**Stanford – Vienna**
**Transatlantic Technology Law Forum**

A joint initiative of
Stanford Law School and the University of Vienna School of Law

# TTLF Working Papers

**No. 49**

## The Limits of Blockchain Democracy: A Transatlantic Perspective on Blockchain Voting Systems

**Yoan Hermstrüwer**

**2020**

# TTLF Working Papers

**Editors: Siegfried Fina, Mark Lemley, and Roland Vogl**

**About the TTLF Working Papers**

TTLF's Working Paper Series presents original research on technology-related and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

## About the Author

Yoan Hermstrüwer is a Senior Research Fellow at the Max Planck Institute for Research on Collective Goods in Bonn, Germany. Prior to his academic career, he passed the First State Exam (J.D. equivalent) and the Second State Exam (bar exam equivalent). From 2014 to 2016, he worked as a law clerk in Germany, South Korea, and at the World Bank in Washington, D.C. He received a Licence en droit (LL.B. equivalent) from Université Panthéon-Assas (Paris 2) and a Ph.D. from the University of Bonn. During his doctoral studies, he was a Visiting Researcher at Yale Law School. His research focuses on technology law, administrative law, constitutional law, matching markets, auctions, (experimental) law and economics, and empirical legal studies. Yoan has been a TTLF Fellow since 2018.

## Acknowledgements

My thanks to Jens Frankenreiter, Justin McCrary, Krishna Gummadi, and the participants of the 2018 International Seminar on the New Institutional Economics in Florence (JITE 2018). All errors are mine alone.

## General Note about the Content



## Suggested Citation

This TTLF Working Paper should be cited as:
Yoan Hermstrüwer, The Limits of Blockchain Democracy: A Transatlantic Perspective on Blockchain Voting Systems, Stanford-Vienna TTLF Working Paper No. 49, http://ttlf.stanford.edu.

## Copyright

**Abstract**

Should political elections be implemented using blockchain technology? Blockchain evangelists have argued that it should. This article sheds light on the potential of blockchain voting procedures and the legal constraints that need to be accommodated. I first identify the upsides of the distributed ledger technology and the normative principles guiding electronic voting systems. Specifically, I elucidate some of the major normative constraints for blockchain voting systems in a transatlantic comparison of U.S. and German constitutional law. I then discuss the technological, economic and normative limitations of blockchain voting procedures. On the one hand, these limitations result from the rules and incentives set by different consensus mechanisms. On the other hand, it is far from clear whether blockchain technology provides sufficient safeguards to ensure identity verification, the secrecy of ballots, and a verification that ballots are cast as intended, recorded as cast, and counted as recorded. Building on principles from constitutional law, I contend that blockchain technology may not provide sufficient safeguards to satisfy the requirements of democratic voting procedures, at least not in the near future.

**Table of Contents**

Introduction ..... 1
I. Blockchain Democracy ..... 5
A. A Problem and a Solution ..... 5
1. Vulnerable Voting ..... 5
2. Blockchain Voting ..... 8
B. Principles of Election Law ..... 10
1. United States ..... 10
2. Germany ..... 13
C. Principles of Cryptoeconomics ..... 15
1. Blockchain Mechanism Design ..... 16
2. Distributed Ledger Technology ..... 18
II. The Virtues ..... 23
A. Immutability ..... 23
B. Political Equality ..... 26
C. Quadratic Voting ..... 28
III. The Limits ..... 31
A. Ensuring Integrity ..... 32
1. Eligibility ..... 32
2. Inclusion ..... 36
3. Accuracy ..... 38
B. Preserving Privacy ..... 46
1. Polling Secrecy ..... 46
2. Ballot Secrecy ..... 49
3. Political Privacy ..... 50
C. Creating Legitimacy ..... 54
1. Procedural Justice ..... 54
2. Trust ..... 57
3. Transparency ..... 60
4. Sovereignty ..... 62
Conclusion ..... 64

## INTRODUCTION

Since its inception, democracy has been organized through centralized entities, such as the nation state or corporations. As Winston Churchill famously stated, “democracy is the worst form of government except for all

those other forms that have been tried from time to time."[1] One of the core challenges in organizing democratic procedures is to determine mechanisms that enable a sound aggregation of political preferences without falling prey to the temptation of overriding the citizens will through the use of money and the abuse of power. Each citizen should have the right to resist corruption and the abuse of power, a republican idea that features prominently in James Madison's writings.[2] Sound voting procedures and competitive elections are fundamental predicates of democracy, providing bulwarks against authoritarian lapses and subtler forms of institutional erosion.[3]

An obvious reason for citizens' discontent with democracy is that the costs of voting usually exceed the expected benefits. Given that the probability of being pivotal is close to zero and that voting can be cumbersome, self-interested or rational voters should be expected to refrain from casting a ballot - a theory that explains what is usually referred to as the *paradox of voting*.[4] These weaknesses are exacerbated by the fact that paper-based elections, especially the ballot counting procedures, are laborious and vulnerable to human errors. Moreover, both traditional voting procedures and electronic voting systems are sometimes considered as being intransparent and not sufficiently exposed to public scrutiny. Voters may therefore feel that electoral processes are rigged and distrust the voting procedures used to produce political outcomes. A particularly worrisome problem is that less affluent voters and minorities are increasingly disconnected from electoral processes, which eventually results in what has been coined as *vote dissociation*.[5] These weaknesses might explain why many citizens lapse into voter apathy or, worse, turn their back on the idea of democracy and the procedures used to elicit the people's political will.[6]

Blockchain evangelists claim that blockchain technology is likely to cure these maladies.[7] Blockchain technology, they argue, makes it closely

---

[1] Winston S. Churchill, 444 Parl. Deb., H.C., 5th ser. (1947), https://winstonchurchill.org/resources/quotes/the-worst-form-of-government/.

[2] The Federalist No. 10, The Federalist: A Collection of Essays, Written in Favour of the New Constitution, as Agreed upon by the Federal Convention, September 17, 1787. Also see Samuel Issacharoff, *On Political Corruption*, 124 HARV. L. REV. 118 (2010).

[3] See Aziz Huq & Tom Ginsburg, *How to Lose a Constitutional Democracy*, 65 UCLA L. REV. 78, 86 et seq. (2018).

[4] ANTHONY DOWNS, AN ECONOMIC THEORY OF DEMOCRACY (1957).

[5] Daniel P. Tokaji, Vote Dissociation, 127 Yale L. J. F. 761 (2018).

[6] In 2016, only 28.5 % of eligible voters participated in the Republican and Democratic presidential primaries, see Jane Susskind, *Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System*, 54 SAN DIEGO L. REV. 785, 788 (2017).

[7] Matthew Daniel, *Blockchain Technology: The Key to Secure Online Voting*, Bitcoin Magazine (Jun 27, 2015), https://bitcoinmagazine.com/articles/blockchain-technology-key-

impossible to tamper with ballots and tinker with the results of the voting procedure, thus increasing the accuracy of the voting procedure.[8] The distributed consensus protocols implemented on the blockchain are believed to decentralize the electoral process and provide additional safeguards against centralized interventions into the voting procedure by malicious entities, including the government.[9] Blockchain technology, the argument further goes, would simplify, accelerate and increase the transparency of voting procedures.[10] The concomitant gains in trust are believed to cure the maladies of voter apathy and low voter turnouts, thus eventually revitalizing participation and paving the way for inclusive democratic systems.[11] But are the proponents of blockchain voting procedures right?

In this article, I argue that the rosy view of blockchain technology as an enabler of truly democratic and decentralized voting procedures is misplaced or, at the very least, overblown. The main reason for embracing a good dose of skepticism is that the blockchain rests on vulnerable collective choice mechanisms and dubious technical safeguards. The adequacy of these mechanisms is often not assessed on the basis of sound theoretical claims, but rather on intuitions about the drivers of trust, transparency, decentralization, and the guarantee of political equality. More specifically, blockchain technology is not designed so as to satisfy the stringent demands for voting procedures enshrined in constitutional and human rights law.

In most democratic societies, constitutional law requires transparent voting procedures. Transparency, in that sense, demands that each step of the voting procedure be subject to public scrutiny - a requirement that is usually considered as one of the most important conditions of

---

secure-online-voting-1435443899; Philip Boucher, *What if blockchain technology revolutionised voting?*, Scientific Foresight Unit (STOA), European Parliamentary Research Service (EPRS), September 2016 - PE 581.918; Ahmed Ben Ayed, *A Conceptual Secure Blockchain-Based Electronic Voting System*, 9 INT. J. NETW. SEC. & APPL. 1 (2017); Baocheng Wang et al., *Large-scale Election Based on Blockchain*, 129 PROC. COMP. SCI. 234 (2018).

[8] Desmond Johnson, *Blockchain-Based Voting in the US and EU Constitutional Orders: A Digital Technology to Secure Democratic Values?*, 10 EUR. J. RISK REG. 330 (2019). In the context of voting in corporate elections, see George S. Geis, *Traceable Shares and Corporate Law*, 113 NW. UNIV. L. REV. 227 (2018); David Yermack, *Corporate Governance and Blockchains*, 21 REV. OF FINANCE 7, 23 et seq. (2017); MICHÈLE FINCK, BLOCKCHAIN REGULATION AND GOVERNANCE IN EUROPE, 30-31 (2019).

[9] On this point, see generally Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359 (2016).

[10] Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, Working Paper (2015), 1, 36 et seq.

[11] Desmond Johnson, *Blockchain-Based Voting in the US and EU Constitutional Orders: A Digital Technology to Secure Democratic Values?*, 10 EUR. J. RISK REG. 330 (2019).

trustworthiness. Trustworthiness, both of the voting procedure and its outcome, are core prerequisites of legitimacy. Voting procedures, moreover, have to provide safeguards to enable free and equal elections that preserve the secrecy of the ballot. These requirements are both enshrined in various constitutions and human rights treaties, including Art. 25(b) of the International Covenant on Civil and Political Rights and Art. 3 of Protocol No. 1 to the European Convention on Human Rights.[12] Finally, voting procedures have to guarantee integrity and reliability. This means that they should not impinge on ballot secrecy or political privacy, that none of the procedural steps should be subject to undue influence, and that the outcome and ballot count should accurately reflect the political preferences the voters held before making up their mind to participate in the election.

Depending on the consensus mechanisms used to validate votes and the procedures used to govern the blockchain, there is a risk that blockchain voting procedures will fall prey to the abuse of power and money.[13] Neither the incentives set by the consensus protocols nor the technical safeguards seem sufficient to guarantee the integrity of the voting procedure. While blockchain technology does not grant a sufficient level of *publicity* with respect to some parts of the voting procedure, it cannot grant sufficient *secrecy* with respect to other parts. The resulting imbalance between publicity and secrecy carries the risk of undermining the verification of voter identities, the verification of ballots, and the prevention of coercion. Even if blockchain technology were to bolster the integrity of the voting procedure, it is not clear whether the decrease of voting costs associated with a shift from offline to online polls would be strong enough to overcome the problem of low voter turnouts.[14]

The objective of this article is not to argue that blockchain democracy is a senseless idea. Blockchain technology is not just an object of governance and regulation; it is a mode of governance. As such, it is likely to change, perhaps revolutionize public decision-making procedures. And in theory, it has several virtues that democratic voting procedures require. Moreover,

---

[12] See European Court of Human Rights, Guide on Article 3 of Protocol No. 1 to the European Convention on Human Rights: Right to free elections (Apr 30, 2019), https://www.echr.coe.int/Documents/Guide_Art_3_Protocol_1_ENG.pdf. Whether these treatment obligations are effective is an empirical question that goes beyond the scope of this article. See, e.g., Kevin L. Cope, Cosette D. Creamer & Mila Versteeg, *Empirical Studies of Human Rights Law*, 15 ANNU. REV. LAW SOC. SCI. 155 (2019).

[13] Yoan Hermstrüwer, *Democratic Blockchain Design*, 175 J. INST. & THEORETICAL ECON. 163 (2019).

[14] Anthony Fowler, *Promises and Perils of Mobile Voting*, Working Paper, Harris School of Public Policy, University of Chicago (2019), 1, finds that the mobile voting experiment conducted in West Virginia in 2018 increased voter turnout by 3 to 5 percentage points.

blockchain democracy, like any other electronic voting system, comes in many flavors: Elections can be implemented in the open internet or in a private network. They might allow for remote voting using portable devices, such as smartphones, or they might require voters to attend a polling place and cast their vote in a physically secluded voting booth. Blockchain technology may be used to count electronic ballots or paper ballots. The counting process may be the only electronic step in the voting procedure or it may be part of an entirely electronic voting procedure. It is well beyond the scope of this article to analyze all the strengths and weaknesses of blockchain voting procedures in all their shades. Rather, I contend that much of the hope placed in completely decentralized electronic voting procedures is misguided and based on erroneous assumptions about the underlying technology, its cryptoeconomic properties, and how the blockchain allocates power.

The remainder of this article is organized as follows. Part I sheds light on blockchain voting, on the constitutional principles determining its use in the United States and Germany, and on the cryptoeconomic principles that blockchain technology is based on. In Part II, I discuss what I consider to be the main virtues of blockchain technology in the context of general political elections. In Part III, I provide an account of the core limitations of blockchain voting procedures in light of constitutional principles. The final part concludes.

## I. BLOCKCHAIN DEMOCRACY

### *A. A Problem and a Solution*

Modern democracies do not only suffer from voter apathy and low voter turnout. They are also subject to vulnerabilities, such as manipulation and errors, that hamper the integrity of both the voting procedures and the outcomes they generate. Blockchain technology is considered as a suitable technology to mitigate these concerns and has been used in several political elections across the United States and European countries.

#### 1. Vulnerable Voting

Citizens, not just in the United States but also in many European countries, feel that the political system and the way that public goods are provided by governments do not adequately reflect their preferences. Voter apathy is not the cause of this increasing frustration, but rather the symptom

of a deeper underlying crisis and a loss of trust in the integrity of public decision making procedures, including political elections. This trust loss may be due to the perception that existing voting procedures are rigged or vulnerable to the falsification of voting outcomes.[15] Even in countries with stable institutions, the recent history of political elections testifies of how vulnerable voting procedures are.

In Germany, for example, several votes cast for the Alternative für Deutschland (AfD), a populist right-wing party, were declared as invalid in recent elections.[16] More prominently, the vote count dispute in the 2000 U.S. presidential elections raised fundamental concerns about the reliability and accuracy of voting technologies, not just in Florida but in the United Sates generally.[17] In the aftermath of the electoral dispute, political scientists estimated the impact of voting technologies on residual votes, that is the difference between the number of voters who appeared in polling places and the number of ballots counted on Election Day.[18] Voting technologies, political science suggests, have a strong effect on residual votes in presidential elections, with an average of 2.3 % between 1988 and 2000.[19]

Election security remains at the core of political debates after the alleged Russian interference in the 2016 U.S. presidential election to harm Hillary Clinton and support Donald Trump.[20] Russian agents allegedly launched attacks on the voting infrastructure in more than twenty States and successfully intruded computer systems in a handful of States.[21] While it remains unclear whether these tampering attempts were successful, there is increasing evidence that the electronic voting infrastructure used in thirteen States is highly vulnerable to hacking and does not provide any voting

---

[15] See, e.g., Marc Hooghe, *Trust and Elections, in* Eric M. Uslaner (ed.), The Oxford Handbook of Social and Political Trust, 617, 620 (2018).

[16] Spiegel Online, AfD-Stimmen fälschlicherweise für ungültig erklärt (May 19, 2017), https://www.spiegel.de/politik/deutschland/wahlpanne-in-nrw-afd-stimmen-falsch-ausgezaehlt-a-1148535.html.

[17] Corporate elections suffer from similar inaccuracies, and outcomes that are closer than 55 % to 45 % do not seem to allow for a clear determination of the winner of the election, see David Yermack, *Corporate Governance and Blockchains*, 21 REV. OF FINANCE 7, 23 (2017).

[18] Stephen Ansolabehere & Charles Stewart III, *Residual Votes Attributable to Technology*, 67 J. OF POLITICS 365 (2005).

[19] Stephen Ansolabehere & Charles Stewart III, *Residual Votes Attributable to Technology*, 67 J. OF POLITICS 365, 374 (2005).

[20] Robert S. Mueller, III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election (Mueller Report)*, U.S. Department of Justice (Mar 2019), https://www.justice.gov/storage/report.pdf.

[21] Jane Susskind, *Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System*, 54 SAN DIEGO L. REV. 785, 796 (2017).

record or paper trail that can be reliably audited in the post-electoral phase.[22]

These concerns are corroborated by a vast amount of evidence.[23] More than forty States keep using electronic voting machines that are more than ten years old or that are not manufactured any more.[24] These technologies are highly vulnerable, and hackers meeting at the annual DefCon conference provide a vivid illustration. Rather than competing over *whether* they can hack voting machines, they organize a contest over *how fast* they can do so.[25] Against this backdrop, it does not come as a surprise that the election administration in Virginia had to decertify 3000 WINvote machines before the 2016 U.S. presidential election and reverted to paper ballots.[26]

The vulnerabilities of electronic voting procedures pose a serious threat to the comprehensiveness, inclusiveness, and integrity of the voting procedure, thereby impeding trust as a central prerequisite of legitimacy. On the one hand, hacks can target ballots once they have been cast, for example by manipulating the software used by polling places or ballot counting facilities. On the other hand, hacks can be intended to suppress votes and block voters from exercising their right to vote, for example by manipulating voter registries or electronic poll books. The resulting manipulations can severely curtail the access to votes for minorities and disenfranchised groups, thus perversely reinforcing social and racial discrimination.[27]

---

[22] Wendy Weiser & Max Feldman, *The State of Voting 2018*, Brennan Center for Justice, New York University School of Law, 2018, 1, 2 et seq.; Lawrence Norden & Wilfred U. Codrington III, *America's Voting Machines at Risk: An Update, Brennan Center for Justice*, New York University School of Law (2018), 1. Estonia was the first country in the world to use electronic voting for national elections in 2005. As of now, almost a third of votes is cast electronically during Estonian elections, see Sven Heiberg et al., *Improving the Verifiability of the Estonian Internet Voting Scheme, in* Robert Krimmer et al. (eds.), Electronic Voting, First International Joint Conference, E-Vote-ID 2016, Bregenz, Austria, October 18-21, 2016 Proceedings, 92.

[23] Deven R. Desai & Joshua A. Kroll, *Trust But Verify: A Guide to Algorithms and the Law*, 31 HARV. J. L. TECH. 1, 14-15 (2017); U.S. Vote Foundation, *The Future of Voting: End-to-End-Verifiable Internet Voting* (2015), https://www.usvotefoundation.org/sites/default/files/E2EVIV_full_report.pdf.

[24] Lawrence Norden & Wilfred U. Codrington III, *America's Voting Machines at Risk: An Update*, Brennan Center for Justice, New York University School of Law (2018), 1.

[25] Ciara Torres-Spelliscy, Election Security Lessons from DEFCON 27 (August 20, 2019), https://www.brennancenter.org/blog/election-security-lessons-defcon-27. For background information on DefCon, see https://www.defcon.org/index.html.

[26] Jane Susskind, *Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System*, 54 SAN DIEGO L. REV. 785, 795 (2017).

