LEGAL CHALLENGES FOR THE USE OF BLOCKCHAIN-BASED E-VOTING SYSTEMS IN GERMANY

Tobias Schulz / Burkhard Schafer

Rechtsanwalt Dr. Tobias Schulz, LL.M. (Edinburgh), RITTERSHAUS Rechtsanwälte Partnerschaftsgesellschaft mbB,
Harrlachweg 4, 68163 Mannheim, D
tobias.schulz@rittershaus.net; www.rittershaus.net

Professor of Computational Legal Theory, The University of Edinburgh, SCRIPT Centre for IT and IP law
Old College, Edinburgh, EH8 9YL
B.schafer@ed.ac.uk; http://www.law.ed.ac.uk/people/burkhardschafer

Keywords: ***Art. 38 Grundgesetz, blockchain-based e-voting, secrecy and publicity of elections***

Abstract: *The authors demonstrate that the use of blockchain-based e-voting systems is generally consistent with German law, particularly with art. 38 of the Grundgesetz. This, however, requires the implementation of effective measure to ensure the publicity and the secrecy of the election and, hereby, meet the legal requirements for e-voting systems developed by the constitutional court of Germany in its judgment from 2009. An amendment of section 35 paragraph 1 of the Bundeswahlgesetz could contribute to more legal clarity when the use of mobile devices is intended.*

1. Introduction

This paper will analyse whether and under which conditions a blockchain based e-voting system can be introduced in Germany. Especially after a judgement of the constitutional court from 2009, which imposed tough restrictions on the use of electronic voting machines, the question arises whether there is still space for «digital elections» in Germany. The essay will start with a description of the technological background of blockchain in general and of blockchain-based e-voting systems (2). Next, it will depict the legal framework for elections in Germany (3). Part 4 then assesses if the introduction of blockchain e-voting platforms is consistent with the existing regulations. The essay ends with a summary and a conclusion (5.).

2. Technological background of the blockchain technology

2.1. Blockchain

Originally, blockchain technology was developed to support the cryptocurrency Bitcoin.[1] A blockchain can be understood as a large ledger. This ledger or file saves the data of every single transaction of Bitcoins from one user to another.[2] The coin itself is no more than an entry within the ledger. But in contrast to a traditional account, the blockchain is decentrally organized and managed by the Bitcoin users themselves.[3] Every user holds a digital copy of the whole ledger. The ledger can be understood as a chain of data «blocks» which stores the relevant information. Once a transaction between two users is conducted, the corresponding

[1] Pignal, Blockchain, The next big thing – Or is it?, The Economist Online, http://www.economist.com/news/special-report/21650295-or-it-next-big-thing (accessed on 18 December 2016), 9 May 2015; Pilkington, Blockchain Technology – Principles and Applications, in: Olleros/Zhegu, Research Handbook on Digital Transformations, Elgar Publishing, Cheltenham 2016, p. 225 (225 f.).

[2] Janschitz, Die Technologie hinter Bitcoins: Wie Blockchain das Internet für immer verändern könnte, http://t3n.de/news/blockchain-588923 (accessed on 18 December 2016), 17 October 2016.

[3] Ibid.

information is processed and saved in a «block» by a software client on the hard drive of every user who is online at that moment. This block, containing the information of many transactions, is eventually added by a single user to the ledger, the blockchain, and then confirmed by all users who also had received and saved the information before through what can be termed a «communal consensus model».[4] Most importantly, once a block is added to the chain, it cannot be changed anymore.[5] Since the ledger itself is public, the user can verify if his transaction was successful, and was accordingly saved in the blockchain.[6]

The user who adds the block to the blockchain has to have solved a very complex (and hence computing time intensive) mathematical task in advance. Crucially, while it is very difficult and computing intensive to solve the task, verifying that the solution is correct is very easy – an intuitive comparison is to a puzzle game which takes a lot of time and effort to assemble, but everyone can with just a look at it confirm or disconfirm if the result is correct. This process is called «mining».[7] This is to ensure the security and reliability of the network: this solution aims to avoid that individual users can confirm their own transactions and, hence, cheat the system. The high computing capacity that is necessary to solve the task makes it very improbable that an individual or even an organisation can take over the system for fraud confirmations.[8] In the Bitcoin system, every user who successfully «mines» a new block, is rewarded with Bitcoins. This is to incentivise the mining on which the whole system depends.[9]

Every user possesses an individual secret key which encrypts the data of his transaction.[10] Furthermore, every user holds a second individual, but public key. If a transaction is conducted, the submitted information is being encrypted by the system with the user´s public key. This is to verify the user´s identity, which, however, remains hidden. If the decrypted information has the format of a valid transaction, this is a proof of the use of a private key.

