Buying Votes in the 21st Century: The Potential Use of Bitcoins and Blockchain Technology in Electronic Voting Reform

BRIANNA BOGUCKI*

INTRODUCTION

With technological advances happening almost constantly, the world and the systems used to run it are changing. Processes are becoming automated and digitized, allowing organizations and individuals to operate complex systems run by computer and eliminating human error and bias. Given the complexity, cost, and time required to conduct a fair and representative election, it was only a matter of time until governments attempted to apply new technological advances to assisting in the running of a democratic system of voting. Thus far, however, few governments have even attempted to institute electronic voting systems, with even fewer implementing them successfully. While some countries, such as Estonia, have largely succeeded, creating an electronic platform to improve the convenience of voting has been difficult, with security being a primary concern.

One potential option that has been suggested for use in electronic voting ("e-voting") is that of bitcoin and blockchain technology, a decentralized system of currency exchange that can be coded to exchange different digital indicators of value, from money, to ownership of fungible goods, to votes.

* BA (Hons), JD (University of Manitoba). At the date of publication, Brianna is an articling-student-at-law at the firm Cochrane Saxberg in Winnipeg, MB. The author would like to thank Dr. Bryan Schwartz for his invaluable feedback and assistance in preparing this article.

While there has been some controversy about the use of bitcoins, particularly given that they are a largely unregulated currency prone to wild market fluctuations, the unregulated nature of the technology is irrelevant to its potential to be used for voting and will therefore not be discussed in this paper. Instead, this document will describe the development and use of bitcoins using blockchain technology, the characteristics of a potential electronic voting system that would be required in order to make it functionally equivalent to current voting methods in Canada, and the applicability of blockchain and bitcoin technology to such a scheme.

The Development of Bitcoin and Blockchain Technology

Though there are now several different types of currency and transactional systems that utilize the blockchain (or similar) technology, blockchain technology was originally a decentralized payment system built to facilitate the transfer and use of bitcoins (BTC), a digital currency not issued by a central bank. Bitcoins, known as a 'cryptocurrency' because of the cryptographic software used to regulate the system through which they are transacted,[1] are "neither a *commodity* currency (backed by gold or some other commodity), nor a *fiat* currency (used by convention as a result of legal edict)."[2] As Abramowicz explains, bitcoins are not simply a currency based on the digital equivalent of dollars, but can also be used to "create and enforce property rights."[3] Indeed, bitcoins can be assigned non-monetary values in order to transact ownership of assets, such as stock in companies or real property, through the blockchain system.[4]

Bitcoins and blockchain technology were developed in order to allow verified peer-to-peer transactions without the need for a central server or verification and facilitation by a third party.[5] Bitcoin technology (and digital currency in general) was developed as an alternative to server-based and third-

[1] "Virtual Currency", *The Columbia Encyclopedia*, by Columbia University and Paul Lagasse (New York: Columbia University Press), online: <http://bit.ly/2vPXaGr>.
[2] Michael Abramowicz, "Cryptocurrency-Based Law" (2016) 58 Ariz L Rev 359 at 361.
[3] *Ibid*.
[4] DutchChain, "The real value of bitcoin and crypto currency technology – the Blockchain explained" (14 October 2014) at 00h.2min.45s, online: Youtube <https://www.youtube.com/watch?v=YIVAluSL9SU>.
[5] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", (2008) *Bitcoin.org* (website), online: <https://bitcoin.org/bitcoin.pdf> at 1 [Nakamoto].

party-dependant commerce systems.[6] Third-party-dependant commerce systems, such as banks, require complex processes to make and reverse transactions, resulting in inefficiencies such as higher transaction costs, minimum amounts for transactions, and an unnecessary cost associated with making "non-reversible payments for non-reversible services" since the cost associated with maintaining a complex system is distributed across a variety of transactions, including simple, one-way exchanges.[7] While server-based systems cut down on the personnel requirements often employed by third party systems, if the server fails, all transaction records are lost and further transactions are unable to be processed.[8] These downtimes result in high costs, with one estimate suggesting that $26.5 billion per year is lost due to server downtimes ($55,000 in annual revenue for small businesses, $91,000 for midsized business, and over $1,000,000 for large businesses) in addition to the negative effects technology failures have on employee morale and company reputation.[9]

The reason why server systems and facilitation of transactions by third parties has thus far been the norm in e-commerce systems is due to the question of trust that arises in any transaction. Using a digital currency without someone to verify the transaction can result in the problem of double spending, where less-savoury individuals attempt to spend the same digital dollars twice.[10] Typically, the third party or server (such as eBay or PayPal) will maintain digital ledgers for its customers; when one customer orders a transfer of funds to another, the third party will deduct the money from the sender's account and move it to the receiver's. Without a third party to verify and facilitate the transaction, the sender's account does not get debited the amount owed to the receiver, giving the sender the chance to attempt to use the 'already spent' money a second time.[11]

---

[6] The Memo, "The Blockchain Explained" (11 November 2015) at 00h.00m.52s, online: YouTube <https://www.youtube.com/watch?v=wyfm92qqSh8> [The Memo].