[27] Jane Susskind, *Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System*, 54 SAN DIEGO L. REV. 785, 790 et seq. (2017); Desmond Johnson, *Blockchain-Based Voting in the US and EU Constitutional Orders: A Digital*

While these vulnerabilities are now widely acknowledged, neither legislators nor the U.S. Supreme Court have been very active in safeguarding equal protection with respect to the right to vote. The Court's decision about the constitutionality of Sections 5 and 4(b) of the Voting Rights Act in *Shelby County v. Holder* has been interpreted as an illustration of the rampant erosion of equal protection standards in the electoral context.[28] The challenged provisions of the Voting Rights Act require States with a history of voter discrimination to receive federal approval before modifying voting practices, a process known as preclearance. The Supreme Court struck down Section 4(b), thus rendering Section 5 inoperable. As a consequence, it is now much more difficult to challenge electoral practices that impede participation by and representation of disenfranchised groups. The result is a weakened protection against discriminatory voting practices and a dilution of the right to vote.[29]

2. Blockchain Voting

Bitcoin was the first application of blockchain technology and remains the most widely used. In the legal sphere, the most prominent application of blockchain technology is the execution of contractual obligations through smart contracts.[30] The most important blockchain platform enabling smart contracts is Ethereum. Ethereum, the intellectual child of computer scientist Vitalik Buterin, performs Turing-complete computations, which implies that computer programs running on conventional computers can also be run on a distributed computer.[31] Rather than relying on courts and the enforcement of contractual obligations using government power, smart contracts rely on distributed consensus. Of course, such a system is subject to important limitations, especially when contracts are incomplete, when contractual terms are vague, or when a contractual obligation depends on a condition.[32]

---

*Technology to Secure Democratic Values?*, 10 EUR. J. RISK REG. 330, 343 (2019).

[28] Shelby County, Alabama v. Holder, 570 U.S. 2 (2013).

[29] Daniel P. Tokaji, *Responding to Shelby County: A Grand Election Bargain*, 8 HARV. L. & POL. REV. 71 (2014).

[30] Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets*, 16 EXTROPY: J. TRANSHUMANIST THOUGHT 1 (1996); Richard Holden & Anup Malani, *Can blockchain address the problem of holdup in contracts?*, Coase-Sandor Working Paper Series in Law and Economics, No. 846 (2017), 1.

[31] Vitalik Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform*, White Paper (2019), https://github.com/ethereum/wiki/wiki/White-Paper; Kevin Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L. J. 489, 506-509 (2018).

[32] The assessment whether a condition has been met can be performed by a third party oracle, and the permission to validate the transaction can then be given once the oracle has

These limitations notwithstanding, blockchain technology has also been used to organize political elections since 2015. A Danish party, the Liberal Alliance, was one of the first political entities to use the blockchain for internal elections.[33] Similar experiments have been conducted in other countries including Switzerland, Sierra Leone, where the blockchain technology offered by Agora was used to tally paper ballots in the presidential election, and Colombia, where Democracy Earth offered Colombian expats a means to participate in a plebiscite on the peace treaty between the Colombian government and the FARC (Fuerzas Armadas Revolucionarias de Colombia).[34]

One objective of these experiments with blockchain voting procedures is to establish more dynamic participatory processes, such as liquid democracy. Under liquid democracy, a hybrid of direct and indirect democracy, voters are constantly involved in the process of voting on specific issues.[35] Yet to prevent the risk of voter exhaustion, voters can decide to delegate decisions if they do not feel like voting themselves. Experiments with liquid democracy have been implemented both by the Pirate party in Germany and by the Democracy Experiment (Demoex) in Sweden.

Recently, blockchain voting procedures have also gained traction in the United States. Voatz, a blockchain-based voting app, for example, was used in the 2018 West Virginia Primary Elections, the 2018 West Virginia Midterm Elections, the 2019 City/County of Denver Municipal General Elections, and the 2019 City/County of Denver Municipal Runoff Elections.[36] Smartmatic-Cybernetica was used in the 2016 Utah GOP

---

formally confirmed the condition. See, e.g., Jens Frankenreiter, *The Limits of Smart Contracts*, 175 J. INST. & THEORETICAL ECON. 149 (2019); Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 362 (2016).

[33] Igor Chepkasov, *Blockchain allows protecting the election from fraud*, Medium (Oct 18, 2017), https://medium.com/boulecoin/blockchain-allows-protecting-the-election-from-fraud-2a0cac9625b7.

[34] On the Colombian use case, see OECD, *Embracing Innovation in Government: Global Trends* (Feb 2017), 80-83, https://www.oecd.org/gov/innovative-government/embracing-innovation-in-government-colombia.pdf; Desmond Johnson, *Blockchain-Based Voting in the US and EU Constitutional Orders: A Digital Technology to Secure Democratic Values?*, 10 EUR. J. RISK REG. 330, 337-338 (2019).

[35] Paul Gölz et al., *The Fluid Mechanics of Liquid Democracy, in* George Christodoulou & Tobias Harks (eds.), Proceedings of the 14th International Conference on Web and Internet Economics (WINE 2018), LNCS Vol. 11316 (2018), 188.

[36] See https://voatz.com/. For government information, see Larry Moore & Nimit Sawhney, *Under the Hood: The West Virginia Mobile Voting Pilot*, White Paper (2019), 1, https://sos.wv.gov/FormSearch/Elections/Informational/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf. For a critical assessment, see David Jefferson et al., *What We Don't Know About the Voatz "Blockchain" Internet Voting System*, White Paper (2019), 1.

Presidential Candidate elections.[37] Yet another blockchain technology deployed by the start-up Votem was used in Montana the same year.[38]

The common objective of these experimental implementations of blockchain voting procedures in the United States is to enable military personnel, their dependents, and other overseas voters to cast their ballot from abroad. To control the eligibility of voters and avoid impacts on the behavior of other voters, the service offered by Voatz uses biometric identity verification and shields the ballots against a public gaze until the end of Election Day. In addition, voters are given a unique hash that enables them to change their vote even once it has been cast (ballot spoiling). To ensure the integrity of the procedure, Voatz also allows post-electoral audits by the electoral administration. West Virginia has announced that it will expand the pilot project in the 2020 U.S. presidential elections.[39]

### *B. Principles of Election Law*

The right to vote is a building block of democratic societies. As such, it is firmly anchored in most constitutional texts, but its specific content chiefly results from the interpretation established by courts and grown into case law. This part sheds light on the constitutional principles uncovered by courts and now guiding the use of electronic voting technologies in the United States and in Germany.

#### 1. United States

The right to vote enshrined in the U.S. Constitution guarantees that each voter has an equal opportunity to express her political will and have her vote counted accurately. The right to vote therefore protects against restrictions diluting the weight of a citizen's vote or imposing a burden on eligible voters to cast their ballot effectively.[40] Moreover, under a majoritarian principle, the right to vote provides an individual guarantee that the electoral process is supported by mechanisms and safeguards to ensure that the candidate or party preferred by most voters wins the

[37] See https://www.smartmatic.com/.

[38] See https://votem.com/. Similar voting services are offered by several other blockchain platforms, including Democracy Earth Foundation, https://democracy.earth/; FollowMyVote, https://followmyvote.com/; Votebox, https://votebox.co/; or Securevote, https://secure.vote/.

[39] Emily Parker, *West Virginia Will Use Blockchain Voting in the 2020 Presidential Election. Why?*, Longhash (Apr 15, 2019), https://en.longhash.com/news/west-virginia-will-use-blockchain-voting-in-the-2020-presidential-election-why.

[40] Reynolds v. Sims, 377 U.S. 533, 555 (1964); Williams v. Rhodes, 393 U.S. 23, 30 (1968).

election. This means that each citizen is entitled to having her ballot counted once and having it protected against any kind of alteration or dilution through ballot box stuffing.[41]

These protections are supplemented by statutory law, notably the Voting Rights Act of 1965 and the 2002 Help America Vote Act adopted in the aftermath of the vote count showdown between George W. Bush and Al Gore in the 2000 presidential elections. In *Bush v. Gore*, the Supreme Court reiterated some basic principles of electoral integrity, emphasizing that "the State may not, by later arbitrary and disparate treatment, value one person's vote over that of another."[42] The voting procedure needs to minimize counting errors and it needs to make sure that remaining counting errors are equally distributed.

Initial attempts to enforce the equal errors standard established in *Bush v. Gore* were unsuccessful. In following legal disputes, the plaintiffs challenged the use of voting technologies that differed in accuracy across counties within one state and claimed a violation of the Equal Protection and the Due Process Clauses.[43] The disparate treatment associated was considered as justified on the grounds that States have wide discretion in assessing the trade-offs associated with voting technologies. This is in line with U.S. Supreme Court case law according to which courts do not apply strict scrutiny in cases pertaining to electoral administration matters unless state election law imposes and unreasonable or discriminatory burden on the right to vote and the state cannot claim any important regulatory interests.[44]

Courts are therefore reluctant to specify residual error rate thresholds beyond which a voting technology may be declared as unconstitutional.[45] In *Curling v. Kemp*, however, the District Court for the Northern District of Georgia held that the challenged direct-recording voting machine (a machine leaving no paper-trail) used in Georgia did not provide sufficient safeguards against being altered, diluted, or not effectively counted.[46] It is important to note that this decision was taken in the context of voting machines that were highly vulnerable to hacking and did not provide any possibility to verify the accuracy of the voting procedure based on paper ballots. Even if paper ballots were to be manually recounted in order to

---

[41] United States v. Saylor, 322 U.S. 385, 387-388 (1944); Gray v. Sanders, 372 U.S. 368, 380 (1963); Reynolds v. Sims, 377 U.S. 533, 555 (1964).

[42] Bush v. Gore, 531 U.S. 98, 104-105 (2000).

[43] Weber v. Shelley, 347 F.3d 1101, 1101, 1106 (9th Cir. 2003).

[44] Anderson v. Celebreze, 460 U.S. 780, 788 (1983); Burdick v. Takushi, 504 U.S. 428, 434 (1992).

[45] Stewart v. Blackwell, 444 F.3d. 843, 876 (6th Cir. 2006). For judicial decisions of lower courts, see Wexler v. Anderson, 452 F.3d 1226, 1233 (11th Cir. 2006).

[46] Curling v. Kemp, 334 F. Supp. 3d 1303, 1324-1325 (N.D. Ga. 2018).

verify the accuracy of the electronic counting procedure, the mere risk of errors in the manual counting procedure warrants neither strict scrutiny nor a declaration of unconstitutionality.[47] Nonetheless, legal scholars in the United States keep scorching the vulnerabilities of electronic voting machines.[48]

Despite the stinging critique of electronic voting procedures, a consistent overhaul of U.S. electoral law is rather unlikely, the main reason being federalism. According to Art. 1 § 4 of the U.S. Constitution regulating the voting procedure, including the time, place, and manner of elections, falls within the competence of state legislatures. The main limitation imposed by the federal constitution on state jurisdiction is that electoral rules may not infringe upon the right to vote.[49] As Jennifer Nou explains, "state primacy over electoral regulation, the lack of existing federal infrastructure to monitor elections nationally," and weak political are likely reasons why electoral administration is fragmented and weak, at least from the point of view of federal government powers.[50]

This might explain why electronic voting machines remain in use. As legal scholars noted a while ago, there seems to be a serious discrepancy between the international best practice standards endorsed by the United States and its own electoral system.[51] Legal scholars have stressed the importance of auditing transparency and that voters should be provided with a reasonable assurance that ballots will be counted accurately.[52] While this does not require that voters should fully comprehend the inner workings of the machine, the voting procedure and the technology on which it rests should be subject to reasonable public scrutiny.[53] It seems that the

---

[47] Wexler v. Anderson, 452 F.3d 1226, 1232 et seq. (11th Cir. 2006).

[48] Lawrence Norden & Wilfred U. Codrington III, *America's Voting Machines at Risk: An Update*, Brennan Center for Justice, New York University School of Law (2018), 1; Jacob Rush, *Hacking the Right to Vote*, 105 VA. L. REV. ONLINE 67 (2019); Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 FORDHAM L. REV. 1711, 1775 et seq. (2005).

[49] Wesberry v. Sanders, 376 U.S. 1, 6-7 (1964); Tashjian v. Republican Party of Connecticut, 479 U.S. 208, 217 (1986). For other impediments (funding of new voting technologies, long-term contracts with manufacturers, close ties to political parties) to an effective reform of voting procedures, see Jacob Rush, *Hacking the Right to Vote*, 105 VA. L. REV. ONLINE 67, 69-72 (2019).

[50] Jennifer Nou, *Sub-Regulating Elections*, 2013 SUP. CT. REV. 135, 137 (2013).

[51] Frank Emmert, Christopher Page & Antony Page, *Trouble Counting Votes? Comparing Voting Mechanisms in the United States and Selected Other Countries*, 41 CREIGHTON L. REV. 3, 32 (2008).

[52] Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 FORDHAM L. REV. 1711, 1780 (2005).

[53] Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 FORDHAM L. REV. 1711, 1780 (2005).

electronic voting technologies in use do not satisfy this requirement. However, as these critical considerations also show, U.S. constitutional law does not impose any principled limitations on the use of blockchain voting procedures other than the general electoral principles enshrined in constitutional law.

2. Germany

According to Art. 38 § 1 of the German Constitution (*Grundgesetz*), members of the German parliament (*Bundestag*) are elected in a general, immediate, free, equal and secret voting procedure. According to Art. 38 § 3 the details specifying these general principles are established by federal law. At least on paper, similar principles apply in the law of the European Union.[54] Unlike in U.S. constitutional law, the States (*Länder*) have no jurisdiction to establish the voting procedure or shape the electoral administration in the context of federal elections.

The core requirements guiding the use of electronic voting machines are derived from the publicity principle enshrined in Art. 38 and Art. 20 § 2 of the German Constitution.[55] The publicity of the election is intended to guarantee an orderly and accurate voting procedure, and it is considered as a fundamental condition for a trustworthy voting procedure. It covers the proposal of candidates, the act of voting, and the determination of the electoral outcome, the only exception being the secrecy of the ballot.[56] According to constitutional doctrine, the publicity principle contains specific safeguards based on the principle of *democracy*, *republicanism* and the *rule of law*.

First, it follows from the principle of democracy that the voting procedure only guarantees democratic legitimacy only if it can be verified so that manipulations can be excluded or, if need be, corrected.[57] The citizens need to be able to scrutinize the voting procedure lest they distrust that the composition of the parliament (*Bundestag*) reflects the voters' true political preferences. Second, republicanism requires that each citizen be able to verify the essential steps of the voting procedure without prior

[54] Matthias Lukan, *Europawahlen vom Wohnzimmer aus?*, EuR 2019, 222.

[55] Martin Morlok, *Art. 38, in* Horst Dreier (ed.), Grundgesetz Kommentar, Bd. II, 3. Aufl., Rn. 126 (2015); Stephanie Schiedermair, *Gefährden Wahlcomputer die Demokratie?*, 62 JuristenZeitung 162, 166 (2007); German Constitutional Court, BVerfGE 123,39 - Wahlcomputer, 2 BvC 3/07, 2 BvC 4/07, 108 (2009).

[56] German Constitutional Court, BVerfGE 121, 266 - Negatives Stimmgewicht, 2 BvC 1/07, 7/07 (2008).

[57] German Constitutional Court, BVerfGE 123,39 - Wahlcomputer, 2 BvC 3/07, 2 BvC 4/07, 108 (2009); Martin Will, *Wahlcomputer und der verfassungsrechtliche Grundsatz der Öffentlichkeit der Wahl*, NVwZ 2009, 700, 701.

technical knowledge.[58] Third, the rule of law warrants transparency and checks on the exercise of public power, including the decisions made by the electoral administration.[59]

Like the U.S. Supreme Court, the German Constitutional Court is deferential and grants discretion to the federal legislator. As a consequence, judicial review does not extend to the question whether the legislator designs useful or politically sensible voting procedures. When reviewing the use of electronic voting technologies, however, the Court applies strict scrutiny. According to the principles mentioned earlier, a voting procedure is considered as unconstitutional if voters cannot reliably verify whether their votes were recorded as cast and counted as recorded. The core concern raised by the court is that electronic voting procedures are based on computations that cannot be verified without technological expertise. According to constitutional doctrine, verifiability needs to be guaranteed on four distinct dimensions.

First, verifiability needs to account for the scope of errors. In a voting procedure that involves decentralized ballot counting facilities, it is highly costly to manipulate a sufficient number of ballots, as this would require large-scale collusion. By contrast, even simple manipulations of software can affect a large number of voting machines and thus potentially have a large impact on the electoral outcome.[60]

Second, verifiability needs to account for the mode of recording ballots. If votes are only recorded electronically, there is no reliable method of determining counting errors or manipulations once the election has ended. Therefore, a procedure in which votes are stored electronically only is considered as insufficiently verifiable. Additional physical supports, such as paper ballots, are required by constitutional law.[61]

Third, a lack of verifiability cannot be compensated by third party certifications or other preventive measures. Neither organizational measures taken before the election nor legal measures, such as criminal sanctions against electoral manipulation, are sufficient to provide adequate checks of the voting procedure.[62]

---

[58] German Constitutional Court, BVerfGE 123,39 - Wahlcomputer, 2 BvC 3/07, 2 BvC 4/07, 109 (2009).

[59] German Constitutional Court, BVerfGE 123,39 - Wahlcomputer, 2 BvC 3/07, 2 BvC 4/07, 110 (2009).

[60] German Constitutional Court, BVerfGE 123,39 - Wahlcomputer, 2 BvC 3/07, 2 BvC 4/07, 118 (2009).

[61] German Constitutional Court, BVerfGE 123,39 - Wahlcomputer, 2 BvC 3/07, 2 BvC 4/07, 120 (2009); also see Martin Will, *Wahlcomputer und der verfassungsrechtliche Grundsatz der Öffentlichkeit der Wahl*, NVwZ 2009, 700, 701.

[62] German Constitutional Court, BVerfGE 123,39 - Wahlcomputer, 2 BvC 3/07, 2 BvC 4/07, 123 et seq. (2009).

Fourth, a restriction of verifiability associated with an electronic voting procedure cannot be justified on the grounds that the use of electronic technology accelerates the ballot counting process. While the Constitution requires that the new parliament can convene shortly after the election (Art. 39 § 2 of the German Constitution), even a procedure relying only on paper ballots makes sure that an official preliminary result can be determined within a few hours after the polling places have been closed.

It is important to note that, even if the residual vote rate is down to 0 %, the voting procedure is not considered as compliant with the constitutional verifiability requirements.[63] In that case, the procedure merely provides a guarantee that the number of recorded or counted ballots is equal to the number of voters who appeared in polling places and cast a ballot. It does not, however, enable citizens to verify whether ballots were actually recorded as cast and counted as recorded. Each essential electoral step must be subject to public scrutiny and control. Such checks are not guaranteed when the recording and the counting process rest on machine-based computations alone, without any additional physical support of votes. Against this backdrop, the use of electronic voting machines was declared as incompatible with Art. 38 and Art. 20 § 2 of the German Constitution. In sum, these considerations illustrate that it would be difficult to reconcile a blockchain voting procedure with the requirements of German constitutional law.

### *C. Principles of Cryptoeconomics*

A blockchain is a decentralized ledger in a peer-to-peer network.[64] Unlike nation states, it does not, in principle, include any centralized institutions exercising the powers attributed to the three branches of government (legislative, executive, judicial branch). Rather, blockchain technology can be qualified as a decentralized peer-to-peer governance system.[65] To govern the behavior of nodes and protect the distributed ledger against malicious behavior, the blockchain builds on a combination of cryptography, game theory, and mechanism design - an amalgam referred to as cryptoeconomics.

---

[63] German Constitutional Court, BVerfGE 123,39 - Wahlcomputer, 2 BvC 3/07, 2 BvC 4/07, 149 (2009).