To sum up, the blockchain technology is characterised by a decentralised organisation, a high level of transparency and a high degree of protection against the manipulation of the stored data through a communal consent system. The decentralised organisation ensures that a loss of data is almost impossible since the blockchain is operated independently of any specific server or user – an attacker would have to change the data on *all* the computers in a network simultaneously.

2.2. Use of blockchain in e-voting systems

Within the last few years, several approaches have been developed to use the blockchain technology in fields other than cryptocurrencies, including e-voting systems. The most famous one, the US open-source platform «followmyvote», takes advantage of the blockchain approach as follows[11]:

Using blockchain for elections faces constraints different from those encountered when used as a currency. In particular, any e-voting system (or indeed any voting system) needs to balance from the beginning two conflicting demands: the integrity of the vote requires that only those legally entitled to vote can do so. This requires that someone verifies the credentials of the voters. On the other hand, the principle of the secrecy of the vote requires that a vote must not be linkable to a voter. If we gave up on secrecy, integrity would be easy: each voting token (the filled-in ballot) would carry the credentials of the voter who cast it, making it trivial to establish that only those entitled to vote cast a ballot, and did so only once. If we gave up on integrity (e.g.

[4] Pignal, op. cit.

[5] Pilkington, op cit., p. 225 (233).

[6] Pignal, op cit.

[7] Pilkington, op. cit., p. 225 (228).

[8] Pignal op cit.

[9] For further general considerations about the incentive for collaborative efforts see Pilkington, op. cit., p. 225 (233).

[10] Pilkington, op. cit., p. 225 (226).

[11] See https://followmyvote.com (accessed on 18 December 2016). See also Dickson, What it takes to secure the elections, https://techcrunch.com/2016/10/12/what-it-takes-to-secure-the-elections (accessed on 7 January 2017), 12 October 2016.

in a low-level opinion poll), secrecy would be easy to ensure, since nowhere in the system would we need to have a list that identifies those entitled to vote. Every voting system tries therefore to balance these demands, though e-voting systems face particular challenges due to the «stickiness» of the electronic medium: too much persistent user-data is inevitably generated during the process.

«Followmyvote» resolves this tension through a multi-stage registration process and the use of encryption.[12] It uses two separately working units, an identity verifier and a registrar. In the physical voting booth, the «ID verifier (in Germany the «Wahlhelfer») ensures that the person who presents themselves to vote are who they claim they are and recorded on the list of people entitled to vote, *and* hands out the ballot paper. Secrecy is ensured through a paper envelope which hides what vote was cast when the voter returns. As with all systems, this is a compromise – it would in theory be possible for the «ID verifier» to clandestinely mark the envelope, or simple to physically open the box and the envelope once the voter has left. This danger is minimised by having more than one Wahlhelfer, typically from different parties present, and impose criminal sanctions for this type of behaviour. «Followmyvote» replicates the effect of the physical envelope through encryption, and the «mutual surveillance» of the ID verifiers/Wahlhelfer by separating the role of the registrar from that of the ID verifier: a voter must have their identity and their public encryption key verified by an Identity Verifier and be issued a ballot by the Registrar. The Identity Verifier reviews the voter's personal information and issues an encrypted (and «blinded») token. On the basis of this information, the Registrar signs and approves the token, sending it to the ballot box which then generates the correct and unique ballot for the voter to use. In this system, the Identity Verifier cannot know how each voter has voted on their ballot, while the Registrar will never know the identity of the voter they issue the ballot to, only that it is to «a» legitimate voter. As we will discuss in more detail below, some forms of e-voting retain a problem with secrecy, but at this point, the blockchain based system manages to reconcile integrity and secrecy of the election in a way that is more secure than its physical counterparts – unlike in physical voting systems, the ID of the voter and the filled-in ballot are never in the same «room», let alone the same hands.

The electoral voting itself follows the blockchain principles. Every voter possesses a «coin», in this case a ballot, which he can transfer to the digital ballot box. As an immediate proof of his vote, the voter can, depending on the device used, print a digital receipt. Every vote is being transferred into a new block of the blockchain. After the digital ballot box has been closed, every voter will be granted access to the blockchain to verify that their vote was casted properly. The use of anonymous voter ID´s stored in the blockchain avoids the disclosure of the real identity.