[7] Nakamoto, *supra* note 5 at 1.

[8] The Memo, *supra* note 6 at 00h.00m.52s.

[9] Chandler Harris, "IT Downtime Costs $26.5 Billion in Lost Revenue", *InformationWeek* (24 May 2011), online: <http://www.informationweek.com/it-downtime-costs-$265-billion-in-lost-revenue/d/d-id/1097919>.

[10] Jerry Brito & Andrea Castillo (2013) "Bitcoin: A Primer for Policy Makers" at 3-4, online: <https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf> [Brito].

[11] *Ibid.*

How Do Bitcoins and Blockchains Work?

The solution to the issues posed by third-party-dependant and server-based systems is, ostensibly, a peer-to-peer transaction system based on "cryptographic proof of trust" that allows individuals to digitally transfer money and ownership of property without the middleman (or middle-server).[12] Instead of being controlled by a central server or third party, the transaction ledger is distributed to all "nodes" in a decentralized global network of computers. The transactions are collected into a block of data, and nodes called 'bitcoin miners' compete to solve a complex mathematical equation in order to verify the transactions in the block who are then, if successful, paid for their efforts with newly-minted bitcoins.[13] The first bitcoin miner to solve the equation verifies the transactions made since the last ledger update (that the parties have the correct information to proceed and enough currency to make the deal go through) and adds these transactions to the digital ledger as a "block" of information, creating a "linear sequence of linked data blocks" that serve as the ledger history for all transactions made on the system.[14] Each block also records a 'hash,' a one-way software function that acts as a fingerprint of the data from the previous block of transactions, and a 'nonce', a random number that must be matched with the hash to satisfy the mathematical equation. This hash function is unable to be reproduced, making it easy to see whether a block has been tampered with and making hacks or other attempted modifications easy to detect (thus preserving the integrity of the chain). This is because in order to "to generate a new block, miners must find a nonce value that, when hashed with additional fields…results in a value below a given threshold",[15] and creating a false hash that satisfies the math problem when combined with the nonce is nearly impossible.[16]

Once a miner has solved the problem required to verify the block, the winning miner transmits the data block to other nodes who did not win the mathematical competition, and they accept the addition of the block to the

---

[12] Nakamoto, *supra* note 5 at 1.
[13] *Ibid* at 4.
[14] TEDx Talks, "Block Chain Revolution | Giovanna Fessenden | TEDxBerkshires" (20 July 2016) at 00h.4m.40s, online: <https://www.youtube.com/watch?v=oMhZTEQZJPI> [TEDx Block Chain].
[15] Elli Androulaki et al, "Evaluating User Privacy in Bitcoin" (2012) *IACR Cryptology ePrint Archive* 596, s 2, online: <http://fc13.ifca.ai/proc/1-3.pdf> [Androulaki et al].
[16] *Ibid.*

chain by verifying that the equation was solved correctly and that the transactions are valid (with correct public and private keys, and sufficient funds available to complete the transaction).[17] If a majority of the miners verify that the transactions are correct, the block is added and each node then updates its copy of the ledger accordingly.[18] The mathematical calculations required to solve the problem also progressively increase in difficulty, so that "[a]s more processing power is dedicated to mining, the protocol will increase the difficulty of the math problem, ensuring that Bitcoins are always mined at a predictable and limited rate."[19] Since the maximum number of minable bitcoins has been capped at 21 million,[20] this should ideally also prevent the devaluing of the currency through inflation (though it may be insufficient in protecting against deflation).[21]

Satoshi Nakamoto, a pseudonym used by the originator of bitcoin and blockchain technologies, defined digital coins "as a chain of electronic signatures."[22] Being digital, each coin is a bit of code that "[e]ach owner transfers…to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership."[23] An individual's public key is akin to a username, while their private key is akin to a password. To transfer bitcoins, the sender will send the coins to the receiver's public key, and "sign" it with their own private key.[24]

---

[17] *Ibid*

[18] TEDx Talks, "New Kids on the Blockchain | Lorne Lantz | TEDxHamburgSalon" (24 March 2016), online: YouTube <https://www.youtube.com/watch?v=A1Vbrxkqjwc> [TEDx New Kids].

[19] Brito, *supra* note 10 at 7.

[20] *Ibid.* The last "satoshi" (0.0000001) of a bitcoin is expected to be mined in 2140, after which miners will be paid with transaction fees rather than new bitcoins.