[64] Rainer Böhme et al., *Bitcoin: Economics, Technology, and Governance*, 29 J. ECON. PERSP. 213 (2015); Christian Catalini & Joshua S. Gans, *Some Simple Economics of the Blockchain*, Rotman School of Management Working Paper No. 2874598, MIT Sloan Research Paper No. 5191-16 (2019), 1.

[65] Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 369 (2016).

1. Blockchain Mechanism Design

While the rules underlying the consensus protocol can be thought of as legal rules, not much is gained from such a normative conceptualization. What really matters is whether the rules can effectively guarantee the integrity of the voting procedure. This requires that all votes are cast as intended, recorded as cast, and counted as recorded. Whether blockchain technology can effectively establish rules to satisfy these requirements of democratic elections depends on the mode of blockchain governance. The mode of blockchain governance or, more specifically, the mode of coordinating human behavior on the blockchain is not based on customary law or social norms. Rather, it primarily rests on elements of code and markets.[66] The central features of this hybrid mode of regulation are cryptographically induced incentives, incentives set by what computer scientists call *consensus protocol* and what economists call *mechanism*. Formally, a mechanism simply denotes a set of strategy-outcome pairs.[67] In the context of blockchain voting, the consensus protocols used to validate votes can be considered as mechanisms in the sense of mechanism design.

Mechanism design serves two distinct analytic functions: one positive, the other normative.[68] In its positive function, mechanism design provides a formal tool to analyze whether the incentives set by a mechanism are such that a well-defined objective given by the social planner can be achieved. It is important to note that standard mechanism design is based on the assumption of rational behavior and common knowledge of preferences and rules.[69] Voting procedures implemented on the blockchain should be intended to realize a given set of democratic principles and objectives enshrined in constitutional law, and mechanism design allows for an assessment of whether this objective can be achieved given a set of legal constraints. In its normative function, mechanism design provides a precise

---

[66] For the classic account, see LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

[67] For such an approach, see generally Leonid Hurwicz, *But Who Will Guard the Guardians?*, 98 AM. ECON. REV. 577, 580-581 (2008); Lewis A. Kornhauser, *Governance Structures, Legal Systems, and the Concept of Law*, 79 CHI.-KENT L. REV. 355 (2004).

[68] Mechanism design is the theoretical foundation of market design, that is, the part of economics that strives to understand how the design of marketplaces affects their functioning and aims at repairing those that are broken, see, e.g., Alvin E. Roth, *The Economist as Engineer: Game Theory, Experimentation, and Computation as Tools for Design Economics*, 70 ECONOMETRICA 1341 (2002); Alvin E. Roth, *Marketplaces, Markets, and Market Design*, 108 AM. ECON. REV. 1609 (2018).

[69] The theory of robust mechanism relaxes these assumptions, see, e.g., Dirk Bergemann & Stephen Morris, *An Introduction to Robust Mechanism Design*, 8 FOUND. & TRENDS IN MICROECON. 169 (2012).

way of formulating conditions for fair social institutions.[70] Yet these conditions cannot be established without considering the relevant set of normative constraints embedded in ethics or the law, such as the constitutional principles discussed above.

On this view, the focus of the analysis should be the respective outcomes when persons adopt a legal strategy (an honest validation of blocks) and when persons adopt an illegal strategy (a malicious validation of blocks). A mechanism (the consensus protocol and the actual voting procedure in which it is embedded) can be considered as being in compliance with constitutional law if the equilibrium outcome of the mechanism aligns with any outcome approved by the respective principle of constitutional law. Therefore, a mechanism needs to make sure that nodes coordinate or cooperate properly, either explicitly or tacitly.[71]

A mechanism can be considered as being safe if it is designed such that participants have an incentive to coordinate or cooperate so as to achieve the intended outcome. If the mechanism satisfies this incentive-compatibility constraint, it can be considered as strategy-proof. And if the mechanism is strategy-proof, it can be considered as safe, since no participant can improve her individual outcome by misrepresenting her preferences or otherwise attempting to game the mechanism.[72] Establishing safe mechanisms on the blockchain, is extremely difficult, because safety requires agreement of network users (nodes) in several dimensions. Nodes need to agree on the rules guiding the validation of transactions or votes, on the transactions or votes that have been performed, and on the value of the underlying cryptocurrency used as an incentive for nodes.[73] The voting procedure implemented on the blockchain can only be considered as safe and in compliance with constitutional safety requirements, if the mechanisms used on the blockchain network satisfy basic safety constraints themselves.

---

[70] For a similar conceptualization, see Zoë Hitzig, Lily Hu & Salomé Viljoen, *The Technological Politics of Mechanism Design*, 87 U. CHI. L. REV. 95, 97 (2019).

[71] Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 370 (2016), argues that blockchain protocols need to be extended to allow for tacit coordination games. The more important question is whether the design of consensus protocols can effectively achieve coordination in equilibrium.

[72] For a more formal definition in the context of the famous deferred acceptance algorithm that is now widely used in school choice, see Lester E. Dubins & David A. Freedman, *Machiavelli and the Gale-Shapley Algorithm*, 88 AM. MATH. MONTHLY 485 (1981).

[73] Joshua A. Kroll, Ian C. Davey & Edward W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*, The Twelfth Workshop on the Economics of Information Security (WEIS 2013), 1, 6 (2013).

2. Distributed Ledger Technology

Each blockchain consists of a sequence of blocks (ledger), and each block contains data. The data can refer to different types of information, such as a financial transaction (e.g. Bitcoin), a contractual obligation (e.g. Ethereum), or a vote (e.g. Smartmatic-Cybernetica). The blockchain provides an authoritative record of any type of social fact, the difference vis-à-vis traditional records being that the blockchain records can be duplicated without allegedly running the risk of producing inconsistent blocks. One of the core objectives of the blockchain is to achieve a qualified and unambiguous agreement about the truthfulness of the stored information and trust in a single truth, without a centralized entity.[74] The most important mechanism to achieve these broader objectives is the consensus protocol.

The foundation that all consensus protocols rely on is public key cryptography.[75] An algorithm, for example SHA-256, creates a pair of a public and a private key that are both assigned to the owner of cryptocoins.[76] The private key is kept secret. The owner can use the private key to sign an assertion that a certain amount of cryptocoins is transferred from one address to another. In other words, she can encrypt a message about an asserted transaction. The recipient of the cryptocoins can use the public key to decrypt the message. If the recipient knows the public key and the encryption algorithm (hash function), she can infer that the encryption stems from the person holding the private key. The recipient will thus know that the person holding the corresponding private key once owned the cryptocoins. However, the recipient has no means of knowing whether the person has already spent the cryptocoins in a previous transaction.

This contractual counterparty risk is usually referred to as the double-spending problem.[77] The conventional solution to this problem is the use of a trusted third party, such as PayPal, that keeps track of payments against payment of a fee. Blockchain technology, by contrast, is intended to

---

[74] See, e.g., Joshua A.T. Fairfield, *Bitproperty*, 88 S. CAL. L. REV. 805, 819-823 (2015).

[75] See Joshua A. Kroll, Ian C. Davey & Edward W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*, The Twelfth Workshop on the Economics of Information Security (WEIS 2013), 1, 3 (2013).

[76] Joseph Bonneau et al., *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, 2015 IEEE Symposium on Security and Privacy, 104, 115 (2015).

[77] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Whitepaper (2008), 1; Jonathan Chiu & Thorsten Koeppl, *Incentive Compatibility on the Blockchain, in* Walter Trockel (ed.), Social Design: Essays in Memory of Leonid Hurwicz, 323, 328 (2019); Jonathan Chiu & Thorsten Koeppl, *The Economics of Cryptocurrencies - Bitcoin and Beyond*, Queen's Economics Department Working Paper No. 1389 (2017), 1, 5.

eliminate the need for a trusted intermediary through the use of consensus protocols or mechanisms. The main objective of consensus protocols is to establish trust in the validity of the transactions recorded in blocks without any centralized trusted party in charge of verifying the transactions that have been broadcast to the public ledger.[78]

In order to maintain an accurate ledger, the consensus protocol needs to achieve consensus - less than unanimity, but more than a majority - at three distinct levels: consensus about the rules used to determine the validity of transactions or votes, consensus on the history of authoritative blocks, and consensus on the value of the cryptocurrency.[79] Perhaps the most important challenge any consensus protocol needs to accommodate is to prevent malicious nodes from hampering consensus.

A traditional consensus protocol used to address the problem of malicious attacks is practical Byzantine fault tolerance (PBFT).[80] This protocol is based on a well-known cryptographic solution to the Byzantine Generals problem. Suppose that generals of different Byzantine army divisions need to coordinate on a joint plan of action through messages. Suppose, moreover, that some generals are traitors and will attempt to foil the plan by forging messages. Securing the joint plan of action is impossible if one third of all generals or more are traitors. Thus the idea of practical Byzantine fault tolerance: a network with $n$ nodes tolerates $m < n/3$ malicious nodes, not more. Rather than relying on a risky assumption about the prevalence of honest nodes, blockchain technology is based on the assumption of selfish behavior and uses cryptocoins to incentivize mining and honest behavior. This assumption reflects the belief that intrinsic motivation and altruism would likely be insufficient to enable cooperation among nodes and prevent malicious behavior.[81] While PBFT is not directly implemented on most blockchains due to its relatively high trust requirements, the prevalent blockchain consensus protocols share the same

---

[78] PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE, 109 (2018).

[79] See Joshua A. Kroll, Ian C. Davey & Edward W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*, The Twelfth Workshop on the Economics of Information Security (WEIS 2013), 1, 6 (2013).

[80] Leslie Lamport, Robert Shostak & Marshall Pease, *The Byzantine Generals Problem*, 4 ACM Transactions on Programming Languages and Systems 382 (1982); Muhammad Saad et al., *Exploring the Attack Surface of Blockchain: A Systematic Overview*, Working Paper (2019), 1, 5, arXiv:1904.03487v1 [cs.CR] 6 Apr 2019.

[81] For a critique of idealizing assumptions about the behavior of nodes, see Christian Cachin & Marko Vukolić, *Blockchain Consensus Protocols in the Wild*, Working Paper (2017) 1, 4. Mining is neither creative nor innovative, but tedious. In that sense, mining differs from creative and innovative activities such as those envisioned by YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006).

concern for safety, the difference being that they set specific incentives to behave honestly instead of taking a leap of faith by requiring trust that a specific threshold of honest nodes is met.

The dominant blockchain consensus protocol goes back to Satoshi Nakamoto who proposed a protocol for Bitcoin known as proof-of-work (PoW).[82] Under PoW, node operators called miners enter a tournament to solve a complex hash cryptopuzzle. The cryptopuzzle is hard to solve but easy to verify. In the tournament, miners compete over the right to add a block containing verified votes or transactions to the blockchain.[83] The difficulty of the cryptopuzzle is such that the right to add a block can be assigned every ten minutes on average.[84] The winner of the tournament is rewarded with a certain amount of cryptocoins, composed of seignorage and a transaction fee. Each miner is thus incentivized to be the first to solve the cryptopuzzle. Since no solution can be inferred by logic, miners have to apply brute force, that is CPU power, to solve the cryptopuzzle.[85] The probability of winning the competition increases with each additional unit of CPU power. PoW can therefore be said to follow the principle one-CPU-one-vote (1CPU1v).

The idea behind PoW is to prevent malicious nodes from attempting to hamper the integrity of the network through forged identities, a phenomenenon commonly referred to as Sybil attacks.[86] A node that wants to remove a previous ("honest") block and replace it with a different ("forged") block in order to obtain a benefit would need more than 50 % of the mining capacity on the blockchain to succeed. Such an attack is usually referred to as a 51 % attack.[87] Rather than making an assumption about the distribution of honest nodes like PBFT, PoW is based on the assumption that it is impossible or extremely costly to achieve monopoly power over CPU units. Against this backdrop, PoW is usually considered as an effective mechanism that prevents dishonest agents from thwarting consensus on a

---

[82] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Whitepaper (2008), 1; KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST, 42 ET SEQ. (2018).

[83] Eric Budish, *The Economic Limits of Bitcoin and the Blockchain*, NBER Working Paper No. 24717 (2018), 1.

[84] ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION (2016).

[85] Gur Huberman, Jacob D. Leshno & Ciamac C. Moallemi, *Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System*, Research Paper 17-92, Columbia Business School, New York (2017), 1.

[86] ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION (2016).

[87] Joshua A. Kroll, Ian C. Davey & Edward W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*, The Twelfth Workshop on the Economics of Information Security (WEIS 2013), 1, 11-12 (2013).

single truth.

Once the cryptopuzzle is solved, the winning miner adds a block to the blockchain containing the number of the previous block, a time-stamp, the hash of the previous block, a nonce (a random value used only once in cryptographic communication), and a group of transactions.[88] The resulting hash chain enables the nodes to verify that none of the preceding blocks has been altered. Altering a previous block would require changing all the hashes up to the block that was added most recently.

Following a typical recommendation, miners usually do not confirm a block before six new blocks have been generated, which means that miners have six unvalidated blocks on their copy of the ledger.[89] This creates latency in the network and explains why validating blocks is time-consuming. By convention, and this is a particularly remarkable feature, each block is added to the longest valid branch of the blockchain. While the longest branch is said to be the authoritative one, the consensus protocol does not contain any specific incentive to spur miners to comply with the longest-branch rule. The longest branch simply represents the chain with the most proof of work.[90] Compliance with the longest-branch rule, however, is not the unique equilibrium of the game that miners play. As a result, the legitimacy of the votes validated in the longest branch is necessarily shaped by psychological forces that cannot be fully contained by the consensus protocol.

A more compelling approach to the question why miners may and usually do comply with the longest-branch rule is to consider mining as a coordination game.[91] A coordination game is a game with multiple equilibria, the typical example being the decision on which side of the road to drive.[92] It does not matter whether drivers use the right or the left lane, as long as all drivers behave consistently. In the mining coordination game, the addition of a block to the currently longest branch is an equilibrium outcome, but coordinating on any other block is an equilibrium as well (Fig.

---

[88] See Joshua A. Kroll, Ian C. Davey & Edward W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*, The Twelfth Workshop on the Economics of Information Security (WEIS 2013), 1, 4 (2013).

[89] Marko Vukolić, *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication*, International Workshop on Open Problems in Network Security (iNetSec), Oct 2015, Zurich, Switzerland, 112 (2015); Rainer Böhme et al., *Bitcoin: Economics, Technology, and Governance*, 29 J. ECON. PERSP 213, 217 (2015).

[90] Kevin Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L. J. 489, 505 (2018).

[91] For a similar conceptualization, see Bruno Biais et al., *The Blockchain Folk Theorem*, 32 REV. FIN. STUD. 1662 (2019); Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 374 et seq. (2016).

[92] ERIC RASMUSEN, GAMES AND INFORMATION: AN INTRODUCTION TO GAME THEORY, 4TH ED., 29 ET SEQ. (2007).

1). The payoffs are equivalent, as long as miners agree on a chain that shall be authoritative.

| | L | R |
|---|---|---|
| L | 1 , 1 | 0 , 0 |
| R | 0 , 0 | 1 , 1 |

Fig. 1: Mining Coordination Game

The currently longest branch simply provides a focal point. The (often intended) effect of focal points, such as the legal obligation to drive on the right lane, is to guide the selection of one of multiple equilibria. The higher the salience of the respective equilibrium behavior, the better the focal point. In this vein, the longest branch can be considered as focal, because it is particularly salient and represents the part of the blockchain that has required the highest investments.[93] It is important to stress, however, that the consensus protocol does not design the payoff structure such that miners have an incentive to choose the longest branch. On the Bitcoin blockchain, for example, the longest-branch rule is simply written down in the reference implementation. Therefore, distributed consensus is not just the result of a mechanism designed to make honest mining incentive-compatible; it is also a social process driven by psychological forces that are partly beyond the control of the core developers or the entity implementing a political election on the blockchain.

Mostly due to the high electricity needs, some blockchains have been moving towards alternative consensus protocols. A prominent "green" alternative to PoW is proof-of-stake (PoS).[94] Unlike under PoW, the incentives for node operators to behave honestly do not result from an investment in CPU power, but from investing a certain amount of cryptocoins.[95] Under PoS, users who are called validators can put a certain

[93] Also see Joshua A. Kroll, Ian C. Davey & Edward W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*, The Twelfth Workshop on the Economics of Information Security (WEIS 2013), 1, 10 (2013). On focal point theory in legal scholarship, see Richard H. McAdams, *Focal Point Theory of Expressive Law*, VA. L. REV. 1649 (2000).

[94] PoS goes back to an idea proposed by Sunny King & Scott Nadal, *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*, Working Paper (2012), 1.

[95] Vitalik Buterin, *A Proof of Stake Design Philosophy* (Dec 30, 2016), https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51; ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION, 231 ET SEQ. (2016); Muhammad Saad et al., *Exploring*

amount of previously acquired cryptocoins at stake, usually through a deposit. Validators are rewarded for their deposit and selected to validate a block based on the proportion of deposited cryptocoins. If the block is correctly validated, the selected validator receives a fee; otherwise, she is penalized. The specific computation of the penalty differs across blockchains, but one way to prevent dishonest behavior is to calculate the penalty in proportion to correlated errors on the blockchain at the time of validation. The stake required by PoS is intended to set similar incentives ("skin in the game") to behave honestly as the investment in CPU power required by PoW. Therefore, PoS can be said to follow the principle one-coin-one-vote (1c1v). The concomitant limitation is that rich validators may keep winning the right to add the next block. This sets an incentive to accumulate coins and makes the validation process centralized around rich validators.

## II. THE VIRTUES

Blockchain technology has properties that make it particularly suitable for electoral purposes, at least in theory. The most obvious advantage of blockchain voting procedures may be that they reduce the individual cost of voting and therefore facilitate democratic participation. Blockchain voting has the potential to mitigate the problem of voter apathy and reduce the voting barriers for minorities and socially marginalized groups. Whether blockchain voting procedures can really achieve this, is an empirical question beyond the scope of this article. Since these potential advantages are not specific to blockchain voting, I shall not discuss them here. Rather, I focus on two other virtues that are specific to blockchain voting procedures: the alleged immutability of the distributed ledger, and the possibility to experiment with traditional concepts of political equality and design voting procedures that account for the intensity of voters' preferences.

### *A. Immutability*

Blockchain voting procedures have the potential to buttress the integrity of the election and the legitimacy of its outcome by increasing the accuracy of counts and preventing the manipulation of ballots. The central feature of blockchain technology enabling these properties is the immutability of the distributed ledger. Once a block containing a set of transactions or votes has been added to the longest branch, it is usually considered as unalterable.[96]

---

*the Attack Surface of Blockchain: A Systematic Overview*, Working Paper (2019), 1, 8, arXiv:1904.03487v1 [cs.CR] 6 Apr 2019.

[96] On a legal perspective, immutability may be the most useful and most challenging

In order to change the ledger, the blockchain would have to be forked up to the block whose records are to be altered (target block). This would require a modification of each block that was added to the blockchain after the target block. Therefore, as the number of blocks added after the target block increases, it becomes increasingly difficult to modify the target block.

Against this backdrop, it becomes clear that immutability is primarily a probabilistic concept.[97] The probability of an immutable block increases as time passes and new blocks are generated. As mentioned earlier, miners usually keep six unvalidated blocks of the Bitcoin blockchain in their private copy of the ledger.[98] This means that a block can be seen as immutable once more than six blocks have been generated. It is important to note, however, that this latency simply results from a convention reflecting the risk preferences of most miners. While miners have an incentive to be the first to solve the cryptopuzzle, they also have an incentive to refrain from prematurely adding blocks, as this could result in a wasted investment in case the branch does not turn out to be the authoritative one. More important transactions may require higer latency, and given the importance of accurate vote counts, blockchain voting procedures are likely to require higher latency than other activities on (public) blockchains.