The system can be used either on fixed computers at the election venues or portable devices like smartphones. The last option would have the advantage of facilitating absentee ballots cast by people unable to travel to the polling station, and avoids lines at the polls. In the recent US election, one allegation of manipulation of the vote was that were polling stations had been strategically understaffed (or too few provided to start with) resulting in lines too long for especially poorer voters who often can't afford to take time off work to cast their vote. However, as with all absentee ballots, this opens up the danger that the voter at the point of casting their vote is put under pressure by third parties. This is not a problem restricted to e-voting and postal votes are as badly affected. Nor is it as we saw a necessary feature of blockchain voting, since in theory only computers at certified polling stations could be allowed to join the blockchain network.

[12] https://followmyvote.com/cryptographically-secure-voting/ (accessed on 11 January 2017).

2.3. Conclusion

To sum up, the blockchain technology might offer a very safe and comfortable way of voting and potentially increase the voter turnout.[13] The immutability of the blockchain prevents any illegitimate action.[14] However, the system has some vulnerable points, which, for systematic reasons, are being discussed below.

Especially one important question in this context is not clearly answered. To ensure the potentially high degree of security of the data in the blockchain, the mining of new blocks as part of the data verification is vital.[15] In a decentralised system, this is done by the voters and their devices – something that clearly «adds value» in countries where trust in centrally, «state managed» election control is limited, but in countries where social trust in the integrity of elections is high to begin with, this «hands off» approach is less obviously superior in ensuring data verification than a decentralised, user-centric approach.

The question then is to which extent the current German electoral law allows the use of such technologies.

3. Legal framework for «digital» elections in Germany

This paragraph will examine if and under what conditions the introduction of a blockchain-based e-voting system is compatible with German law. Relevant for this question are in particular art. 38 paragraph 1 of the German constitution (hereinafter: «GG»)[16] and its interpretation by the constitutional court, and the Bundeswahlgesetz («Federal Election Law»)[17] which specifies the principles laid down in the constitution.

3.1. Art. 38 Grundgesetz

Art. 38 GG stipulates the basic principles for elections in Germany. In paragraph 1 it states:

«*Members of the German Bundestag shall be elected in general, direct, free, equal and secret elections. They shall be representatives of the whole people, not bound by orders or instructions, and responsible only to their conscience.*»

Corresponding regulations can be found in all state constitutions («Landesverfassungen»).[18] It is generally acknowledged that art. 38 paragraph 1 GG, furthermore, implies the publicity of the election.[19] This means that the voters have the right to get informed about the lawfulness of the electoral process.[20] All essential steps of this process including the voting itself and the determination of the final results have to be verifiable by the public.[21]

3.2. Judgement of the constitutional court

The interpretation of art. 38 paragraph 1 GG has been substantially specified by a judgement of the constitutional court of Germany concerning the use of voting computers during the federal elections 2002 and 2005.[22]

[13] Noizat, Blockchain Electronic Vote, in: Chuen, Handbook of Digital Currency, Elsevier, Amsterdam et al. 2015, p. 453 (460).

[14] See also European Parliamentary Research Service, What if blockchain technology revolutionised voting?, http://www.europarl.europa.eu/RegData/etudes/ATAG/2016/581918/EPRS_ATA(2016)581918_EN.pdf (accessed on 18 December 2016), September 2016.

[15] Some authors, however, argue that even the decentralisation is not vital as long as the immutability of the system can be ensured, see Pilkington, op. cit., p. 225 (234) with further references.

[16] Grundgesetz für die Bundesrepublik Deutschland, Federal Law Gazette no. 1/1949, p. 1, 23 May 1949.

[17] Bundeswahlgesetz, Federal Law Gazette part I no. 21/1956, p. 383, 9 May 1956.

[18] See, for example, art. 31 paragraph 1 of the constitution of Northrhine-Westphalia: «Members of parliament shall be elected in general, direct, free, equal and secret elections.»

[19] Butzer, Art. 38 GG, in: Epping/Hillgruber, Beck´scher Online Kommentar Grundgesetz, Beck, Munich, 30th edition 2016, recital 79 with further references. See also section 31 Bundeswahlgesetz.

[20] Ibid.

[21] Ibid.

[22] BVerfGE 123, p. 39.