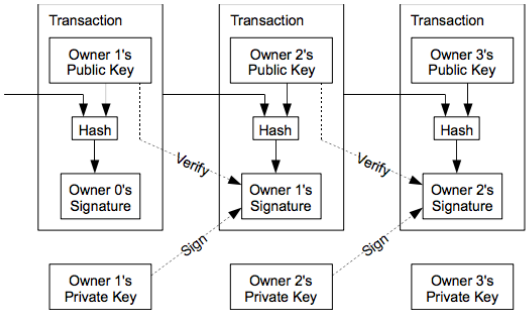
[21] Adam Hayes, "Why is Deflation Bad for the Economy?", *Investopedia,* online: < http://www.investopedia.com/articles/personal-finance/030915/why-deflation-bad-economy.asp>.

[22] Nakamoto, *supra* note 5 at 2.

[23] *Ibid.*

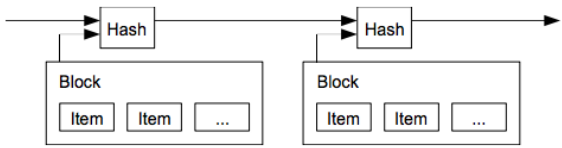
[24] Brito, s*upra* note 10 at 5; Nakamoto, *supra* note 5 at 2 (diagram).

Figure 1. Visual representation of the bitcoin transfer process



These transactions are also stamped with a hash that acts as a timestamp and confirmation of previous data in the chain. Since the hash function describes the data from the previous block, the information from the previous block must already be there in order to be included in the hash, thereby validating the previous data's existence at the point in time at which the last block was added.[25]

Figure 2. Visual representation of the hash function



Nodes are programmed to always attempt to extend the longest chain, and not all chains need to receive every block for it to be accepted; since only a simple majority of nodes are required in order to accept a block,[26] any of the rest of the nodes who miss a block can request their chains be updated once they receive subsequent blocks, and update their chains accordingly.[27]

[25] Nakamoto, *supra* note 5 at 2 (diagram).
[26] TEDx Block Chain, *supra* note 14.
[27] Nakamoto, *supra* note 5 at 4.

The Non-Digital Value of Bitcoins: Are Bitcoins Worth Anything Away from a Computer?

The simple answer to whether bitcoins are worth anything anywhere other than the internet appears to be 'mostly, no'. While banks, stock exchanges, and other institutions are exploring the potential uses for blockchain and bitcoin technology,[28] since bitcoins are neither a commodity-based or *fiat* currency there are few places where bitcoins can be exchanged for actual cash dollars that can be spent at locations that do not take bitcoins as payment. This is distinct from other network-based electronic money transfer systems such as credit and debit cards. While those cards also work on an electronic system, they are backed by *fiat* or commodity-based currency, allowing them to be used interchangeably with regular money. Bitcoins, by contrast, can only be transacted in certain places, likely due to the reluctance of most mainstream retailers to accept an unbacked digital currency.

The main ways to buy and sell bitcoins with the result of receiving actual cash are through the use of certain websites,[29] a company that acts a bitcoin broker,[30] or by buying or selling coins to an individual by meeting in an online forum or in person. Additionally, some internet-based companies will allow you to pay for goods and services using bitcoins through the use of a digital wallet, or to put bitcoins towards digital reward cards that can be used on the websites for brick-and-mortar stores that do not currently accept bitcoins as payment.[31] Additionally, 'coloured coins' may be used to assign something other than monetary value to bitcoins. The use of coloured coins "allows [the] attaching metadata to Bitcoin transactions and leveraging the Bitcoin infrastructure for issuing and trading immutable digital assets that can represent real world value."[32] Essentially, small packets of data can be

---

[28] See Daniel Gasteiger's speech for examples of potential future uses of this technology. TEDx Talks, "Blockchain Demystified | Daniel Gasteiger | TEDxLausanne" (25 April 2016) at 00h.5m.35s, online: YouTube <https://www.youtube.com/watch?v=40ikEV6xGg4>.

[29] "How to Sell Bitcoin", *CoinDesk* (23 October 2015), online: <http://www.coindesk.com/information/sell-bitcoin/>.

[30] Alexandra Posadzki, "ATMs that swap cash for Bitcoins coming to Canada this fall", *The Canadian* Press (8 September 2013), online: <http://www.ctvnews.ca/canada/atms-that-swap-cash-for-bitcoins-coming-to-canada-this-fall-1.1445199>.

[31] Clare O'Connor, "How to Use Bitcoin to Shop at Amazon, Home Depot, CVS and More", *Forbes* (17 February 2014), online: Forbes <www.forbes.com>.

[32] "Colored Coins Protocol Specification", *GitHub* (19 April 2016), online: <https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki/Introduction>.

attached to bitcoins and the transfer of that data can be equated later to the transfer of physical assets.

