# Democratic online referendums with opn.vote

Joerg Mitzlaff [1]

[1] openPetition gGmbH, Am Friedrichshain 34, 10407 Berlin, Germany

**Abstract.** opn.vote, a protocol for democratic referendums via the internet, is presented. First, the requirements for democratic online referendums are presented and discussed. Subsequently, existing approaches are presented and evaluated. opn.vote uses an identity-based blind signature scheme. It is shown that privacy is ensured without having to trust a central authority. The verifiability of the referendum is guaranteed, as massive manipulation of the vote can be detected. The outlook shows how manipulation can be detected even in individual cases.

**Keywords:** Internet-voting system, E-voting, Online-voting, Blind signature, End-to-end verifiable, Democracy.

## 1. Referendums versus election

In elections, voters can choose between persons and between parties, which are then to represent the interests of the voter in parliament until the next election. In referendums, participants can choose directly between bills on one or more issues, which must then be implemented in a binding way by parliament. The protocols and principles governing democratic referendums and elections do not differ. In this sense, the terms referendum and election are used synonymously here. Germany does not have referendums on the federal level yet.

## 2. Requirements for democratic elections

The violation of basic democratic election principles must be penalized by governing entities. Otherwise they would have no meaning. In order for a possible fraud to be made public there needs to be an independent press interested in the publication of electoral fraud.

### 2.1. Entitlement

Every person entitled to vote must be allowed to vote. Those not entitled to vote must be excluded from voting. No person of electoral age belonging to the electoral area shall be excluded from voting. The exact criteria for eligibility to vote is defined by the organizers of the election.

### 2.2. Accessible

In the interest of a high democratic legitimacy of the election result through a high voter turnout, the electoral process should be made as simple as possible and reflect what people are used to nowadays.

### 2.3. Equal

Each voter has one electoral vote. Each voter's vote counts equally in determining the overall result. The voter has the right not to cast his or her vote. The voter has the right to cast an invalid vote.

### 2.4. Privacy

Every voter has the right to a non-public ballot in which the privacy of the ballot is preserved indefinitely.

### 2.5. Immutable

Votes cast are immutable and cannot be deleted. The addition of additional votes without entitlement to vote must be prevented. In particular, the addition of votes not cast by eligible voters must be excluded.

### 2.6. Verifiable

Every voter has the right to verify compliance with all prior requirements. The verification must be possible and comprehensible with reasonable effort and without expert knowledge. A possible violation of the basic democratic election principles must be recognisable and provable.

**Proof of entitlement:** Currently, the state has exclusive control over the citizens register and electoral roll. Each citizen should be able to check the electoral roll if there are reasons for suspecting inaccuracies.

**Proof of privacy:** The voting procedure must ensure the separation of persons and ballot paper. For on-site elections, voting booths must be set up and they must be used by everyone. For elections outside the polling station, the person voting must affirm on oath that he or she has personally signed the ballot paper. Electoral districts must not be too small so that enough ballot papers in the ballot box make personal allocation impossible.

**Proof of integrity:** Election observers must ensure that ballots are not invalidated or made valid during the ballots count. The election committee and election observers must ensure that each voter is checked against the electoral roll and that everyone votes only once. The electoral board and election observers must ensure that ballot boxes are empty before they are sealed, that ballot boxes are permanently supervised or correctly sealed until they are counted, that only registered ballot boxes are counted, that each ballot paper is counted correctly, that the count results from each electoral district are passed on correctly and that the sum of the results is correct.

### 2.7. Unaffected

In Germany, interim election results on election day, e.g. by questioning when leaving the polling station, may not be published. Voters should not be influenced by the decisions of other voters. In Germany it is not prohibited to publish one's own vote.

### 2.8. Free

Influencing the election by bribery, coercion, force or blackmail must be prohibited by law and penalized.

## 3. Requirements for online voting

From a user perspective, online voting must be as easy and secure as online shopping or online banking.