In 2005, about 2 million voters used electronic voting machines of the Dutch manufacturer Nedap.[23] Here, a software program guided the voter through the electoral process. The vote was saved electronically and after every vote the machine needed to be unlocked by a supervisor for the next voter.[24] The machine saved all relevant information about the individual vote on a hard drive, the so-called digital ballot-box, which was located inside the machine and sealed.[25] The analysis of the results was conducted by the system through an internal process. At the end, a datasheet with the final results could be printed out by an integrated printer.[26]

The court came to the conclusion that the regulation that allowed the use of the voting computers («Bundeswahlgeräteverordnung»/«Federal Voting Machine Regulation») was incompatible with art. 38 paragraph 1 GG for the following reasons: The regulation permitted the use of voting machines which did not allow the voter or the supervisor at the polling station to verify that each individual vote had been registered and counted properly.[27] The judges emphasized that the exclusively machine-internal analysis of the count was also a violation of art. 38 paragraph 1 GG with regard to the publicity-criterion, the printable sheet notwithstanding. Hence, the regulation was declared void, and with that the use of all voting machines that shared the problematic features of Nedap impossible.

Importantly though, the court made it clear that the decision did not mean a general ban of e-voting systems. Indeed, it gave some examples of possible technical solutions compatible with the requirements of art. 38 paragraph 1 GG. Consistent with the constitutional requirements could be, for instance, a system which printed out a summary for the voter that allowed them to validate instantly the correct recording of their digital vote.[28] This paper sheet could also be used for any post-electoral controls.[29] Another possibility could be to record a «classical» paper-based vote by a digital pen whose data could be used for the verification of the results afterwards. At the same time, the court pointed out that this enumeration was not meant to be exhaustive.[30]

3.3. Bundeswahlgesetz

Art. 38 of the German constitution finds a further concretization in the Bundeswahlgesetz whose section 35 permits the use of voting machines. Its paragraph 3 empowers the Ministry of the Interior to adopt regulations like the aforementioned «Bundeswahlgeräteverordnung» to lay down further details.

3.4. Discussion

Every electoral system has to balance conflicting demands. We discussed above the inevitable tension between integrity (only eligible voters vote, and only once) with secrecy of the ballot. German law adds several other, equally conflicting demands: The election is *general*, which means registration and verification must not be too burdensome. In particular, choice of voting methods should not disadvantage one social group over another. One reason for e-voting has traditionally been to fight decreasing participation rates in elections, enabling people to vote who at present may feel excluded. The more inclusive however the process, the greater the danger for the integrity of the election. The election has also to be *public* and *transparent* – it is not enough that de facto, only eligible voters vote and their vote is counted correctly, it is also necessary that this is seen to be done – through a public vote that can be checked for correctness after the event. This requirement obviously clashes with the ideal of a secret ballot. The most transparent and public form of election – raising your hands

[23] Will, Neue Zeitschrift für Verwaltungsrecht 2009, p. 700 (700).

[24] BVerfGE 123, p. 39 (41).

[25] Ibid.

[26] Ibid.

[27] BVerfGE 123, p. 39 (85).

[28] Cf. Henning/Budurushi/Volkamer, Elektronische Wahlen durch Stimmzettelbelege? Untersuchung möglicher Umsetzungen des Öffentlichkeitsgrundsatzes, Multimedia und Recht 2014, p. 154 (155).

[29] BVerfGE 123, p. 39 (73).

[30] BVerfGE 123, p. 39 (74).

(or, in Switzerland, your sword) at the market square optimises publicity and transparency, but at the expense of secrecy. Different types of election may require to find different ways to balance these requirements, taken also account of costs and effort. The German constitution lays down which values must be considered and protected, and the Constitutional Court in interpreting art. 38 laid down some benchmarks that indicate «outer limits» for optimising some values at the expense of others. Moving from a solely physical voting system to one that combines e-voting and physical voting will inevitably shift the balance between the competing values that jointly make an election fair. The question is therefore not if the introduction of e-voting changes the balance between these competing values – it inevitably will – but if it impacts on some values negatively to such a degree that it is not any longer acceptable. In the next section, we will show how blockchain based voting changes the balance between these competing interests, and also argue that these changes still remain within the scope of «permissible balancing» under German electoral law.