Moreover, the extent to which the distributed ledger can be considered as immutable depends on the behavior of nodes in the mining coordination game. When it comes to validating a transaction or vote and shaping the rules underlying validation, nodes can adopt two different strategies: voice and exit.[99] Nodes can exercise voice by submitting blockchain amendment proposals; or they can exit by leaving the blockchain or deviating from the default software rules proposed by the clients. The latter will entail a soft fork if the software update is backward compatible. If the software update is not backward compatible, the blockchain will be split by a hard fork.[100] A

---

blockchain characteristic, see, e.g., Richard Holden & Anup Malani, *Can blockchain address the problem of holdup in contracts?*, Coase-Sandor Working Paper Series in Law and Economics, No. 846 (2017), 1, 18-19.

[97] Vitalik Buterin, *On Settlement Finality*, Ethereum Blog (May 9, 2016), https://blog.ethereum.org/2016/05/09/on-settlement-finality/.

[98] Rainer Böhme et al., *Bitcoin: Economics, Technology, and Governance*, 29 J. ECON. PERSP 213, 217 (2015). Other blockchains, such as Ethereum, offer faster block confirmation. Depending on the degree of control over the network, lower latency implies lower safety and lower confidence in the truthfulness of the validated transaction.

[99] On voice and exit as responses to declining performance of organizations, see generally ALBERT O. HIRSCHMAN, EXIT, VOICE, AND LOYALTY: RESPONSES TO DECLINE IN FIRMS, ORGANIZATIONS, AND STATES (1970).

[100] When a soft fork occurs, both updated and non-updated nodes can validate new blocks. When a hard fork occurs, only updated nodes can validate new blocks. See Joseph Bonneau et al., *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, 2015 IEEE Symposium on Security and Privacy, 104, 113 (2015).

hard fork disrupts immutability if one side of the hard fork disregards a transaction or vote that has been previously validated.

While a hard fork requires almost the unanimity of nodes, a soft fork only requires a majority.[101] Forks can be quite dangerous, since they create competing versions of the blockchain. In the context of voting, it could therefore be that a vote has been validated more than once, thus creating a double-voting problem. Another problem occurs if votes are simultaneously validated and invalidated, thus creating a censorship problem. The blockchain is not immune against such modifications of the ledger. As a consequence, votes recorded on the blockchain also remain vulnerable to tampering.

Finally, the extent to which the distributed ledger can be considered as immutable also depends on whether the respective blockchain is permissionless or permissioned. Many proposals for blockchain voting procedures are based on public and permissionless blockchains, such as Bitcoin or Ethereum. Other systems, such as Votebook, are based on permissioned blockchains, where a centralized electoral organization grants permission to nodes to verify votes, add blocks, and thus modify the ledger.[102] Why does the difference matter?

On a permissionless blockchain, like Bitcoin or Ethereum, the distributed ledger is based on open source code. There is no centralized authority deciding which nodes should be admitted, how the behavior of nodes should be coordinated, and whether the blocks validated by certain nodes should be excluded. Any person can become a miner, and any person can easily verify the validity of blocks. The upside of permissionless blockchains is that they guarantee a high level of transparency, at least - and this is a crucial caveat - for those able and willing to participate in the blockchain ecosystem. The downside is that they require a sound mechanism design, meaning that the consensus protocols need to be robust against attacks. As a consequence, both code and sound incentive constraints are particularly important in permissionless blockchain ecosystems.

On a permissioned blockchain, by contrast, a centralized authority decides which nodes should be allowed to validate and verify blocks. The leading permissioned networks are Hyperledger, an IBM product, and R3

---

[101] Joseph Bonneau et al., *SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, 2015 IEEE Symposium on Security and Privacy, 104, 113 (2015). If a node does not adopt the update, it might waste investments on blocks that the remainder of the networks does not consider as authoritative, while an update provides an insurance of compatibility on all branches. Risk-averse nodes may thus have an incentive to update and deviate from the old set of rules.

[102] Kevin Kirby, Anthony Masi & Fernando Maymi, *Votebook: A proposal for a blockchain-based electronic voting system*, New York University, Whitepaper (2016), 1.

Corda. The permission can extend to reading data, writing data, or both. While permissioned blockchains come with substantially less demanding design requirements with respect to the distributed consensus mechanism, they have two important downsides.

First, they are less decentralized than permissionless blockchains, thus creating a honeypot of power at the level of the centralized authority, that is the core developers. The core developers are in control of the consensus protocol and can decide how access should be provided. Permissioned blockchains therefore lack a system of publicly governed checks and balances. Second, permissioned blockchains reintroduce two problems that distributed consensus protocols are actually intended to solve: a central point of failure and the need for trust. On the one hand, the distributed ledger becomes vulnerable to attacks targeted at the small community of core developers and their coding decisions. On the other hand, if the nodes admitted to the network are not trustworthy, the integrity of the block content is at risk. This entails a responsibility of the centralized authority to closely monitor the behavior of nodes. On permissioned blockchains, as in other governance systems, the corollary of responsibility is power. A centralized authority acting responsibly will therefore have to take effective measures to correct errors in distributed consensus or nip attempts to falsify the voting outcome in the bud.

### *B. Political Equality*

Democracy is sometimes defined as government by the people, by the majority, or, under a stringent standard, by unanimity. In addition, under all these approaches, democracy requires consent of the governed, lest society be placed under the yoke of autocracy or plutocracy. While many majoritarian and consent-based concepts are somehow correct, they do not directly capture the problem of how popular sovereignty should be distributed. In order to be operational, democracy requires a decision about how the power to give consent should be allocated, what the participation constraints should be, and how consent could actually translate into legitimacy.

A foundational principle that accounts for the distribution of sovereignty is that of political equality.[103] According to philosopher Charles Beitz, political equality makes sure that each citizen has an equal claim to power in the decision-making process over the basic institutions governing society.[104] Political equality thus ensures fair participatory terms. In the

[103] DARCY W.E. ALLEN, CHRIS BERG & AARON M. LANE, CRYPTODEMOCRACY: HOW BLOCKCHAIN CAN RADICALLY EXPAND DEMOCRATIC CHOICE, 9 ET SEQ. (2019).

[104] CHARLES BEITZ, POLITICAL EQUALITY: AN ESSAY IN DEMOCRATIC THEORY (1989).

context of voting procedures, the most formal realization is the principle one-person-one-vote (1p1v). Accordingly, the principles of political equality and equal representation enshrined in many constitutional laws, including U.S. constitutional law, are usually operationalized through 1p1v.[105] This foundational principle that voting procedures build on can be considered as *egalitarian consent*.

Blockchain technology poses two distinct challenges to the principle of egalitarian consent, but to understand these challenges, it is indispensable to distinguish between two layers of decision-making procedures: the voting decisions made in the election and the decisions taken by the nodes to validate the votes.[106]

First, while the election may follow the principles of egalitarian consent and 1p1v, the decision-making procedure to validate blocks follows the principles encoded in the respective consensus protocols.[107] Under PoW, for example, the right to validate blocks is granted according to the principle 1CPU1v, while PoS implements 1c1v. This entails a mismatch between the realization of political equality off the blockchain and the allocation of voting power on the blockchain ("block validation power"). This will not be a problem, as long as the distribution of block validation power buttressed by the respective consensus protocol allows for a reliably correct validation of blocks and compliance with 1p1v in the political election conducted on the blockchain. In theory, the deviation from 1p1v *on* the blockchain will guarantee that 1p1v is respected *off* the blockchain, that is in the election whose votes are to be validated. Non-compliance with 1p1v on the blockchain will thus be a virtue. If, however, nodes are driven by political interests, they can attempt to accumulate power over CPU units (under PoW) or coins (under PoS) and alter the course of the validation process according to their own political preferences. In that case, the consensus protocol will entail severe limitations to the integrity of the blockchain voting procedure.[108]

---

[105] Gray v. Sanders, 372 U.S. 368, 381 (1963); Reynolds v. Sims, 377 U.S. 533 (1964).

[106] Also see Yoan Hermstrüwer, *Democratic Blockchain Design*, 175 J. INST. & THEORETICAL ECON. 163 (2019).

[107] As mentioned earlier, the block validation process also depends on the governance decisions of the core developers and whether the blockchain is permissionless or permissioned. In the Bitcoin scaling debate, the administrator of the Bitcoin.org website claimed: "One of the great things about Bitcoin is its lack of democracy.", https://www.reddit.com/r/Bitcoin/comments/3rejl9/coinbase_ceo_brian_armstrong_bip_101_is_the_best/cwoc8n5/. For a critique, see Kevin Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L. J. 489, 550-551 (2018).

[108] I will further discuss the concomitant problems in Part III. For a comprehensive summary of the safety risks on the blockchain, see Muhammad Saad et al., *Exploring the Attack Surface of Blockchain: A Systematic Overview*, Working Paper (2019), 1, arXiv:1904.03487v1 [cs.CR] 6 Apr 2019.

Second, the process to validate votes is based on consensus. The notion of consensus is foreign to common theories of democracy. Most democratic theories rest on an implementation of simple majorities, supermajorities, or unanimity. Consensus, by contrast, denotes something in between supermajorities and unanimity. It denotes a general agreement, but it does not require the absence of any malicious or deviant actor. Consensus can be seen as the result of large-scale cooperation or coordination in a public goods game.[109] And this result is best achieved if a large fraction of actors believes that others will agree as well. This is in line with experimental evidence showing that most people are conditional cooperators and will reciprocate cooperation only if they trust others to cooperate.[110] If consensus cannot be achieved, compliance with 1p1v is at risk. And since consensus largely depends on the measures taken to induce reciprocity (e.g. through focal points), those who wield the power to take these measures also decide whether and when to comply with 1p1v in the political election conducted on the blockchain.[111]

### *C. Quadratic Voting*

The problem of the traditional concept of political equality implemented through 1p1v is that it does not account for the intensity of preferences. The dangerous flip-side of political equality is that it may result in a tyranny of the majority.[112] A majority determining a certain political outcome may make a small gain, while imposing a large loss on the minority. The risk inherent in 1p1v, therefore, is that it might yield a Pareto inefficient outcome. Suppose that Alice and Bob prefer $a$ over $b$ and that Carol prefers $b$ over $a$. If the outcome is determined by ordinal preferences, $a$ will be adopted. Suppose, by contrast, that these preferences are cardinal and that $a = 2$ and $b = 1$ for Alice and Bob, while $a = 2$ and $b = 5$ for Carol. Under an efficient voting procedure that accounts for cardinal preferences,

---

[109] Mining not only requires cooperation, as mentioned earlier, but also cooperation. In that sense, it could also be characterized as a mixed-motive game, e.g. a hawk/dove game. See generally Richard H. McAdams & Janice Nadler, *Testing the Focal Point Theory of Legal Compliance: The Effect of Third-Party Expression in an Experimental Hawk/Dove Game*, 2 J. EMP. L. STUD. 87 (2005).

[110] Urs Fischbacher, Simon Gächter & Ernst Fehr, *Are people conditionally cooperative? Evidence from a public goods experiment*, 71 ECON. LETTERS 397 (2001).

[111] Such coordinating measures have also been referred to as "coordination flags," see Vitalik Buterin, *Notes on Blockchain Governance*, Vitalik Buterin's website (Dec 17, 2017), https://vitalik.ca/general/2017/12/17/voting.html.

[112] A potential result of a tyranny of the majority is civil disobedience. For a comprehensive account of democracy-enhancing disobedience, see Daniel Markovits, *Democratic Disobedience*, 114 YALE L. J. 1897 (2005).

$b$ should be adopted, since $b$ (7) yields a higher social welfare than $a$ (6).

The blockchain offers an interesting playground for new voting mechanisms that eliminate some of the inefficiencies associated with 1p1v.[113] Economists have developed voting mechanisms that allow voters with intense preferences to cast more votes. One of the most prominent voting mechanisms is the Vickrey-Clarke-Groves mechanism (*VCG mechanism*).[114] Under the allocation rule of the VCG mechanism, the good is provided to the highest bidders. The most important feature, however, is the payment rule: Each winning bidder is charged a price that compensates the negative externality imposed on the other bidders who were not pivotal in determining the outcome. In addition, the VCG mechanism is strategy-proof, since each bidder has an incentive to bid her true valuation for the good.

One of the most prominent proposals building on the idea of the VCG mechanism is quadratic voting.[115] Under a quadratic voting rule, each voter is assigned a number of votes and allowed to buy and sell votes. Each voter can cast as many votes as she has, but she has to pay a price, which is the square of the number of votes cast. For example, if one vote costs one dollar, casting two votes costs four dollars, and casting three votes costs nine dollars. The general idea of such a system is to account for the intensity of preferences, induce truthful preference revelation, and compensate voters for the externalities imposed on them by other voters casting more votes.

The blockchain is particularly well-suited for quadratic voting, since it allows to assign vote budgets to voters, and keep track of budgets and vote transfers on the decentralized ledger. One of the potentially most promising use cases for quadratic voting using blockchain technology may be corporate elections.[116] Unlike political elections, corporate voting is

---

[113] Darcy W.E. Allen et al., *Cryptodemocracy and its institutional possibilities*, REV. AUSTRIAN ECON. 1 (2018).

[114] The VCG mechanism is a generalization of the sealed-bid second-price auction for multiple items, see William Vickrey, *Counterspeculation, Auctions, and Competitive Sealed Tenders*, 16 J. FIN. 8 (1961); Edward H. Clarke, *Multipart Pricing of Public Goods*, 11 PUB. CHOICE 17 (1971); Theodore Groves, *Incentives in Teams*, 41 ECONOMETRICA 617 (1973). For an application to corporate voting, see Yair Listokin, *The Vickrey-Clarke-Groves "Pivotal Mechanism" as an Alternative to Voting for Organizational Control*, 16 THEOR. INQ. L. 267 (2015).

[115] Steven P. Lalley & E. Glen Weyl, *Quadratic Voting: How Mechanism Design Can Radicalize Democracy*, 108 AEA PAPERS AND PROCEED. 33 (2018); Jacob K. Goeree & Jingjing Zhang, *One man, one bid*, 101 GAMES & ECON. BEHAV. 151 (2017). For a general overview, see ERIC POSNER & E. GLEN WEYL, RADICAL MARKETS: UPROOTING CAPITALISM AND DEMOCRACY FOR A JUST SOCIETY, 80 et seq. (2018).

[116] Eric A. Posner & E. Glen Weyl, *Quadratic Voting as Efficient Corporate Governance*, 81 U. CHI. L. REV. 251 (2014).

proportionate to ownership and does not follow 1p1v. But even political elections could be implemented using a quadratic voting procedure. One proposal recently advanced by Eric Posner and Glen Weyl is based on quadratic voting operated at the district level for representatives, at the state level for senators, and at the federal level for the president.[117] Under this proposal, voters could spend their vote budget at each level and, thus, concentrate their votes on the levels they care about most.

While quadratic voting is a promising means to account for the intensity of preferences, it is far from being a panacea to save fainting democracies. The most obvious problem is that political parties, candidates and voters are likely to resist the idea of putting price tags on votes.[118] Even to the extent that quadratic voting is robust against collusion and fraud, it is not clear whether quadratic voting is a suitable mechanism to advance democratic legitimacy.[119]

First, quadratic voting requires safeguards against the circumvention of vote budgets. Voters who want to preempt the squared marginal cost of additional votes could set up multiple identities and acquire only one vote under each identity. This problem can only be prevented to the extent that an effective identity verification system is embedded in the blockchain voting procedure. Satisfying this condition is likely to require some centralized trusted third party or cryptographic methods.[120] As a result, the blockchain voting procedure might become even more complex.

Second, quadratic voting can only yield efficient outcomes if votes can be traded. Trading votes implies that voters will incur potentially high transaction costs.[121] These transaction costs will present a severe obstacle to Coasian bargaining.[122] The mechanical consequence of an inefficient market for voting rights is that votes will not be allocated such that an efficient outcome in the quadratic voting procedure can be obtained. This problem is likely to be further exacerbated if voters are subject to an

---

[117] Eric A. Posner & E. Glen Weyl, *Voting Squared: Quadratic Voting in Democratic Politics*, 68 VAND. L. REV. 441 (2015); ERIC A. POSNER & E. GLEN WEYL, RADICAL MARKETS: UPROOTING CAPITALISM AND DEMOCRACY FOR A JUST SOCIETY, 120-122 (2018).

[118] Josiah Ober, *Equality, legitimacy, interests, and preferences: historical notes on Quadratic Voting in a political context*, 172 PUBLIC CHOICE 223 (2017). For a broader perspective on the monetization of votes Sam Fox Krauss, *Moral Market Design*, 28 KANSAS J. L. & PUB. POL. (2019).

[119] On robustness, see E. Glen Weyl, *The robustness of quadratic voting*, 172 PUBLIC CHOICE 75 (2017).

[120] Sunoo Park & Ronald L. Rivest, *Towards secure quadratic voting*, 172 PUBLIC CHOICE 151 (2017).

[121] Darcy W.E. Allen et al., *Cryptodemocracy and its institutional possibilities*, REV. AUSTRIAN ECON. 1, 10 (2018).

[122] Generally see Ronald Coase, *The Problem of Social Cost*, 3 J. L. ECON. 1 (1960).

endowment effect.[123] As a consequence, voters might have a higher valuation for votes that they hold than votes held by others. If votes are initially equally distributed in the electorate, as would most likely be the case, the endowment effect could reinforce the effect of transaction costs and prevent an efficient trade of voting rights. Moreover, experimental evidence suggests that people derive value from being an entitled member of the electorate and that this *rights utility* is independent of the utility derived from actually exercising the right to vote.[124] To the extent that this effect occurs in the context of quadratic voting, we would simply observe an accrual of voting rights in the hands of persons deriving high rights utility. However, we would not necessarily observe higher turnouts and a more accurate revelation of intense preferences.

Third, quadratic voting builds on the idea that outcomes generate specifiable utilities that translate into cardinal preferences over outcomes. While this assumption may hold when voters have to decide specific issues, like building a bridge in their municipality, it is unlikely to hold for political elections in representative democracies. The main problem that voters face in a representative democracy is that the causal link between the outcome of the election, producing a winning candidate, and a specific policy outcome is diluted, and hard to fully apprehend due to the ramifications of conditionally probable outcomes. Even if voters have ordinal preferences over parties or candidates, they will not have any means to engage in a reliable calculus of their vote. Voters are therefore likely to be subject to preference uncertainty and be driven by general concerns for the economy and society.[125] The potential of quadratic voting to account for preference uncertainty is limited.

Some of these problems are not specific to quadratic voting and exist in any voting procedure. The upshot of these considerations, however, is that quadratic voting may be better suited for small-scale, issue-specific voting procedures than for general political elections.

## III. THE LIMITS

Democratic elections conducted on the blockchain are subject to several legal and technical requirements, and these requirements are much more

---

[123] On the endowment effect, generally see Greg Klass & Kathryn Zeiler, *Against Endowment Theory: Experimental Economics and Legal Scholarship*, 61 UCLA L. REV. 2 (2013).

[124] Stephan Tontrup & Rebecca Morton, *The Value of the Right to Vote*, Public Law & Legal Theory Research Paper Series Working Paper No. 15-52, Law & Economics Research Paper Series Working Paper No.15-24 (2015), 1.