### 3.1. Ownership of devices

Online voting requires control over one's own devices and operating systems. No applications may be forcibly installed on a device without the possibility of uninstalling them, whether by an authoritarian state or a company. Participants in an online election need media literacy to be able to say with a high degree of confidence that their network connection and device are not controlled by malware. Remote access by secret services must not be allowed. Operating systems must be able to allow root rights. Websites and smartphone apps must give a clear understanding of which election steps are controlled by their own device and which steps run on the remote election platform.

### 3.2. Anonymous internet

Participants in an online election must be able to disguise their communication with the election platform through services such as public internet access points, VPN, Tor or proxy servers. The election platform must not be allowed to request real person information with the help of the internet provider, given the IP address.

### 3.3. Usability

The basic democratic election principle of accessibility must make it as easy as possible for people to participate in an online election. All common devices (laptop, tablet, smartphone), operating systems (Windows, macOS, Linux) and browsers (Chrome, Firefox, Safari, Edge) must be supported. Interfaces must be easy to navigate by guiding to the most likely next possible steps, especially in the event of an error. They must be easy to read in a simple language and self-explaining. The election process should be interrupted as little as possible. The election process should involve as few media breaks as possible and should require only one device.

### 3.4. Interruption resistant

It must be possible to interrupt the voting process at any time without losing the right to vote or the vote cast.

### 3.5. Free of charge

According to the democratic election principle of accessibility, people without financial means must not be excluded from voting. The costs of organizing and running an election are taken care of by the community through donations or taxes. The democratic election principle of verifiability requires a sufficient number of participants to invest personal time in order to be able to ensure the correctness of the election.

### 3.6. Scalability

Resource consumption does not increase more than linearly per participant on the election platform. The financial costs per participant decrease towards zero as the number of participants increases.

### 3.7. Open source

With the publication of the source code of the election software, independent third parties must be able to verify whether the election protocol has been implemented correctly. Election software requires extensive intrusion testing and testing results must be published.

## 4. Expectations of democratic online elections

There is no internet voting protocol that can meet all the democratic election principles equally. Since the technical possibilities evolve, the debate about the best possible voting protocol should go on continuously.

### 4.1. Comfort versus control

If the effort to verify the election is too high, the democratic election principle of accessibility is violated. Depending on how much the participants trust the organizers of the election or the election platform, the need for control rises or falls. Participants want to be able to decide for themselves how much convenience and how much control they want.

### 4.2. Online versus offline

The last federal election in Germany in 2021 had a postal vote share of 47.3%. Constitutional lawyers see a need for regulation if the proportion of postal votes rises above 50%. Online votes would have to be constitutionally legitimized in the same way as a postal vote.

### 4.3. Single abuse versus mass abuse

No existing electoral protocol, online or offline, can prevent a violation of democratic election principles in individual cases. It must be ensured that mass abuse can always be detected and proven with reasonable effort.

### 4.4. Penalizing versus guarantee

In a highly democratic society an election protocol does not have to be able to guarantee all democratic principles directly if the violation of a principle can also be prevented by legal means. The less the rule of law is guaranteed in a system, the more important it becomes to guarantee the democratic election principles in the election protocol.

## 5. Expectations of an election protocol

In 2009, the Federal Constitutional Court banned the use of voting computers in Germany based on the requirement that "all essential steps of the election must be publicly verifiable".

Without any prior knowledge, it must be comprehensible why a vote remains private. No other person or institution has to be trusted to ensure that a vote and the voter stays disconnected. Online voting must be as secure as voting in a polling booth. Here, the voter has full control that his or her vote remains secret.

Without any prior knowledge, it must be possible to check the validity of his or her own vote within a few *minutes*. With a good mathematical understanding, the voting protocol and its principles must be understood within a few *hours*. At the level of a computer science student in the 3rd semester, the implementation of the protocol must be comprehensible on the basis of a scientific paper and the open source code within a few *days* and its correctness must be able to be confirmed.

There are about 1 million IT professionals in Germany. If only a small proportion of them is actually proving the validity of the implementation, the democratic election principle of verifiability is given. If it takes distinguished expert knowledge to understand a voting protocol, the democratic election principle of verifiability is not given.