4. Compatability of blockchain-based e-voting systems with the German law

4.1. Publicity of the election

This first criterion in this context is the requirement of «publicity». As we saw, according to the interpretation of the Constitutional Court, every e-voting system has to be equipped with a function for the voter to verify that their vote was counted.

A blockchain-based voting machine or platform has no difficulties to fulfil this criterion. As we saw, transparency is indeed one of the main characteristics of the technology. As exemplified by the «followmyvote» system, every voter can validate that their «transaction», in this case the casting of the vote, has been processed successfully. «Followmyvote» has also incorporated a printing mechanism to allow also paper-based confirmations. After the digital ballot boxes have been closed, every single voter has access to the blockchain and the information gathered there.

Hence, in this regard, any comparable system can fulfil the central demands of the constitutional court concerning the publicity of the election. Technologically, it can be ensured that every voter can check individually if their vote was counted. In fact, the blockchain technology makes it possible to go even beyond the court´s demands by granting access to the ballot box to everyone.

4.2. Secrecy of the election

Transparency though as we argued conflicts potentially with secrecy. Secrecy of the ballot ensures the freedom from any influence by the state or third parties.[31] Not even the voter can waive the secrecy requirement.[32] We saw above that in some aspects, blockchain based e-voting can enhance secrecy in comparison to physical voting. However, as soon as voters operate from internet-connected devices, the question arises how their identity can be effectively hidden to meet the requirement of secret voting. Here, the blockchain with its high level of transparency and traceability poses some technical challenges.

As seen, «followmyvote» makes use of a complex system of identity verification on the one hand and registration on the other hand, which together with encryption obscure the voter´s identity. This means that nowhere in the ledger, information is held that would allow identification of who casts a specific vote, not even for the registrar who issued the election token. However, the very process of casting the vote can still present problems, if done through a web-based application. This enables, at least in theory, different institutions like the Internet Service Provider or the operator of the election software that the voter uses, to trace back the vote and, finally, determine the internet access used. In most cases, this would allow public institutions to get the voter´s identity.

[31] Klein, Art. 38 GG, in: Maunz/Dürig, Grundgesetz Kommentar, Beck, Munich 2016, recital 110, 111; Henning/Volkamer/Budurushi, Transparentes e-voting, Die öffentliche Verwaltung 2012, p. 789 (794).

[32] Klein, ibid. This means that in Germany, taking a «selfie» while casting the vote would be illegal.

There are 3 possible answers to this challenge. First, we note that as discussed above, a determined Wahlhelfer could, also in the physical booth, «hack» the system. The effort would be considerable, it would involve conspiring with several parties, and the punishment, if caught, severe. The same situation exists in the case of e-voting: it would require considerable effort, require collusion of several parties, and carry the same punishment to trace back the IP address of a voter and link it with their vote. What changes though is the potential scale of such an attack and with that the benefits for the attacker. A single Wahlhelfer could only ever hope to gain access to a few votes, while collusion of an ISP could give the attacker thousands or more IDs. This could make this type of attack more attractive.

Second, if this risk is deemed unacceptable, it would be possible to use technology other than the blockchain proper to protect this aspect of voting. What would be required is a mechanism to anonymize the IP-address, for example, the use of the TOR network.[33] Such a measure would potentially impact on the generality of the vote, making it more cumbersome and possibly requiring a certain degree of technical knowledge by the voter. If this too was deemed unacceptable, then operating from computers that reside physically in the polling stating would be another option, but one that again would mean that a key objective of e-voting, increased participation and with that generality of the vote, would be unlikely to be fulfilled.

4.3. Further general security considerations

All the criteria mentioned in art. 38 paragraph 1 GG, which make the election a democratic election, are potentially endangered if the system in use is vulnerable. The consensus-based transaction assurance of the blockchain technology promises a very high degree of security. This consensus building in turn is achieved through the «mining» process mentioned above. Only in a decentrally organised system consisting of many different users, the security can be granted. In case a single entity represents more than 50% of the whole network, the risk of manipulations and fraud increases dramatically.[34]

Hence, there must be an incentive for the users to participate in the «mining» – maintaining the integrity of the electoral process become a civic role for all. Since this comes along with costs for electricity, it can be doubted that even the conscientious citizen will do this for the purpose of free and democratic elections only. Participation could be incentivised, through e.g. tax reductions or a nominal fee of the type a Wahlhelfer currently gets, or through a general legal duty.

