DISTRIBUTED ELECTION AUTHORITY: DELIMITING THE DEMOCRATIC PROSPECTS OF BLOCKCHAIN VOTING SYSTEMS

(DRAFT FOR DISCUSSION)

Jungroan Lin

B.PAPM, Carleton University, 2018

M.A., University of British Columbia, 2019

May 2019

1. Introduction

Across a wide range of scholars in democratic theory, a consensus has emerged that presupposes the need for free and fair elections within the most minimal definition of democracy (Levitsky and Way 2002; Levitsky and Way 2015; Munck 2016; Merkel 2004; Altman 2013). While in Western Liberal democracies that baseline had generally been assumed, the recent rise of elections using electronic voting (e-voting) mechanisms has generated concern over the security of elections against electronic voter fraud, manipulation, and hacking (Beaulieu 2016). Regardless of whether or not these elections have been affected by voter fraud or electronic hacks, at least two key concerns are worth taking seriously. Firstly, the use of electronic voting has often led to the increased *perception* that elections could be affected by fraud (Alvarez et al. 2018; Beaulieu 2016; Halpern 2018). Secondly, the lack of a 'paper trail' means that votes could not be retraced to an immutable source, further contributing to concerns about the legitimacy and security of elections.

Blockchain technology provides one means by which these challenges presented by electronic voting systems might be ameliorated. The key defining feature of a blockchain is its database structure – a “permanent, distributed digital ledger, resistant to tampering and carried out collectively by all the nodes of the system.” (Atzori 2017, 45). The permanent ledger theoretically addresses the 'paper trail' problem, while the 'carrying out' portion of the technology is generally achieved through a process called proof-of-work, a verification process relying on computational power of all computers working on a distributed network (explained further below). Despite the technological promise of blockchain-enabled voting systems (BEV) as an improvement upon past e-voting systems, we have yet to see full-scale implementation of a BEV in any national election. Further, the academic research on blockchain elections has mostly been in the realm of computer science, taking theoretical and small-scale experimental forms, including, at best, extremely limited socio-political considerations of BEV systems. In addressing this gap, this exploratory paper aims to answer two primary questions: (1) what are the competitive advantages and challenges that a BEV system theoretically presents that past e-voting systems did not, and (2) what are the conditions that could lead to the full-scale adoption of BEV at the national level in the near future. Additionally, this paper theorizes a politically conscious BEV system for Canadian federal elections.

2. Electronic voting (E-voting)

E-voting is the process of casting a vote into an electronic database where it is then tabulated within with other electronic votes. This is in contrast to traditional voting which is generally done physically through paper ballots. Yi and Eiji (2013) separate e-voting into voting done remotely through the internet (connecting to the internet through mobile devices or one's personal computer) and e-voting done at polling stations (where voters would then submit their vote through electronic devices present at these stations) as the two main systems. Goos et al. (2016) also identify kiosk voting as another form whereby voting machines would be present in gas stations, shopping malls, libraries, and other common spaces in addition to official polling places (139).

With regards to government elections, e-voting is usually added as a supplementary measure to paper ballots, rather than a replacement. This additional option is meant to improve voter turnout by targeting active internet users and people located far away from polling stations. Further, e-voting systems offer possible efficiency gains during vote tabulation and could potentially guard against human error when counting paper ballots. In a study of internet

voting approaches in Halifax and Markham, Goodman (2010) finds that supplementary internet voting made the electoral process more convenient and accessible for electors, showing early potential to engage otherwise non-voters. In their deeper quantitative review of elections in ninety-eight Ontario municipalities between 2000-2014, Goodman and Stokes (2018) find that internet voting leads to an increase in voter turnout by roughly 3.5% and up to 16%, explained by reducing the physical cost of voting for voters. Vassil et al. (2016, 459) suggest on a similar vein that e-voting should be thought of “as an enabler for political participation” by improving the efficiency of the voting process for citizens. However, in Swiss cantons Geneva and Zurich, e-voting, again as a supplement to poll station voting and postal voting was not found to significantly increase total voter turnout in referendums (Germann and Serdült 2017). Thus current evidence shows that, at best, e-voting can lead to modest increases in voter turnout, even in nations where digital-enabled government services are institutionalized like Estonia (Solvak and Vassil 2017; Vassil et al. 2016).To boot, e-voting tends to be more 'sticky' and 'addictive' than traditional voting – voters who cast their ballot electronically are more likely to vote in subsequent elections than voters who cast a paper ballot, and e-voters will prefer to e-vote in future elections (Solvak and Vassil 2017; Crothers 2015).

This paper identifies five key challenges faced by e-voting systems. One of the most common critiques of e-voting is best captured by the concept of a 'digital divide', a “gap between various socio-demographic groups in terms of access to and usage of computers and information technology.” (Goos et al. 2016, 146) This *accessibility* gap assumes that younger voters are more likely to opt for remote internet voting options (Mendez and Serdult 2017; Goos et al. 2016). However, the negative impact of e-voting on older voters was found to be non-existent in the Swiss case; instead, a positive relationship was found between age and internet vote retention, further affirming the 'stickiness' of e-voting (Mendez and Serdult 2017, 519). Accessibility issues go hand-in-hand with discussions of digital literacy, however, can be lessened through having an accessible front-end interface for users that is easy to navigate.

Another critique consistently brought to the table is in relation to the *social cohesion* aspect of traditional elections. Neymans (2002) identifies three symbolic functions which go beyond the fundamental purpose of elections of choosing a candidate for office: signifying voter support for democracy, emphasizing voter equality upon entering the voting booth, and providing forced opportunities for introspective deliberation by requiring voters to spend time commuting and waiting at the polling station for their turn to vote. The physical act of voting is also argued to encourage political discussion between friends and family and subsequently drive voter turnout (Unt et al. 2017, 2). Cynics further warn that the remote nature of internet voting turns voting into ‘yet another on-line activity’ which endangers the social nature of voting and possibly leads to a decline in the sense of civic duty desired by democracies (ibid., 1). However, in Estonia where e-voting is most prevalent, household voting patterns exhibited during paper-based elections were mostly replicated in electronic elections (ibid.; Vassil et al. 2016).

The possibility of *hacking*, whereby an “attacker gains access or control of digital devices, data servers, or digital services such as social media accounts,” is a further risk of e-voting whether done remotely or at polling stations (Tenove 2017). E-voting done at a polling booth or kiosk where the computers are secured leaves elections vulnerable to hacks done on the database where votes are stored. For example, Ukraine’s central server was hacked in 2014 through the deletion of files before the end of the election, resulting in false election results and compromised reporting systems (Ibid., 31). Similar issues arose in Kenya’s 2017 election,

and even western liberal democracies such as the United States may have had elections potentially compromised in the last decade (Ibid.) If voting is done remotely, additional issues arise. Connections to the voting site can be faked and individuals may be tricked into downloading malware or giving up information (Goos et al. 2016; Tenove 2017). Previously infected personal computers may also be a source of vulnerabilities.

In addition to problems of *accessibility*, *hacking*, and *social cohesion*, e-voting faces challenges of *transparency* and *anonymity*. Regular internet protocols do not allow voters to verify for certain whether their vote has been properly stored or not. Traditional e-voting systems are only transparent insofar as the front-end interface provides information; once the vote is cast, the election authority has complete control over transparency and can choose to withhold any degree of information. Further, internet-enabled voting provides no back-end software guarantee. One such example would be e-voting done through Google Forms (a front-end voting interface) which is then linked to Google Sheets (a back-end data repository). If the election authority wishes, it can alter vote results on Google Sheets before publishing results to the public – transparency is completely non-guaranteed and contingent upon a central authority.