Certifications in themselves are no guarantee for a democratic election protocol if the criteria according to which they are certified are not strict enough or are simply the wrong criteria. The criteria according to which certification bodies issue security certificates and the depth of testing must be open to the public.

## 6. Existing internet-voting systems

The German Federal Office for Information Security defined "security requirements for online voting products" in 2008. A new version is expected by the end of 2022. A Technical Guideline "IT Security Requirements for Conducting an Electronic Election" is expected in the third quarter of 2022. The European Council recommended standards for online elections in 2017. The German parliament held a public expert discussion on "E-voting - alternative forms of voting and their security" on 6 April 2022.

### 6.1. Zero knowledge proof systems

Existing commercial applications are essentially based on complex zero knowledge proof schemes. In these cryptographic protocols, the system knows who has cast the vote, but the ballot paper itself is encrypted. The encrypted ballot papers are now mixed over several stages and re-encrypted with different keys each time until it is no longer possible to trace who a ballot paper came from. (Mix network). The complex Zero Knowledge Proof procedure can be used to prove that there was "no cheating" on the way. The mathematical theory and the concrete software implementation are so complex that only few experts can understand or disprove the functioning of the system. The verifiability of the system is possible in theory but the cost of a full verification of an implementation is immeasurable. A German provider of an Internet-voting system based on zero knowledge proof is the company Polyas. To the knowledge of the author neither the source code nor public intrusion test results are available. Keys for decryption and re-encryption are stored on a central server. This means that an administrator of the system can decrypt the ballot paper after all anyway. Internationally known is the Spanish company Scytl, which did not pass the intrusion test of its implementation in Switzerland in 2019.

### 6.2. Blockchain and smart contracts

Decentralized systems, as they are being discussed in scientific research with blockchains and smart contracts, are still too complex to use and too expensive in terms of transaction costs. In order to maintain decentralization, participants must acquire a wallet of a cryptocurrency and invest in digital currency in order to participate in a vote. A current implementation of the blockchain voting protocol is snapshot. Since the blockchain is based on proof-of-stake it fails the democratic election principle of equality.

## 7. opn.vote

opn.vote will be developed as a free product of openPetition gGmbH for democratic online referendums. The idea for the product arose from supporting a self-organized nationwide referendum in 2021. Online voting will help to significantly reduce the costs of paper, printing, postage and return postage and the high time and personnel costs of opening, sorting and counting the votes received in future self-organized referendums.

Besides the support of referendums, democratic election principles can be applied in the same way to signing online petitions, “Volksinitiativen” and “Volksbegehren”. Here, too, approval quotas for a certain cause must be verifiable, ideally while preserving the privacy of the signatories. Online signatures for “Volksinitiativen” are already possible in Schleswig-Holstein today.

### 7.1. opn.vote guarantee

Democratic online referendums can be organized easily. It is practicable to use with deliberate restrictions and offers added value to our participatory democracy. Access to the referendum is guaranteed for all entitled persons, double voting is prevented. A secret ballot can be guaranteed. Verification of one's own vote and the sum of all votes is guaranteed. A

verification of the voting protocol is feasible for a large audience. The voting software is low-threshold, interruption-resistant, free of charge, scalable and will be made public as open source code.

### 7.2. opn.vote limitations

The participant is assumed to have malware-free hardware and software. It is assumed that this requirement is met for most participants. A guaranteed secret ballot requires a less user-friendly interruption of the voting process or IP address obfuscation between voting steps. Voting can be sabotaged if the voting platform itself is compromised. Compromising the voting platform cannot be prevented, but it can be detected by checking one's own ballot and the overall result. The publication of an intermediate referendum result during the voting period cannot be ruled out if the organizers sabotage their own referendum or the voting platform has been compromised. The uncoerced casting of an online vote cannot be guaranteed. The organizers of the referendum must be trusted on a case-by-case basis not to invent votes or to cast votes themselves that have not been cast. Mass abuse of the organizers can be ruled out by subsequent audit of the participants list by statistical sample analyses of random participants. The outlook shows ways in which the restrictions mentioned here can be further reduced.

