ZIPAR *Discussion Paper Series*

Blockchain for the people
Blockchain technology as the basis for a secure and reliable e-voting system

Marko Kovic*[a]

[a]ZIPAR – Zurich Institute of Public Affairs Research

June 2017

*marko.kovic@zipar.org

ZIPAR

About ZIPAR

The Zurich Institute of Public Affairs Research (ZIPAR) is an independent, nonpartisan, nonprofit thinktank based in Zurich, Switzerland. ZIPAR is devoted to bringing perspectives and insights from social science into society at large, with a focus on the areas of democracy, technology, and rationality.

Recommended citation

Kovic, Marko (2017): *Blockchain for the people. Blockchain technology as the basis for a secure and reliable e-voting system.* ZIPAR Discussion Paper Series, Volume 1, Issue 1. Zurich, Switzerland.

Copyright

Acknowledgements

This discussion paper has benefitted greatly from the feedback and inputs of Emre Akbulut.

Summary

English

E-voting in the sense of location-independent, individualized voting over the Internet has a number of potential benefits. For example, e-voting can reach and mobilize voters who do not participate in traditional voting procedures, such as ballot voting in person or voting via mail. However, e-voting bears a fundamental risk: If an e-voting system is compromised, all votes that are cast can potentially be manipulated and corrupted. That is why e-voting, despite all of its potential benefits, has not yet been introduced on a large scale. Today, however, there is a possible solution for the fundamental risk of e-voting: the blockchain technology. The blockchain is a distributed, digital, and open ledger that makes tampering practically impossible if the technology is implemented correctly. In this discussion paper, we argue that a blockchain-based e-voting system can mitigate the risk associated with e-voting because the distributed nature of the blockchain makes a tamper-proof e-voting system possible. In practice, the crucial aspect of a blockchain-based e-voting system is a truly distributed e-voting architecture: Blockchain-based e-voting can only work when no single entity, not even the government, is in full control of the e-voting infrastructure.

Deutsch

E-Voting als ortsunabhängiges, individualisiertes Wählen und Abstimmen über das Internet hat eine Reihe potenzieller Vorteile. E-Voting kann beispielsweise Wählerinnen und Wähler mobilisieren, die die klassischen Partizipationswege der Abstimmung an der Urne oder der Briefabstimmung eher nicht nutzen. E-Voting ist aber mit einem fundamentalen Risiko behaftet: Wenn ein E-Voting System kompromittiert wird, dann können potenziell alle abgegebenen Stimmen nach Belieben manipuliert werden. Das ist der Grund, warum E-Voting noch nicht flächendeckend im Einsatz ist. Es gibt eine mögliche Lösung für das fundamentale Sicherheitsrisiko von E-Voting: Die Blockchain-Technologie. Blockchain ist ein verteiltes, digitales und offenes Register, welches Manipulation so gut wie unmöglich macht, wenn die Technologie korrekt implementiert wird. In dem vorliegenden Diskussionspapier argumentieren wir, dass ein Blockchain-basiertes E-Voting-System das Risiko von E-Voting beheben kann. Für die praktische Anwendung ist der zentrale Aspekt eines Blockchain-basierten E-Voting-Systems die Bedingung, dass die Blockchain-basierte E-Voting-Architektur wirklich verteilt ist: Blockchain-basiertes E-Voting funktioniert nur, wenn kein einziger gesellschaftlicher Akteur, auch nicht die Regierung, die E-Voting-Infrastruktur komplett kontrolliert.

Contents

List of Figures

List of Tables

1 Introduction: The elusive quest for electronic voting

1.1 Voting matters, a lot

Democracy is a fuzzy idea. Indeed, it is fuzzy to such a degree that it is sometimes described as a «essentially contested concept» [1] because there are many aspects to the concept that cannot be clearly answered. However, there is at least one principle that serves as the baseline understanding of democracy: In order to be considered democratic, a political system has to be based on the principle of *popular sovereignty*.

Popular sovereignty means that the people who are *subject to* polity-wide binding rules should be the very *authors* of those rules. Consequently, citizens should actively assume the role of legislators, and do so permanently, in order to create the laws that they subject themselves to. That, of course, is practically impossible in most cases, for two reasons. First, if all members of a given polity were to act as legislators, they would not have much time do to anything else. Second, and no less important, the very politics of a legislative body that consists, basically, of the entire population, is hard to conceive even as a thought experiment, much less as a practical, real-world solution. Even if all citizens decided to do nothing but legislate, they probably would not be able to get anything done.

The argument that not all members of a polity can act as legislators all of the time is, of course, almost trivial. After all, Rousseau derided that idea centuries ago by explaining that this pure form of «direct democracy» was reserved for the gods, not men [2]. However, even though popular sovereignty cannot be achieved in the form of real direct democracy, there is a normative second-best institutional configuration that satisfies the condition of popular sovereignty to a sufficient degree and therefore makes a democratically legitimate polity possible: *Representative democracy.* Representative democracy is such a polity, as the name suggests, in which a small subset of citizens is tasked with acting as legislators on behalf of the general population.

The subset of citizens who act as legislators have a very distinct relationship with the general population. For example, that subset could be appointed as legislators by means of lottery, but we would not consider such a legislative body to be democratic in the sense of being an embodiment of popular sovereignty [3]. In order for legislative representatives to have democratic legitimacy, representatives do not only have to be chosen *from among* the people, but also *by* the people. Representative democracy, it follows, cannot be merely proceduralist (such as the luck of the draw in a lotter), but rather, it has to be a system of *proceduralized popular sovereignty* [4, 5].

Proceduralized popular sovereignty is possible through voting, and through voting only. Through the act of voting, citizens aim to elect the candidates and parties whose preferences are most closely aligned with their own[1]. Voting, in this sense, is a direct and explicit manifestation of popular sovereignty. This means that, from a normative point of view, voting is not about the candidates, but all about the voters. After all, elected representatives are merely the agents of the sovereign people who, by means of voting, make use of the power that they have as principals [6, 7].

In summary, representative democracy is possible only with proceduralized popular sovereignty, and proceduralized popular sovereignty means free and fair voting. Voting, however, does not only matter in normative principle, but also very much in empirical practice. Making free and fair voting possible is a lot of work. One promising way to make voting a bit simpler, both logistically and in terms of citizen participation, is electronic voting, or *e-voting*.