Advantages to the Blockchain System

There are several advantages of the blockchain system of currency transfer. The first is that the system provides "immutable preservation of data integrity."[33] Due to the fact that each transaction is imprinted with the hash information of the previous block, when combined with the consensus mechanism required to approve blocks it becomes nearly impossible to change or falsify information in subsequent blocks. To do so, the attacker would have to modify a block; this would reflect in the hash of the next block, and affect all subsequent blocks.[34] Since a majority of nodes must accept the block of transactions as valid in order for the block to be added to the blockchain, the attacker would essentially have to change the desired block and then create a false chain longer than the 'real' chain on every computer that has access to the chain around the world, beginning from the block that they want to modify.[35] While making such a change is theoretically "possible, [it is] computationally impractical" to do so.[36]

Furthermore, if hackers attempt to subvert the system by generating a second, competing block chain – essentially creating a new block from which nodes would continue to branch off, thereby creating a new chain branch from a certain point rather than attempting to change aspects of the data in an already-existing blockchain – he or she would have to do so faster than other, legitimate chains were being built, since nodes always attempt to extend the longest chain.[37] For example, if there were ten blocks in the blockchain, and the hacker wanted to change block six, he or she would have to create blocks to replace blocks six through ten (with proper transactions and authentication), and then attempt to create an eleventh block, all before the original chain added its eleventh block. Nakamoto further suggests that even if a hacker were successful in creating an alternate chain, the only thing the hacker would be able to accomplish is undoing previously-made transactions, as legitimate nodes will recognize invalid transactions (for

[33] TEDx Block Chain, *supra* note 14 at 00h.04m.05s.
[34] Kibin Lee et al, "Electronic Voting Service Using Block-Chain" (2016) 11:2 J Digital Forensics, Security & L 123 at 126 [Lee].
[35] TEDx Block Chain, *supra* note 14 at 00h.07m.25s.
[36] *Ibid.*
[37] Nakamoto, *supra* note 5 at 6-7.

example, transactions that transfer money that does not exist) and refuse to accept blocks containing them.[38] A hacker would therefore be unable to spend bitcoins that are not his or her own.

The relevance of this level of security and data integrity as it applies to voting is that it makes it difficult, if not impossible, to corrupt the transactional chain and artificially falsify voting transactions after they have occurred. Going back and changing someone's vote would be extremely difficult once voters have established their vote on the blockchain, as it would likely require changing the transaction (either by changing the destination of the vote or by removing the vote completely) as discussed above. In fact, Lorne Lantz has suggested the use of e-voting over the blockchain as a way for corrupt governments with a history of rigging elections to regain the support and trust of their voters.[39]

Other advantages provided by the blockchain system are those provided by having a distributed, decentralized system.[40] Having a decentralized system rather than a system with a centralized server and access point nodes inherently protects against server outages and IT issues that occur as a result of many people attempting to access a specific server at the same time. This is a situation that seems likely to occur during the electronic voting process when people all over the country attempt to access the same server (or set of servers) at the same time to cast their votes. A decentralized system would also protect against Denial of Service (DoS) attacks like the one experienced by the NDP in 2012, wherein the NDP's server was "bombard[ed]… with repeated attempts at communication to try to slow it down or crash it altogether", leaving delegates unable to cast votes for the next NDP leader.[41]

In the case of a blockchain system, if one node in the blockchain system fails, the remaining nodes continue processing data independently of the downed node, unlike when a central server goes down, and takes the rest of the system with it until it can be repaired or restarted. Furthermore, once the downed node comes back online, it can 'catch up' to the other nodes on the blockchain and update its copy of the ledger once the missing blocks in the chain are detected as missing. This should allow for relatively uninterrupted system access for voters, as even if one computer were to go down voters

---

[38] *Ibid.*

[39] TEDx New Kids, *supra* note 18 at 00h.13m.01s.

[40] TEDx Block Chain, *supra* note 14 at 00h.07m.52s.

[41] Laura Payton, "NDP site the weak link in online attack during 2012 leadership vote", *CBC News* (4 March 2014), online: <http://www.cbc.ca/news/politics/ndp-site-the-weak-link-in-online-attack-during-2012-leadership-vote-1.2557861>.

could continue voting (making transactions) while other computers continued forming blocks and verifying transactions (votes placed). The blockchain system could possibly face efficiency issues here, however, since voters could need to wait from several minutes up to an hour – the time it takes the miners to solve the mathematical problem allowing them to add blocks to the chain, verify transactions, and then to build on additional blocks to ensure the transaction will not be lost due to a fork in the chain – to ensure that their votes had gone through and had been successfully recorded.

A third advantage of using blockchain technology is that it solves the problem of validating user identity without requiring the user to provide personal information. Typically, financial institutions that facilitate transactions between parties require the parties to provide a certain amount of disclosure as to their identities in order to verify that they are who they claim to be and they have the funds they wish to transact. For example, PayPal may require you to connect a bank account in addition to proving other information such as name, address, and credit card information.[42] While this information may or may not be shared with the other party, parties cannot remain completely anonymous due to the facilitating party's knowledge of their identifying information. Furthermore, even with security measures in place, identity theft remains a major issue in Canada, with almost $10.5 million in losses recorded from over 20,600 people in 2014.[43] A study funded by the U.S. Department of Justice spoke to individuals incarcerated for identity theft, and found that "[r]egardless of [the offenders'] chosen lifestyle, they were primarily motivated by the quick need for cash and see identity theft as an easy, relatively risk-free way to get it."[44] Of particular interest is one anti-theft quality of blockchain systems that can protect identities both in regular commercial transactions and when voting: the fact

[42] "Frequently Asked Questions – The Verification Process" (2016) *PayPal* (website), online: <www.paypal.com/ca>. Because PayPal allows anyone to buy and sell, even individuals wanting to remain solely as buyers may be required to verify their accounts after transferring a certain amount of money.