4.4. Compatability with section 35 Bundeswahlgesetz

Section 35 of the Bundeswahlgesetz establishes, in concretization of art. 38 paragraph 1 GG, the further rules for the use of voting machines which can be used instead of ballots and ballot boxes.

Here, the question arises of what device falls under the definition of a «Wahlgerät» (voting machine). As the wording of «Wahlgerät», i.e. voting machine, or the term «Bauart», i.e. the construction type[35], already implies, when adopting this provision, the legislator primarily thought of fixed single-purpose machines in the polling stations (like the Nedap voting machines) rather than of software-based solution like blockchain that runs on a variety of multi-purpose domestic devices. At the time of the adoption of section 35 in the year 1999, it was probably hard to imagine to use Internet-based portable devices to vote. However, the used expression «Gerät»/«machine» does not necessarily exclude portable solutions. Thus, the use of the blockchain e-voting software on fixed desktop computers located in the polling stations would be covered by the provision in

[33] For a detailed description of the functioning of the TOR network see, for example, Watson, The TOR Network: A Global Inquiry, Washington University Global Studies Law Review 2012, p. 715 (719).

[34] This is called the 51%-problem, see, for example, Heires, The Risks and Rewards of Blockchain Technology, Risk Management, March 2016, p. 4 (7).

[35] See section 35 paragraph 3, no 1 Bundeswahlgesetz.

any case. The use on mobile devices or computers at home would, arguably, be covered.[36] Nonetheless, a clarification in the regulation itself would helpful to avoid any uncertainties.

4.5. Conclusion

Generally, a blockchain-based e-voting system could fulfil the tough requirements the constitutional court of Germany has set up for the use of voting machines because it allows the voter to validate the vote.[37] However, a well-working «mining» system is vital for the security and reliability. Examples from Denmark show that the system generally works.[38]

Systems, which combine the digital electoral process with the printout of a paper which then needs to be interpreted afterwards by the counting staff, might be the safest approach, and the constitutional court might have been originally in favour of their use.[39] But this technology contravenes the original purpose of e-voting, namely to reduce the bureaucratic burden for the public. A paperless and mobile system should be preferred.

5. Summary and outlook

The authors could demonstrate that the use of corresponding systems like «followmyvote» is generally consistent with German law, although the authors recommend an amendment of s. 35 of the Bundeswahlgesetz. However, the discussion also *only* showed that even though different democratic values are enhanced or impacted on differently by blockchain-based solutions, this remains within the parameters given by the German constitution and the Constitutional Court. What this paper did not do was to ask if these parameters are in the light of new technologies *sensible* ones. Our main claim was that ever electoral system is with necessity a compromise between several values, further constrained by affordability and practicability. Blockchain voting could also add functionality that currently has no counterpart in traditional voting (for instance the possibility of the Followmyvote system to change a vote if done before the closing date – thus addressing a fear voiced in the US election that the significant number of early postal voting meant a disengagement from the on-going political debate and encouraged partisan voting). Even more radically, supporters of the so-called «fluid democracy» endorse the use of blockchain e-voting for a much more radical change of the current system towards a model in which almost every essential public question will be decided by the citizens, using devices which can allow a quick and unbureaucratic voting and a transfer of voting rights to another person.[40]

This paper did not try to answer the legal implications or societal benefits of such a use of the blockchain, but neither should our claim of the compatibility of blockchain-based e-voting with current law preclude a debate on whether our law is still fit for the technological age.

[36] Different opinion: Hahlen, § 35 Bundeswahlgesetz, in: Schreiber, Bundeswahlgesetz, 9th edition, Carl Heymanns, Cologne 2013, recital 6.

[37] See also Seedprf, Germany: The Public Nature of Elections and its Consequences for E-Voting, in: Barrat/Maurer, E-Voting Case Law: A Comparative Analysis, New York 2016, p. 23 ff.

[38] Shanavelt, Danish political party adopts blockchain-based system for internal voting, http://www.bitcoinx.com/danish-political-party-adopts-blockchain-based-system-for-internal-voting (accessed on 18 December 2016), 22 April 2014; Daniel, Blockchain Technology: The Key to Secure Online Voting, Bitcoin Magazine, https://bitcoinmagazine.com/articles/blockchain-technology-key-secure-online-voting-1435443899 (accessed on 18 December 2016), 27 June 2015.

[39] See Henning/Budurushi/Volkamer, op. cit., p. 154 (155) for further examples of systems which print out a so-called «Voter Verifiable Paper».

[40] Daniel, op. cit..