1.2 The benefits of e-voting

The idea of e-voting, understood as *location-independent, individualized voting over the Internet*, has been around at least since the 1990-ies, when adoption of that technology, in the sense of both Internet penetration and online content and services, began to expand strongly. E-voting is not just a utopian idea of Internet evangelists, but, in many countries, an actual political project: Governments and parliaments in a number of countries have been pursuing the possibility of e-voting for the better part of the past two decades [8, 9]. In some countries, notably Estonia, some forms of e-voting are already in use and in relatively high demand [10, 11]. The reasons for this «official», governmental interest in e-voting are twofold: E-voting has both *normative* and *practical* benefits.

Normatively, e-voting is desirable because it expands the repertoire of voting venues for citizens. Here, of course, the premise is that e-voting is not a substitution for existing, traditional means of voting, but rather an expansion of those means. When e-voting is understood in this complementary manner, the normative argument in its favor is almost trivial. The voting process as a part of the polity should be constituted in such a manner so as to make voting as accessible as possible. Even though the United States, one of the biggest democratic countries, has experienced a wave of voter restriction laws in recent years [12, 13], the normative goal in democracies has to be a lowering of resources necessary to participate in the political process, not the opposite.

Practically, e-voting has at least two important properties. First, tying in

[1] This is the prototypical, but not the only voting behavior that typically rational voters will engage in.

with its normative desirability, e-voting can lower the cost of participation for some, if not all citizens. Traditional means of voting require the investment of certain amounts of resources, such as time and money. For example, the most common voting method, voting by physically visiting a polling place in order to cast one's ballot, means an investment of time as well as, in some cases, money. Obviously, it takes time to physically reach a polling place, and to return from the polling place. This process can also require financial resources, either directly (as travel expenses) or indirectly (as opportunity costs[2]). E-voting can, potentially, greatly reduce opportunity costs since it can allow citizens to vote using their own computer or smartphone. In that regard, e-voting has the potential to not only be a viable voting option, but the most efficient one. Even when compared to postal voting, an established method of location-independent physical voting, the opportunity costs of e-voting are lower: Filling out and sending a letter is not a lot of work, but it is more work than operating voting software on a computer or smartphone[3].

The second practical property of e-voting that makes it important is its potential *mobilization effect*: People who do not vote in a given voting situation might be incentivized to do so with the option of e-voting. This potential mobilization effect goes beyond e-voting's general property of reducing opportunity costs described above. There are two ways in which e-voting can have a mobilizing effect. The first one is the mobilization of a stratum of the population that has particulary favorable views of all things digital. A large cohort of people today are sometimes labeled as «digital natives» or «millennials» [15, 16], and one of the shared traits of that generational[4] stratum is the fact that digital natives are mostly used to interfacing and exchanging information with individuals, groups and organizations digitally. That does not mean that physical interpersonal relationships are in decline among digital natives, but rather that digital means of sharing information and of obtaining goods and services are not only becoming ever more popular, but that they have become the *status quo* for digital natives. A typical example is media use: The idea of reading or even subscribing to physical,

[2] This is not a cynical comment. In a democracy, citizens should, of course, value the fact that they can vote and they should, consequently, be willing to forgo some alternative choices in favor of voting. That is precisely what they are doing when, for example, citizens take half a day off at their place of work in order to vote at a polling place. That scenario is a direct example of opportunity costs: When voting, citizens forgo the salary they could have earned during the time it took them to complete the vote [14].

[3] The amount of resources necessary to make a decision can be thought of as about the same in both cases. But, after having made your choice, there's a difference: In e-voting, you can cast your vote then and there, while in postal voting, there's the additional step of mailing the voting letter.

[4] Of course, this is not a generation in the biological sense, but rather in the sociological sense of a cohort of people who have been socialized in similar circumstances and share similar preferences, attitudes and values.

printed newspapers is becoming a quaint notion of a time before their time for many people, as witnessed by steadily falling newspaper circulation [17]. The general preference of digital natives for digital processes can be leveraged by e-voting, resulting in greater overall participation. This potential mobilizing effect is hinted at by the greater enthusiasm that younger people express for e-voting [18, 19].

The second potential mobilizing effect of e-voting is more universal. A crucial factor of e-voting is the specific user experience of the e-voting application. When e-voting applications are designed with human cognition in mind, they can increase the probability that a given voter will, *ceteris paribus*, vote. Even though we humans like to think that we think rationally, errors in our cognition, so-called cognitive biases [20, 21], abound. Fortunately, our knowledge of cognitive biases as universal phenomena can also inform how we design choice situations. In the context of e-voting, this means that e-voting applications can be engineered so as to *nudge* citizens into voting. Nudging, a concept that stems from behavioral economics [22], is the idea that the contexts within which individuals make choices can be designed in such a way so as to make a desired outcome more probable by exploiting cognitive biases. While nudging is paternalistic [23], it is not coercive; individuals still have all choice options. Furthermore, nudging in the context of e-voting is normatively sound, since the goal is not to nudge voters into specific political preferences, but only into expressing their *existing* preferences. Nudging in e-voting can be achieved in many ways. For example, an e-voting smartphone app could send users push notifications on their smartphone, reminding them that they can vote for the, say, upcoming electionß. In this example, the user is not at all forced to vote, but the app notifications simply gently nudge the user into voting by reminding her or him that an election is coming up. This potential mobilizing effect of nudging in e-voting is absent in traditional forms of voting[5].

1.3 The dangers of e-voting

In the preceding subsection 1.2, e-voting was showered with praise – and the arguments presented in favor of e-voting are so uncontroversial that they verge on the trivial. Why, then, is e-voting not a standard voting method but still somewhat of an experimental technology? The answer is as unambiguous as are the potential benefits of e-voting: Compared to other means of voting, *e-voting carries the greatest risk.*

[5] Generalized nudging efforts also exist for traditional voting. For example, when voters receive a small symbolic reward after voting, such as an «I have voted» button, non-voters might be nudged into voting through perceived social desirability – not having a button identifies you as a non-voter.

In terms of their benefits, voting procedures have a normative and a pragmatic dimension. In terms of risks, another dimension is relevant: The *logistics of voting*. When talking about voting in the normative, democratic abstract, it is easy to forget that voting entails a lot of logistic work as well: Votes have to be delivered, transported and counted. As citizens in Western democracies, we take the logistic dimension of voting as a matter of course. We are so used to the logistic dimension simply being taken care of that we tend to forget it even exists. But it is very real, and it is present in every form of voting. For example, in in-person ballot voting, one's vote has to be physically cast, usually by filling out an official document, the ballot (be it on paper or in electronic form when using voting machines). Then, the vote needs to be transported or transmitted from one place to another, in order to officially count it along all other votes.

