Lucerne University of Applied Sciences and Arts

HOCHSCHULE LUZERN

Informatik

FH Zentralschweiz

Evaluation of the blockchain vote in the city of Zug

After receiving IDs issued from the city of Zug, 72 digital ID holders took part in a consultative vote from 25 June to 1 July 2018. By holding this test vote online, the blockchain-based proof of concept, eVote, was regarded as a novel yet practical voting approach that can be used in real life. This report presents the various benefits of using a decentralized voting solution, the underlying architecture of the system and feedback from citizens who participated in the vote.

Centralized or decentralized? That is the question

A decentralized voting system underpinned by blockchain has many advantages over traditional, centralized, paper-based systems.

Before going further, it is essential to understand the distinction between centralized and decentralized voting systems. The defining characteristic of a decentralized system is that there is no single entity taking control. A decentralized system also implies it is distributed, meaning that any information processed – whether via computing or data storage – is shared across multiple nodes. By this definition, traditional paper-based voting is considered to be centralized. It is also important to recognize that most other so-called eVoting mechanisms, whether through voting machines or online, are also centralized. Although they are distributed in a sense, the decisions are still made centrally.

A decentralized voting system brings the benefits of online voting with added benefits enabled by blockchain. For instance, there is no geographical restriction: votes can be cast anywhere through the internet, which can certainly boost turnout. Beyond that, we outline its major advantages below:

Security

The primary advantage of a decentralized voting system is security. The data's authenticity is guaranteed throughout the poll.

Firstly, with effective identity management, it is infeasible for hackers to impersonate voters. Secondly, techniques like digital signatures protect the integrity of the data, meaning votes cannot be tampered with in transit. Thirdly, the blockchain is immutable – once a vote has been recorded, it cannot be removed or altered.

As the data is stored across multiple nodes, even if one or several nodes are hacked, the voting data cannot be destroyed by hackers. As long as there are enough nodes, it is almost impossible for the whole system to be compromised.

Stability

As mentioned above, data can be distributed across a decentralized system. Tasks can also be redistributed from overloaded nodes to idle nodes, balancing the system. Because of this, not even a single-node fault can cause a system outage, resulting in a better user experience since voters can always get a timely response.

Trust

In a decentralized voting system, a set of entities validate the votes, and every entity must agree how a vote has been cast before recording it. A validator may not only be the organizer of the poll, a government for example, but it could also be various accredited institutions: these can range from the UN, to particular political parties, and even to local councils. Such a process ensures that even a corrupt government cannot forge the votes. In other words, the decentralized system protects against internal falsification.

Reassurance
When using paper ballots, voters have limited information about their vote. They are often untraceable once placed into the box or sent by mail — voters do not truly know whether their vote has been counted. However, in a decentralized voting system, once all votes are validated and recorded, voters can opt in to receive a notification that confirms their vote has been documented.

Transparency
A centralized system is usually closed-source to prevent the leak of security breaches making it a black box for the end users. In contrast, a decentralized voting application can be open-sourced to allow any person or institution to audit its functions, which increases transparency. In addition, open-source software encourages peer reviews, meaning more developers can contribute to continually improve the system, which further improves its security.

The verifiable electronic voting system

eVote is the next-generation voting solution that, due to its blockchain nature, makes voting instantaneous, anonymous, secure, transparent, auditable and immutable.

eVote allows local and federal authorities to:

- Set up and inform participants about a new poll, processing the results within minutes
- Save time and money on operational costs
- Engage more people via an instant and secure way to vote, regardless of the voter's location
- Significantly improve trust in voting systems since blockchain is fundamentally immutable

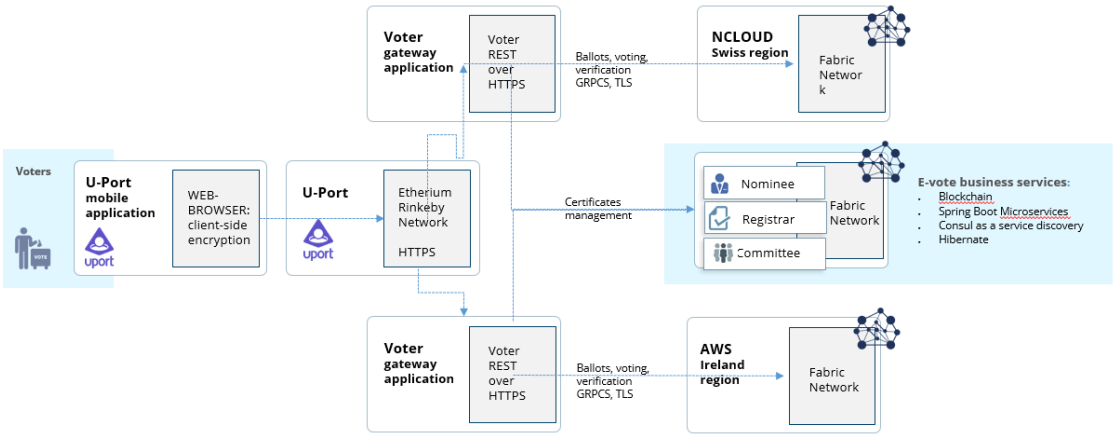
eVote enhances the voting process with the following features:

- As an anonymized process, this solution does not reveal any personal information from voters and keeps their votes private
- Voters can view and change their own votes at any time during the poll
- While anonymous, the legitimacy of the participants is still validated by an external identity system, with every user having the power to verify every vote
- Due to being securely encrypted, all voting data is tamperproof

eVote brings together the following technology:

- Homomorphic encryption – a cryptosystem that allows users to calculate encrypted data as if it were unencrypted, without seeing or disclosing this data. E.g. users can add encoded numbers together without decoding them. eVote uses Paillier for homomorphic encryption.
- Digital signature – a mathematical proof that confirms the signer has submitted data to the system and cannot deny having submitted it. The signature guarantees the data was not altered in transit through the blockchain system.
- Client-side encryption – the voters' private keys are isolated directly on their own PCs, where they are used for private data encryption.
- Zero-knowledge proofs – are a method where one party can prove to another party that a given statement is true, without conveying any information apart from the fact that the statement is indeed true.

How does the eVote solution work? Easily.



Voting Process Definitions:

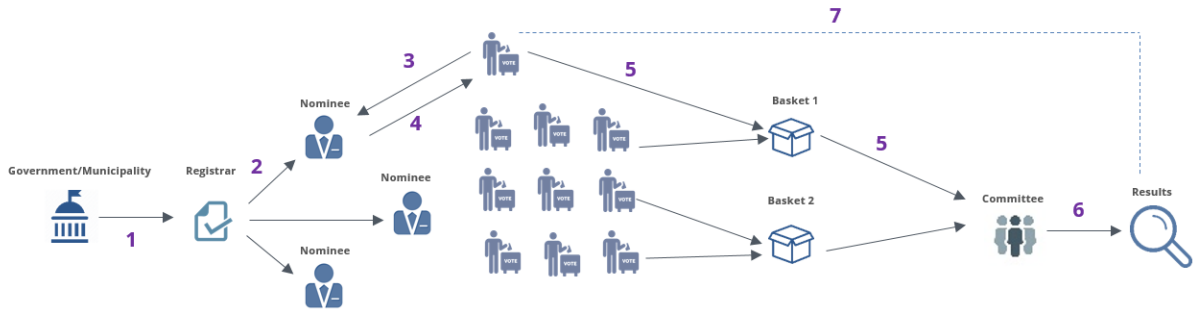
Roles:

- **Registrar** is an authority who initiates and manages a voting poll
- **Nominee** is an authority who verifies and confirms the voters' eligibility to vote (by recognizing voters by their digital ID) and provides voters their ballots
- **Voter** is a person who holds a digital ID and votes
- **Voting Committee** is an authority who counts, verifies and submits the voting results

Terms:

- **Poll** is a group of questions included during a particular round of voting
- **Ballot** is a unique collection of answers for each voter, e.g. for an individual poll
- **Baskets** are decentralized and immutable data storage containers where voters submit their ballots.

What does the voting process look like?



Pre-vote
Before voting begins, every voter obtains a confirmed U-Port digital ID from the authorities.

Step 1
The government or municipality initiates a new round of voting, sending all necessary information about what will be voted on to the appointed registrar.

Step 2
The registrar creates a new poll (with a list of questions and choices, when that vote opens and closes, etc.) on the blockchain and assigns the voting executors, nominees and committee.

Step 3
A voter can then log in to a dedicated voting portal[1] to generate a unique set of keys: one private, and one public[2]. The private key is kept in the user's private wallet, whereas the public key is sent to a nominee alongside a request for a new ballot.

By having a public key, a voter can prove their identity on the blockchain and that their answers are associated with their identity without actually disclosing their answers or identity. And by having a private key, a voter can sign their ballot and prove it belongs to their ID.

Step 4
A nominee authenticates the voter using the U-Port digital ID, issuing them an individual ballot.

Step 5
The voters vote, with their answers encrypted through the committee's public key. This key is included in each poll and based on the Pailler encryption system. The voter signs their ballot using their individual private key and adds it to the blockchain. The votes are then aggregated into decentralized baskets and replicated between network nodes on the blockchain.