Even if a transparent voting process is enabled where a person can track his/her own vote, the problem of *anonymity* arises. Attempting to identify errors in the system when the secrecy of the voter and vote decision must be guarded is extremely difficult, presenting a technological paradox. Furthermore, if the central server is hacked, any promise of voter anonymity can be completely disregarded. The single point of failure represents a significant security and user privacy shortcoming which can be too easily compromised whether on purpose or incidentally (Zhang et al. 2018, 402). Goos et al. (2016, 137) even go so far as to argue that “so far no technical solution to guarantee anonymity and verifiability has been found.”

3. Blockchain-enabled voting (BEV)

The blockchain data structure is often attributed to Bitcoin's inception, but its origins can be further traced back to David Chaum’s work through the 1970-80s, which aimed to solve the ‘traffic analysis problem’: “the problem of keeping confidential who converses with whom, and when they converse.” (1981, 84). His public key cryptography solutions used digital pseudonyms as a public key to be subsequently verified against a private key held by an anonymous holder. (Chaum 1981, 86) This concept of ‘Chaumian Blinding’ was the basis for many of the early e-cash protocols, and eventually Blockchain technologies (Ethereum 2018). Though this offered an original solution to the anonymity problem, it still relied on a central intermediary to ensure the validity of transactions.

Bitcoin applies this concept in its cryptographic solution, however, explicitly rejects the idea of a central intermediary. Instead, Bitcoin and many other blockchains are supported by a distributed transaction database that is shared among network participants, updated through consensus rather than through approval by a unitary actor (Atzori 2017; Swan 2017). All participants (miners) on the network have access to a permanent record of any data ever added onto the blockchain. Each transaction – whether it is a financial exchange or simply an exchange of textual information (as would be the case for voting) – is recorded with a unique cryptographic signature, timestamped, and maintained in a “tamper-proof auditable history of all transactions.” (Swan 2017, 6). With the lack of central trust, an alternative verification process ensuring that the information is accurate must be applied, which currently is most often operationalized through ‘proof-of-work’.The example of Bitcoin’s proof-of-work helps to

illustrate this concept. The Bitcoin network itself attempts to package many transactions together into ‘blocks’. Upon block creation, a competition starts, where an unknown number must be found – basically ‘guess and check’. The number tends to be extraordinarily long and thus requires a significant amount of computational power to discover (Ethereum 2018). The first miner to discover that number is paid out a small reward, which for the Bitcoin system is 12.5 bitcoins. Subsequently, the transaction is verified and becomes part of the immutable chain of blocks, each subsequent block containing all the data from previous blocks (Ibid.).

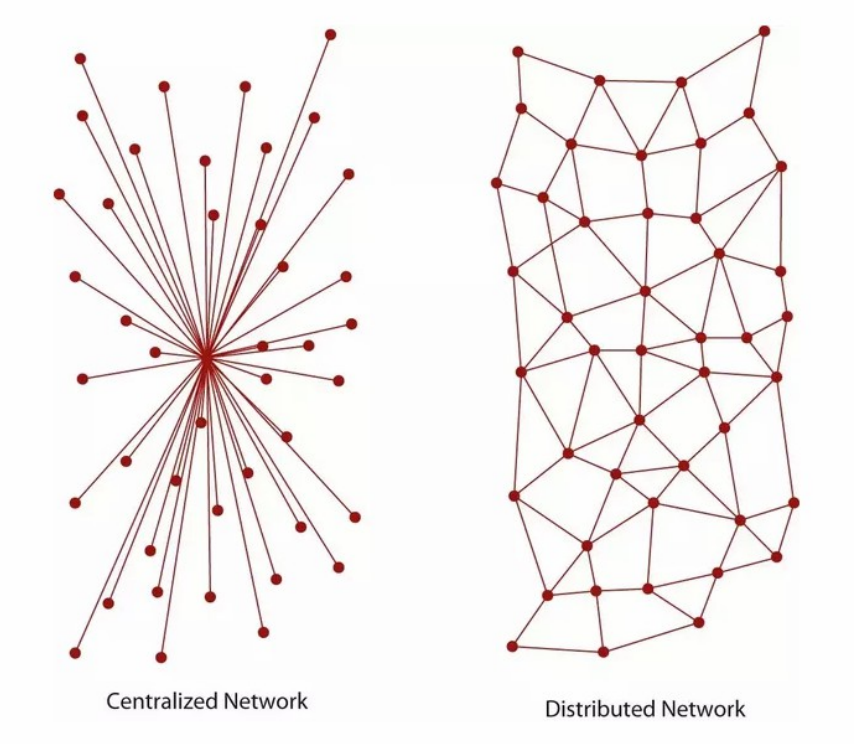


Figure 1. Centralized vs Distributed Network (taken from Segupta 2017)

By including cryptographic measures while using a distributed network structure, a blockchain system makes a fairly strong argument for providing a solution to the technological paradox of *transparency* and *anonymity*. The use of a public key as a digital pseudonym allows users to hide their identities, while the proof-of-work verification method removes the need for a trusted central governing intermediary. Instead, every network participant is able to transparently trace any and all transactions made on the blockchain, which has an immutable data structure that cannot be altered.

While no national elections have yet to be run on a blockchain system, several proofs-of-concept give us insight into what a functional blockchain-enabled voting system (BEV) might look like. Zhang et al. (2018) developed a native blockchain protocol on the HyperLedger Fabric (shown in *Figure 2*) with three unique features: *distribution voting*, *distributed tally*, and *cryptography-based verification*. *Distribution voting* involves assigning multiple ballots to each voter, whose voting intention is signified by the statistical mode of their ballots, creating an additional anonymity check whereby a voter's vote intention can only be revealed if the majority of his/her voting ballots is manually exposed by dishonest miners (ibid., 402). *Distributed tallying* is the assignment of vote tallying to all peers on the network. Their concept relies on a 'no tally no voting' principles, whereby if peers do not correctly perform the tally assigned to them, they are marked as dishonest peers and any ballots cast by them are

discarded (ibid., 405). The un-tallied ballots from the honest voter are then distributed to another party to tally. The *cryptography-based verification* uses the blockchain as a public immutable ledger holding a list of public keys corresponding to vote intentions that are decrypted against private keys distributed to random peers (ibid., 405-406). While their proof-of-concept provides a high degree of security against vote fraud and identity leaks, the model is fairly cumbersome to execute. The distribution voting mechanism requires a voter to cast multiple ballots for a single vote intention. Increases in identity security are positively related to the number of multiple ballots per vote intention; thus, a balance must be struck between efficiency and security. The distributed tallying feature requires that every voter subsequently be a miner. While this may work in a small-scale election among cryptocurrency experts, expecting every member of the electorate to perform a cryptographic verification is totally unrealistic.