Every one of those three logistic aspects of voting – casting, transportation, and counting – is present in e-voting as well. When a citizen casts a vote by means of e-voting, a piece of digital information is created. That information is created with the help of a device that the voter is using, such as their laptop computer or their smartphone. If the digital voting information remains on that device, it is not of much use – the information needs to be delivered to the government in order to be processed. Therefore, individual digital voting information has to be created (casting the vote), delivered to some destination (transportation), and it needs to be processed there (counting).

The three logistic dimensions of voting – casting votes, transporting them and, finally, counting them – are potential *attack vectors*. If some actor wants to tamper with elections that are, in principle, free and fair[6], then they can attack the node of casting votes, the node of transporting them, and the node of counting them. An example of an *attack on the vote casting node* is a manipulation of the paper ballots that are filled out manually. It is not impossible that one could, given sufficient access, corrupt a ballot in such a manner that the ballot becomes invalid, all without the affected voter noticing anything. In cases where ballots are counted with the help of digital scanners, some manipulations to the ballot might affect the scanning process, but not be obvious to the naked eye.

An example of *attacking the transportation node* are mail-in ballots. When it is possible to mail in ballots as a form of early voting before the actual day of the vote, the ballot is processed as mail. This means that, in principle, employees of post offices can manipulate the mailed-in ballots, for example by not forwarding some of them to their destination, but instead just throwing them into the trash.

An example of an *attack on the counting node* are people who manually count

[6] Of course, we are talking about voting in democratic systems. If the voting situation is flawed *a priori*, then these attack vectors will be of little importance, because the whole affair is s sham. Many authoritarian countries regularly conduct such non-free, undemocratic elections [24, 25].

votes on election day. A small group of conspiring people could, conceivably, deliberately introduce concerted errors in their vote counts in order to skew the results in some manner. They could, for example, conspire to declare ballots invalid, or simply lie about the number of votes in favor of some candidates.

These attack vectors are real in contemporary voting systems. However, they pose more of a theoretical than an actual threat. The reason for that is their *limited scalability*: Attacks on the nodes of casting votes, transporting votes, and counting nodes require a lot of resources with very limited impact. Say, for example, that a presidential candidate wanted to tamper with the voting process. In order to obtain any significant advantage from attacking the three nodes, the candidate would have to invest an inordinate amount of resources in the form of money, time, and, most importantly, people. The same is true for outside actors who might want to tamper with the vote. For example, the amount of resources necessary for a foreign government to systematically and successfully attack the three voting nodes is enormous, and it would require a conspiracy of gargantuan proportions.

The danger of vote tampering in traditional voting, then, is real, but the potential damage is very limited, and the probability of such tampering is small, not least because the return on investment of such tampering is very small. In other words, the *risk* of tampering with traditional voting procedures is small.

The situation is *very* different with e-voting. Successful attacks on the nodes of vote casting, vote transportation, and vote delivery in e-voting require very few resources and they reap, potentially, tremendous rewards. The *risk* of tampering with e-voting, therefore, is *very large.* Even if we believe that the probability for a successful manipulation of a voting procedure is very small, the risk is large simply because the potential damage is so great. And tampering with e-voting is not a theoretical threat and unfounded fear: Time and again, security researchers have demonstrated that various e-voting systems that have been deployed or developed can be tampered with [26, 27, 28, 29, 30]. The tampering risks of traditional voting methods and of e-voting are juxtaposed in Table 1.

Table 1: *Comparison of the risks of tampering for traditional voting and for Internet-based e-voting.*

	traditional voting	*e-voting*
Resource requirements	high	low
Damage	low	high
Probability	low	high
Overall risk	low	high

The probability that a breach will occur is described as high in Table 1. This means that, given the low resource requirements and the very large rewards, the probability that e-voting in any voting process will be breached if there is intent to breach it is too high – it is greater than 0. This is what makes the risk of implementing e-voting too high to actually implement it. In light of this risk, implementing e-voting is irrational, and ongoing implementation efforts should be halted.

The above risk assessment is true for all current iterations of e-voting. Even though current e-voting solutions are carefully engineered to make them as secure as possible, they cannot, ultimately, lower the risk of tampering to an acceptable level[7]. However, there is a piece of technology that can: the *blockchain*.

2 Enter the blockchain: A distributed, transparent, digital ledger

2.1 The paradoxical trust machine: Generating trust by not trusting anyone

One of the more remarkable aspects of human civilization is the fact that we are able to trust each other even in situations where trust cannot be expected to arise naturally. For example, if you are interacting with a stranger, meaning a person you are not connected to neither through kinship nor through pre-existing friendship, it is often in your rational self-interest to distrust the stranger as much as possible. Yet this rational behavior leads to bad overall outcomes, as examples from game theory such as the famous prisoner's dilemma [31] so amply demonstrate. The relevance of trust is not limited to the micro level of individuals. For example, from a society-wide perspective, trust is the necessary condition for sustainable democracies; this is sometimes described with the concept of social capital [32, 33, 34].

It is safe to say that without trust, the scope of human interaction and transaction is severely limited. The more we trust each other, the better. But trust is not a resource that materializes out of thin air, and, arguably, it shouldn't. Many forms of interactions and relationships are fairly complex and risky. As rational actors, we are rightly hesitant to, so to speak, trust our trust in situations where the stakes are high and we are unable to assess whether our trust and honesty is reciprocated. That is why, in many different situations, we rely on third parties and on formalized agreements in order to generate trust between us and other people or organizations. This is what happens every time you sign a contract, for

[7] Remember: No voting method is completely *risk-free* in terms of tampering. The risk of traditional voting methods is simply low enough to make them reliable.

example.

In 2008, a mysterious person, or perhaps group of people, going by the pseudonym of Satoshi Nakamoto introduced a peculiar bit of technology to the world: Bitcoin [35]. Bitcoin was the first «cryptocurrency»: A form of currency that works entirely over the Internet, without the need for something like state-approved ledgers (banks), and where users accordingly enjoy much greater privacy than with regular, state-sponsored money. What makes Bitcoin so important is not Bitcoin in and of itself, but rather the underlying technology that made Bitcoin possible; the so-called *blockchain*, a revolutionary digital ledger. But the blockchain is not a regular digital ledger that involves a third party – there *is* no third party.