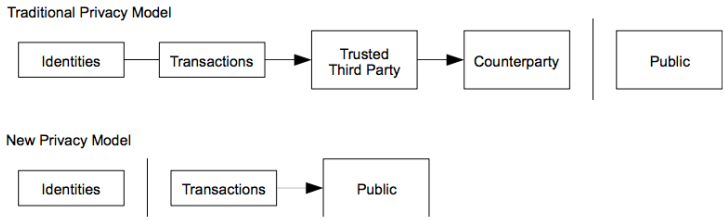
[43] Canadian Anti-Fraud Centre, "Annual Statistical Report 2014" *Government of Canada Canadian Anti-Fraud Centre* (website), online: <www.antifraudcentre-centreantifraude.ca>.

[44] Heith Copes & Lynne Vieraitis, "Identity Theft: Assessing Offenders' Strategies and Perceptions of Risk" (2007), U.S. Department of Justice at 2, online: <https://www.ncjrs.gov/pdffiles1/nij/grants/219122.pdf> [Copes & Vieraitis].

that the blockchain IDs used in transactions can be assigned anonymously, without the need for identity validation.[45]

In contrast to regular transactions wherein the nature of the transaction and identity of the parties are known to a third party but kept from the public, the blockchain system makes the transactions public, while making it possible to keep the users almost completely anonymous,[46] or by incorporating pseudonyms where it is necessary for an individual to identify themselves (i.e. to ensure that the same person who is spending bitcoins is the person who initially received them).

Figure 3. Comparison of privacy models



Bitcoin users create bitcoin addresses through the use of 'wallets.' These wallets typically generate a new bitcoin address for every potential transaction, since "once addresses are used, they become tainted by the history of all transactions they are involved with."[47] Since anyone can see the address to which bitcoins were sent, it is important to generate a new address for every transaction in order to avoid building transaction history available to the public.

Bitcoin addresses are generated from a combination of a public and private keys. Since the addresses are randomly generated and only used once, it is nearly impossible to track certain keys to certain bitcoin users, though this does not account for other methods of identification, such as IP address logging[48] or the utilization of bitcoin transfer websites that require you to provide personal information.[49] Furthermore, repeated transactions using

---

[45] Nakamoto, *supra* note 5 at 6.
[46] *Ibid.*
[47] Copes & Vieraitis, *supra* note 44.
[48] "Protect your privacy" *Bitcoin.org* (website), online: <https://bitcoin.org/en/protect-your-privacy>.
[49] Brito, *supra* note 10 at 8.

bitcoins can be utilized in analyses that may allow multiple similar transactions to be linked to the same user through the amount and type of transaction, or location of the transaction. In a study by Androulaki et al., the authors estimated that "behaviour-based clustering techniques can unveil, to a large extent, the profiles of 40% of Bitcoin users, even if these users try to enhance their privacy by manually creating new addresses."[50] While these results do present concerns about the level of anonymity and identity protection that is actually achieved relative to the amount that is promised, the parameters of the study included an assumption that the individual attempting to connect profiles had some familiarity with the area and circumstances in which transactions took place,[51] and was basing their analysis on 25 transactions per user. Since individuals would likely be casting far fewer than 25 votes at a time if blockchain technology were employed in electronic voting, the potential for identification of a user would be ameliorated by the lack of information; however, given the importance of total anonymity in the voting process, this concern should not be taken lightly.

Incorporating Blockchain Technology into the Canadian Voting Process

In their report "Establishing a Legal Framework for E-Voting in Canada",[52] Schwartz and Grice describe several "attributes and values that Canadians currently have under the paper-based system" that an electronic voting system should emulate or to which it should be functionally equivalent in order to justify the use of such systems for Canadian elections. Whether blockchain technology may be an appropriate solution for the concerns described will be addressed for the majority of the points. While the report focusses on both the requirements needed to be fulfilled by electronic voting in general and characteristics of a legislative framework to implement it, this paper will focus on the former. The modified[53] list of ideal characteristics is:

> facilitated accessibility and reasonable accommodation, voter anonymity..., accurate and prompt results, comprehensible and transparent processes, system security and

[50] Androulaki et al, *supra* note 15, s 7.
[51] "[W]e assume that A can have access to the (public) addresses of some vendors along with (statistical) information such as the pricing of items or the number of their clients within a specified amount of time." *Ibid*, s 3.1.
[52] Bryan Schwartz & David Grice, Elections Canada, *Establishing a Legal Framework for E-Voting in Canada* (Ottawa: Elections Canada, 2013) [Schwartz & Grice].
[53] The list has been edited for topicality and brevity.