### 7.3. opn.vote protocol

The opn.vote protocol uses an identity based blind signature scheme. The voting platform does not know who has cast the vote, so the ballot paper does not have to be encrypted when casting the vote at the online ballot box. A blind signature generated by the referendum register ensures that only registered participants can take part in the referendum. The protocol used here does not apply the blind signature to the ballot paper itself, but to the voting entitlement [1]. This makes it possible to separate registration and voting, and it is no longer possible to trace the participant, even in the case of collaboration between the register and the ballot box.

The flow chart in the appendix gives an overview of the communication between the actors involved.

**Voting request:** The voting request is an application for voting entitlement to the organizers of the referendum. The organizers manage the register of all participants in a referendum. The application contains a randomly generated string of characters (token) that the applicant creates for himself and that only he knows personally. The application is sent to the registry in an encrypted form, like a sealed envelope with the application paper, so that the application cannot be viewed by the registry. Technically, the application is encrypted with a cryptographic key pair, which was also previously generated by the applicant. Before the application is sent, the token and key pair must be stored by the applicant. This is the only way to ensure that a voting entitlement that is lost later can be reapplied for. In addition to the application, the applicant must identify himself to the registry as authorized with his name and address. The registry identifies the applicant either with his or her electronic identity card or with a PIN confirmation letter sent to the applicant's postal address.

**Voting entitlement:** If the applicant is successfully identified, the register checks the eligibility to vote, typically citizenship, place of residence and minimum age. If the applicant has not previously submitted a voting application and checks were passed, the application is approved for participation. The register signs the application blindly, as if with an embossed stamp through the envelope onto the application paper, i.e. without having seen the application itself. Technically, this is the blind signature process. The applicant must now decrypt the still encrypted and now signed application, just like opening a sealed envelope. The application with the embossed stamp of the register entitles the applicant to participate in the vote. Technically, the cryptographic scheme of the blind signature ensures that the signature of the register is preserved when the signed application is decrypted. The person entitled to vote can save the entitlement to vote for a later vote or proceed with the vote immediately.

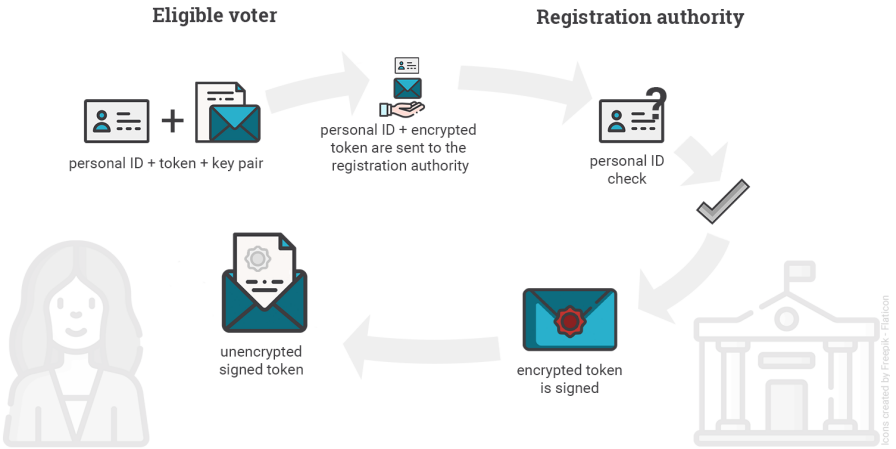



**Fig. 1.** Blind signature scheme for voting entitlement

**Voting:** Voting is possible during the voting period set by the organizers. Eligible voters log in to the referendum page of the online ballot box with their voting entitlement. The ballot box checks whether the signature of the register in the voting entitlement is valid and, if successful, returns a page with the ballot. The completed and signed ballot goes back to the online ballot box. The online ballot box stores voting entitlement together with the vote cast and sends a signed receipt back to the participant. The participant checks locally whether the receipt corresponds to his own vote cast immediately. A vote may be repeated several times. During the vote count, only the last vote cast per voting entitlement is counted. If vote cast receipts are repeatedly incorrect, the online ballot box is corrupted and the referendum must be stopped.