The blockchain as a digital ledger has three key properties. First, it is completely *free and open-source software*. Anyone is free to use, distribute and build upon the blockchain source code. Second, the blockchain is a *distributed* digital ledger. A transactional system that relies on the blockchain as a ledger works in such a way that many copies of the ledger communicate within the network, and transactions are not simply registered and processed by one copy of the ledger, but by a majority of all copies of the ledger. Third, the blockchain is, in principle, a *radically transparent* ledger. The blockchain is not a secretive database where no one is able to monitor transactions. On the contrary, the blockchain is radically transparent in that all transactions that have ever taken place in a given network and application (such as Bitcoin) are registered.

These properties are what makes the blockchain such a potent ledger that creates «trustless trust» [36]; trust without the need for a trusted third party. Every transaction has to be approved by and recorded on the whole blockchain network. Even if one or several copies of the ledger become corrupted, they cannot infest the whole network of ledgers. Instead, the network will simply not arrive at consensus and prevent the transaction from taking place [37].

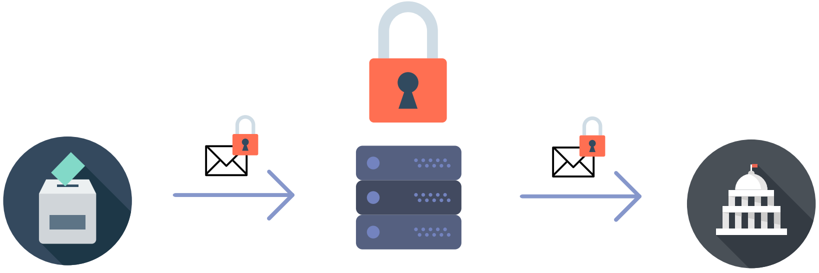
Blockchain technology is not revolutionary *per se*, because its individual technological and cryptographical components existed before blockchain. But blockchain as a specific combination of ideas and principles has the potential to enable transactions in many different aspects of society to take place in a manner that was not possible before bitcoin [38, 39, 40]. One of the areas where blockchain can make a categorical impact is e-voting.

2.2 Blockchain and e-voting

In subsection 1.3, we have argued that and why e-voting bears a significant risk. That risk is so great, in fact, that the only solution is not to employ e-voting at all: If an e-voting system is tampered with, the potential consequences are far-reaching. This is where the unique properties of the blockchain become relevant: The architecture of a blockchain-based network means that tampering is conceptually not possible when correctly implemented, because a blockchain network is strictly transparent, distributed and consensus-based. There is nothing inherent to blockchain technology that limits its use to either or other forms of cryptocurrencies economic transactions. Indeed, the idea of implementing blockchain technology for a tamper-proof e-voting system is slowly gaining traction [41, 42].

For individual citizens as end users, a blockchain-based e-voting system might not differ much from a regular e-voting system. In both cases, a person is using some digital interface on some peace of hardware and simply casting their vote. However, the underlying processes in the two different systems are quite different. This difference is visible if we try to summarize the logic of regular and of blockchain-based e-voting. The logic of regular e-voting is depicted in Figure 1.

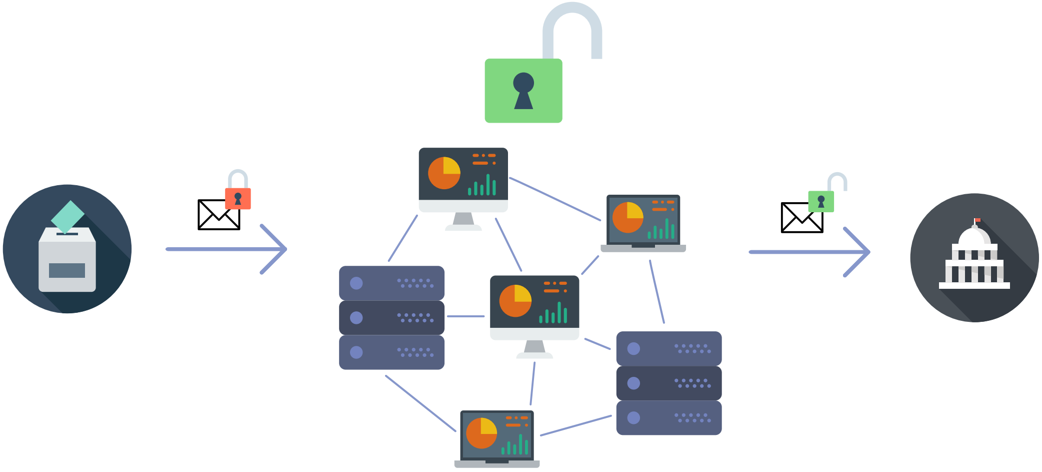
Figure 1: *The logic of regular e-voting.*



Regular e-voting is fairly straightforward and, in principle, easy to understand. You cast your vote, and your vote is sent as an encrypted peace of information to a server. Everything on that server is also encrypted and secured as strongly as possible. The government has access to that encrypted information because they have to count the votes. Overall, then, regular e-voting aims to protect the voting process as strongly as possible and to limit access to voting information to the government. The principle of blockchain-based e-voting, as depicted in Figure 2, is quite different.

At the beginning of blockchain-based voting, an individual citizen casts their vote and that peace of information is encrypted – using blockchain-based e-voting does *not* mean that everyone can see how everyone voted. However, the vote as an encrypted piece of information enters not a single server, but an entire distributed blockchain network, and everything in that network is fully transparent and public. An encrypted vote is validated on the blockchain network by consensus mechanism, and every vote is publicly registered on distributed copies of the ledger, i.e., the blockchain. The government can see how the votes have been cast and count the votes, but this information is not limited to the government.

Figure 2: *The logic of blockchain-based e-voting.*



The blockchain that contains the votes is public and perfectly transparent, but it protects voters. This means that, in blockchain-based e-voting, everyone can *count* the votes, but no one knows *who* cast which vote.

Regular e-voting and blockchain-based e-voting, then, follow categorically different operational principles. This difference also has an impact on the dimension of risk. In table Table 1, the risks of traditional voting and regular e-voting over the Internet are compared. Table 2 adds blockchain-based e-voting to that comparison.