> risk assessment, detection of problems and remedial contingencies..., effective and independent oversight, and cost justification and efficiency[54]

Essentially, a blockchain-based voting system would require some type of confirmation of voter eligibility, after which voters would be assigned a random key pair. Voters would then be able to vote by sending small amounts of bitcoins to their desired candidates. Finally, votes will be secured on the blockchain and a tally will be computed. Overall, a blockchain-based voting system should include all of the advantages of blockchain and bitcoin technology while complying with the values outlined by Schwartz and Grice as being necessary for the construction of an effective electronic voting system.

Facilitated Accessibility and Reasonable Accommodation

The first requirement of internet voting is that it be as or more accessible to voters than current paper-based voting methods. While on its face internet voting is commonly touted as having the potential to be more accessible to Canadians than paper-based voting due to the pervasiveness of the internet, important and novel obstacles arise when attempting to implement and carry out internet-based voting. One of the main arguments against the adoption of internet voting is due to the presence of a "digital divide", a divide in accessibility to voting services due to the inequity of internet availability to certain segments of the population.[55] While factors such as one's location, gender identity, and level of education do not seem to have strong effects, familiarity and amount of computer savvy and age are important factors, with younger individuals being far more likely to vote online than their older counterparts.[56] Furthermore, a report by the Canada-Europe Transatlantic Dialogue cited a variety of reasons for further divide, particularly based on economic inequality for users with cheaper, more easily accessible computers and internet connections.[57]

While ideally a blockchain-operated system would be relatively easy-to-use (in order to minimize the learning curve for those unfamiliar with using certain types of technology), if the voter is unable to transmit their vote through the system due to a faulty or non-existent internet connection, the

---

[54] Schwartz & Grice, *supra* note 52 at 6-7, 29-30.
[55] Dimitris A Gritzalis, ed, *Secure Electronic Voting* (New York: Springer Science and Business Media, LLC, 2003) at 154.
[56] Canada-Europe Transatlantic Dialogue, *A Comparative Assessment of Electronic Voting*, (Ottawa: Elections Canada, 2010) at 18 [Canada-Europe].
[57] *Ibid* at 16.

efforts put into making a simple system will be moot. While internet connections may be available at polling stations, it is conceivable that the connection would slow down with everyone attempting to transmit their vote. Further, while there exists mobile technology (such as using iPads over a 3G or 4G network) that could bring the internet to those who do not have access to it despite being in an area where internet is available, access to these systems may also be compromised in rural or otherwise out-of-service areas. Schwartz and Grice suggest that it is necessary to consider measures that will help provide increased access to required technologies, whether it be by allowing people to use their personal electronics or by providing resources such as help lines to assist those unfamiliar with using the internet.[58] In any case, non-electronic means of voting should also be available for those uncomfortable voting through electronic means, to make sure all Canadians feel comfortable exercising their right to vote.

Voter Anonymity

Schwartz and Grice emphasize the requirement to protect voter anonymity and ensure that voters are not being subjected to undue influence when they go to vote.[59] In a process familiar to anyone who has participated in an election, initially voters are required to identify themselves to preceptors at polling stations, who confirm their eligibility to vote and hand them a ballot. The ballot contains no personal information, and once the individual records his or her vote, the ballot is put into a secured ballot box to be counted once polls close. In contrast, absentee voters receive and submit their ballots by mail. They receive a blank ballot in an envelope, which itself is in an outer envelope. The voter marks their ballot, encloses it in the inner envelope, and then signs the outer envelope – the voter's signature and information on the outer envelope will allow Elections Canada to verify the voter as someone eligible to vote, and the inner envelope keeps the individual verifying the information on the outer envelope from seeing how the person voted.

A similar double envelope process using public key cryptography has been used for electronic voting in the past; essentially, the voter would "pack" their vote into a ciphertext that would be encrypted in a bitcoin "envelope" using Elections Canada's public key. The voter would then "sign" an outer envelope

[58] Schwartz & Grice, *supra* note 52 at 18.
[59] *Ibid* at 29.

using their private key, which would be used by Elections Canada to identify the voter as someone eligible to vote. Before processing, the private key would be "stripped off" and subjected to other encryption methods to ensure anonymity.[60] While this specific electronic process is mentioned due to being particularly analogous to current paper-based voting methods, other methods have been investigated and summarized in literature on the topic.[61]