**Voting result:** After the end of the voting period, the register publishes an encrypted list of all participants for having the option of auditing the list of eligible voters. The ballot box publishes all cast ballots in plain text, with the voting entitlements of the participants. The referendum result is derived directly from the published votes.

**Verification:** After the publication of the referendum result, each participant can check his or her vote entitlement in the list of published votes, whether their vote was

counted correctly. The overall result can be determined and verified simply by adding up the published individual votes. Each voting entitlement should have a valid signature of the register.

**Why is privacy guaranteed even if the voting system is compromised?** The register knows the name and address of the participant. The register signs a voting request, but it cannot see it itself. In order to see the voting request, it would have to break the RSA cryptographic scheme of the blind signature, which is not possible with today's computers.

The ballot box sees the signed voting entitlement, which itself does not allow any conclusion about a person, as it only contains the voter's token, which has not been communicated to anyone else.

Even if the ballot box collaborates with the register, the register does not know to whom it should attribute the voter's token because it cannot have seen it.

Participants are notified if they use the same IP addresses for both the voting request and the voting with an explanation of how to anonymize or change their IP address. This makes it impossible for the system to correlate an online voting request to an online vote cast via the IP address.

The ballot box does not store any cookies and has no cross-site tracking built in, so that it is not possible to draw conclusions about the participant's identity through activities on both sites, register and ballot box after all.

Future quantum computers could break today's secure blind signatures. It is to be expected that quantum cryptographically secure digital signature schemes will replace current signature schemes to compensate for this danger.

**Why is the verifiability of the votes cast ensured even if the ballot box is compromised?** There is no incentive for an attacker to manipulate the votes cast in the voting system, as it is sufficient if only one of the participants can prove a discrepancy between the published vote and their own vote receipt and the election would thus be annulled.

Each participant can check his or her own vote. If enough participants check their vote, the statistical probability suggests that manipulation will be detected even in individual cases. The aim is to achieve a verification rate of at least 50%. A manipulation of at least 1% of the votes cast would then be statistically detectable in every 2nd election.

In order not to be able to sabotage the election by reporting a false fraud, the ballot paper has a valid signature of the participant and the voting receipt has a valid signature of the ballot box.

### 7.4. opn.vote field test

opn.vote is currently being developed at openPetition digital democracy lab in Berlin and will be used for the first time in early 2023 for the second Germany-wide self-organized online referendum of ABSTIMMUNG21 e.V.

Participants have the choice between an online vote and a paper based vote. A double vote by letter and online is made impossible. Before the voting documents are sent out, an address comparison is made with the registered participants for online voting. After the ballot papers have been sent out, participation remains only possible via online vote.

## 8. Outlook

Possible extensions of the opn.vote protocol are presented here to overcome the limitations of opn.vote mentioned before. Ensuring control over one's own device as well as IP address obfuscation are general challenges in the use of the internet and are not the focus of opn.vote.

### 8.1. Improve uncoercibility

It should be possible to override an online vote with an on-the-spot vote on election day [2]. This eliminates the incentive to force voters to cast their vote in a particular way. Overriding online votes at the polling station cannot be detected by the coercer afterwards.

### 8.2. Improve robustness

The possibility of sabotage of the entire referendum can be further reduced via decentralized online ballot boxes. Decentralized ballot boxes with decentralized casting and counting of votes minimize the risk of sabotage to one of these ballot boxes at a time. The register remembers at which ballot box a participant has voted. In case of sabotage, a repetition of the referendum has to be organized only for the fraudulent ballot box. A governing procedure is needed in order to provide independent ballot box services.

The risk of publishing an interim referendum result can be reduced if the private key needed to decrypt votes cast is shared among all ballot box operators.

### 8.3. Improve transparency

A repeated, incremental publication of the list of encrypted eligible voters and the list of encrypted cast ballots reduces the risk of subsequent manipulation of the lists. The InterPlanetary File System (IPFS) is suitable for this purpose as an audit-proof archive. Daily or hourly IPFS records are chained together like in a blockchain with the platform signature and a time stamp so that a subsequent manipulation of the lists can be detected.