Table 2: *Comparison of the risks of tampering for traditional voting, Internet-based e-voting, and Internet-based e-voting that utilizes the blockchain.*

	traditional voting	*e-voting*	*blockchain-based e-voting**
Resource requirements	high	low	high
Damage	low	high	low
Probability	low	high	low
Overall risk	low	high	low

**This applies only to a properly implemented blockchain-based e-voting system.*

A blockchain-based e-voting system has much lower risk than regular e-voting – the risk of blockchain-based e-voting is as low as the risk of traditional voting. However, this is only possible with a *properly* implemented blockchain-based e-voting system. In order to produce such a system, it is not enough to engineer a working technical implementation of blockchain-based transactions as transactions of votes. From a technical point of view, blockchain-based e-voting is fundamentally feasible and, in essence, only a matter of resources (time and labor). The main challenge for creating a proper blockchain-based e-voting system is not technical in nature, but rather *social*: Blockchain-based e-voting can only be implemented when different societal stakeholders are involved in the supervision and maintenance of the system.

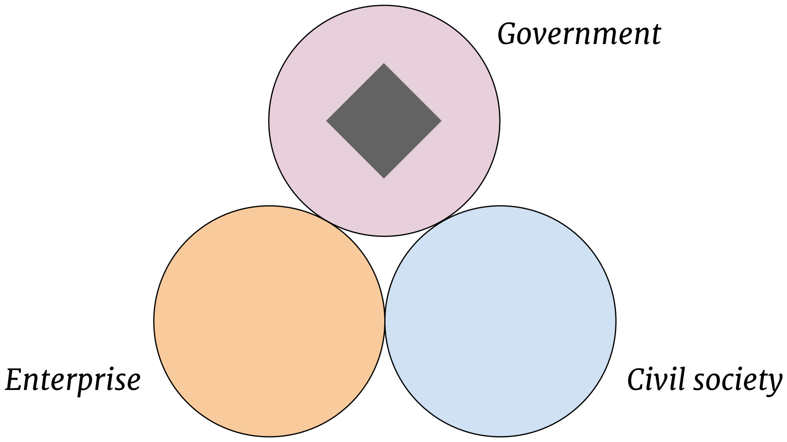
3 Building a blockchain-based e-voting system

3.1 Public service, but not exclusively government-run

Traditionally, voting in a procedural, logistical sense is made possible by the government. That is sensible, of course: Providing voting infrastructure is a public service that the government should provide to its citizens. This is an uncontested fact. While the question of the proper scope of governmental activity in different areas of society is an ongoing political debate, no one seriously disputes the government's duty to provide and maintain the means for free and fair elections.

The current paradigm of voting infrastructure whereby government alone is in charge of voting infrastructure can, in principle, also be applied to blockchain-based e-voting. This is summarized in Figure 3[8].

Figure 3: *A centralized and government-run blockchain-based e-voting system. The black diamond represents the e-voting infrastructure.*



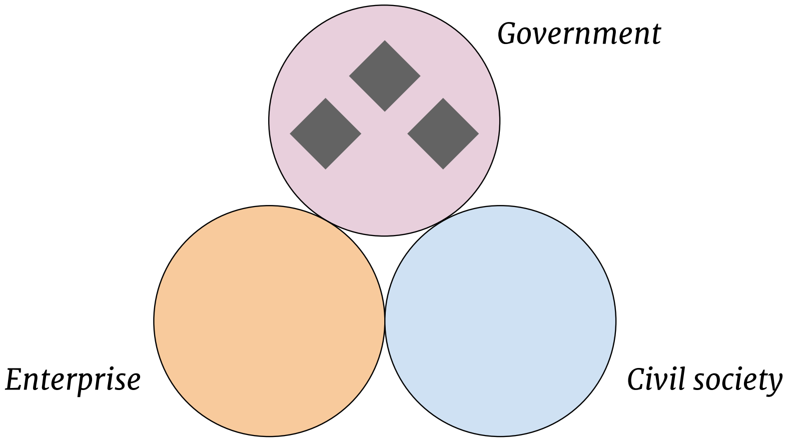
If we simply apply the current voting infrastructure paradigm to blockchain-based e-voting, then, as depicted in Figure 3, all blockchain-based e-voting infrastructure is run by the government. Even though this solution might seem natural

[8] In Figure 3, society is figuratively depicted as three sub-spheres: Government, civil society and enterprise (economy). Understanding society as comprised of these three sectors is a common heuristic for thinking about the structure of society [43].

(simply replicate digitally what we have been doing physically), this model has a fatal flaw: When all blockchain-based e-voting infrastructure is maintained in a centralized manner by the government, then the whole affair becomes pointless, since the system is not tamper-proof anymore. If a blockchain-based e-voting system is run centrally by the government, then potential corruptors need only infiltrate one network, the government's, in order to tamper with votes. The traditional paradigm of voting infrastructure, then, is not suitable for blockchain-based e-voting. Even though this is a purely practical conclusion, it does mean that a paradigm shift is necessary.

A first step to improve the structural nature of a blockchain-based e-voting system is to introduce distribution within the network. This means that the blockchain nodes that validate votes are not all located in one government-run network. Instead, the government distributes the relevant blockchain nodes over different networks, both digital and physical, in order to minimize risk concentration. This configuration is depicted in Figure 4.

Figure 4: *A pseudo-distributed and government-run blockchain-based e-voting system. The black diamonds represent the e-voting infrastructure.*



A government-run *distributed* blockchain-based e-voting system is preferable to a government-run *centralized* system. Such a system is potentially less vulnerable than a completely centralized implementation of a blockchain-based e-voting system, but it still represents a considerable risk. In principle, government-run computer networks are always connected at some level; if not physically, then through political chain of command[9]. Furthermore, if a blockchain-based e-voting system is run exclusively by the government, the performative principle of the blockchain is violated: The blockchain generates trust because no one actor holds

[9] People are potential attack vectors for tampering as well, not just software and hardware.

all the information. The same must be the case for blockchain-based e-voting. This principle is depicted in Figure 5.