[125] For a critique of the utilitarian model, see Bernd J. Hartmann, *Self-Interest and the Common Good in Elections and Referenda*, 13 GERMAN L. J. 259 (2012).

stringent than those applying to other areas, such as smart contracts between private parties. First, blockchain voting procedures need to maintain the integrity of the election. This requires specific precautions targeting the vulnerabilities before the election (voter registration), during the election (voter identification, vote casting), and after the election (vote counting, auditing of the counting procedure). Second, blockchain voting procedures need to strike a balance between publicity and privacy. More specifically, some parts of the procedure, such as *access to* the voting booth, require some degree of public scrutiny and transparency, while others, such as *behavior in* the voting booth, require full privacy. Third, blockchain voting procedures need to create legitimate political outcomes. Creating legitimacy is the core function of any voting procedure, and I doubt whether blockchain technology in its current state of development is sufficiently safe and transparent for the general electorate to perform this function.

### *A. Ensuring Integrity*

The core prerequisite of democratic elections is to respect the political preferences of citizens without providing an undue advantage to a subset of citizens. This can only be achieved if the eligibility of voters is verified and respected, if the voting procedure does not otherwise discriminate citizens, and if the outcome of the voting procedure accurately reflects the voters' preferences.

#### 1. Eligibility

Any democratic voting procedure requires some mechanism to verify active (right to vote) and passive (right to be elected) eligibility. An accurate voter authentication or verification is the first prerequisite to guarantee the right to an equal suffrage and prevent the risk of double-voting. Without such a verification system, neither the voting procedure nor the voting outcome would be sufficiently protected against fraud and allegations of being rigged.

In small-scale elections, formal verification mechanisms may be dispensable. The main reason is that all or most eligible persons know each other and can organize elections under public scrutiny so as to minimize the risk of irregularities, such as double-voting. Even if the eligibility is to be verified without impinging on the privacy of voters, it is easier to achieve this objective in boardroom elections than in large-scale elections.[126]

[126] Teogenes Moura & Alexandre Gomes, *Blockchain Voting and its effects on Election Transparency and Voter Confidence*, Proceedings of the 18th Annual International Conference on Digital Government Research, 574 (2017).

In large scale-elections, control through public scrutiny and transparency is much more difficult to achieve. In principle, the government provides safeguards and procedures to guarantee that the person claiming access to the ballot box is identified as the person registered in the voting register (abstract eligibility) and that this person has not already cast her vote (concrete eligibility).[127] Under German law, for example, municipalities maintain a register of eligible voters and verify the identity of the eligible person before she casts her vote.[128] Similar verifications need to be performed in blockchain voting procedures.

The main challenge is to verify the eligibility without impinging on the secrecy of the ballot. The problem is that blockchain technology is not designed with a view to identity verification. To the contrary, it is designed to provide privacy and enable pseudonymous transactions as far as possible. Technically, however, it cannot be qualified as anonymous, since a record of the transaction and the encrypted identity is maintained on the public ledger.[129] Nonetheless, blockchain technology does not provide adequate mechanisms for identity verification, at least not for now. Existing blockchain technologies do not by design involve any mechanism that is able to generate trust in the identity of voters. Neither do they rely on any trusted third party to control the identity of voters. Therefore, it is hard to conceive of a blockchain voting procedure that does not rely on some connection between a trusted authentication organization and the blockchain.

One way to guarantee identity verification is to involve trusted third parties as an intermediary between the voter and the authentication organization.[130] The authentication organization can be a public election committee or a private entity and holds a voter registration list including personally identifiable information. The voter sends a secret message hash to the trusted third party and the authentication organization. The trusted third party reports the secret message hash to the authentication

---

[127] See Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 386 (2016) notes that a voter could own several Bitcoin addresses and that it is therefore impossible to implement 1p1v elections on the blockchain without any third party tracking the identities of voters.

[128] Section 17 § 1 and Section 14 § 1 and § 2 of the German Federal Elections Act (Bundeswahlgesetz).

[129] See, e.g., Christian Catalini & Joshua S. Gans, *Some Simple Economics of the Blockchain*, Rotman School of Management Working Paper No. 2874598, MIT Sloan Research Paper No. 5191-16 (2019), 1, A5. For a clear account of the relationship between privacy, anonymity, and pseudonymity, see Kobbi Nissim et al*., Bridging the Gap Between Computer Science and Legal Approaches to Privacy*, 31 HARV. J. L. & TECH. 687, 706 et seq. (2018).

[130] Kibin Lee et al., *Electronic Voting Service Using Block-chain*, 11 J. DIGIT. FORENSICS, SEC. & LAW 123, 127 (2016).

organization. This authentication organization then performs a matching between the secret message hash and the personally identifiable information and decides whether the voter is eligible or not. If the voter is authenticated as eligible, the trusted third party confirms the eligibility of the voter and invites her to send a secret message (the vote) to the trusted third party. The trusted third party then verifies whether the message matches the previously received secret message hash and, if that is the case, stores the vote.

Another way to guarantee identity verification is to rely on a blind signature or Anonymous Kerberos as authentication mechanisms.[131] A blind signature is a digital signature with a secret-key encryption protocol.[132] The specificity of a blind signature is that the sender of the message signs a message without knowing its content and that the blind signature can later on be publicly verified. Kerberos, by contrast, is a trusted third party authentication mechanism.[133] Under this mechanism, the authentication organization issues an anonymous identifier (credential) that the voter then uses with a session key to access the trusted third party. The authentication service will know the voter's identity without knowing her public key. The trusted third party, by contrast, will not know the voter's identity and issue a cryptocoin that the voter can then spend on a candidate. The transfer of the cryptocoin to the candidate counts as a vote in her favor.

The core challenge of systems like Kerberos is to maintain the secrecy of the ballot at two distinct levels. On the one hand, information derived from a private key, such as a public key, a public key hash, or an address, has to be kept away from the authentication organization and cannot be used as an ID or otherwise be linkable to a voter's identity.[134] Otherwise, the authentication organization would know how the voter voted, if the address is attached to the vote and each vote is registered on a public blockchain. On the other hand, the ID used by the authentication organization cannot be shared with the trusted third party, since the trusted third party would then know how the voter voted.[135] Multiple cryptocoin

---

[131] Stefano Bistarelli et al., *End-to-End Voting with Non-Permissioned and Permissioned Ledgers*, 17 J. GRID COMPUTING 97, 98 (2019).

[132] David Chaum, *Blind Signatures for Untraceable Payments*, Advances in Cryptology: Proceedings of CRYPTO '82, 199 (1982). For an application to blockchain voting procedures, see Yan Zhu, Zichuan Zeng & Chunli Lv, *Anonymous Voting Scheme for Boardroom with Blockchain*, 14 INT. J. PERFORM. ENGIN. 2414 (2018).

[133] Jennifer G. Steiner, Clifford Neuman & Jeffery I. Schiller, *Kerberos: An Authentication Service for Open Network Systems*, Proceedings of the USENIX Winter Conference, 191, 194-195 (1988).

[134] Stefano Bistarelli et al., *End-to-End Voting with Non-Permissioned and Permissioned Ledgers*, 17 J. GRID COMPUTING 97, 103 (2019); Kibin Lee et al., *Electronic Voting Service Using Block-chain*, 11 J. DIGIT. FORENSICS, SEC. & LAW 123, 128 (2016).

[135] Kibin Lee et al., *Electronic Voting Service Using Block-chain*, 11 J. DIGIT. FORENSICS, SEC. & LAW 123, 127 (2016).

requests from the same anonymous identifier should be denied by the trusted third party.

These considerations show that ballot secrecy and trust can only be guaranteed as long as no personally identifiable information is shared between the authentication organization and the third party. One of the core problems is that this guarantee can only be provided if the authentication and the confirmation of the right to vote (e.g. through the disbursement of a cryptocoin) are performed by two institutionally separate organizations. Moreover, these institutions cannot share the public key or the ID, since doing so would break anonymity and impinge on ballot secrecy. Finally, a reliable authentication relies on an impeccable commitment to morality on the part of the trusted third party. The upshot is that cryptographic arrangements are unlikely to provide sufficient safeguards for ballot secrecy and political privacy without an additional enforcement mechanism.[136] Such an enforcement mechanism requires the threat of physical force in the offline world. Without the threat of physical force, the authentication organization and the trusted third party could not be prevented from sharing those pieces of information that break anonymity or from colluding. And the most likely *locus* of this enforcement power is the government, a centralized authority.

Moreover, all verification systems rely on behavioral requirements that may often not be satisfied. On the one hand, any verification system based on public-private-key encryption relies on the assumption that the private key is kept private. Once the private key is transmitted to other persons, authentication cannot be guaranteed any more. On the other hand, the possibility to transmit the private key also creates a new risk of extortion or corruption, since dishonest agents may now be able to pay bribes or pressure voters to relinquish their private key. Like the relationship between the authentication organization and the third party, the relationship between key holders and parties with an interest in obtaining access to the key needs to be regulated, with the threat of physical force if necessary.

Even if all of these constraints are taken into account, it is far from clear whether transactions and votes can be effectively kept pseudonymous on the blockchain. On Bitcoin, for example, users can be identified by linking Bitcoin addresses and transactions recorded on the blockchain to the originator of IP addresses.[137]

---

[136] The problems of ballot secrecy and political privacy are further discussed in Part III.B.

[137] Alex Biryukov, Dmitry Khovratovich & Ivan Pustogarov, *Deanonymisation of Clients in Bitcoin P2P Network*, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS'14), 1 (2014); Péter L. Juhász et al., *A Bayesian approach to identify Bitcoin users*, 613 PLoS ONE 13 e0207000 (2018).

Some providers of blockchain-based voting procedures, such as the Democracy Earth Foundation, have proposed the use of biometric information or videos of the respective voter and a validation of her identity on the blockchain.[138] The most important feature of this verification system is that it is highly decentralized and that it relies on the blockchain both as a voting registry and as a system to count and validate votes. However, this proposal suffers from several shortcomings.

First, it is not clear how the secrecy of the ballot can be effectively maintained if an eligible and a personally identifiable vote are stored on the same blockchain. Second, this system rests on the assumption that the voter registry contains biometric information that can be matched to voters. The reality is, that election authorities in most countries, including the United States, do not maintain voter registries containing biometric information.[139] And even if biometric information were to be used, the authentication procedure would require mechanisms to detect attempts to defeat the biometric system through forged biometric features ("spoofing").[140] Third, automatic identification methods yield relatively high error rates, especially for minorities. The upshot is that, even in blockchain voting procedures, some centralized entity, most likely the government, will be needed to organize the authentication procedure and the verification of voter eligibility.

2. Inclusion

A distinct, but related limitation results from the fact that some voters may be technology illiterates or blockchain luddites. In that case, a purely blockchain-based voting procedure could entail more or less direct forms of discrimination. While some tech-savvy voters may benefit from the flexibility gains associated with blockchain voting procedures (e.g. mobile voting), others may not have the knowledge required to use the applications for blockchain voting.[141] This, in turn, carries the risk of manipulated or

---

[138] Democracy Earth, *The Social Smart Contract: An Open Source White Paper*, Version 0.2 (Jan 25, 2018), 1, 16 et seq.

[139] David Jefferson, *The Myth of "Secure" Blockchain Voting*, U.S. Vote Foundation (2019), https://www.usvotefoundation.org/blockchain-voting-is-not-a-security-strategy\#_ftn1.

[140] For an illustration of this risk, see Diaa M. Uliyan, Somayeh Sadeghi & Hamid A. Jalab, *Anti-spoofing method for fingerprint recognition using patch based deep learning machine*, ENGIN. SCI. & TECH., AN INT. J., in press (2019).

[141] For a critique of the voting technology divide in the 2000 U.S. presidential elections in Florida, see Paul M. Schwartz, *Voting Technology and Democracy*, 77 N.Y.U. L. REV. 625 (2002). See generally Lilian Mitrou et al., *Electronic Voting: Constitutional and Legal Requirements and Their Technical Implications, in* Dimitris A. Gritzalis (ed.), Secure

biased election outcomes, since access to the procedure could be structured so as to hamper the participation on the part of tech illiterates, thus giving more educated and affluent social groups more influence on the election outcome.[142]

While constitutional law, both in the United States and Germany, does not require that each voter should fully understand the inner workings of the voting procedure, its complexity should not systematically prevent certain social groups from understanding its essence, lest the procedure violate non-discrimination principles.[143] As the technology divide across different social groups closes, voting procedures will likely become more inclusive. Yet, in the meantime, the right to equality requires voting procedures designed to limit the impact of the divide.

One way to guarantee equal access would be to restrict the casting step to paper ballots and only organize the tally on the blockchain. The main advantage of this approach is that paper ballots, even when hand-counted, produce the lowest rate of residual votes and can thus be considered as being the safest support of votes.[144] Another way would be to offer a hybrid procedure that enables voters to cast either paper ballots or electronic ballots. This model would give all voters the liberty to choose one of the voting options. Finally, it would be possible to have voters cast paper ballots by default and enable them to opt out if they prefer to cast an electronic vote. This comes close the absentee voting options offered under many electoral laws, including Germany.[145] Overall, the voting procedure needs to make sure that the design of ballots, be they paper ballots or electronic ballots, does not discriminate specific social groups and minorities.

---

Electronic Voting, 43, 45 (2003).

[142] See generally Lilian Mitrou et al., *Electronic Voting: Constitutional and Legal Requirements and Their Technical Implications, in* Dimitris A. Gritzalis (ed.), Secure Electronic Voting, 43, 46 (2003).

[143] This would translate into vote dissociation and a disconnection of the socially disenfranchised. For a general account, see Daniel P. Tokaji, *Vote Dissociation*, 127 YALE L. J. F. 761 (2018).

[144] Stephen Ansolabehere & Charles Stewart III, *Residual Votes Attributable to Technology*, 67 J. OF POLITICS 365, 377 et seq. (2005).

[145] Section 36 of the German Federal Elections Act (Bundeswahlgesetz). In Germany, absentee voting is considered as compatible with the right to free and secret elections, see German Constitutional Court, BVerfGE 21, 200 - Briefwahl I, 2 BvC 2/66, 16 et seq. (1967) and BVerfGE 59, 119 - Briefwahl II, 2 BvC 1/81, 19 et seq. (1981). The court explicitly states that voters will usually be able to prevent others from observing their vote. Formally, Section 66 § 3 of the Federal Elections Regulation (Bundeswahlordnung) imposes a corresponding obligation on voters. If a voter cannot comply, she may feel compelled to refrain from voting, but such an abstention is not seen as unconstitutional.

3. Accuracy

Any democratic voting procedure requires mechanisms that prevent voters from voting more than once ("double-voting") and avoid having an invalid vote counted as valid.[146] Structurally, this problem is identical to the double-spending problem. Since bits can be copied and pasted at zero cost and, thus, have the features of a pure public good, there is no guarantee that the same information will not be used to perform a transaction more than once if no further constraints are imposed on the use of the information. PoW, the consensus protocol designed for Bitcoin, is precisely intended to solve this problem.[147] While PoW is designed to buttress the resilience and tamper-proofness of the distributed ledger by making mining very costly, blockchain technology is far from providing all-around safeguards against double-voting. To understand why, it makes sense to formalize the double-voting problem as a mechanism design problem.[148]

One of the most promising ways to tamper with votes and implement a double-vote is a 51 % attack (majority attack).[149] The likelihood of such an attack depends on the incentives set by the mechanism used to validate votes.[150] Under PoW, for example, the rewards for honest mining must be sufficiently large to prevent malicious miners from attacking the network. In other words, the mining mechanism needs to be incentive-compatible. Incentive-compatibility is given if the expected cost of an attack $c_a$ exceeds its benefits $B_a$:

$$c_a > B_a \tag{1}$$

Under PoW, the rewards $R$ are constantly declining at the rate $\delta$, where $0 < \delta < 1$. Miners therefore earn:

$$R_t = \delta R \tag{2}$$

---

[146] Section 14 § 4 of the German Federal Elections Act (Bundeswahlgesetz).

[147] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Whitepaper (2008), 1.

[148] For an analogous approach in the general blockchain context, see Jonathan Chiu & Thorsten Koeppl, *Incentive Compatibility on the Blockchain, in* Walter Trockel (ed.), Social Design: Essays in Memory of Leonid Hurwicz, 323, 328 (2019); Eric Budish, *The Economic Limits of Bitcoin and the Blockchain*, NBER Working Paper No. 24717 (2018), 1.

[149] Muhammad Saad et al., *Exploring the Attack Surface of Blockchain: A Systematic Overview*, Working Paper (2019), 1, 11-12, arXiv:1904.03487v1 [cs.CR] 6 Apr 2019.

[150] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Whitepaper (2008), 1, 4.

The expected cost of the attack depends on the number of controlled units of CPU power $n_p$, the cost of controlling them $c_p$ and the constantly declining rewards for earning the right to validate a block $R_t$. Therefore, the expected cost of the attack is given by:

$$c_a = n_p c_p - \delta R \tag{3}$$

Substituting (2) and (3) into (1), we can see that the mechanism used to validate votes under PoW is incentive-compatible if

$$n_p c_p - \delta R > B_a \tag{4}$$

This simple formalization yields two important insights. First, assuming a constantly decreasing $\delta$, the likelihood of an attack should decrease over time, since the expected cost of an attack increases. The intuition is that controlling many CPU units bears costs that may not be recoverable if the mining rewards $R_t$ are too low. Declining rewards or a loss of the cryptocurrency value, however, do not just reduce the incentives of an attack; they reduce the mining incentives altogether. In theory, such a reduction of mining incentives should cause a decrease in the demand for CPU units and a decline in $c_p$, that is the cost of controlling them. It follows from the analysis that the incentive compatibility constraint would likely not be satisfied in case of a sharp drop of $c_p$, thus increasing the risk of an attack.[151]

Second, an increase in the rewards will also increase the incentives to attack the blockchain. At the same time, rational miners will refrain from validating blocks containing votes if the transaction fees offered for such blocks are lower than those offered for the validation of other blocks.[152] To accelerate the procedure, the transaction fees for the validation of votes, that is $R$, would have to be increased.[153] Increasing transaction fees or maintaining them at a high level makes sure that the mining process to validate votes remains sufficiently attractive for a sufficient number of

[151] This conclusion is close to that of Joshua A. Kroll, Ian C. Davey & Edward W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*, The Twelfth Workshop on the Economics of Information Security (WEIS 2013), 1, 8 (2013). In their model, declining consensus about value can entail a direct loss of consensus about rules, and vice versa.

[152] Sven Heiberg et al., *On Trade-Offs of Applying Block Chains for Electronic Voting Bulletin Boards*, Report 2018/685, Cryptology ePrint Archive, International Association for Cryptologic Research 10 (2018).

[153] Pierre Noizat, *Chapter 22: Blockchain Electronic Vote, in* David Lee Kuo Chuen (ed.), Handbook of Digital Currency, 453, 458 (2015).

miners. The attractiveness of the blockchain network is a core condition for network effects to subsist, and network effects are key in maintaining the security of the network and the accuracy of the vote counting process.[154] The higher the number of miners, the higher the quantitative threshold to achieve consensus about the content of blocks, and the higher the security of the vote counting process.

