasks in a fully decentralised manner while ensuring rigorous properties. BitBallot relies on a peer to peer protocol allowing peers to carry in a cooperative fashion the voting process as well as the computation of the tally.

One of the main novelties of BitBallot is that voters *pull* the ballots of other voters, instead of *pushing* their own ballot into the system. We claim that this technique, which strongly differs from classical systems, greatly simplifies the protocol while ensuring desirable properties of privacy in a rather straightforward manner.

The system has been implemented at the browser level, and relies on open standards such as HTML5 and JavaScript, available on any smartphone, tablet or laptop. For the synchronisation of ballots handled by the participants, we developed a torrent, that allows a fully decentralised management of the election by the voters.

Our experiments on a simulation platform show very reasonable results, both for the amount of knowledge handled by peers, as for the convergence speed, which at this stage is linear in the number of voters. The system, accessible on smartphones, has been tested at this stage by students to grade their teachers.