Figure 5: *A partially distributed blockchain-based e-voting system run by the government, civil society and enterprise. The black diamonds represent the e-voting infrastructure.*

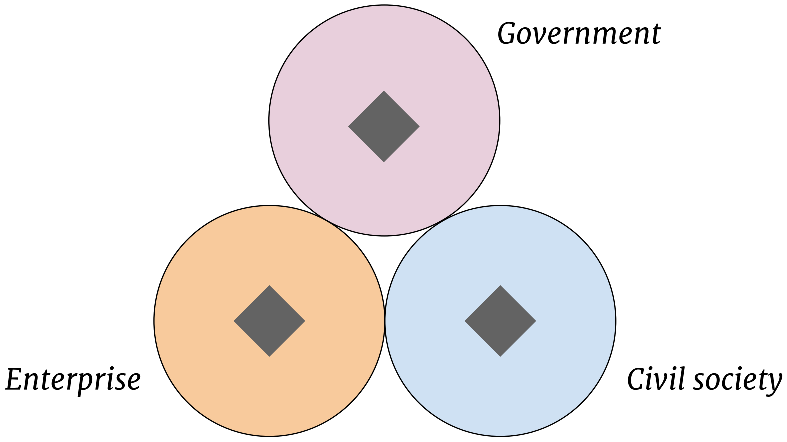
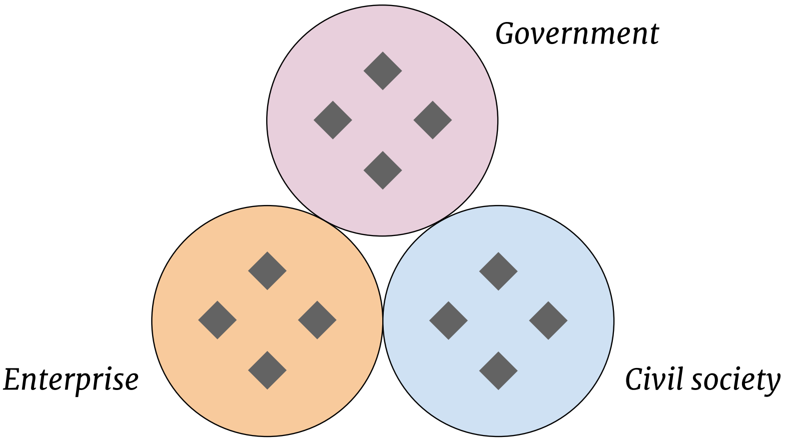


Figure 5 is the symbolic depiction of a blockchain-based e-voting in which all three sectors of society, government, enterprise, and civil society are involved. Such a model approximates the logic of a distributed network: The system is not exclusively government-run, but in addition, business and civil society organizations are involved as well. However, in this model, the distribution is minimal: Only a select few business and civil society organizations are involved the in the blockchain-based e-voting system. This means that security concerns persist: If only a few actors run the e-voting system, it might still make sense for nefarious actors to tamper with some of them. That is because such nefarious actors could gain control of a majority of the nodes in the network that perform the validations of vote transactions with relative ease, simply because there are few such nodes.

Therefore, the optimal model of a blockchain-based e-voting system needs to implement *strong* distribution – so strong that tampering becomes practically impossible. This ideal form of a blockchain-based e-voting system is depicted in Figure 6.

A blockchain-based e-voting system as depicted in Figure 6 can be considered a fully distributed system. This means that it represents a structural realization of the idea behind the blockchain: The digital ledger works because the network is set up in such a way that it is tamper-proof. This means that no single entity involved in the maintenance of the blockchain-based e-voting system operates a majority of the blockchain network. Instead, the network nodes are distributed among actors from government, enterprise and civil society. When a blockchain-based e-voting system is set up in such a manner, its theoretical tamper-proofness

Figure 6: *A fully distributed blockchain-based e-voting system run by the government, civil society and enterprise. The black diamonds represent the e-voting infrastructure.*



becomes a practical one.

3.2 Blockchain-based e-voting and anonymity

The focus of this discussion paper is not the technical dimension of a blockchain-based e-voting system, but rather, its social dimension. This could leave the impression that there is a ready-to-use blockchain-based e-voting solution. That is not the case: A blockchain-based e-voting system needs to built, and extensively tested. But doing so is a fundamentally feasible software engineering task, and therefore, simply a function of resources (time and money). One technical aspect of a future blockchain-based e-voting system, however, is not simply a matter of resources: The question of *anonymity*.

In order to use blockchain-based services, users do not provide their identity. Instead, the default operating method of the blockchain is one of *pseudonymity*. Blockchain-based transactions rely on tried and trusted form of cryptography, so-called public-key cryptography [44]. The general idea of public-key cryptography is that transactions are secured by using two pairs of keys, a public and a private one. Every user has a public and a private key. If user A wants to send some information to user B, user A encrypts the information with user B's public key. Then, after having received the information in its encrypted form, user B can decrypt it with his private, secret key. The blockchain does not use public-key encryption for encrypting information. Instead, it uses public-key encryption for creating *digital signatures*. In blockchain-based networks, a user's public key is a user's address that she or he uses to receive transactions. A user who initiates a transaction and sends some information to another user's address can sign his message using his private key. No one has access to that user's private key, but anyone who has access to that user's public key is able to verify the signature. If user A wants to send some information to user B on a blockchain-based network, user A is sending the information to user B's address, which is her or his public key. When user B receives the message, she or he is able to verify that the message really did come from user A, because user A's address, her or his public key, is publicly known.

The verification function via public-key cryptography is one of the core components of the blockchain. However, its downside is that it is not truly anonymous, but rather pseudonymous. The main reason why the blockchain works is its inherent transparency; the blockchain can work as a public ledger precisely because it is public, and therefore, precisely because all transactions are recorded. In the context of blockchain-based e-voting, this means that not only the fact *that* user pseudonyms have voted is recorded, but furthermore, *how* they voted is recorded as well. This can be a potential problem, since free and fair elections require *ballot secrecy.* Therefore, a viable e-voting solution, blockchain-based or otherwise, has to offer ballot secrecy [45, 46].

Blockchain pseudonymity can become a problem when users' private keys become compromised. In order to keep the risk of private key compromises as low as possible, private key management must not be centralized in any way. Only individual citizens can have access to their own private key, an no one else. Furthermore, private and public keys have to be generated anew for every single vote. This will ensure that no citizen is using the same pseudonym, a public key, more than once. If voters use the same pseudonyms, meaning the same public keys, over the course of several voting instances, it is conceivable that voter identities could be estimated in a probabilistic manner. This is especially relevant in voting settings that involve a low number of people, such as elections in small municipalities.

The risk of exposing individual identities of the pseudonyms that are used on the blockchain network is not, strictly speaking, a risk of blockchain technology, but rather a risk of Internet-based technology in general. So-called «hacking» of individual users and user data is oftentimes not contingent on the specific software application in question, but on users themselves. One of the most successful «hacking» paradigms is social engineering [47], whereby users are manipulated into giving up sensitive information about themselves. Social engineering does not exploit bugs and errors in software, but rather the biases and irrationality of us humans. This general risk of Internet-based technology is also present in blockchain-based e-voting (as well as in regular e-voting), but it is not a security risk inherent to blockchain technology. But, of course, users of Internet-based applications should seek to minimize their own risky behavior, and the introduction of blockchain-based e-voting can serve as an opportunity to educate users about safe behavior with regards to their sensitive user data.