It is not clear, however, whether transaction fees can be maintained at or increased to a level providing a reasonable degree of network security without government intervention. The reason is that miners face a prisoner's dilemma when deciding whether to accept a fee (Fig. 2).[155] If a miner (call her Miner 1) rejects a tiny fee to induce users to pay higher fees (*Cooperate*), another miner (call her Miner 2) might accept the fee (*Defect*). Miner 2 will thus prevent Miner 1 from credibly pressuring users to pay higher fees. In equilibrium, all miners will accept any transaction fee that offsets the cost of mining, that is $c_p$. One way to mitigate this problem would be to use taxpayer money to remunerate miners. Another would be to have political parties and candidates contribute to a mining budget that could then be used to disburse the transaction fees.

| | C | D |
|---|---|---|
| C | 2 , 2 | 0 , 3 |
| D | 3 , 0 | 1 , 1 |

Fig. 2: Mining Rewards Prisoner's Dilemma

An additional threat to the accuracy of the vote counting process results from the fact that block capacity is limited and that the blockchain can only process a certain amount of blocks per second. On the Bitcoin blockchain, for example, blocks are found at a low constant rate where the expected number of blocks approximates a Poisson distribution.[156] Mining a new block takes approximately ten minutes on average.[157] This means that approximately seven transactions can be validated per second at maximum

[154] Joshua A.T. Fairfield, *Bitproperty*, 88 S. CAL. L. REV. 805, 823-825 (2015).

[155] Also see Joshua A. Kroll, Ian C. Davey & Edward W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*, The Twelfth Workshop on the Economics of Information Security (WEIS 2013), 1, 12 (2013).

[156] ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION (2016).

[157] Rory Bowden, Holger Paul Keeler, Anthony E. Krzesinski & Peter G. Taylor, *Block arrivals in the Bitcoin blockchain*, CoRR, abs/1801.07447, 2018.

throughput.[158] Given that the expected number of validated blocks approximates a Poisson distribution and the latency in the network, it may take much longer than ten minutes to have a vote recorded. Assuming that 5 votes could be validated per second, it would take one minute to validate 300 votes, and one day to validate 432.000 votes. No matter how high the transaction fees, it might take up to several days to validate all votes at the country level. This makes the vote counting procedure quite cumbersome and impractical for large-scale elections. The limited scalability obviously poses serious limits to an implementation in larger countries, such as the United States or Germany. One potential, but technically demanding solution would be to use several blockchains simultaneously. Another solution is to reduce the block interval in order to accelerate the block validation process.

The block interval belongs to the core parameters of the blockchain network, and altering it involves an important trade-off between scale and security (speed and integrity). The reason is that the block interval is inversely correlated to the difficulty of the hash cryptopuzzle. The easier it gets to solve the cryptopuzzle, the faster the mining process and the lower the block interval. This also means that less CPU power is needed to tamper with blocks and attack the network. Any increase of the mining rewards needs to account for the trade-off between scale and security: As the rewards increase, an attack on the network might become more likely. It might thus be impossible to increase the speed of the voting procedure without simultaneously increasing the risk of an attack. By the same token, maintaining high mining rewards can also be necessary to maintain stable network effects. This illustrates that optimizing the blockchain parameters for a secure vote counting process is akin to squaring the circle.

A related significant threat under PoW results from the fact that miners run the risk of wasting CPU power on blocks that will ultimately not be authoritative. This sets an incentive for miners to form coalitions and join mining pools.[159] Mining pools serve as a mutual insurance against the risk of wasting CPU power, but they also entail an accrual of CPU power and work against the much heralded virtue of decentralization. On the Bitcoin blockchain, for example, four mining pools hold more than 50 % of average mining power.[160] On Ethereum, three mining pools hold more than 60 % of

---

[158] Kyle Croman et al., *On Scaling Decentralized Blockchains, in* Jeremy Clark et al. (eds.), FC 2016 Workshops, International Financial Cryptography Association 2016, LNCS Vol. 9604 (2016), 106.

[159] Ittay Eyal & Emin Gün Sirer, *Majority Is Not Enough: Bitcoin Mining Is Vulnerable*, 61 Communications of the ACM 95 (2018); Loi Luu et al., *Demystifying Incentives in the Consensus Computer*, Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 706 (2015).

[160] Adem Efe Gencer et al., *Decentralization in Bitcoin and Ethereum Networks*,

average mining power.[161] These mining pools also participate in a hardware arms race by investing in application-specific integrated circuits (ASICs) that are supposed to accelerate the solution of hash cryptopuzzles.[162]

In principle, this increases the risk of a 51 % attack. Facing a declining issuance rate of cryptocoins, mining pool members may have an incentive to change the consensus protocol in order to secure revenues.[163] They might for instance try to alter the coordination rule (e.g. the focal point provided by the longest branch) guiding the addition of new blocks. Under these circumstances, non-members have an incentive to follow the mining pool strategy in order to prevent the risk of losses from extending a branch that will ultimately not be authoritative. This would shift coordination to a new equilibrium and entail forks. Forks generated by 51 % attacks entail substantive risks for the accuracy of the voting procedure, especially a risk of double-votes and vote censorship. These risks are worrisome for two distinct reasons, a political one and an economic one.

First, most mining pools are nowadays located in China.[164] While the Chinese government will not necessarily attempt to regulate the activities of mining pools, this makes blockchain elections vulnerable to the exercise of a single foreign power and poses a non-negligible threat to the independence of the electoral process. One potential solution to this problem is the use of permissioned blockchains administered by the national elections administration. Their task would be to control the admission of foreign nodes and prevent foreign powers from taking control over the blockchain network and the outcome of the voting procedure.

Second, the risk of double-voting and vote censorship seems higher than the risk of double-spending in applications involving payments, such as cryptocurrency transfers and smart contracts. If rational payment recipients anticipate a double-spending risk, they have an incentive to refuse to accept payments.[165] In the long run, this would reduce the incentive for mining

---

Financial Cryptography and Data Security (FC) 2018, 1 (2018), https://arxiv.org/abs/1801.03998.

[161] Adem Efe Gencer et al., *Decentralization in Bitcoin and Ethereum Networks*, Financial Cryptography and Data Security (FC) 2018, 1 (2018), https://arxiv.org/abs/1801.03998.

[162] Joshua A. Kroll, Ian C. Davey & Edward W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*, The Twelfth Workshop on the Economics of Information Security (WEIS 2013), 1, 11 (2013).

[163] See Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 383 (2016).

[164] KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST, 120 (2018).

[165] Joshua A. Kroll, Ian C. Davey & Edward W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*, The Twelfth Workshop on the Economics of Information Security (WEIS 2013), 1, 12 (2013).

pools to perform attacks. In the voting context, however, no such natural protection exists, since the validation of votes is not associated with any tangible monetary stakes of any contractual counterparty.

While a monopoly over CPU power creates serious vulnerabilities to a 51 % attack, smaller fractions of mining power may actually be sufficient to hamper the accuracy of votes.[166] Minority pools can benefit from malicious strategies such as the temporary block withholding attack. Under this strategy, dishonest miners withhold discovered blocks on a private branch, while honest miners keep mining on the public blockchain. This strategy entails an intentional fork on the blockchain. Once the dishonest miners have discovered a sufficient number of blocks to exceed the length of the public chain, they reveal the blocks.[167] In principle, even single miners can attempt an attack by mining a block containing a transaction without immediately adding it to the blockchain (Finney attack).[168] The miner can then use the same cryptocoins in a new transaction. Afterwards, the miner can publish the previous block, thus invalidating the previous transaction and successfully double-spend the coins. While the Finney attack is time-sensitive and rather unlikely if block intervals are sufficiently short, it does illustrate that the blockchain is vulnerable to the acts of a few actors.

Perhaps more important is the fact that the integrity of the vote counting process does not only depend on the behavior of nodes. It also depends on the level of trust in the value of the underlying cryptocurrency used to set the right incentives for nodes. The so-called Goldfinger attack provides a vivid illustration.[169] The idea underlying this attack named after Ian Fleming's culprit Auric Goldfinger is to destroy the value of the respective cryptocurrency in order to increase the value of assets off the blockchain. A Goldfinger attack may be motivated by the search for gains from arbitrage or by hackers seeking to destabilize trust in the cryptocurrency. There are innumerable ways to influence trust in the value of the cryptocurrency, and it is normatively disputable whether the integrity of the vote counting process should depend on a parameter that is as difficult to control as trust in money.

One tool that has been proposed to facilitate cooperation in the block validation process and fend off malicious actors is to implement a procedure

---

[166] Muhammad Saad et al., *Exploring the Attack Surface of Blockchain: A Systematic Overview*, Working Paper (2019), 1, 15-16, https://arxiv.org/abs/1904.03487\#.

[167] Ittay Eyal & Emin Gün Sirer, *Majority Is Not Enough: Bitcoin Mining Is Vulnerable*, 61 Communications of the ACM 95 (2018).

[168] Muhammad Saad et al., *Exploring the Attack Surface of Blockchain: A Systematic Overview*, Working Paper (2019), 1, 15, https://arxiv.org/abs/1904.03487\#.

[169] Joshua A. Kroll, Ian C. Davey & Edward W. Felten, *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*, The Twelfth Workshop on the Economics of Information Security (WEIS 2013), 1, 13-14 (2013).

akin to an all-pay auction over the right to add a checkpoint to a block.[170] Under the rules of an all-pay auction, each bidder pays her bid, irrespective of whether she submits the winning bid. A similar system could be used to elicit the extent to which nodes support the validity of a specific branch in the blockchain. Nodes bidding for the winning checkpoint proposal would receive the bids submitted in favor of the losing checkpoint proposal. The core idea of this proposal is to facilitate consensus. Rather than relying on the longest-branch rule as a focal point and centralized checkpointing decisions by the core developers, the all-pay auction is intended to capture the nodes' valuation for specific versions of the blockchain based on the expectation of the winning proposal.

The problem of this approach is that it remains unclear why a procedure to allocate the right to add a checkpoint should provide a better focal point than the longest branch. It may well be that the focal point is set by the first, the last, the most vocally advertised, or the most discussed proposal.[171] The most important downside of such a procedure may be that it shares the features of a Keynesian beauty contest (2/3 beauty contest).[172] The goal of a 2/3 beauty contest is to pick a real number between 0 and 100, the winner being the player picking the number that is closest to 2/3 of the average number picked by all players. The Nash equilibrium of this game is 0. Experimental evidence, however, shows that people fail to correctly guess the right number.[173] Against this backdrop, it is far from clear whether checkpointing is an adequate mechanism to stabilize consensus

Overall, the double-voting problem discussed here epitomizes a broader

---

[170] Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 390 et seq. (2016).

[171] Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 392 (2016) admits these weaknesses.

[172] JOHN MAYNARD KEYNES, THE GENERAL THEORY OF EMPLOYMENT, INTEREST, AND MONEY, 156 (1936): "[T]he competitors have to pick out the six prettiest faces from a hundred photographs, the prize being awarded to the competitor whose choice most nearly corresponds to the average preferences of the competitors as a whole; so that each competitor has to pick not those faces which he himself finds prettiest, but those which he thinks likeliest to catch the fancy of the other competitors [...]. We have reached the third degree where we devote our intelligences to anticipating what average opinion expects the average opinion to be. And there are some, I believe, who practice the fourth, fifth and higher degrees." Technically, the beauty contest is closer to a unique bid auction, where a bidder wins the auction if she submits the lowest unique bid.

[173] See, e.g., John Duffy & Rosemarie Nagel, *On the Robustness of Behavior in Experimental Beauty-Contest Games*, 107 ECON. J. 1684 (1997); Antoni Bosch-Domènech et al., *One, Two, (Three), Infinity, ... : Newspaper and Lab Beauty-Contest Experiments*, 92 AM. ECON. REV. 1687 (2002); Felix Mauersberger & Rosemarie Nagel, *Levels of Reasoning in Keynesian Beauty Contests: A Generative Framework, in* Cars Hommes & Blake LeBaron (eds.), Handbook of Computational Economics, Vol. 4, Heterogeneous Agent Modeling, 541 (2018).

set of vulnerabilities of the blockchain voting procedure, especially with respect to the validation of votes. It provides a mere example of how malicious behavior on the blockchain can potentially harm the accuracy of the vote counting process. The analysis of the vulnerabilities that may result in a double-vote shed light on two important challenges that a secure blockchain voting procedure needs to accommodate: an economic one and a normative one.

The economic challenge is to design validation mechanisms so as to make an accurate block validation incentive-compatible and prevent attempts to tamper with votes. My analysis suggests that the commonly used blockchain consensus protocols, such as PoW, are not up to the task. Lacking safeguards against various types of attacks, these mechanisms might not be suited to ensure stability and accuracy in the process of validating block content, such as votes.[174] It seems that there is no perfectly decentralized or peer-to-peer mode to organize democratic voting procedures that are sufficiently resilient.[175]

The normative challenge results from the fact that the common consensus protocols are not grounded on egalitarian principles. Both 1CPU1v hard-coded into PoW and 1c1v hard-coded into PoS provide power to those who can afford to invest in CPU units or cryptocoins. There is a risk that financially powerful actors use the rules of the consensus protocol as a backdoor to bypass the usual checks and balances intended to limit the influence of such power in democratic elections. Moreover, the decisions made by the core developers may not be perceived as legitimate by the blockchain community. This might spur participants of the blockchain ecosystem to engage in collusion or initiate forks. The procedure underlying the validation of votes is therefore vulnerable to the very risks that democratic procedures should be designed to avoid.

In sum, other rules than those embedded in code and produced by the validation incentives are needed to verify the consistency of the ledger and ensure the integrity of the voting procedure. Internal consistency is guaranteed if the votes are recorded and counted exactly as they were cast. If a mismatch is identified during a post-electoral audit, the ledger should be corrected. In that case, the alleged immutability and tamper-proofness of the distributed ledger becomes self-defeating in that it exacerbates the very

---

[174] Also see Scott J. Shackelford & Steve Myers, *Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace*, 19 YALE J. L. & TECH. 334, 381 (2017).

[175] For a similar thought, see Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 404 (2016), who claims that "we should not expect or want peer-to-peer decision-making to take over our central democratic institutions."

problem it was intended to prevent in the first place.[176] To solve this problem, the voting system could take recourse to human auditors who could broadcast the corrected version of the vote to the blockchain and have it validated, potentially through a smart contract.

### *B. Preserving Privacy*

Democratic elections need to strike a complex balance between transparency and privacy. On the one hand, the voting procedure has to satisfy the demands of transparency, thus enabling citizens to understand and trace all the procedural steps between the decision to attend the polling place and the announcement of the electoral outcome. On the other hand, some elements of democratic voting procedures call for strong protections of privacy in order to ensure freedom from coercion and manipulation.

#### 1. Polling Secrecy

Any democratic voting procedure requires some mechanism that prevents voters from being strongly influenced by the voting behavior of others or their belief about the voting behavior of others. On the view of traditional voting models proposed by Anthony Downs or Gordon Tullock, each voter should only be driven by the expected effect of her individual vote on the outcome of the procedure.[177] Research in political psychology and behavioral economics, however, shows that voting behavior is far from being exogenous to social interactions and comparisons with reference groups.

For example, voters may refrain from casting a ballot if they believe that the outcome of the elections cannot be turned. Or they may fall prey to a bandwagon effect: Rather than voting strategically, voters may simply follow their desire to behave in conformity with a perceived majority and vote for the candidate they believe will be the winner of the election.[178] A

---

[176] Sven Heiberg et al., *On Trade-Offs of Applying Block Chains for Electronic Voting Bulletin Boards*, Report 2018/685, Cryptology ePrint Archive, International Association for Cryptologic Research 9 (2018).

[177] ANTHONY DOWNS, AN ECONOMIC THEORY OF DEMOCRACY, 7 (1957); GORDON TULLOCK, TOWARD A MATHEMATICS OF POLITICS (1967).

[178] Haldun Evrenk & Chien-Yuan Sher, *Social interactions in voting behavior: distinguishing between strategic voting and the bandwagon effect*, 162 PUBLIC CHOICE 405, 407 et seq. (2015), who correctly point out that it is difficult to know whether voters want to be on the winning side because they have a tendency to vote for winners or because they hold the erroneous belief that their vote will be pivotal. Also see Rebecca Morton & Kai Ou, *What motivates bandwagon voting behavior: Altruism or a desire to win?*, Working Paper (2015), 1.

bandwagon effect can be seen as infringing on the freedom of the vote, but even if one does not assume coercion in the legal sense, such as *vis compulsiva*, it could have deleterious consequences for the outcome of the election.

To prevent the risk of bandwagon effects, many electoral laws contain specific provisions that prohibit the diffusion of polling results or votes before the end of the voting procedure. Under German law, for example, the publication of results of surveys conducted among voters after they have cast their votes shall be inadmissible before the end of the voting procedure.[179] Such confidentiality requirements make sure that other citizens' voting behavior remains sufficiently opaque during the election and that voters cannot form beliefs about the potential outcome of the election based on observed voting behavior. Therefore, all votes or interim results should remain sufficiently opaque up to the very end of the voting phase.

Such safeguards cannot be established on the blockchain, especially if it is public and permissionless. Public blockchains, such as Bitcoin or Ethereum, are designed to offer nodes and the general public unrestricted access to the ledger. This implies that any interested and tech-savvy voter can observe how other people voted or that information about current voting behavior can be divulged to the public before the end of the voting procedure. Providing access to this information before the polling places have been closed is incompatible with the aforementioned principle of polling secrecy.

Computer scientists have proposed different cryptographic solutions to the problem of polling secrecy, but it is far from clear whether these solutions can effectively guarantee compliance with the legal principle. Some solutions like Open Vote Network are based on a self-tallying voting protocol that is implemented as a smart contract on Ethereum and eliminates the need for a central tallying authority.[180] Under this protocol, votes are encrypted and tallied in an open procedure that enables any person to tally the votes once all votes are cast. The upside of this protocol is that it effectively preserves ballot secrecy, since voters would have to collude to reveal a vote that has been cast. The downside is that the last voter to cast her ballot is the first who can tally the votes.[181]

---

[179] Section 32 § 2 of the German Federal Elections Act (Bundeswahlgesetz). According to Section 75 § 3 of the German Federal Elections Regulation (Bundeswahlordnung), the same holds for absentee ballots cast before Election Day.

[180] Patrick McCorry, Siamak F. Shahandashti & Feng Hao, *A Smart Contract for Boardroom Voting with Maximum Voter Privacy, in* Aggelos Kiayias (ed.), Financial Cryptography and Data Security, LNCS Vol. 10322 (2017), 357, 358.

[181] Patrick McCorry, Siamak F. Shahandashti & Feng Hao, *A Smart Contract for Boardroom Voting with Maximum Voter Privacy, in* Aggelos Kiayias (ed.), Financial

This creates strategic problems. On the one hand, if the last voter knows the tally, her voting behavior may be influenced by this knowledge. On the other hand, if the last voter dislikes the outcome of the tally, she can simply refrain from casting her vote, thus wrecking the entire voting procedure. The technicalities of this self-tallying protocol illustrate how vulnerable a decentralized tallying protocol can be. More generally, most blockchain applications, such as Bitcoin or Ethereum, are designed to enable as much transparency of block content as possible without infringing on the privacy of the persons involved in the transaction. Polling secrecy, by contrast, requires both temporary secrecy of block content and permanent personal privacy.

A viable solution to the problem of polling secrecy may be the use of zero-knowledge proofs.[182] Zero-knowledge proof is a cryptographic method that enables its user to prove that a particular decision, say a vote, has been reached and that it satisfies specific conditions without revealing what the actual decision is.[183] It thus enables an agent to prove that he knows something or made some decision without having to reveal what she knows or decided. In the blockchain context, for example, ZCash enables coinholders to prove that a transaction is valid (= verify encrypted information) without revealing their identity, the identity, or that of the recipient (= without decrypting the information).[184] How do zero-knowledge proofs work?