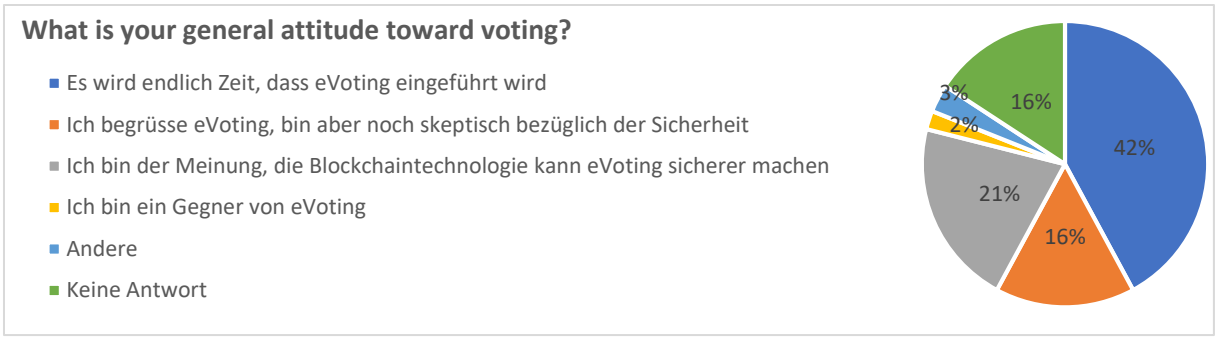
Step 6
Once voting closes, the committee retrieves all anonymized and encrypted ballots from the blockchain, checks their authenticity by verifying all signatures (and a number of cryptographic proofs), then finally calculates the results. After, the committee submits the results to the blockchain along with a generated zero-knowledge proof equivalent to the encrypted sum of votes and decrypted results.

Step 7
Any participant on the blockchain can verify the results by applying a mathematical proof and a committee's public key to a sum of encrypted voting results. A voter can also verify that their own ballot was counted by using their public key. Thus, no one can decrypt individual submissions from other voters, but everyone can rest assured the results were not and cannot be corrupted.

Findings of the online survey by the City of Zug

Subsequently, the City of Zug conducted an online survey of 95 city residents with digital IDs to capture feedback from the community. The findings of the survey are the following: More than three quarters of those surveyed welcome the introduction of eVoting into their voting system and 21% believe blockchain technology can make electronic voting more secure. Only 2% opposed to the introduction of eVoting. Despite a generally high level of approval, some are still sceptical about the security of eVoting. In addition to this, many survey participants believe the Zug population should still have the option to vote by mail in addition to eVoting. More than three quarters of voters already had a digital ID. This means that around 25% of the participants acquired a digital ID for the test vote.

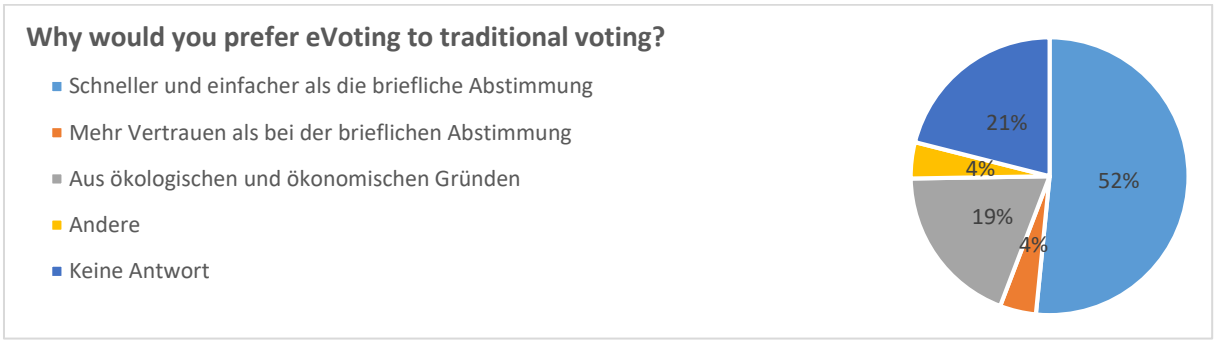
[1] If a voter does not trust any available parties, they can run a private blockchain node by request.
[2] A voter's public key is registered on the blockchain by the nominee during authorization. The nominee anonymizes every voter during this process.