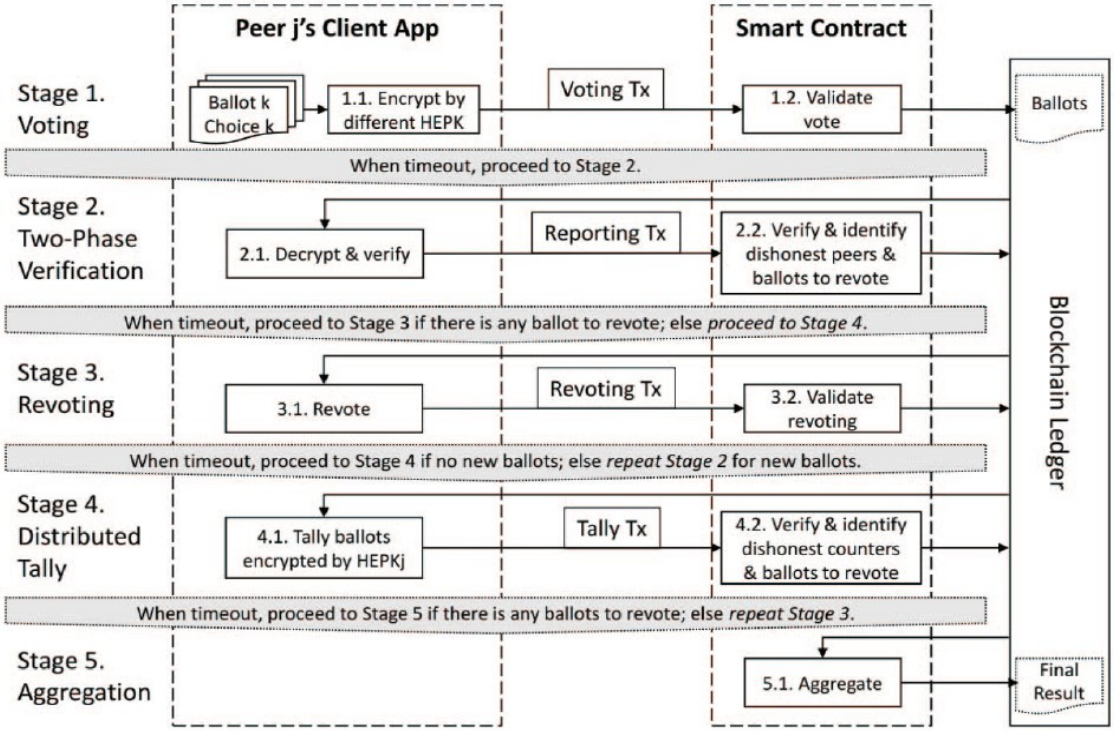


Figure 2. Zhang et al.'s (2018) blockchain voting protocol

Wang et al. (2018) provide a more scalable model of a BEV, based on the Ethereum architecture and abandoning the proof-of-work verification mechanism altogether due to its computational inefficiency. Instead, it uses the delegated proof-of-stake (DPoS) model, which relies on elected 'witnesses' who generate blocks. This election can be done among peers on the blockchain, aiming to select witnesses who are can be neutral with regards to the vote. In essence, the DPoS model limits the mining process to limited set of actors who are democratically selected, thereby reducing the need for significant computational requirements of proof-of-work which ensures security through difficulty (Bitshares 2019). In their simulation, Wang et al. find that their model, tested in a five-candidate election, is able to generate a new block in roughly 0.1% of the time that it takes to generate a block on the Bitcoin blockchain while also experiencing only marginal shifts with significant increases in voter count (2018, 237). Though this system is far more efficient and retains the anonymity element of a

blockchain voting system, the selection of witnesses poses a problem of bias. There is no such thing as a completely neutral actor, and competing parties voting on witnesses will likely choose to nominate those that would act in their respective interests if we assume game-theoretic rationality.

A BEV system based on a consortium blockchain whereby block generation is done in a supervised environment among presents an alternative model of verification. Shahzad and Crowcroft (2019) use this method in their model (shown in *Figure 3*), whereby the blockchain is owned by a governing body and cannot be accessed from the outside. While the verification is done by a central authority here, that central authority still uses cryptographic block generation methods; the voter's identity is still encrypted at the point of voting and their vote is almost immediately reflected on the blockchain upon being cast. This somewhat deviates from blockchain principles of rejected a central authority, however, the use of blockchain technology here still provides greater transparency and security (due to the immutability of transactions) than traditional e-voting systems.

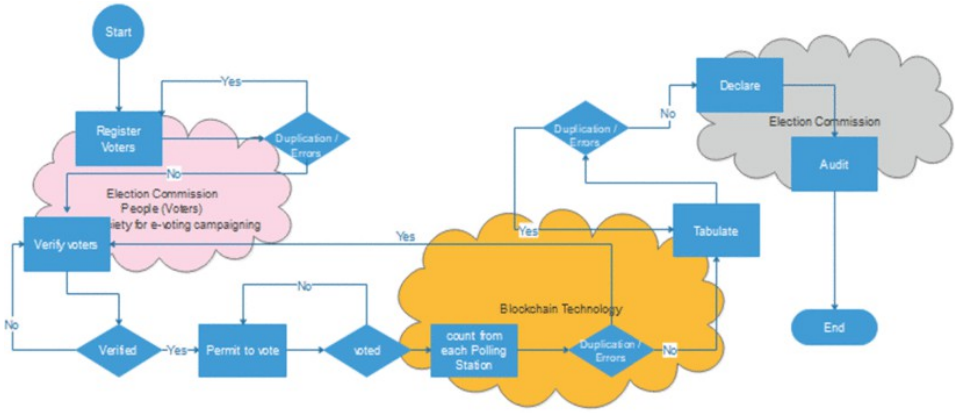


Figure 3. Shahzad and Crowcroft's (2019) Consortium BEV Model

In a more concrete example, Follow My Vote is an organization which has partnered with the BitShares blockchain to develop their own proof of concept BEV system. Voters begin by registering on the system, proving their identity through a government issued ID (such as a SIN number).

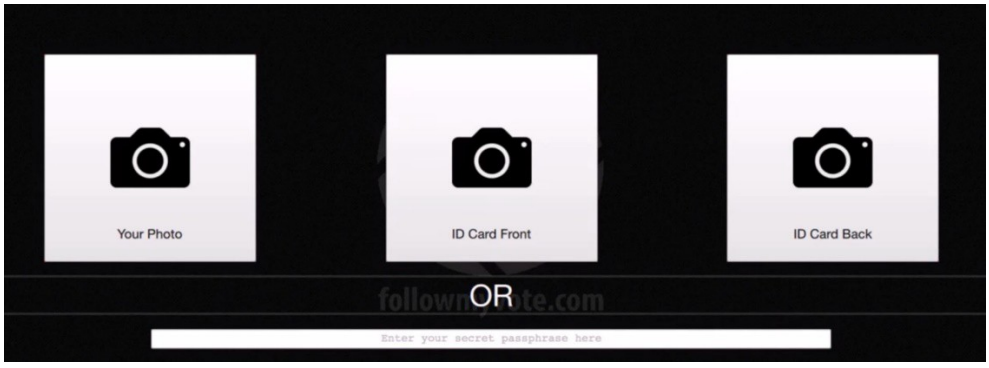
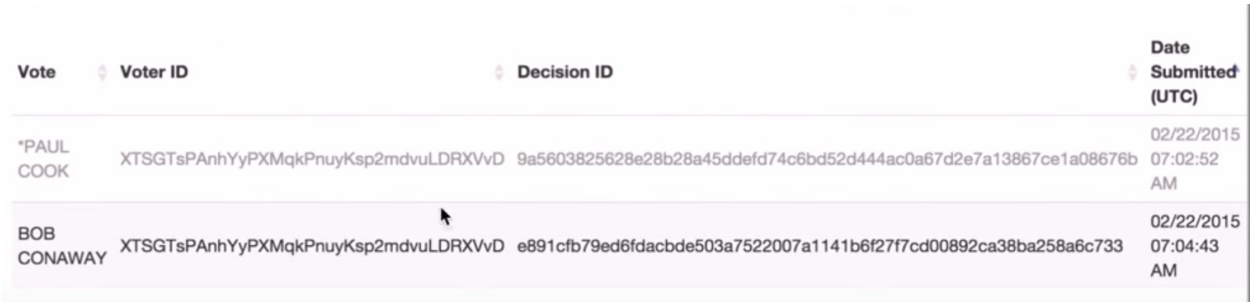


Figure 4. Follow My Vote (2016) Registration Stage

The system in return creates a ‘blinded token’, a random number that has been obscured so that the information within cannot be read directly, but can be verified as correct. Following, a built-in registrar matches the token and with the unique voter, before a ‘token identity’ is created from the ‘blinded token’, which has no visible link back to the voter’s actual identification. At this stage, the voter has been given a unique voting account which has been

verified and can be used to vote through the platform. This account cannot be linked back to his or her voter identification due to the ‘blinded token’ middle stage (Follow My Vote 2015). Despite the complexity of the underlying code structure of the Follow My Vote BEV concept, the front-end interface remains fairly simple, providing only simple instruction and core information to the majority of users.