A publication of votes cast even in real time would give the participant the additional security that his vote has been received unchanged. A further check of the vote after the vote would then be dispensable. This would increase the rate of proven votes and thus would reduce the possibility of fraud in the ballot box remaining undetected.

### 8.4. Improve trust

The dependence on the trustworthiness of the register can be reduced by distributed registration authorities. In order to receive a vote entitlement, the signatures of a minimum number of registration authorities are required [3]. The registration authority verifies the identity of the participant by means of an identification card and signs the participant's eligibility to vote. In order to eliminate collaboration between registration authorities, an external randomness generator determines by which registration authorities a participant needs to be verified. The random values must be published in a public bulletin board. A

governing procedure is needed in order to provide independent registration authority services.

### 8.5. Improve equality and entitlement

The dependence on a central state authority for issuing identification cards can be reduced by a decentralized identification procedure. This decentralized procedure can be a frequent event or in advance of an election or referendum. All eligible persons meet at a certain time and in a certain place to issue a unique voting authorisation to each other [4]. Since a person can only be at one place at a time, it is ensured that this person only receives one voting entitlement. It also ensures that this person is real and not a sock puppet. This assumes that all other social, economic and religious obligations at that particular time need to stand down temporarily. This gathering would give the opportunity to celebrate self empowerment, self-organized democratic elections and democracy as an achievement from all of us.

## 9. Conclusion

The question of whether or not online elections should take place via the internet has already been decided. The scientific research has been made and the technical solutions are built and they are already being actively used, be it for commercial interests or politically motivated. Sometimes they help autocratic states to manipulate an election even more easily. Sometimes they help democratic states to show themselves as technically advanced without being able to guarantee basic democratic election principles like voters privacy [5]. E-voting systems are being used in real elections without sufficient transparency, evaluation and public discourse.

It is up to all of us to make sure that collaborative online decision making on the internet becomes democratic online decision making. There needs to be a broad knowledge of when an internet-voting election result is democratically legitimate.

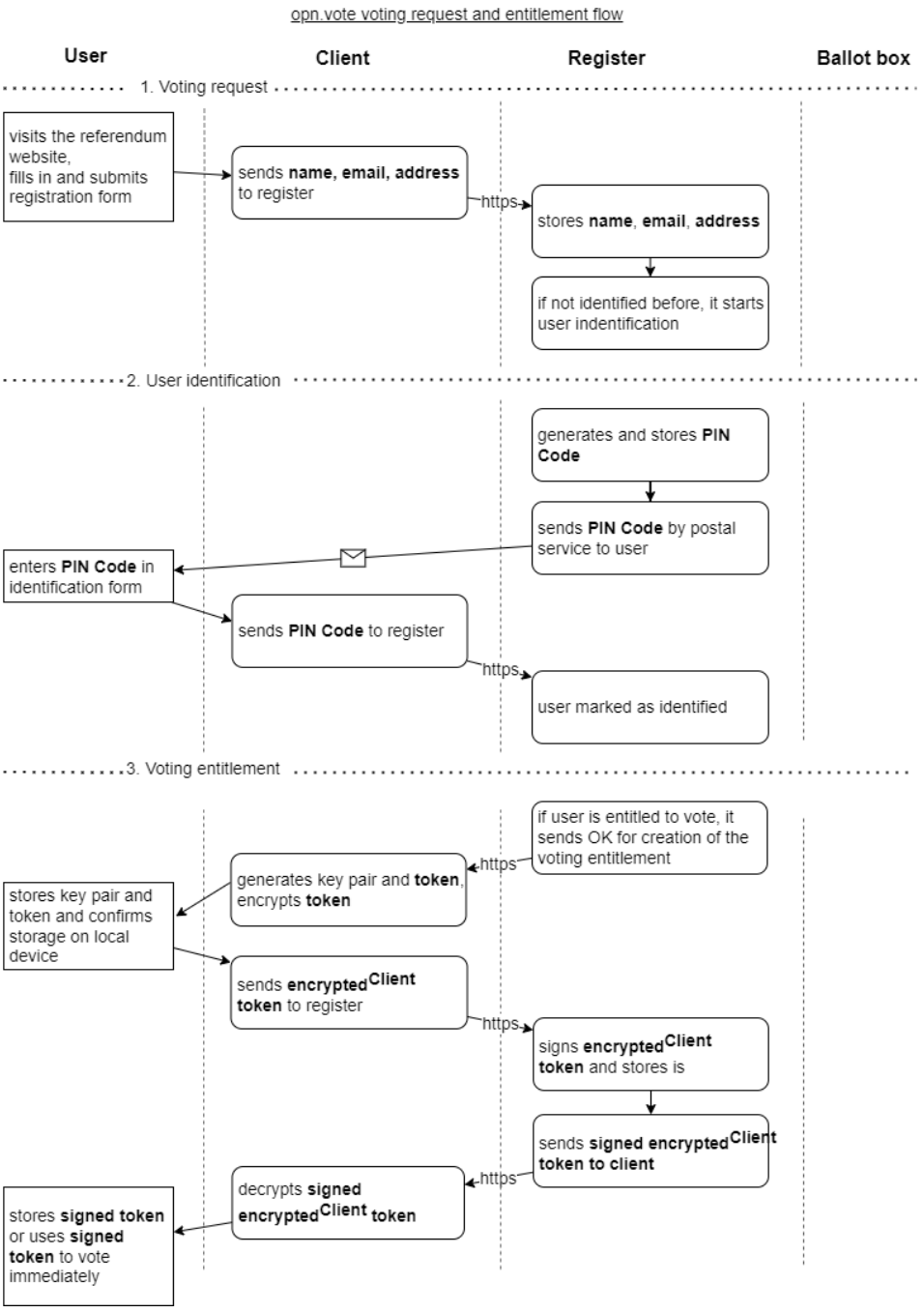
There will be no fully automatic, democratic online voting. It needs control of the process by the participating people themselves. Many people are still needed to govern and check online registration, online votes cast and online election results.