Translation of above:

- "I am glad we are making eVoting an option!"
- "I welcome eVoting, but I am skeptical about its security."
- "In my opinion, blockchain technology can make eVoting more secure."
- "I am against eVoting."
- Other
- No Answer

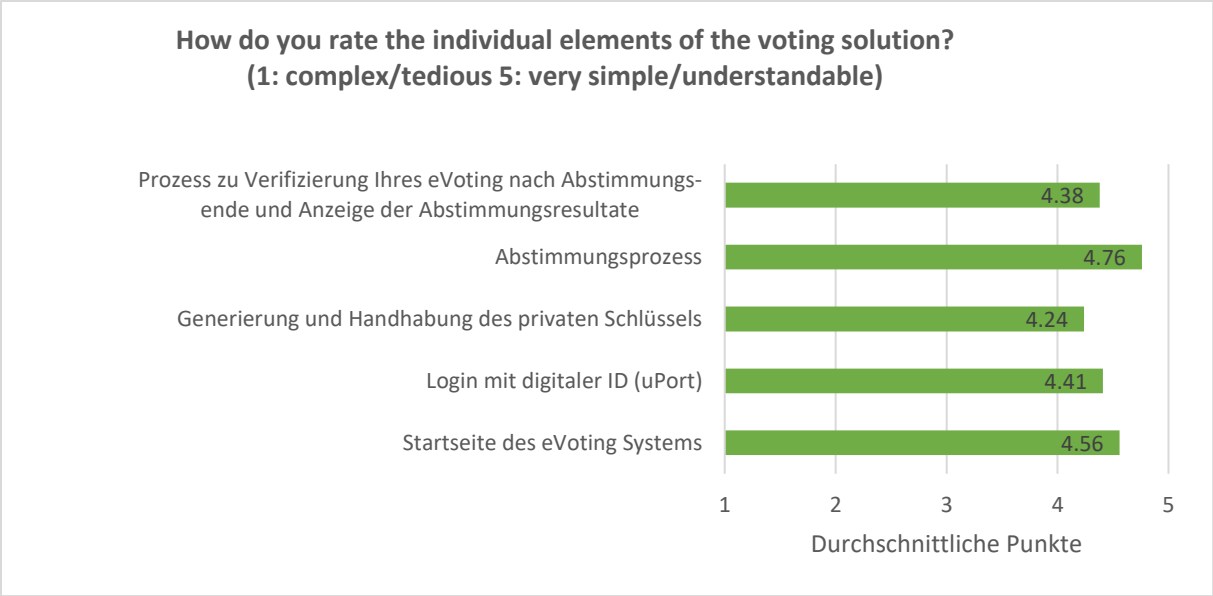
Then, participants explained why they prefer eVoting to traditional voting. 52% said the main reason why eVoting should be introduced was to make voting easier and quicker than filling out a ballot. Ecological and economic arguments were also mentioned.



Translation of above:

- Faster and simpler than voting by mail
- More trustworthy than voting by mail
- Environmental and economic reasons
- Other
- No Answer

Although most participants were very satisfied with how the test vote went, the survey showed that a number of factors can be improved to ensure a smoother voting process. Some voters faced technical problems with their digital ID, which made it impossible for them to vote. The individual elements of the voting solution were rated very positively by the participants. Participants thought the voting process was simple and easy to understand, with the solution's start page remarkably appealing. Nevertheless, the way private keys were handled along with how the steps were explained to the participants could be improved.



Translation of above:

- Process to verify a vote has been cast and how to view the results of the poll
- The overall voting process
- Generation and use of private keys
- Log in with digital IDs
- eVoting system start page

Finally, participants actively used the space for comments at the end of the survey. Many said that the media did not report enough on the voting process, meaning there was a lack of awareness that negatively affected turnout. Some did not know about the blockchain-based vote or only heard last minute. Some reported that they only found out about the voting trial after it had taken place. Unfortunately, for technical reasons, it is not possible to notify digital ID owners via the uPort app that there is an imminent vote. While the uPort app runs other platforms worldwide, the City of Zug did not develop its own app for the test vote due to a lack of funding.

The ability to use digital IDs in the city of Zug was introduced on 15 November 2017, and is still in a pilot phase. In addition to the eVoting solution, there are various other applications in evaluation or already in operation as pilot projects for the use of the digital ID, including sharing city bicycles via an app. Borrowing books from the library will follow next.

Conclusion and Outlook

This proof of concept was a success and is a significant milestone that demonstrates blockchain-based evoting systems work. Nearly all technical expectations of the vote were met. We were able to gather valuable insights to make improvements for future polls. To make the evoting system dependable and secure, tests like these are essential in order to build a working, reliable solution. A link to the code will be made publicly available on various sources, such as the city of Zug website, Hochschule Luzern's Blockchain Lab website and Luxoft.com. All project partners will continue to contribute towards further improving the solution, finding further use cases and sharing new findings with the community.

Zug, 30 November 2018