Vote	Voter ID	Decision ID	Date Submitted (UTC)
*PAUL COOK	XTSGTsPAnhYyPXMqkPnuyKsp2mdvuLDRXVvD	9a5603825628e28b28a45ddefd74c6bd52d444ac0a67d2e7a13867ce1a08676b	02/22/2015 07:02:52 AM
BOB CONAWAY	XTSGTsPAnhYyPXMqkPnuyKsp2mdvuLDRXVvD	e891cfb79ed6fdacbde503a7522007a1141b6f27f7cd00892ca38ba258a6c733	02/22/2015 07:04:43 AM

Figure 5. Encrypted Vote Decision (Follow my Vote 2016)

4. Blockchain Voting (BEV) re: the key challenges of e-voting

As previously noted, e-voting systems face at least five key challenges. For some of these, blockchain technologies offer very benefit in comparison to traditional e-voting, while for other dimensions – most notably transparency and hacking – it offers groundbreaking potential. Taking into consideration the proofs-of-concept described in conjunction, I illustrate here the potential benefits of BEV while hoping to identify possible risks/pain points in developing a BEV system.

4.1 Accessibility

If the digital divide was not already an insurmountable pain point when it came to internet voting, it would seem on the surface that blockchain technology would exponentially increase this gap. Swan (2017) acknowledges that the technology is complicated – that “even the basics are difficult to understand” and may act as a “barrier to effective decision-making and the ongoing implementation and use of the technology.” In the same breath, Shermin (2017) cautions that the general population would have to put trust in experts on a technology they are unable to understand (499).

In actuality, these critiques do not necessarily apply differently to BEV systems and traditional e-voting systems. From a user-perspective, a blockchain voting system would see very little change on the front-end of things; so long as web-designers are competent, the end-user would only interact with a friendly interface and be provided with necessary and easy to access information, as demonstrated in the Follow My Vote registration menu in *Figure 4*. The primary difference in a blockchain voting system would be how votes are verified, i.e. through the blockchain as opposed to through a central authority. That said, digital literacy at the developer level may be a legitimate concern. Back-end developers familiar with common coding languages like Java and Python would need to retrain in order to learn how to develop on blockchain platforms.

4.2 Hacking

Likely the area with most potential for a blockchain voting system is the aversion of hacks such as the aforementioned cases in Ukraine and Kenya. Without a need for a central authority, the state no longer becomes the single point of failure (Atzori 2017, 46). Instead, the distributed nature of data storage combined with the immutable public ledger ensures that votes cast would be valid, secure, and permanent. If one computer was to crash, data would

still be held on countless other machines.

Many of the individual-level challenges would still plague BEV. If a person attempting to vote is tricked into giving up their personal information by malicious advertisers or otherwise, blockchain technologies do not offer a foolproof fix. The concerns previously mentioned by Goos et al. (2016) and Tenove (2017) regarding remote voting would be the same challenges here, with responsibility ultimately lying in the hands of individual voters. However, the use of smart contracts “a set of promises, specified in digital form, including protocols within which the parties perform on these promises” can be designed to avoid malicious outcomes (Yuan et al. 2018, 544). Smart contract logic is build into many blockchains, such as Ethereum, whereby developers are able to write contract conditions that when met, result in the execution of an action. In the case of BEV, a hypothetical smart contract condition such as uploading a selfie alongside government identification could prevent fraudulent votes from hacked computers.

Further, it is important to emphasize that blockchains are not completely invulnerable to hacks. Basic blockchain structures are susceptible to '51% hacks', or when a malicious actor is able to create the longest chain of blocks by hacking a majority of existing blocks before a new block is introduced (Kshetri and Voas 2018). Any hack amounting to less than this will be corrected by the consensus mechanism provided by proof-of-work verification, which defaults to the longest chain. A 51% on Bitcoin is estimated to cost over $1.4 billion USD (Moos 2018). Additionally, such a hack would be immediately detected by all network participants, thus while it could completely disrupt an election, the forging of fraudulent election results is still not avoided.

4.3 Social cohesion

Because blockchain voting at the voter level would not necessarily lead to any differences in voting activity in comparison to e-voting, the impact of BEV on social cohesion would be limited and likely not detrimental. Though perhaps a slight stretch, because BEV systems allow for public checks on election processes and results, this opportunity for any member of the public to access this type of information may lead to an increased sense of civic duty within individuals. On the flip-side, this sort of scenario creates an incentive to free-ride on the activity of others and may not result in increased civic engagement.

4.4 Transparency

Transparency is generally viewed as desirable and “something to be fostered and enabled” in public institutions (Bannister and Connolly 2011). If enabled, e-transparency can restore previously losses in public trust towards governmental institutions (Ibid.). Perceived transparency of government has been found to positively correlate with strong government-public relationships and even contributes to national pride (Hong 2014).

In previous e-voting systems, voters have been unable to verify what has happened with their vote due to the inherent ‘nature of computers that their inner workings are not visible” to the public (Goos 2016, 137). In contrast, blockchain technologies are designed for transparency; the fact that each transaction can be seen by every participant on the network without relying on a central intermediary guarantees equal access to information (Li et al. 2017). Additionally, blockchains are open-source by default – that is to say anyone can see the actual written code which establishes the original infrastructure. The immutability of blockchain technology ensures that network participants are able to see information which has not been tampered with by malicious actors. Blockchain creates the opportunity for radical transparency (Shermin

2017) rather than merely incremental dissemination of information from the state, ultimately creating opportunities to rebuild public trust in government institutions.

However, should a state BEV system take a private or consortium blockchain structure as in Shahzad and Crowcroft's (2019) model, transparency *can* be limited. The blockchain administrator can choose to only show the data on the blockchain to peer nodes (like other miners) and possibly hide the details of the blockchain election from the public. While this in large part defeats the purpose of implementing BEV, we should be wary of states implementing private blockchain elections under the guise of transparency, when in reality they may simply be introducing e-voting in 'new clothes'.

4.5 Anonymity

Though Goos et al. (2016) argue that anonymity and transparency for e-voting systems are technologically irreconcilable, a blockchain voting system would allow for both through public/private key encryption of voters and vote decisions. *Figure 5* in the prior section showed the information provided to a user by Follow My Vote, a blockchain based voting system. Both the ‘Voter ID’ and ‘Decision ID’ are public keys which can be verified by anyone. Each participant would be able to see that voter ‘XTSGTsP...’ exercised his/her franchise in favor of decision ‘9a560382...’, but they would not be able to identify the actual voter by name. However, each of these public keys can be matched to a private key seen only by the voter him/herself. The Follow My Vote system also displays rough vote percentages as votes are tabulated, rather than showing exact numbers as a means of hedging against traceability to individuals.

The distribution voting idea proposed by Zhang et al. (2018) offers a more elegant solution to this anonymity risk without sacrificing exact election result transparency. By requiring multiple ballots per vote intention, distribution voting makes it so that even if a malicious actor is somehow able to trace a single ballot to an individual, that information alone will not reveal the individual's vote intention; instead they would need to trace enough ballots to constitute a majority of that individual's total ballots cast.

4.6 Efficiency: an additional challenge

Whereas the cost of counting additional votes using a mix of an internet protocol and database software is negligible, BEV has traditionally relied on proof-of-work mining as a means of verifying the correctness of information. This verification method is inherently inefficient – the high computational power required to generate a new block *is* the safeguard against vulnerabilities. This demand not only leads to a slower verification process that would cause to delays in the publication of election results, but the environmental cost of mining is significant.

Foteines (2018) estimates that annually, Bitcoin and Ethereum mining combined – both of which rely on proof of work verification – produce roughly 43.9 million tonnes of carbon dioxide equivalent, in large part because the majority of cryptocurrency mining happens in China which is primarily powered by coal. Roughly speaking, this is comparable to 6.8 million average European citizens (ibid.). In addition to energy cost, mining generates significant technological waste due to the requirement of countless high-end central processing units and graphics processing units. While these can be resold to be used for their intended purpose as regular computer parts after mining, consumers may be reluctant to purchase worn goods thus mining companies looking to offload a significant number of used components at a single time may struggle to find willing buyers. The DPoS and consortium

models outlined above offer more efficient alternatives to proof-of-work, however, sacrifice degrees of data distribution and transparency.