Suppose that there is a ring-shaped cave with one entrance on each side.[185] The two paths, A and B, are connected by a door inside the cave, but the door can only be opened with a secret spell. Alice claims she knows the spell and wants to prove it to Bob without revealing the spell. To deliver the proof, Alice takes a random path. Bob then tells Alice which path she should return on. If Alice never fails to return on the requested path, this is proof that she knows the spell.

Zero-knowledge proof protocols might be a viable method of proving the validity and number of votes without revealing their content before the end of the election. But even if such a cryptographic solution can be implemented, it will likely be difficult to effectively preserve polling

---

Cryptography and Data Security, LNCS Vol. 10322 (2017), 357, 359.

[182] For the initial conception, see Shafi Goldwasser, Silvio Micali & Charles Rackoff, *The knowledge complexity of interactive proof systems*, 18 SIAM J. COMP. 186 (1989).

[183] Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PENN. L. REV. 633, 668-669 (2017).

[184] Eli Ben-Sasson et al., *Zerocash: Decentralized Anonymous Payments from Bitcoin*, 2014 IEEE Symp. on Sec. & Priv. 459 (2014).

[185] For this famous example, see Jean-Jacques Quisquater et al., *How to Explain Zero-Knowledge Protocols to Your Children, in* Gilles Brassard (ed.), Advances in Cryptology - CRYPTO' 89 Proceedings, LNCS Vol. 435 (1990), 628.

secrecy without any centralized oversight. If a centralized authority is required to preserve polling secrecy, one may well wonder whether the benefits of decentralizing the vote counting process really outweigh the overall costs required to centrally monitor the other parts of the blockchain voting procedure.

2. Ballot Secrecy

Any democratic voting procedure should provide safeguards against coercion. Arguably, the most important design feature against coercion in offline elections is the private voting booth. The core function of the private voting booth is to protect ballot secrecy and make it impossible for voters to prove how they voted. This is also a core concern underlying the design of laws allowing absentee voting.[186] If voters could prove how they voted, votes could be turned into tradeable commodities or bargaining chips. Voters could be blackmailed or bribed to have them vote in a certain way, and interested parties could engage in vote buying.

Many electoral laws contain specific provisions intended to prevent these risks. German law, for example requires measures to ensure that the voter cannot be observed while putting a mark on the ballot paper and folding it.[187] Similarly, the ballot box needs to be designed such that the secrecy of the ballot is preserved. In the United States, the Massachusetts Ballot Act of 1888 was the first state law to establish ballot secrecy at the state level. At present, most elections are run using secret ballots (Australian ballots). Moreover, U.S. federal law prohibits offers to make an expenditure to any person to vote or withhold his vote or acts by which a person solicits, accepts, or receives any such expenditure are prohibited by federal criminal law.[188]

Blockchain technology does not provide any comparable safeguards. Specifically, blockchain technology does not set any barriers for voters that prevent them from proving how they voted.[189] If votes are not cast in a

---

[186] Lilian Mitrou et al., *Electronic Voting: Constitutional and Legal Requirements and Their Technical Implications, in* Dimitris A. Gritzalis (ed.), Secure Electronic Voting, 43, 51 et seq. (2003).

[187] Section 33 § 1 of the German Federal Elections Act (Bundeswahlgesetz). According to Section 34 § 2, each voter has an obligation to fold her paper ballot such that nobody can see how she voted and to then put it into an urn.

[188] 18 U.S.C. § 597. However, Art. IV § 2 of the Constitution of West Virginia provides that in all elections "the voter shall be left free to vote by either open, sealed or secret ballot, as he may elect."

[189] Patrick McCorry, Siamak F. Shahandashti & Feng Hao, *A Smart Contract for Boardroom Voting with Maximum Voter Privacy, in* Aggelos Kiayias (ed.), Financial Cryptography and Data Security, LNCS Vol. 10322 (2017), 357, 366; Stefano Bistarelli et

physically secluded, private booth, voters may be inclined to sell their votes to those who observe them.[190] Since voters can always prove how they voted, malicious actors should have a willingness to pay for votes. Conversely, the possibility to prove may also induce malicious actors to extort votes, thus exposing voters to the risk of voting under duress. Voters therefore face a serious threat of coercion.

It is important to note that these problems are not software issues, but hardware issues. The absence of physically secluded voting booths also bears the risk of bringing in social norms and behavioral habits into a procedure intended to preserve the freedom of choice and immunity from social influences on the act of voting. The problem is particularly acute under blockchain voting procedures that allow for mobile or home voting. Consider the tech literate caretaker who wants to "help" the elderly with their political choice. Or consider the employer who offers some "advice" to his employees when casting their electronic ballot at lunchtime.

The only way to effectively maintain ballot secrecy at a large scale is to establish physical barriers rendering a proof factually impossible. If ballot secrecy is to be maintained, the voting procedure requires rules that force voters to attend polling places, have their identity verified, and use a voting booth.[191] These architectural safeguards could and probably should be backed by legal rules imposing sanctions on third parties who take measures aimed at infringing on ballot secrecy.

### 3. Political Privacy

Any democratic voting procedure requires safeguards against intrusions on political privacy. Providing such safeguards is particularly important in voting procedures based on technologies that can be used to amass vast amounts of data relating to electoral behavior. Political privacy not only covers ballot secrecy in the narrow sense, but also personal data generated before and after the election. Personal data relating to electoral behavior and data required for the verification of eligibility or voter authentication is valuable both for commercial and political purposes.

In most of the United States, it is common practice to gather data

---

al., *End-to-End Voting with Non-Permissioned and Permissioned Ledgers*, 17 J. GRID COMPUTING 97 (2019).

[190] The problem is not that breaking ballot secrecy would entail a market for votes. Under a quadratic voting system (see Part II.C.), for example, there should be no objection to buying and selling votes, as long as voters are free to choose and no market failure occurs. The real problem results from the unintended deviation from the principle of egalitarian consent.

[191] Ryan Osgood, *The Future of Democracy: Blockchain Voting*, COMP116: Information Security, 1, 14 (2016).

including name, address, signature, date of birth, phone number, gender, the social security number, party affiliation, and sometimes voter history in voter registration databases.[192] These databases are disseminated to all kinds of organizations, including political parties, commercial and news organizations. Most notably, the primary and secondary purposed to which this data may be processed are unrestricted, and only some States redact parts of the databases before releasing them for secondary purposes. German law, by contrast, is much more restrictive in that it only allows the transmission of the name, a doctoral title if applicable, and the address to political parties and campaigns.[193] These data may only be used for purposes of the upcoming campaign and have to be deleted afterwards.

Political privacy can be seen as a core prerequisite of free democratic elections. Therefore, legal scholars in Germany and, more broadly, Europe tend to argue that election authorities are not allowed to disseminate data falling within the scope of political privacy for purposes other than political campaigns.[194] While U.S. legal scholars have been struggling to determine adequate constitutional foundations to justify the need for privacy, two distinct sets of arguments have recently emerged.

The first set of arguments is based on the idea of intellectual privacy and the behavioral effects resulting from an unwanted gaze.[195] People who are or fear that they could be subject to observation will likely behave in conformity with existing or assumed social expectations. Surveillance bears the risk of generating a normalizing effect and curtailing the panoply of sometimes deviant and unpleasant behaviors that democratic societies need to flourish. Moreover, surveillance may deter people from expressing their ideas and opinions, thus resulting in self-censorship and chilling effects.[196]

The idea to provide safeguards against chilling effects is strongly anchored in modern First Amendment doctrine, but it has only recently been extended to intrusions into intellectual privacy.[197] To the extent that

---

[192] Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, WISCONSIN L. REV. 861, 868 et seq. (2014).

[193] Section 50 § 1 of the Federal Registration Act (Bundesmeldegesetz).

[194] A broader dissemination is considered as being incompatible with the right to privacy granted by Art. 8 of the European Convention of Human Rights, see Lilian Mitrou et al., *Electronic Voting: Constitutional and Legal Requirements and Their Technical Implications, in* Dimitris A. Gritzalis (ed.), Secure Electronic Voting, 43, 53 (2003).

[195] Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, WISCONSIN L. REV. 861, 905 et seq. (2014).

[196] For a classic account, see Frederick Schauer, *Fear, Risk, and the First Amendment: Unraveling the "Chilling Effect"*, 58 B.U. L. REV. 685, 730 (1978). For a recent account, see Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERK. TECH. L. J. 117 (2016).

[197] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1948 et seq. (2013); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1905 (2013).

surveillance stifles creative and innovative thoughts and behaviors, it qualifies as an unjustifiable restriction of free speech. Nonetheless, the U.S. Supreme Court remains skeptic of an extension of chilling effects theory to intrusions into privacy. In *Laird v. Tatum* and *Clapper v. Amnesty International*, the Supreme Court maintained the fear of chilling effects does not provide a sufficient basis to assume specific harm and a violation of constitutional rights.[198] The German Constitutional Court, by contrast, has recognized a right to informational self-determination and has justified it on the grounds that a person who does not know who knows what and when about her may refrain from exercising those rights that are considered as preconditions of a liberal democracy.[199]

Perhaps the most striking difference in justifying the use of the chilling effects theory is that legal scholars in Germany have questioned neither its psychological foundations nor its empirical basis.[200] This is in line with the fact that empirical legal studies and social science approaches to the law have played and still play a relatively small role in continental legal scholarship. U.S. legal scholars, by contrast, have criticized the lack of substantive empirical evidence in support of chilling effects.[201] While it is true that empirical evidence remains scant, the main reason being the difficulty to measure chilling effects, scholars have been able to show their occurrence and specify the underlying psychological forces.[202]

But even to the extent that more and better empirical evidence is needed to provide a sound account of chilling effects, the theory should not be discarded on merely empirical grounds. The main reason is that the chilling effects theory should primarily be considered as a normative theory that reflects a constitutionally grounded set of risk preferences. As mentioned earlier, the chilling effects theory is embedded in a set of value judgements

---

[198] Laird v. Tatum, 408 U.S. 1, 15 (1972); Clapper v. Amnesty International, 133 S. Ct. 1138, 1152 (2013).

[199] German Constitutional Court, BVerfGE 65, 1 - Volkszählung, 1 BvR 209, 269, 362, 420, 440, 484/83 (1983).

[200] But see YOAN HERMSTRÜWER, INFORMATIONELLE SELBSTGEFÄHRDUNG (2016).

[201] Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 480 (2015); Leslie Kendrick, *Speech, Intent, and the Chilling Effect*, 54 WM. MARY L. REV. 1633, 1657 (2013); Vincent Blasi, *The Pathological Perspective and the First Amendment*, 85 COLUM. L. REV. 449, 482 (1985).

[202] Yoan Hermstrüwer & Stephan Dickert, *Sharing is daring: An experiment on consent, chilling effects and a salient privacy nudge*, 51 INT. REV. L. ECON. 38 (2017); Alex Marthews & Catherine Tucker, *Chapter 18: The Impact of Online Surveillance on Behavior, in* David Gray & Stephen E. Henderson (eds.), The Cambridge Handbook of Surveillance Law, 437 (2017); Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERK. TECH. L. J. 117 (2016).

implicitly enshrined in constitutional law.[203] Accordingly, both the First Amendment and the right to informational self-determination contain a commitment to err on the side of caution. This commitment is based on the implicit assumption that citizens are risk-averse and that the constitutional rights that would be curtailed by risk-averse behavior are too precious to incur the risk of conforming behavior. The law therefore requires neither a case-specific nor a perfect proof of chilling effects.

The second set of arguments rests on the idea of voter manipulation through microtargeting.[204] On the one hand, data recorded in voter registration databases can be used to target specific voters and motivate them to vote in favor or against certain political parties or candidates. On the other hand, the entities holding personal data can use it to exclude certain voters from targeted information and disconnect them from ongoing political debates in order to demobilize them. Both strategies have the potential to exacerbate existing inequalities.[205] By creating insular discourses and preventing a shared understanding of common political problems, these actors can drive a wedge between different voter groups. The fragmentation of voter groups bears the risk of resulting in a breakdown of a public discourse based on a commonly shared sense of facts and political problems.

These risks exist on both sides of the Atlantic, but the legal safeguards to prevent them differ substantially. In the European Union, the rules guiding the processing of political data are relatively strict. According to Art. 8(1) of the European General Data Protection Regulation (EU-GDPR) the processing of data revealing political opinions is prohibited, at least in principle. Art. 8(2) EU-GDPR allows for several exceptions to this principle, for example, when a person has given her consent or when processing is necessary for reasons of substantial public interest.[206] If political data is processed, each person is entitled to transparent information under Art. 12, 13, and 14 EU-GDPR, including information about the data

---

[203] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1950 (2013).

[204] Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, WISCONSIN L. REV. 861, 905 et seq. (2014); Frederik J. Zuiderveen Borgesius et al., *Online Political Microtargeting: Promises and Threats for Democracy*, 14 UTRECHT L. REV. 82 (2018).

[205] Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, WISCONSIN L. REV. 861, 908 et seq. (2014).

[206] For an analysis of the problems associated with consent, see Yoan Hermstrüwer, *Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data*, 8 JIPITEC 9 (2017). On the (behavioral) economics of privacy, see generally Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LIT. 442 (2016); Alessandro Acquisti, Leslie K. John & George Loewenstein, *What Is Privacy Worth?*, 42 J. LEG. STUD. 249 (2013).

processing entities, the data processing purposes, the right to withdraw consent, the right to object to data processing, the right to access the data, or the right to erasure. The EU-GDPR thus sets relatively sharp limits to the use of political data. In the United States, no similar protections exist. But recent proposals are aimed at requiring political actors to disclose how they process and use campaign data and attach specific disclaimers to political ads in order to draw people's attention to the fact that they are exposed to partisan information.[207]

### *C. Creating Legitimacy*

The ultimate challenge that any democratic voting procedure needs to account for is how public powers and government authority can be endowed with democratic legitimacy and how the institutions operated by these powers can remain stable over time. This is a particularly daunting challenge when it comes to implementing blockchain voting procedures.

#### 1. Procedural Justice

Several legal theories have attempted to establish the fundamental conditions for legitimacy. While legitimacy is grounded on consent or representation in some theories, other theories of democratic legitimacy are grounded on the ability to establish a political truth.[208] In the theoretical framework proposed by H.L.A. Hart, the stability of the legal order and the outcomes generated by its institutions are ultimately determined by a "rule of recognition," a meta-rule identifying what counts as law that serves as a focal point in the coordination over which rules should be accepted as law and which outcomes should be accepted as legitimate.[209] All these legitimacy theories build on some general or inter-subjectively shared agreement on what is right or true, but they do not specify the conditions under which such an agreement can be formed.

One of the main conditions for achieving such an agreement and, as a consequence, establishing legitimacy is procedural justice.[210] From the perspective of procedural justice theories, the stability of institutions depends not just on the institutions themselves but also on the resilience of

---

[207] Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, WISCONSIN L. REV. 861, 910-921 (2014).

[208] David Estlund, *Making truth safe for democracy, in* David Copp, Jean Hampton & John Roemer (eds.), The Idea of Democracy, 71 (1993).

[209] H.L.A. HART, THE CONCEPT OF LAW, 107 et seq. (1961).

[210] Tom Tyler, *Achieving peaceful regime change: Why do losers consent?*, Yale Law School Working Paper (2013), 1.

the procedures leading to their installment. Legitimacy results from the procedures through which an institution is endowed with power, and this source of legitimacy is very different from the procedures that an institution uses in the exercise of its power.[211] Elections are often assessed as one of the building blocks of fair procedures to select public authorities both in the eyes of voters who supported the winning candidates and those who opposed them, one reason being that they have the potential to establish acceptance of election outcomes, even among citizens who voted for the losing party or candidate.

In democracies, these procedures require participation opportunities or voice, either through a direct procedure (voting) or through an indirect procedure (representation). Political elections are not just fundamental decisions over the allocation of legislative, executive and judicial power in democracies; they are the main source for the legitimacy of the authority attached to the decisions of the three branches. Democratic procedures induce citizens to accept outcomes and political leaders, even when these outcomes and leaders are seen as unfavorable by some citizens.[212] If the voting procedure is flawed or not sufficiently resilient, there is a risk that the institutions arising from these procedures will suffer from a lack in legitimacy, a concern that was prominently raised in the aftermath of *Bush v. Gore*.[213]

The central deontological premise of legitimacy models building on procedural justice theories is that the adherence to fair electoral procedures serves as the main source of legitimacy.[214] The ontological flip-side of procedural justice is that it is expected to foster the stability of the institutions and the acceptance of outcomes they generate. It enables a smooth transition between different representatives holding power and contributes to institutional stability by reconciling the winners and losers of an election and preventing rebellions and social unrest.[215] The procedural justice approach squares well with other legitimacy theories that have emerged in the social sciences over the last three decades, especially in economics and psychology.

Research in the psychology of procedural justice and in behavioral

---

[211] Tom R. Tyler, *Legitimacy and legitimation*, 57 ANN. REV. PSYCH. 375 (2006).

[212] Tom Tyler, *Achieving peaceful regime change: Why do losers consent?*, Yale Law School Working Paper (2013), 1, 3.

[213] BRUCE ACKERMAN (ED.), BUSH V. GORE: THE QUESTION OF LEGITIMACY (2002).

[214] Tom Tyler, *Achieving peaceful regime change: Why do losers consent?*, Yale Law School Working Paper (2013), 1, 5.

[215] Tom Tyler, *Achieving peaceful regime change: Why do losers consent?*, Yale Law School Working Paper (2013), 1, 3; Celia M. Gonzalez, C. & Tom R. Tyler, *The psychology of enfranchisement: Engaging and fostering inclusion of members through voting and decision-making procedures*, 64 J. SOC. ISS. 447 (2008).

economics shows that people derive utility not just from outcomes but also from the procedures generating outcomes.[216] The general commonality of the conclusions inferred from these studies is that people not only have preferences over outcomes, but also over procedures. In sum, people derive *procedural utility*, a concept that captures both the non-instrumental pleasure derived from the procedure and the fact that procedures are instrumental in generating outcome acceptance.

Against this backdrop, it is far from clear to what extent blockchain voting procedures can actually satisfy basic procedural justice requirements. The reason is that blockchain voting procedures may not confer a sufficient degree of control which may be the most important adjusting screw in the machinery of procedural justice. The procedural justice theory proposed by John Thibaut and Laurens Walker, for example, makes a distinction between *process control* and *outcome control*.[217] Process control refers to the ability to control the inputs of the decision making procedure, influence the rules guiding the interpretation of evidence, and exercise voice. Accordingly, a legal procedure giving people the right to be heard offers a reasonable degree of process control.[218] Outcome control, by contrast, refers to the ability to attack the outcome and alter it even once the decision has been made. When individuals can exercise process control and outcome control, the respective decisions are perceived as fairer.[219]

In the blockchain context, voters have only limited process control. Process control would require enabling the electorate to modify consensus protocols and influence the algorithms used to validate votes. On permissioned blockchains, process control is necessarily limited, since the ultimate responsibility and power to shape the algorithm rest with a central authority. While voters may have more process control on permissionless blockchains, at least in theory, the set of realistic options to control consensus protocols and algorithms is likely to be de facto constricted. Only few voters will be tech-savvy enough to actually operate nodes and shape

---

[216] For the psychology of procedural justice, see E. ALLAN LIND & TOM R. TYLER, THE SOCIAL PSYCHOLOGY OF PROCEDURAL JUSTICE (1988). For research in in behavioral economics, see Bruno S. Frey, Matthias Benz & Alois Stutzer, *Introducing Procedural Utility: Not Only What, but Also How Matters*, 160 J. INST. & THEORETICAL ECON. 377 (2004); Alois Stutzer & Bruno S. Frey, *Political participation and procedural justice: An empirical study*, 45 EUR. J. POL. RESEARCH 391 (2006).