Technology can bring elections and referendums into the digital space, but it cannot replace election organizers and election observers.

## 10. References


1. O. &. D. A. Cetinkaya, „Pseudo-Voter Identity (PVID) Scheme for e-Voting Protocols,“ 2007. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4159926
2. R. K. R. F. S. &. D. E. Haenni, „TrustVote: A proposal for a hybrid e-voting system,“ 2009. [Online]. Available: https://www.researchgate.net/profile/Eric-Dubuis/publication/266046766_TrustVote_A_Proposal_for_a_Hybrid_E-Voting_System/links/573c306d08aea45ee841550d/TrustVote-A-Proposal-for-a-Hybrid-E-Voting-System.pdf
3. R. E. D. E. &. H. R. Koenig, „Why Public Registration Boards are Required in E-Voting,“ 2010. [Online]. Available: https://dl.gi.de/handle/20.500.12116/19497
4. B. Ford, „Identity and Personhood in Digital Democracy: Evaluating Inclusion, Equality, Security, and Privacy in Pseudonym Parties and Other Proofs of Personhood,“ 2020. [Online]. Available: https://arxiv.org/abs/2011.02412
5. D. &. M. T. Clarke, „E-voting in Estonia,“ 2016. [Online]. Available: https://arxiv.org/pdf/1606.08654

# 11. Appendix


opn.vote voting request and entitlement flow
User
Client
Register
Ballot box
1. Voting request
visits the referendum website, fills in and submits registration form
sends name, email, address to register
https
stores name, email, address
if not identified before, it starts user indentification
2. User identification
generates and stores PIN Code
sends PIN Code by postal service to user
enters PIN Code in identification form
sends PIN Code to register
https
user marked as identified
3. Voting entitlement
if user is entitled to vote, it sends OK for creation of the voting entitlement
https
generates key pair and token, encrypts token
stores key pair and token and confirms storage on local device
sends encrypted Client token to register
https
signs encrypted Client token and stores is
sends signed encrypted Client token to client
https
decrypts signed encrypted Client token
stores signed token or uses signed token to vote immediately

opn.vote voting and verification flow