5. Enabling conditions for BEV

Though in theory blockchain voting systems solves the technological paradox between anonymity and transparency while reducing system vulnerability to hacks, uptake of Blockchain voting at the state level has been almost completely absent. Recent reports of Sierra Leone running a secret election using blockchain technology were quickly debunked and proven completely false – in fact, the electronic database was run off of Microsoft SQL and developed on C++, both of which are just standard programming languages (Varshney 2018; Biggs 2018). The closest that a nation has come to implementing Blockchain voting is Estonia, with Nasdaq Inc partnered in an effort to potentially implement an experimental blockchain voting system building upon its existing internet voting system (Irrera 2017).

In the most recent Estonian parliamentary election, 44% of the electorate cast their vote electronically through remote means (E-Estonia 2019; Aasmae 2019). Estonia's current electronic voting system, i-Voting, uses a public key infrastructure to encrypt voter data, similarly to how many blockchain systems encrypt user data. While the voting system itself is not blockchain-enabled, Estonia utilizes blockchain technology to maintain an immutable record of citizen identification cards which are used as a means of authentication for accessing the i-Voting system (Jun 2018). In their analysis of Estonian i-Voting, Springall et al. (2014) found that the system was both vulnerable to a variety of different technological attacks and additionally lacked the transparency provided by BEV which would have show when malicious actions were performed by hackers. However, Estonia is still a useful case to consider due to the integration of blockchain technology in its voting system to *some* degree and the evidence of experimentation with BEV technologies.

This paper borrows the analytical framework from Goos et al. (2016) which was used to offer an exploratory analysis of internet-based e-voting systems. This analysis aims to uncover why Estonia is on the verge of implementing a blockchain voting system, suggest drivers of blockchain voting initiatives, and identify possible barriers/weak areas in the Estonian case which may lead to the failure of sustainable implementation. The qualitative framework considers five separate contextual dimensions. The first of these, *history and background* aims to give a general overview of relevant affairs; for this paper, both the historical context of e-voting in Estonia as well as the timeline of experimental blockchain technology development are examined. *Motivational* context explains the interest in blockchain voting. The *legal context* identifies relevant legal frameworks in place to the implementation of blockchain voting systems. *Organizational context* examines systems in place to facilitate blockchain voting and the institutions involved in the possible implementation and administration of a blockchain voting system. Finally, the *socio-political context* takes into account factors such as attitudes and behavior towards e-voting, blockchain, and technological adoption.

5.1 History and Background

Estonia is regarded as one of the most technologically progressive nations in the 21st century and has been actively using e-voting systems since 2005 (Ibid., 153). The first of these elections was in October 2005 at the local level, however, by March 2007 a national parliamentary election was conducted which allowed for internet voting, the first of its sort globally; while in 2005 only 1.9% of voters used the internet, the 2007 election saw 5.4% of voters utilize this option (Alvarez et al. 2009, 498). More recently, e-voting rates seem to have capped out at roughly one third of the population (31.3% in 2014 and 30.5% in 2015) given

the option of both e-voting and paper ballots (Goos et al. 2016).

Estonia has had a relationship with blockchain technology for almost as long, with early forms of internal testing beginning in 2008 under the title of 'hash-linked time-stamping' (e-Estonia 2018). By 2012, blockchain technologies were being used for many data registries including health, judicial, legislative, security, and commercial code systems (Ibid.). Both e-voting initiatives and blockchain initiatives have been implemented from the top-down perspective of the state, usually led by the Prime Minister (Goos et al. 2016; Alvarez et al. 2009). This has been in part attributed to the relative youth of the government; in 1992 when the foundation for e-government was being created, government employees had an average age of 35 years (*The Economist* 2013).

5.2 Motivational context

The Estonian government states that its exploration of blockchain technologies is driven by goals of keeping information secure, ensuring data integrity, and mitigating internal threats (e-Estonia 2018). Additionally, the instantaneous nature of blockchain verification allows flaws to be detected immediately in contrast to the average 7-month detection time averaged by organizations (Ibid.). Estonia sees itself as a leading country in Blockchain developments (*Coin Telegraph* 2017) and would logically strive to maintain this leadership.

There are also various global drivers to blockchain development at the state level. Some of the blockchain solutions developed by Estonia have been adopted by NATO, the U.S. Department of Defence, and the European Union (e-Estonia 2018). For these actors, Estonia is an effective experimental lab for innovations to be both tested and operationalized in a real-life setting. Companies attempting to deploy blockchain technologies are also likely to want Estonia to push their technological limits. Verizon is one example of a company who plans to partner with Guardtime technology, one of blockchain companies which Estonia had previously established a private-public partnership with (Vill 2018). Lastly, any actors involved to any degree with cryptocurrencies would likely want to see the continued advancement of blockchain technologies in any domain, as this would lead to increased interest in the technology, financial growth in cryptocurrencies, and thus individual capital.

5.3 Legal context

The key piece of legislation relating to blockchain voting is the *Digital Signatures Act*, originally passed in March 2000. It "provides the conditions necessary for using digital signatures and digital seals, and the procedure for exercising supervision over the provision of certification services and time-stamping services." (*Digital Signatures Act*). It, in practice, mandates identity cards which include embedded digital certificates that can be used for online authentication of individuals when combined with one's PIN number (Alvarez et al. 2009, 499). These digital signature cards are incredibly useful for blockchain voting systems, especially if we look towards the Follow My Vote model of participant authentication. While that system relies on webcam facial recognition paired with government-issued ID to prove identification, implementation in Estonia could skip this 'selfie authentication' entirely, which may be prone to flaws in facial recognition software.

5.4 Organizational context

Two primary organizations control e-voting operations in Estonia – the National Electoral Committee which establishes technical requirements for e-voting, and the Electronic Voting Committee which administers the e-voting system (Goos et al. 2016). In terms of implementing a blockchain voting system, a key private organization has emerged in Nasdaq

Inc, who recently completed a proxy voting test on a blockchain system in Estonia, leveraging the digital identification system already in place (Waterman 2017; Irrera 2017). This private-public partnership further complicates the organizational context due to Nasdaq's accountability to shareholders and issuers; thus, they must justify their blockchain initiatives in terms of overall profits and organizational growth. That said, these are all organizations which would provide a top-down approach to blockchain voting technology, which in contrast to bottom-up initiatives, are more efficient, convenient, and lower cost (Oni et al. 2016). Fatelli and Riofrancos suggest that institutions created by social mobilization are more likely to develop into strong institutions than those imposed from above or through 'best practice' diffusion (2018). However, in a comparative analysis between Switzerland's bottom-up approach to e-voting and Estonia's previous top-down approaches, the latter proved to be far more resilient (Mendez and Serdult 2017).

Interestingly, a blockchain voting system could very well remove the need for the Electronic Voting Committee – or at least its administrating role. Instead, once a system is properly designed and implemented, the elections should be self-executing since the registration, voting, and tallying processes would be done automatically through the blockchain, and subsequently verified by any and/or all participants in the election.

5.5 Socio-political context

Estonia is commonly referred to as an "ICT friendly nation." (Goos et al. 2016, 153). The government prides itself on its 'paperless government' and some ICT experts even refer to the nation as 'e-Stonia' (Alvarez et al. 2009, 500). The government does not consider blockchain as an alien technology, but instead sees it as part of its digital roadmap which began with e-Governance, moved through i-Voting, and most recently is developing e-Residency to allow temporary and permanent residents to receive a digital ID and access to public services (e-Estonia 2018). Further, for some younger Estonians, the internet has been described as a "symbol of democracy and freedom." (Kingsley 2012). The socio-political context is fairly favorable towards a blockchain voting system, given the familiarity with not only blockchain technology itself, but also more broadly with general technological change and advancement.