Another, more troubling aspect of online voting is its potential to encourage the exercise of undue influence.[62] This issue pervades many types of voting, and could be particularly prevalent when an individual is in an unmonitored environment – for example, their home or workplace.[63] The issue is also more likely to arise where individuals are allowed to vote unmonitored, but may only cast one ballot.[64] This is an inherent issue with the use of blockchain technology, and may be one of the biggest barriers to its adoption along with the difficulty of bridging the digital divide. While it is theoretically possible to override transactions before they are accepted by the blockchain (by double-spending your bitcoins, or in this case, ballotcoins and appending a higher transaction fee to your latter purchase and hoping that in doing so miners are encouraged to process your latter transaction first, leaving you with no ballotcoins with which to complete the first transaction),[65] it is difficult to do so. This problem has been ameliorated in Estonia, where individuals are allowed to cast multiple ballots with only the last one counting,[66] but this could be difficult for blockchain voting methods where private keys are anonymized for every transaction (using the same private key is unwise because it risks voter anonymity). Anonymizing private keys brings its own challenges, however, if the new votes come from different keys, election officials will be unable to tell which votes are true and should be counted. In theory, allowing multiple votes should assist an individual in being able to cast a vote at a time when they are not in the presence of the

---

[60] Christian Meter, *Design of Distributed Voting Systems* (MA Thesis, Heinrich-Heine-Universität Düsseldorf, 2015) [unpublished] [Meter]. This paper also contains an extensive review of various types of electronic voting systems, as well as their pros and cons.

[61] *Ibid*. See also the discussion in Canada-Europe, *supra* note 56.

[62] Schwartz & Grice, *supra* note 52 at 156.

[63] *Ibid.* See also Timothy Frye, Ora John Reuter & David Szakonyi, "Political Machines at Work: Voter Mobilization and Electoral Subversion in the Workplace" (2014) 66:2 World Politics 195.

[64] Meter, *supra* note 60 at 61.

[65] "How to Clear a Stuck Bitcoin Transaction" (29 July 2015), *Bitzuma*, online: <bitzuma.com/posts/how-to-clear-a-stuck-bitcoin-transaction/>.

[66] Meter, *supra* note 60 at 25.

person wishing to exert influence, even if they had been forced to vote previously, but systems would need to be designed to accommodate this.

Accurate and Prompt Results

Promptness, and particularly accuracy, of results are crucial to the voting process. Schwartz and Grice stress the importance of making sure sufficient time is allowed for electronic votes to be cast (and if necessary, recast) and for election regulators to respond to technical difficulties.[67] Furthermore, it is important that individuals have faith that the voting system will accurately record their vote. Schwartz and Grice suggest that individuals trust paper ballots due to their track record over the extensive period of time during which they have been in use.[68] This theory is corroborated by Smith, who found that voters feel most confident in the accuracy of paper-based voting systems, and least confident in mobile-phone-based voting systems.[69] According to Blockchain Technologies Corp. CEO Nick Spanos, currently paper ballots are the only truly accurate methods for counting elections, since in that case the actual, physically marked ballots are available, whereas if the validity of election results calculated by a machine are called into question the only real option for determining whether there was an error is by looking at the software's source code.[70]

Unlike other methods of electronic vote calculation that utilize software to record and count the votes, the blockchain system does not rely primarily on specialized software to calculate votes, but instead counts each vote as a transaction that must be validated by a majority of network users. With a large number of people required to approve each block of transactions, erroneous transactions should be quickly weeded out, helping to ensure the validity of each vote. Furthermore, each blockchain transaction provides the sender with a receipt, allowing them to make sure that their vote has been sent to the particular candidate. Therefore, while blockchain technology does suffer from the slight stigma affecting electronic voting methods, it is likely

---

[67] Schwartz & Grice, *supra* note 52 at 8.

[68] *Ibid* at 18.

[69] Rodney Smith, "Confidence in paper-based and electronic voting channels: evidence from Australia" (2016) 51:1 Austl J Political Science 68 at 68 [Smith].

[70] "Paper Ballots Are the Only Secure Way to Run an Election says Blockchain Technologies Corp., Developers of Cutting Edge Blockchain Voting System/Machine", *ICT Monitor Worldwide* (6 September 2016), online: <http://www.prweb.com/releases/2016/09/prweb13658526.htm>.

better equipped than many systems to provide voters with perceptions of accuracy and peace of mind.

Promptness may be another issue with blockchain technology. Since each block takes about ten minutes to update, and there are a finite number of transactions in a block, it may take an extended period of time to confirm whether someone's vote has been received. While this is less likely to be a problem for individuals voting at home or at work (assuming the transaction succeeds), if an individual travels to a polling station because they do not have internet capabilities at their home they may be required to wait for confirmation that their vote has been processed. While not ideal, the use of electronic calculation may mean that votes will be recorded and counted much more quickly than they would be if they had been processed by hand.