4 Conclusion: A paradigm change for e-voting

E-voting is, in principle, a highly desirable technology. However, given the fundamental risk of e-voting as it has been hitherto proposed and in light of real-world hacking demonstrations, all implementation of e-voting should be stopped. No matter how well guarded a centralized e-voting system is, it remains fundamentally insecure, because *any* centralized, black-boxed computer system is fundamentally insecure. The only way to overcome this fundamental insecurity of e-voting is to embrace and implement a paradigm change. The manifestation of this paradigm change is the *blockchain* technology.

The blockchain is a distributed, transparent and fundamentally secure digital ledger. Rather than through centralization and black-boxing, the blockchain works through distribution and openness – and that is precisely why a blockchain-based e-voting system is tamper-proof.

The interest in e-voting is not likely to subside any time soon, from the point of view of citizens as well as from the point of view of governments. It is therefore only rational that governments explore and invest in e-voting that is based on transparent and open technology. The most reliable such technology to date is the blockchain.

References

[1] Walter B. Gallie. “Essentially Contested Concepts”. In: *Proceedings of the Aristotelian Society* 56 (1955), pp. 167–198 (cit. on p. 5).

[2] Jean-Jacques Rousseau. *Du contract social, ou, Principes du droit politique.* Amsterdam: Marc-Michel Rey, 1762 (cit. on p. 5).

[3] Bernard Manin. *The Principles of Representative Government.* Cambridge ; New York: Cambridge University Press, 1997. isbn: 978-0-521-45258-8 (cit. on p. 5).

[4] Jürgen Habermas. “Popular sovereignty as procedure”. In: *Deliberative Democracy: Essays on Reason and Politics.* Ed. by James Bohman and William Rehg. Cambridge, Mass: The MIT Press, 1997, pp. 35–65. isbn: 978-0-262-52241-0 (cit. on p. 5).

[5] Jürgen Habermas. “Three Normative Models of Democracy”. In: *Constellations* 1.1 (1994), pp. 1–10. doi: 10.1111/j.1467-8675.1994.tb00001.x (cit. on p. 5).

[6] Kaare Strøm. “Delegation and accountability in parliamentary democracies”. In: *European Journal of Political Research* 37.3 (2000), pp. 261–289. doi: 10.1111/1475-6765.00513 (cit. on p. 6).

[7] Paul Mitchell. “Voters and their representatives: Electoral institutions and delegation in parliamentary democracies”. In: *European Journal of Political Research* 37.3 (2000), pp. 335–351. doi: 10.1111/1475-6765.00516 (cit. on p. 6).

[8] Robert Krimmer, Stefan Triessnig, and Melanie Volkamer. “The Development of Remote E-Voting Around the World: A Review of Roads and Directions”. In: *E-Voting and Identity.* Ed. by Ammar Alkassar and Melanie Volkamer. Lecture Notes in Computer Science 4896. Springer Berlin Heidelberg, 2007, pp. 1–15. isbn: 978-3-540-77492-1 978-3-540-77493-8 (cit. on p. 6).

[9] Jon H. Pammett and Nicole Goodman. *Consultation and Evaluation Practices in the Implementation of Internet Voting in Canada and Europe.* Tech. rep. Ganieau: Elections Canada, 2013 (cit. on p. 6).

[10] Dylan Clarke and Tarvi Martens. “E-voting in Estonia”. In: *arXiv:1606.08654 [cs]* (2016) (cit. on p. 6).

[11] Kristjan Vassil, Mihkel Solvak, Priit Vinkel, Alexander H. Trechsel, and R. Michael Alvarez. "The diffusion of internet voting. Usage patterns of internet voting in Estonia between 2005 and 2015". In: *Government Information Quarterly*. Open and Smart Governments: Strategies, Tools, and Experiences 33.3 (2016), pp. 453–459. DOI: 10.1016/j.giq.2016.06.007 (cit. on p. 6).

[12] William D. Hicks, Seth C. McKee, Mitchell D. Sellers, and Daniel A. Smith. "A Principle or a Strategy? Voter Identification Laws and Partisan Competition in the American States". In: *Political Research Quarterly* 68.1 (2015), pp. 18–33. DOI: 10.1177/1065912914554039 (cit. on p. 6).

[13] Seth C. McKee. "Politics is local: State legislator voting on restrictive voter identification legislation". In: *Research & Politics* 2.3 (2015), p. 2053168015589804. DOI: 10.1177/2053168015589804 (cit. on p. 6).

[14] John Gibson, Bonggeun Kim, Steven Stillman, and Geua Boe-Gibson. "Time to vote?" In: *Public Choice* 156.3-4 (2012), pp. 517–536. DOI: 10.1007/s11127-011-9909-5 (cit. on p. 7).

[15] Janna Anderson and Lee Rainie. *Millennials will benefit and suffer due to their hyperconnected lives*. Tech. rep. Washington DC: Pew Research Center, 2012 (cit. on p. 7).

[16] John Gorham Palfrey and Urs Gasser. *Born Digital: Understanding the First Generation of Digital Natives*. Basic Books, 2013. ISBN: 978-0-465-01383-8 (cit. on p. 7).

[17] Amy Mitchell and Jesse Holcomb. *State of the News Media 2016*. Tech. rep. Washington, D.C.: Pew Research Center, 2016 (cit. on p. 8).

[18] Uwe Serdült, Micha Germann, Maja Harris, Fernando Mendez, and Alicia Portenier. "Who are the Internet Voters?" In: *Electronic Government and Electronic Participation*. Ed. by Marijn F.W.H.A. Janssen, Frank Bannister, Olivier Glassey, Hans Jochen Scholl, Efthimios Tambouris, Maria A. Wimmer, and Ann Macintosh. Washington, DC: IOS Press, 2014. ISBN: 978-1-61499-428-2 (cit. on p. 8).

[19] Thomas Milic, Michele McArdle, and Uwe Serdült. *Haltungen und Bedürfnisse der Schweizer Bevölkerung zu E-Voting*. Tech. rep. Aarau: Zentrum für Demokratie Aarau, 2016 (cit. on p. 8).