5.6 Discussion

After considering the above contextual elements for Estonia, it becomes clear why the nation is setup to be the first state to run national elections on a blockchain voting platform. Estonia has a history of technological innovation stemming from top-down initiatives in the 1990s and have carved out a niche as a global leader in this area. Both the nation and its citizens pride themselves on technological progressiveness and would likely see blockchain voting as the next logical step. Coincidentally, the government had already been experimenting with what was essentially a blockchain platform back in 2008, so it possesses a technical familiarity as well. Additionally, the *Digital Signatures Act* and the consequence of mandatory digital identification cards for each citizen creates another point of leverage for a potential blockchain voting system, which would otherwise have to puzzle through alternative authentication methods such as the aforementioned facial recognition-based authentication.

The motivational and organizational contexts also suggest that conditions at the current time would favor the implementation of blockchain-related technologies. Positive drivers for implementation come from within the government and from various global actors including states interested in adopting the same technologies and corporations looking to build a relationship with Estonia to establish themselves as the leaders in the private sector

blockchain industry. Additionally, the ridiculous spike in cryptocurrency value and public interest in blockchain recently serve as another motivator for developing this technology. The key actors mostly seem to embrace the technology primarily to ensure secure databases and increase transparency (and subsequently public trust). This analysis does warn of a potential spoiler in the Electronic Voting Committee, which could potentially aim to prevent the adoption of a blockchain voting system in order to ensure its own survival as an organization since a blockchain voting system would not require an independent election administrator.

6. Politically conscious BEV for Canadian Federal Elections

Thus far, the Canadian government has not signaled any clear intent to pursue BEV concepts for its federal elections, though a variety of non-voting related blockchain projects are underway. It clearly recognizes the potential utility of blockchain technology as a means of improving existing online voting systems, but recognize that “there is a lot [it does] not know about blockchain that future research and development can help to understand and apply.” (Canada 2017) So far though, Elections Canada's foray into blockchain mostly involves monitoring initiatives around the world which may inform their research and development in the future (The Conference Board of Canada 2018). Here, I sketch a BEV system for Canadian federal elections as a guiding concept for the Government of Canada, cognizant of the elements identified in section 4 and approaches described in section 2 of this paper.

A consortium-based blockchain structure built on the Ethereum blockchain or another blockchain capable of smart contract logic is proposed. A publicly visible ledger keeping track of each vote cast creates a more transparent structure whereby all citizens can see moment-to-moment changes in election activity. This public ledger places an obligation on the public to hold the electoral process accountable, and in that endeavor, could foster a sense of civic duty among citizens while encouraging citizens to pursue a high degree of digital literacy which would help to engage with the information in greater depth. Further, the public ledger would detect any abnormal/malicious activity, preventing server-side vote fraud.

The voter registration process would be done at the time of voting, using two-factor authentication. Following existing voting requirements, voters must present proof of identity and proof of address via documentation approved by Elections Canada, which include identification cards like drivers licenses, health cards, passports, citizenship cards, etc. These documents could be uploaded either as pictures or scans. Supplementing this would be a requirement for voters to, at the same time, take a 'selfie' picture to verify that they are actually present to vote. This would safeguard against the vast majority of user-device software hacks – trying to create a malicious software that can simultaneously submit identification information while accurately capturing a picture of the voter through hacking the camera is incredibly difficult. The Follow My Vote interface (*Figure 4*) gives an idea of what elements a simple, accessible user interface for voters should include. The voter registration system still leaves remote voters vulnerable to the possibility of in-person coercion.

Voting would be done either in-person or remotely through mobile phones or personal computers. Ideally, the election would be conducted complete on the blockchain (as opposed to supplementing a paper ballot system) to ensure vote transparency and security across the whole election. In addition to using any of standard public/private key encryption practices, this paper suggests the use of distribution voting as proposed by Zhang et al. (2018) – multiple ballots per vote intention – to further protect voter anonymity.

The consensus mechanism on the blockchain should be done through proof-of-work by Elections Canada, the agency responsible for conducting federal election. This setup

addresses the single point-of-failure issue by maintaining a distributed ledger of vote transactions on every miner within elections Canada. While leaving the consensus process on a public blockchain would remove the need for a central trust, the relative inefficiency of proof-of-work combined with the significant number of blocks needed to keep track of information from over 17 million votes would be environmentally neglectful and also lead to significant delays in tabulating results. A DPoS structure would fit poorly here as well. Hypothetically, a DPoS system would see competing political parties nominate 'witnesses' to perform block generation. The composition of blockchain miners would thus run the risk of duplicating the political dynamics and demographics of Canada onto a new technological arena for political struggle. Elections Canada, as “the independent non-partisan agency responsible for conducting federal elections and referendums” (Elections Canada 2019a), is well-positioned to take up the responsibility of tabulation and verification, as this is already within their mandate. Further, the electorate places a significant level of trust in Elections Canada with over 80% of respondents in a government survey placing “quite a lot” or “a great deal” of confidence in the institution (Elections Canada 2019b).

The consortium BEV system proposed here is not a completely idealized solution. It still relies on a central intermediary to perform the verification/consensus process. However, because all activity would be recorded on a public and immutable ledger, this system would be far more transparent by default than a non-BEV system. The consortium structure is chosen as a means of striking a balance between transparency and efficiency, while still keeping the security characteristics of BEV.

7. Concluding thoughts

This paper has identified the theoretical advantages of a blockchain voting system in comparison to past e-voting systems. The areas with greatest value-added potential include preventing and detecting hacks on a central repository of information, enabling a fully transparent and up-to-date history of votes, and solving the previously irreconcilable problems of anonymity and verifiability. In recognizing that a blockchain voting system has yet to actually be implemented at the state level, this paper has preemptively attempted to illustrate possible conditions which would lead to a blockchain voting system. The inherently transparent and secure principles of this technological platform suggest a promising route for addressing the challenges faced by previous e-voting systems while potentially increasing citizen engagement in ensuring electoral processes. As a nation with blockchain elements within its voting system and significant components of its public administration apparatus enabled by blockchain, the case study of Estonia is helpful in exploring conditions which possibly enable the adoption of a top-to-bottom BEV system.

Though blockchain voting can enable far more secure and transparent elections as the newest revolutionary platform technology, it is not without risks. Diebert warns us that “the very technologies that many heralded as ‘tools of liberation’... are now being used to stifle dissent and squeeze civil society.” (2015, 64). There is a possibility that a dominant ‘techno-elite’ rises who are able to control the discourse leading up to elections, manipulate and confuse participants, and even alter the system itself (Atzori 2017, 50). Further, the relative youth of blockchain technology and its virtual absence as an platform for state elections mean significant uncertainty for its future path of development.

As BEV systems are implemented, comparative empirical work could better define the factors which lead to the adoption of blockchain voting. Further theoretical exploration of blockchain technology on other areas of public administration is also a promising endeavor – its

transparency and security characteristics make it a fitting technological platform for digital identification, real property tracking, auditing, and deliberative democracy. Finally, this paper gives very little insight on the actual effectiveness of BEV systems on addressing the identified challenges on e-voting, and future research should take into account a possible disconnect between promised benefits and realized benefits.

References

Aasmae, Kalev. 2019. “Online Voting: Now Estonia Teaches the World a Lesson in Electronic Elections.” *ZDNet*, March 8, 2019. https://www.zdnet.com/article/online-voting-now-estonia-teaches-the-world-a-lesson-in-electronic-elections/.

“About Us.” 2019. Elections Canada. https://www.elections.ca/content.aspx?section=abo&dir=mis&document=index&lang=e.

Alvarez, R. Michael, Ines Levin, and Yimeng Li. 2018. “Fraud, Convenience, and e-Voting: How Voting Experience Shapes Opinions about Voting Technology.” *Journal of Information Technology & Politics* 15 (2): 94–105. https://doi.org/10.1080/19331681.2018.1460288.