[217] JOHN W. THIBAUT & LAURENS WALKER, PROCEDURAL JUSTICE: A PSYCHOLOGICAL ANALYSIS (1975).

[218] See, e.g., PASCAL LANGENBACH, DER ANHÖRUNGSEFFEKT: VERFAHRENSFAIRNESS UND RECHTSBEFOLGUNG IM ALLGEMEINEN VERWALTUNGSVERFAHREN (2017).

[219] JOHN W. THIBAUT & LAURENS WALKER, PROCEDURAL JUSTICE: A PSYCHOLOGICAL ANALYSIS (1975); Min Kyung Lee et al., *Procedural Justice in Algorithmic Fairness: Leveraging Transparency and Outcome Control for Fair Algorithmic Mediation*, 3 PROC. ACM HUM.-COMPUT. INTERACT. 182:1 (2019).

the rules underlying the validation of votes. Moreover, the consensus protocols that are now most commonly used, specifically PoW, are likely to be incompatible with the political preferences of an increasing fraction of the electorate, especially in the European Union. Given the high energy requirements of PoW, current blockchain voting procedures are based on a principle that ecologically conscious voters object. This could be an additional roadblock on the way to achieving large-scale process control and acceptance.

The ability to exercise outcome control appears to be limited as well, paradoxically for reasons that are usually considered as normative advantages of blockchain technology. Due to the immutability of the blockchain, it is basically impossible to modify the content of validated blocks. Hence, it is impossible to undo or, in the more likely event, correct the result of the blockchain voting procedure by invalidating spoiled votes. Outcome control, however, requires a possibility to change the voting history if facts discovered after the election would legally justify or even require an invalidation of votes (e.g. in the case of facts establishing the ineligibility of voters). To the extent that the law prescribes the retroactive invalidity of spoiled ballots, the immutability of the distributed ledger is incompatible with the flexibility required by the law.[220]

In sum, these considerations illustrate that several blockchain design features hailed as legal advantages can also be considered as legal downsides, especially with respect to procedural justice. Process control requires the ability for all voters to assess the rules of the blockchain voting procedure and monitor compliance with these rules, for example by serving at polling places. Yet operating a node to validate votes on the blockchain requires technical knowledge that only a small minority of voters have. Outcome control requires flexibility in the modification of decision outcomes. Yet blockchain voting procedures are designed to precisely make the voting outcome immune against post-electoral modifications.

### 2. Trust

Any democratic voting procedure requires rules and safeguards making sure that voters and those affected by the election can and do trust the integrity of the voting procedure and the accuracy of the election outcome.[221] Trust, in the words of sociologist Niklas Luhmann, is a social

---

[220] Jeremy M. Sklaroff, *Smart Contracts and the Cost of Inflexibility*, 166 U. PA. L. REV. 263, 291 et seq. (2018) makes a related argument in the context of smart contracts.

[221] Lilian Mitrou et al., *Electronic Voting: Constitutional and Legal Requirements and Their Technical Implications, in* Dimitris A. Gritzalis (ed.), Secure Electronic Voting, 43, 54-56 (2003).

mechanism that reduces complexity and operates as an alternative to rational prediction.[222] On this view, trust does not require perfect verifiability. Rather, it presumes that the trustors do not or cannot fully verify the behavior of the trustee. It enables people to accept risks and the vulnerability to specific actions of other agents in control of a process and its outcome without being able to exercise full control themselves. Trust can thus be considered as a compensatory condition of democratic legitimacy when process and outcome control are limited.

In the electoral context, voters should be able to trust that their ballot reflects the actual candidate they intended to cast a vote for, that their ballot was recorded as cast, and that their ballot was counted as recorded. It is essential that all social groups trust the integrity of the voting procedure and the accuracy of the election, since a lack of trust negatively affects voter turnout and may thus infringe on the legitimacy of the institutions resulting from the election.[223] A specific problem arising in the context of political elections is that those who voted for the winning party or candidate trust the outcome of the election more than voters who cast their ballots for the losers (winner-loser-effect).[224]

The traditional response to prevent trust deficits from destabilizing political institutions supported by winning majorities is to establish rules guiding the supervision of elections and post-electoral control. On the one hand, traditional voting procedures both in the United States and the European Union are based on centralized government control and supervision by the electoral administration. On the other hand, the electoral administration is embedded in a robust setup of institutional checks and balances, including judicial control.[225] The downside of this system of shared control by the executive and judicial branches is that it may be difficult to understand for citizens. To the extent that voters are subject to information asymmetries and therefore distrust the monitoring institutions, there is a risk of a failure of the political market. Voters may be unable to distinguish between real threats, such as limited access to voting for the disenfranchised, and fictitious threats, such as purported manipulations of the law by immigrants. On this view, the rise of populist movements on

---

[222] NIKLAS LUHMANN, TRUST AND POWER, 27 et seq. (1979).

[223] R. Michael Alvarez, Thad E. Hall & Morgan H. Llewellyn, *Are Americans Confident Their Ballots Are Counted?*, 70 J. POL. 754 (2008).

[224] Teogenes Moura & Alexandre Gomes, *Blockchain Voting and its effects on Election Transparency and Voter Confidence*, Proceedings of the 18th Annual International Conference on Digital Government Research, 574 (2017).

[225] Under Art. 41 § 2 and Art. 93 § 1 Nr. 5 of the German Constitution, elections to the national parliament (Bundestag) are subject to judicial control by the German Constitutional Court (Wahlprüfungsbeschwerde). Also see Martin Morlok, *Art. 41, in* Horst Dreier (ed.), Grundgesetz Kommentar, Bd. II, 3. Aufl., Rn. 24 (2015).

both sides of the Atlantic can be considered as the result of massive trust deficits and weak institutional trust anchors.[226]

The procedural safeguards provided by blockchain voting procedures are substantially more complex than those embedded in traditional voting procedures. And as I have shown in the previous sections, blockchain technology suffers from significant security loopholes and vulnerabilities. This begs the question whether blockchain voting procedures provide sufficient trust anchors so as to enable the citizens to take the necessary leap of faith. A democratic voting procedure does not require maximum security. But the security level needs to be such that the sensitive balance between transparency and secrecy, between publicity and privacy is not disrupted. Moreover, the technology should provide anchors for what social scientist call *systemic* and *personal* trust. I doubt whether blockchain technology meets these requirements.

Systemic trust refers to the confidence in the reliability of an abstract principle or social institutions.[227] The foundations of systemic trust can be described as the product of a cognitive assessment of how the institution or mechanism operates. Blockchain voting procedures require trust in the underlying infrastructure and the technology underlying the electoral process. While the consensus protocols are said to enable trust among nodes, this does not imply that the consensus protocols necessarily establish trust among those who are affected by the nodes' decisions. Consensus protocols and the encryption methods used to preserve the secrecy of the ballot and political privacy are beyond any control of the general public. It is therefore not clear why voters should trust validating nodes without further ado. One potential trust anchor is to establish tools allowing voters to check whether their vote was counted.[228]

Personal trust refers to the expectation vis-à-vis a specific person or group.[229] Unlike systemic trust, it operates at the micro-level and often requires a strong emotional foundation. Establishing such a foundation will usually not be possible without being familiar with the person and repeated interactions. In the context of blockchain voting procedures, those who need to be trusted are the core developers. They wield the ultimate power to alter the course of the blockchain, for example by reverting a fork, or to stabilize

---

[226] This does not rule out other explanations for the crisis of democracy, especially rising inequality. See, e.g., Aziz Huq & Tom Ginsburg, *How to Lose a Constitutional Democracy*, 65 UCLA L. REV. 78, 81 et seq. (2018); DANIEL MARKOVITS, THE MERITOCRACY TRAP: HOW AMERICA'S FOUNDATIONAL MYTH FEEDS INEQUALITY, DISMANTLES THE MIDDLE CLASS, AND DEVOURS THE ELITE, 46 et seq. (2019).

[227] NIKLAS LUHMANN, TRUST AND POWER (1979).

[228] Kevin Kirby, Anthony Masi & Fernando Maymi, *Votebook: A proposal for a blockchain-based electronic voting system*, New York University, Whitepaper (2016), 1.

[229] NIKLAS LUHMANN, TRUST AND POWER (1979).

its basic structure, for example by including checkpoints. If a software update is considered as generally accepted, the core developers sometimes make the authoritative decision to include a checkpoint in a block, thereby making it impossible to alter the content of blocks prior to the checkpointed block.[230]

It remains fundamentally unclear whether voters can and should trust the core developers. Ultimately, the main source of trust is the belief that the blockchain is supervised and governed by a benevolent dictator. The incident known as The DAO hack provides a vivid illustration. The DAO, a decentralized autonomous organization created in 2016, was a crowdfunding platform designed to perform corporate operations entirely through Ethereum smart contracts. In June 2016, hackers executed a series of perfectly valid smart contracts to siphon off one third of The DAO's funds.[231] Vitalik Buterin and other Ethereum developers had to convince a majority of nodes to perform a hard fork in order to return the stolen funds.[232] This episode illustrates that the blockchain is far from being a trustless technology. On the contrary, it heavily relies on trust in a rather centralized group of core developers. Without sound governance structures or a group of benevolent dictators able to prevent the blockchain from rigging the election, it will likely be impossible to establish trust.

Even if the ballot counting procedure can be fully decentralized, blockchain voting procedures do not eliminate the need for a conventional electoral administration that schedules the election, creates ballots, provides IDs, authenticates voters, and announces the election results. These centralized government authorities need to be trusted as well. To the extent that blockchain voting procedures cannot be implemented without trustworthy government authorities, one may wonder why citizens should not entrust this entity with the ballot recording and counting procedure as well.[233] The costs of establishing trust in the blockchain and its developers may well exceed the benefits of a decentralized ballot count.

### 3. Transparency

---

[230] See Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 385 et seq. (2016).

[231] Kevin Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L. J. 489, 517 (2018).

[232] The result was a split of the Ethereum blockchain, with a branch running the old software (Ethereum Classic) and a branch running the new software (Ethereum). See KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST, 67 et seq. (2018).

[233] See, e.g., Morgan E. Peck, *Do You Need a Blockchain?*, IEEE Spectrum October 2017, 38, 39 (2017).

The use of an election is *per se* insufficient to guarantee legitimacy. From the perspective of procedural justice theories, legitimacy not only requires that the election outcome adequately reflects the voters' preferences. As I have discussed in the previous section, voters also need to trust that the voting procedure effectively achieves this. Institutional safeguards and a governance system based on checks and balances are one way of generating trust. Another is to establish transparency.

While it is not easy to precisely determine the conditions for transparency, the comprehensibility of a blockchain voting procedure can be seen as a central building block of transparency. The debate surrounding the "right to an explanation" mentioned in Recital 71 EU-GDPR illustrates increasing concerns over how to explain algorithm-based processes and outcomes to those affected.[234] The claim for explanations and algorithmic transparency is prominent in the context of machine learning and, at first glance, it appears to be similarly appealing in the context of blockchain technology, specifically with respect to consensus protocols. At a closer look, however, the analogy between the transparency of machine learning algorithms and blockchain consensus protocols seems overblown, at least in the context of blockchain voting procedures.

The transparency problem associated with blockchain voting procedures does not primarily result from the complexity or opacity of the algorithms.[235] Rather, it is very difficult to convey convincing information on the reasons why blockchain voting procedures should be considered as sufficiently safe. The previous discussion on the vulnerabilities of blockchain voting procedures, on the contrary, suggests that transparency may create further distrust in the integrity of blockchain voting procedures rather than trust. This, of course, does not mean that governments tinkering with blockchain voting procedures should refrain from establishing transparency. Rather, shedding light on the risks of blockchain voting procedures also elucidates the dimensions on which traditional voting procedures can be considered as transparent.

One of the main reasons why fully paper-based elections can be considered as transparent is that each step of the procedure is public and can easily be understood. Each voter can observe how ballots are put into boxes and counted.[236] Moreover, the physical connection between each step of the

---

[234] Some legal scholars argue that this right is enshrined in Art. 22 EU-GDPR, but a grammatical and teleological interpretation do not prompt this conclusion. See, e.g., Margot E. Kaminski, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L. J. 189 (2019); Aziz Z. Huq, *A Right to a Human Decision*, 105 VA. L. REV. (2020).

[235] Nonetheless, disclosing the code underlying consensus protocols is unlikely to clarify the inner workings of the blockchain. See generally Deven R. Desai & Joshua A. Kroll, *Trust But Verify: A Guide to Algorithms and the Law*, 31 HARV. J. L. TECH. 1 (2017).

[236] See Teogenes Moura & Alexandre Gomes, *Blockchain Voting and its effects on*

procedure is relatively easy to understand. Finally and perhaps most importantly, paper ballots make sure that the ballot counting procedure remains physically reproducible. If ballots validated and stored on the blockchain network and the copies maintained by the nodes are destroyed, the election result cannot be reproduced.

A final reason why blockchain voting procedures may not be seen as sufficiently transparent or secure relates to centralization. In a way, and this seems in contradiction with the purported virtue of blockchain decentralization, traditional paper-ballot based voting procedures are more decentralized than blockchain voting procedures. Paper ballots are cast, counted and recorded in polling places spread all over the country. This physical decentralization provides a natural obstacle against manipulation at a large scale.[237] The reason is that each person involved in the counting procedure has an interest in preventing counting errors that benefit parties or candidates with a political affiliation that is not shared by her. As long as the electoral administration and polling places involve persons with diverse and divergent political views, the procedure will be secured against manipulation and fraud through a system of reciprocal checks and balances.

4. Sovereignty

A final limitation results from the fact that the blockchain is, by design, subject to the control of a few tech-savvy experts. Therefore, the decision process underlying the adoption of consensus protocols and, more generally, of the rules guiding blockchain technology is fundamentally centralized, at least much more so than blockchain evangelists admit.[238] This begs the question whether blockchain voting procedures can be reconciled with the fundamentally democratic idea that, in democratic societies, all institutions should be subject to the sovereignty of the people.

Under systems of off-chain governance, many of the basic governance decisions are primarily made by the core developers. Nodes may submit improvement proposals or refuse to update and adopt new protocols, but they do not make immediate governance decisions. These governance decisions are not subject to public scrutiny; at least they are much less visible and transparent than the legislative and administrative decisions guiding traditional voting procedures. While the process of validating

---

*Election Transparency and Voter Confidence*, Proceedings of the 18th Annual International Conference on Digital Government Research, 574 (2017), who also point out that the procedure does not induce trust if vote records are not available to the general public.

[237] In tight races, of course, small-scale manipulation can be sufficient to tilt the scales.

[238] Also see Kevin Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L. J. 489, 550-551 (2018).

blocks may be decentralized, the process of altering the underlying consensus protocol is not, at least not under systems of off-chain governance. On the Bitcoin or the Ethereum blockchain, for example, the nodes may submit blockchain amendment proposals, but the decisions on how the consensus protocol should evolve are ultimately made by the core developers.[239]

Systems of on-chain governance, by contrast, are more democratic in that they give nodes the right to vote on amendments of the consensus protocol.[240] Some blockchain networks such as Tezos and decentralized applications (*dapps*) such as Aragon implement systems of on-chain votes pertaining to essential modifications of the protocol, thus empowering coinholders to preempt conflicts over governance among core developers.[241] On-chain voting bolsters procedural justice and has the potential to increase cohesion in the respective blockchain community and avoid forks. The problem, however, is that on-chain democracy suffers from the same maladies as other democratic systems, especially low voter turnout and whale voting.[242] One way to avoid whale voting based on short-term interests is to establish lock mechanisms under which coinholders who have staked their coins for a longer time have more voting rights.

Finally, blockchain networks are global, with servers and nodes being located in several different jurisdictions around the globe.[243] Therefore, blockchain technology cannot be fully supervised by national authorities. Furthermore, legal liability regimes do not easily apply to agents running the servers and nodes in foreign jurisdictions. It follows that the state performing the election will be deprived of means to exercise tight control over the voting procedure. While this need not be harmful, it is not easily compatible with the idea that the sovereign in a democracy, the people, should be able to determine the conditions of democratic government, including the procedures intended to aggregate the citizens' preferences.

Democracy rests on conditions that cannot be guaranteed by the constitutional or legal framework it produces.[244] This statement about

---

[239] These proposals are referred to as Bitcoin Improvement Proposals (BIP) and Ethereum Improvement Proposals (EIP), see ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION (2016).

[240] Yoan Hermstrüwer, *Democratic Blockchain Design*, 175 J. INST. & THEORETICAL ECON. 163, 166 (2019).

[241] See https://tezos.com/ and https://aragon.org/.

[242] Whale voters are users who hold vast amounts of voting rights and have the power to exercise pivotal votes.

[243] See generally David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

[244] For the original citation, see Ernst-Wolfgang Böckenförde, *Die Entstehung des Staates als Vorgang der Säkularisation, in* Ernst-Wolfgang Böckenförde (ed.), Recht,

essential constitutional preconditions is very much in line with the answer that Benjamin Franklin gave when asked what sort of government the Constitutional Convention had established: "A republic, if you can keep it." This does not mean that governments choosing to use blockchain voting procedures may legitimately disregard the limited reach of jurisdiction and government power in the regulation of the blockchain. On the contrary: to the extent that democracy requires a sovereign expression of those affected by the institutions resulting from that very expression of sovereignty, governments opting for blockchain voting procedures should take measures to avoid that the interests of those not primarily affected by the resulting institutions become too onerous in determining the election outcome.

## CONCLUSION

Constitutional designers constantly struggle to design inclusive voting procedures that are secured against undue manipulation and provide an accurate reflection of the voters' political preferences. In this article, I have argued that blockchain technology does not provide adequate procedural safeguards to organize democratic elections writ large. In support of my argument, I have adopted the perspective of mechanism design and computer science to shed light on the virtues and, more specifically, the limitations of blockchain voting procedures. To reflect these limitations in light of constitutional principles guiding the use of electronic voting procedures, I have adopted a comparative law perspective and discussed what I believe to be the most important constitutional constraints in the United States and in Germany. In comparison to German courts, U.S. courts have been rather reluctant to formulate precise conditions for the implementation of electronic voting procedures, especially the constitutional standards pertaining to the integrity of electoral processes.

Blockchain technology is likely to pave the way towards new modes of decision-making and governance without recurring to law and institutions based on the idea of centralized government power. On the one hand, it offers new modes of achieving trust without a single trusted third party. On the other hand, and in contrast to the mode of centralized governance envisioned by Thomas Hobbes, it relies on a peer-to-peer network infrastructure and thus operates in a decentralized way. When it comes to organizing democratic elections, blockchain technology has the potential to facilitate access to elections and make participation much more flexible.

Nonetheless, blockchain technology is not a silver bullet. The core function of any voting procedure is to provide legitimacy. Legitimacy

---

Staat, Freiheit, 92, 112 (1991): "The liberal, secular state lives on conditions that it cannot guarantee itself."

requires procedures that the voters can and do trust. The extent to which trust is justified strongly depends on how secure, accurate, transparent, and traceable the voting procedure is. Satisfying these conditions on the blockchain is likely to be complex and costly. Designing secure blockchain voting procedures is likely to require a relatively high degree of centralized oversight. In light of these shortcomings, the advantages of blockchain technology and decentralized governance are not as clear in the context of general political elections as in other contexts. Therefore, we should not expect blockchain voting procedures to revitalize participation in large-scale political elections and address the symptoms or causes of fainting democracies.

* * *