[20] Amos Tversky and Daniel Kahneman. "Judgment under Uncertainty: Heuristics and Biases". In: *Science* 185.4157 (1974), pp. 1124–1131. DOI: 10.1126/science.185.4157.1124 (cit. on p. 8).

[21] Martin Hilbert. "Toward a synthesis of cognitive biases: how noisy information processing can bias human decision making". In: *Psychological bulletin* 138.2 (2012), pp. 211–237. DOI: 10.1037/a0025940 (cit. on p. 8).

[22] Richard H. Thaler and Cass R. Sunstein. *Nudge: Improving Decisions About Health, Wealth, and Happiness.* New York: Penguin Books, 2009. ISBN: 978-0-14-311526-7 (cit. on p. 8).

[23] Richard H. Thaler and Cass R. Sunstein. "Libertarian Paternalism". In: *The American Economic Review* 93.2 (2003), pp. 175–179 (cit. on p. 8).

[24] Jennifer Gandhi and Ellen Lust-Okar. "Elections Under Authoritarianism". In: *Annual Review of Political Science* 12.1 (2009), pp. 403–422. DOI: 10.1146/annurev.polisci.11.060106.095434 (cit. on p. 9).

[25] Andreas Schedler. "Electoral Authoritarianism". In: *Emerging Trends in the Social and Behavioral Sciences.* John Wiley & Sons, Inc., 2015. ISBN: 978-1-118-90077-2 (cit. on p. 9).

[26] Barbara Simons and Douglas W. Jones. "Internet Voting in the U.S." In: *Commun. ACM* 55.10 (2012), pp. 68–77. DOI: 10.1145/2347736.2347754 (cit. on p. 10).

[27] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman. "Attacking the Washington, D.C. Internet Voting System". In: *Financial Cryptography and Data Security.* Ed. by Angelos D. Keromytis. Lecture Notes in Computer Science 7397. Springer Berlin Heidelberg, 2012, pp. 114–128. ISBN: 978-3-642-32945-6 978-3-642-32946-3 (cit. on p. 10).

[28] Reto E. Koenig, Philipp Locher, and Rolf Haenni. "Attacking the Verification Code Mechanism in the Norwegian Internet Voting System". In: *E-Voting and Identify.* Ed. by James Heather, Steve Schneider, and Vanessa Teague. Lecture Notes in Computer Science 7985. Springer Berlin Heidelberg, 2013, pp. 76–92. ISBN: 978-3-642-39184-2 978-3-642-39185-9 (cit. on p. 10).

[29] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman. "Security Analysis of the Estonian Internet Voting System". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.* CCS '14. New York, NY, USA: ACM, 2014, pp. 703–715. ISBN: 978-1-4503-2957-6. DOI: 10.1145/2660267.2660315 (cit. on p. 10).

[30] J. Alex Halderman and Vanessa Teague. "The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election". In: *E-Voting and Identity.* Ed. by Rolf Haenni, Reto E. Koenig, and Douglas Wikström. Lecture Notes in Computer Science. Springer International

Publishing, 2015, pp. 35–53. ISBN: 978-3-319-22269-1 978-3-319-22270-7. DOI: 10.1007/978-3-319-22270-7_3 (cit. on p. 10).

[31] Anatol Rapoport and Albert M. Chammah. *Prisoner's Dilemma: A Study in Conflict and Cooperation.* University of Michigan Press, 1965. ISBN: 978-0-472-06165-5 (cit. on p. 11).

[32] Alejandro Portes. "Social Capital: Its Origins and Applications in Modern Sociology". In: *Annual Review of Sociology* 24.1 (1998), pp. 1–24. DOI: 10.1146/annurev.soc.24.1.1 (cit. on p. 11).

[33] James S. Coleman. "Social Capital in the Creation of Human Capital". In: *American Journal of Sociology* 94 (1988), S95–S120. DOI: 10.1086/228943 (cit. on p. 11).

[34] Robert D. Putnam. "Bowling Alone: America's Declining Social Capital". In: *Journal of Democracy* 6.1 (1995), pp. 65–78. DOI: 10.1353/jod.1995.0002 (cit. on p. 11).

[35] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System.* 2008 (cit. on p. 12).

[36] Kevin D. Werbach. *Trustless Trust.* SSRN Scholarly Paper ID 2844409. Rochester, NY: Social Science Research Network, 2016 (cit. on p. 12).

[37] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* Princeton: Princeton University Press, 2016. ISBN: 978-0-691-17169-2 (cit. on p. 12).

[38] Melanie Swan. *Blockchain: Blueprint for a New Economy.* "O'Reilly Media, Inc.", 2015. ISBN: 978-1-4919-2047-3 (cit. on p. 12).

[39] William Mougayar and Vitalik Buterin. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology.* Wiley, 2016. ISBN: 978-1-119-30031-1 (cit. on p. 12).

[40] Siraj Raval. *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology.* Sebastopol, CA: O'Reilly Media, 2016. ISBN: 978-1-4919-2454-9 (cit. on p. 12).

[41] Kibin Lee, Joshua I. James, Tekachew Gobena Ejeta, and Hyoung Joong Kim. "Electronic Voting Service Using Block-Chain". In: *Journal of Digital Forensics, Security and Law* 11.2 (2016), pp. 123–136 (cit. on p. 13).

[42] Christian Meter. "Design of Distributed Voting Systems". In: *arXiv:1702.02566 [cs]* (2017) (cit. on p. 13).

[43] Amitai Etzioni. "The Third Sector and Domestic Missions". In: *Public Administration Review* 33.4 (1973), pp. 314–323. DOI: 10.2307/975110 (cit. on p. 15).

[44] Arto Salomaa. *Public-Key Cryptography*. Springer Science & Business Media, 2013. ISBN: 978-3-662-03269-5 (cit. on p. 18).

[45] Jörgen Svensson and Ronald Leenes. "E-voting in Europe: Divergent democratic practice". In: *Information Polity* 8.1,2 (2003), pp. 3–15 (cit. on p. 19).

[46] Dimitris A Gritzalis. "Principles and requirements for a secure e-voting system". In: *Computers & Security* 21.6 (2002), pp. 539–556. DOI: 10.1016/S0167-4048(02)01014-3 (cit. on p. 19).

[47] Christopher Hadnagy. *Social Engineering: The Art of Human Hacking*. John Wiley & Sons, 2010. ISBN: 978-1-118-02971-8 (cit. on p. 19).