Altman, David. 2013. “Bringing direct democracy back in: toward a three-dimensional measure of democracy.” *Democratization* 20 (4): 615-641. DOI: 10.1080/13510347.2012.659020.

Alvarez, R. M., Hall, T. E., & Trechsel, A. H. 2009. Internet voting in comparative perspective: The case of Estonia. *Political Science and Politics*, 42 (3): 497–505.

Bannister, Frank and Regina Connolly. 2011. "The Trouble with Transparency: A Critical Review of Openness in e-Government." *Policy & Internet* 3 (1): 158-187. doi:10.2202/1944-2866.1076. http://resolver.scholarsportal.info/resolve/19442866/v03i0001/158_ttwtacrooie.

Beaulieu, Emily. 2016. “Electronic Voting and Perceptions of Election Fraud and Fairness.” *Journal of Experimental Political Science* 3 (1): 18–31. https://doi.org/10.1017/XPS.2015.9.

Beroggi, Giampiero E.G. 2014. “Internet Voting: An Empirical Evaluation.” *Computer* 47 (4): 44-50.

“Cautious Optimism: Adopting Blockchain to Improve Canadian Government Digital Services.” 2018. The Conference Board of Canada. https://www.conferenceboard.ca/temp/d5c44c08-adaf-4fc0-a8a6-5400b6999c3a/9591_Cautious%20Optimism_BR.pdf.

Chaum, David L. 1981. “Untraceable electronic mail, return addresses, and digital pseudonyms.” *Communications of the ACM* 24 (2): 84-88.

Clarke, Amanda, and Jonathan Craft. 2017. “The Vestiges and Vanguards of Policy Design in a Digital Context: POLICY DESIGN IN A DIGITAL CONTEXT.” *Canadian Public Administration* 60 (4): 476–97. https://doi.org/10.1111/capa.12228.

Cooley, Rafer, Shaya Wolf, and Mike Borowczak. 2018. “Blockchain-Based Election Infrastructures.” In *2018 IEEE International Smart Cities Conference (ISC2)*, 1–4. Kansas City, MO, USA: IEEE. https://doi.org/10.1109/ISC2.2018.8656988.

Crothers, Charles. 2015. “Using the Internet in New Zealand Elections and Support for E-Voting.” *Political Science* 67 (2): 125–42. https://doi.org/10.1177/0032318715610165.

Digital Signatures Act. 2000. Version published October 30, 2013. Accessed March 24, 2018.

“Delegated Proof-of-Stake Consensus: A Robust and Flexible Decision Making Protocol.” n.d. *Bitshares* (blog). Accessed May 22, 2019. https://bitshares.org/technology/delegated-proof-of-stake-consensus/.

Diebert, Ron. 2015. “Cyberspace Under Siege.” *Journal of Democracy* 26 (3): 64-78.

Ethereum. “White Paper: A Next-Generation Smart Contract and Decentralized Application Platform.” https://github.com/ethereum/wiki/wiki/White-Paper**.**

Falleti, Tulia G. and Thea N. Riofrancos. 2018. “Endogenous Participation: Strengthening Prior Consultation in Extractive Economies.” *World Politics* 70 (1): 86-121.

Foteinis, Spyros. 2018. “Bitcoin’s Alarming Carbon Footprint.” *Nature* 554 (7691): 169–169.

https://doi.org/10.1038/d41586-018-01625-x.
Follow My Vote. “The Online Voting Platform.” Accessed March 24, 2018. https://followmyvote.com/.
Follow My Vote. 2015. “How Our Voter Registration Process Works.” Accessed March 24, 2018. https://www.youtube.com/watch?v=GcAz9mZW1_c.
Follow My Vote. 2016. “Verifiable Blockchain Voting Software Demo.” Accessed March 24, 2018. https://www.youtube.com/watch?v=R53pDz4vp1s.
Germann, Micha, and Uwe Serdült. 2017. “Internet Voting and Turnout: Evidence from Switzerland.” *Electoral Studies* 47 (June): 1–12. https://doi.org/10.1016/j.electstud.2017.03.001.
Goodman, Nicole. 2010. “The Experiences Of Canadian Municipalities with Internet Voting.” *CEU Political Science Journal* 5 (4): 492–520.
Goodman, Nicole, and Leah C. Stokes. 2018. “Reducing the Cost of Voting: An Evaluation of Internet Voting’s Effect on Turnout.” *British Journal of Political Science*, May, 1–13. https://doi.org/10.1017/S0007123417000849.
Goos, Kerstin, Bern Becker and Ralf Linder. 2016. “Electronic, Internet-Based Voting.” in *Electronic Democracy in Europe: Prospects and Challenges of E-Publics, E-Participation and E-Voting*.
“How did Estonia become a leader in technology?” *The Economist explains*. https://www.economist.com/blogs/economist-explains/2013/07/economist-explains-21.
“How Estonia Brought Blockchain Closer to Citizens: GovTech Case Studies.” Coin Telegraph. https://cointelegraph.com/news/how-estonia-brought-blockchain-closer-to-citizens-govtech-case-studies.
Huckle, Steve, and Martin White. 2016. “Socialism and the Blockchain.” *Future Internet* 8 (4): 49. https://doi.org/10.3390/fi8040049.
“I-Voting.” n.d. E-Estonia. Accessed May 22, 2019. https://e-estonia.com/solutions/e-governance/i-voting/.
Irrera, Anna. 2017. “Nasdaq successfully completes blockchain test in Estonia.” *Reuters*. https://www.reuters.com/article/nasdaq-blockchain/nasdaq-successfully-completes-blockchain-test-in-estonia-idUSL1N1FA1XK.
Jun, MyungSan. 2018. “Blockchain Government - a next Form of Infrastructure for the Twenty-First Century.” *Journal of Open Innovation: Technology, Market, and Complexity* 4 (1): 7. https://doi.org/10.1186/s40852-018-0086-3.
Kingsley, Patrick. 2012. “Battle for the internet: Digital diplomacy: Estonia: Switched-on nation that became an internet titan.” *The Guardian*.
Kshetri, Nir, and Jeffrey Voas. 2018a. “Blockchain-Enabled E-Voting.” *IEEE Software* 35 (4): 95–99. https://doi.org/10.1109/MS.2018.2801546.
———. 2018b. “Blockchain-Enabled E-Voting.” *IEEE Software* 35 (4): 95–99. https://doi.org/10.1109/MS.2018.2801546.
Levitsky, Steven and Lucan A. Way. 2002. “The Rise of Competitive Authoritarianism,” Journal of Democracy, 13(2): 51-65.
Levitsky, S. & Way, L. 2015. “The Myth of Democratic Recession.” *Journal of Democracy* 26 (1): 45-58.
Li, Kejiao, Hui Li, Hanxu Hou, Kedan Li, and Yongle Chen. 2017. “Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain.” In *2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 466–73. Bangkok: IEEE. https://doi.org/10.1109/HPCC-

SmartCity-DSS.2017.61.
Mendez, Fernando and Uwe Serdult. 2017. “What drives fidelity to internet voting? Evidence from the roll-out of internet voting in Switzerland.” *Government Information Quarterly* 34: 511-523.
Merkel, Wolfgang, 2004. “Embedded and Defective Democracies” *Democratization*, Vol. 11, no. 5, (December), pp. 33-58.
Moos, Mitchell. 2018. “Analysis: Bitcoin Costs $1.4 Billion to 51% Attack, Consumes as Much Electricity as Morocco.” *CryptoSlate*, November 29, 2018. https://cryptoslate.com/analysis-bitcoin-costs-1-4-billion-to-51-attack-consumes-as-much-electricity-as-morocco/.
Munck, Gerardo L. 2016. “What is democracy? A reconceptualization of the quality of democracy,” Democratization, Vol. 23, no. 1, pp. 1-26.
Neymanns, H. (2002). Die Wahl der Symbole: Politische und demokratietheoretische Fragen zu Online-Wahlen. In H. Buchstein & H. Neymanns (Eds.), Online-Wahlen (pp. 24–37). Opladen, Germany: Leske und Budrich.
“Online Voting: A Path Forward for Federal Elections.” 2017. Government of Canada. https://www.canada.ca/en/democratic-institutions/services/reports/online-voting-path-forward-federal-elections.html#toc18.
Pawlak, Michał, Aneta Poniszewska-Marańda, and Natalia Kryvinska. 2018. “Towards the Intelligent Agents for Blockchain E-Voting System.” *Procedia Computer Science* 141: 239–46. https://doi.org/10.1016/j.procs.2018.10.177.
Persily, Nathaniel. 2017. “The 2016 U.S. Election: Can Democracy Survive the Internet?” *Journal of Democracy* 28 (2): 63-76. DOI: https://doi.org/10.1353/jod.2017.0025.
Saito, Kenji and Hiroyuki Yamada. 2016. "What’s so Different about Blockchain? — Blockchain is a Probabilistic State Machine." *2016 IEEE 36th International Conference on Distributed Computing Systems Workshops (ICDCSW)*: 168-175. doi:10.1109/ICDCSW.2016.28. http://resolver.scholarsportal.info/resolve/23325666/v2016inone/168_wsdabbiapsm.
“Security and Safety.” n.d. E-Estonia. Accessed May 22, 2019. https://e-estonia.com/solutions/security-and-safety/.
Segupta, Ankur. 2017. “Blockchain Vs Tangle.” https://steemit.com/blockchain/@ankursengupta/blockchain-vs-tangle.
“Success Stories.” n.d. E-Estonia. Accessed March 24, 2018. https://e-estonia.com/.
Shahzad, Basit, and Jon Crowcroft. 2019. “Trustworthy Electronic Voting Using Adjusted Blockchain Technology.” *IEEE Access* 7: 24477–88. https://doi.org/10.1109/ACCESS.2019.2895670.
Shermin, Voshmgir. 2017. “Disrupting Governance with Blockchains and Smart Contracts.” *Strategic Change* 26 (5): 499–509. https://doi.org/10.1002/jsc.2150.
Shin, Laura. 2016. “Republic of Georgia to Pilot Land Titling on Blockchain with Economist Hernando De Soto, BitFury.” *Forbes*, April 21. Accessed December 11, 2016. http://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#7be4ec0e6550.
Shukla, Shalini, A N Thasmiya, D O Shashank, and H R Mamatha. 2018. “Online Voting Application Using Ethereum Blockchain.” In *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 873–80. Bangalore: IEEE. https://doi.org/10.1109/ICACCI.2018.8554652.
Solaiman, Irene. 2018. “Defending Vote Casting: Using Blockchain-Based Mobile Voting Applications in Government Elections.” Harvard Kennedy Institute Belfer Center. https://www.belfercenter.org/publication/defending-vote-casting-using-blockchain-

based-mobile-voting-applications-government.
Solvak, Mihkel, and Kristjan Vassil. 2018. “Could Internet Voting Halt Declining Electoral Turnout? New Evidence That E-Voting Is Habit Forming: Internet Voting and Habit Formation.” *Policy & Internet* 10 (1): 4–21. https://doi.org/10.1002/poi3.160.
Springall, Drew, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman. 2014. “Security Analysis of the Estonian Internet Voting System.” In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS ’14*, 703–15. Scottsdale, Arizona, USA: ACM Press. https://doi.org/10.1145/2660267.2660315.
“Survey of Electors on Communications with Electors.” 2019. Elections Canada. https://www.elections.ca/content.aspx?section=res&dir=cons/sece&document=p8&lang=e.
Swan, Melanie and Primavera de Filippi. 2017. “Toward a Philosophy of Blockchain: A Symposium.” *Metaphilosophy* 48 (5).
Tenove, Chris, Jordan Buffie, Spencer McKay, and David Moscrop. 2018. *Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy*. Centre for the Study of Democratic Institutions.
Unger, Jonathan, Anita Chan, and Him Chung. 2014. “Deliberative Democracy at China’s Grassroots: Case Studies of a Hidden Phenomenon.” *Politics and Society* 42 (4): 513-535. DOI: 10.1177/0032329214547344
Unt, Taavi, Mihkel Solvak, and Kristjan Vassil. 2017. “Does Internet Voting Make Elections Less Social? Group Voting Patterns in Estonian e-Voting Log Files (2013–2015).” Edited by Frederic Amblard. *PLOS ONE* 12 (5): e0177864. https://doi.org/10.1371/journal.pone.0177864.
Vaccari, Lorenzino, Francesco Pignatelli, David Allessie, and Maciej Sobolewski. 2019. “Blockchain for Digital Government: An Assessment of Pioneering Implementations in Public Services.” 29677. EUR, Scientific and Technical Research Series.
Vassil, Kristjan, Mihkel Solvak, and Piret Ehin. 2016. “More Choice, Higher Turnout? The Impact of Consideration Set Size and Homogeneity on Political Participation.” *Journal of Elections, Public Opinion and Parties* 26 (1): 78–95. https://doi.org/10.1080/17457289.2015.1102920.
Vassil, Kristjan, Mihkel Solvak, Priit Vinkel, Alexander H. Trechsel, and R. Michael Alvarez. 2016. “The Diffusion of Internet Voting. Usage Patterns of Internet Voting in Estonia between 2005 and 2015.” *Government Information Quarterly* 33 (3): 453–59. https://doi.org/10.1016/j.giq.2016.06.007.
Vill, Meelis. 2018. “Verizon to deploy blockchain platform based on Guardtime technology.” *Guardtime*. https://guardtime.com/blog/verizon-to-deploy-blockchain-platform-based-on-guardtime-technology.
Wampler, Brian. 2008. “When Does Participatory Democracy Deepen the Quality of Democracy? Lessons from Brazil.” *Comparative Politics* 41 (1): 61-81.
Wang, Baocheng, Jiawei Sun, Yunhua He, Dandan Pang, and Ningxiao Lu. 2018. “Large-Scale Election Based On Blockchain.” *Procedia Computer Science* 129: 234–37. https://doi.org/10.1016/j.procs.2018.03.063.
Waterman, Shaun. 2017. “Nasdaq says Estonia e-voting pilot successful.” *Cyberscoop.* https://www.cyberscoop.com/nasdaq-estonia-evoting-pilot/.
Yavuz, Emre, Ali Kaan Koc, Umut Can Cabuk, and Gokhan Dalkilic. 2018. “Towards Secure E-Voting Using Ethereum Blockchain.” In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, 1–7. Antalya: IEEE. https://doi.org/10.1109/ISDFS.2018.8355340.

Yi, Xun and Eiji Okamoto. 2013. “Practical Internet voting system.” *Journal of Network and Computer Applications* 36: 378-387.

Yuan, Rui, Yu-Bin Xia, Hai-Bo Chen, Bin-Yu Zang, and Jan Xie. 2018. “ShadowEth: Private Smart Contract on Public Blockchain.” *Journal of Computer Science and Technology* 33 (3): 542–56. https://doi.org/10.1007/s11390-018-1839-y.

Zhang, Wenbin, Yuan Yuan, Yanyan Hu, Shaohua Huang, Shengjiao Cao, Anuj Chopra, and Sheng Huang. 2018. “A Privacy-Preserving Voting Protocol on Blockchain.” In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 401–8. San Francisco, CA: IEEE. https://doi.org/10.1109/CLOUD.2018.00057.

Zissis, Dimitrios, and Dimitrios Lekkas. 2011. “Securing E-Government and e-Voting with an Open Cloud Computing Architecture.” *Government Information Quarterly* 28 (2): 239–51. https://doi.org/10.1016/j.giq.2010.05.010.