Comprehensible and Transparent Processes

Schwartz and Grice emphasize the point that "transparency is directly related to the amount of information that is available to the public, as well as to intermediaries."[71] Ironically, while one of the key aspects of blockchain technology is that it is nearly completely transparent, its origin is shrouded in secrecy. The seminal paper creating bitcoin and blockchain technology, "Bitcoin: A Peer-to-Peer Electronic Cash System"[72] was written under the pseudonym Satoshi Nakamoto; at this point, the paper's original author has yet to be confirmed. Previously, this paper discussed Schwartz and Grice's observation that not only do people have to know how to use an electronic voting system, but they also need to believe that the system will accurately and efficiently record their votes.[73] Whether or not the level of uncertainty surrounding the origin of blockchain technology will diminish voter faith in the blockchain system as a potential electronic voting method remains to be seen. While it is possible that the secrecy may present warning signs to some (both individuals with low-level computer skills who cannot bring themselves to believe in a system whose origin cannot be traced to a certain individual, and those tech-savvy individuals who see blockchain technology as a

[71] Schwartz & Grice, *supra* note 52 at 41.

[72] Nakamoto, *supra* note 5.

[73] "Even though one can look at technological attempts to minimize the risks associated with Internet voting, it is crucial to recognize that it is not sufficient to render the voting system intrinsically trustworthy. The system must in practice be trusted by the Canadian public, and not only by a particular group of government bureaucrats or information technology specialists who work on the project." Schwartz & Grice, *supra* note 52 at 18.

potentially risky system to base the election on), others may be satisfied simply knowing how the system works and how to use it, albeit with computer-literate people wanting additional details on the process.

Despite the technology's secretive origins, blockchain technology is itself extremely transparent in that it relies on a public ledger of all transactions made on the system where anyone – including election officials, technical analysts, or the average voter – can view which transactions have gone through. However, just because the data is available does not mean that it is of any utility. The blockchain method of transferring bitcoins is a relatively new concept. Its multi-layered complexity may stymie the average observer from making use of the data, and the idea that people's votes would be publically viewable by anyone in the world and would be protected by the 'magic' of the blockchain system may be difficult to justify to individuals who are not technologically savvy. That being said, this can be remedied by hiring individuals familiar with blockchain technology to check the data and report on trends that Canadians would like to know about. Information about the system should be made public, but in its simplest terms, voters would simply need to know how their vote was being kept secure, and how to actually use the system to vote.[74] Of the various barriers to implementation that legislators would need to overcome, public faith in (and comprehension of) the system is not insignificant, but it is also not insurmountable.

System Security and Risk Assessment

System security is one of the primary concerns with any form of electronic voting, but blockchain technology is unique in that its security comes through its transparency. While other countries have restricted access to their program source codes or made only certain parts of their source code available to public scrutiny,[75] nothing would be withheld on the blockchain system except the identities of voters, which would be coded by private keys. In a typical transaction a new private key would be generated by an individual's wallet for each new transaction; since Elections Canada would need to verify that the person voting is eligible to do so, an alternative method of generating a private key may need to be used. For example, in Estonia, keys are stored in a "tamper-resistant hardware security module" and can only be accessed via a

[74] *Ibid* at 44.
[75] Schwartz & Grice, *supra* note 52 at 47.

password from a quorum of the National Electoral Committee.[76] Alternatively, allowing a random private key to be generated and then using the receipt of the vote as confirmation could suffice, though this may cause issues with knowing which votes to disregard if multiple votes are allowed.

A major security concern is the ability to keep the identities of voters private while still making sure they are eligible to vote. While one study claims to have been able to show that user's profiles can be discerned under certain conditions, the study relied on 2011 statistics that estimated the number of bitcoin users to be around 60,000[77] and that the user seeking to identify transaction makers had access to certain location-specific information.[78] Since the number of bitcoin users has grown exponentially to over 10.1 million users as of November 25th, 2016,[79] it is likely to be considerably more difficult to discern the locations of users, particularly if users across the country are able to vote at their convenience over a period of time.

The blockchain system's transparency relative to other systems also has other advantages, though admittedly the level of transparency demanded by the blockchain system raises other questions about how to keep voting tallies private until votes can be verified and counted. The fact that the system's data is publically available would allow anyone with familiarity with the system to monitor transactions and report errors to Elections Canada. Even if an individual with less-than-honest intentions was to attempt to exploit vulnerabilities in the system, the system would be significantly resistant to hacking due to the computational difficulty of being able to rewrite blocks with enough speed to update the blockchain across all of the computers in the network. Should an attacker attempt to override the system, he or she would be limited to "undoing" their vote, rather than being able to cancel, make, or "steal" other votes. Given that security and transparency are two important characteristics of an electronic voting system, the fact that the

---

[76] Sven Heiberg, Peeter Laud & Jan Willemson, "The Application of I-voting for Estonian Parliamentary Elections of 2011" E-Voting and Identity: Lecture Notes in Computer Science 208 (SpringerLink, 2011), s 2.2, online: <http://research.cyber.ee/~jan/publ/evote2011.pdf>.

[77] Elli Androulaki et al, "Evaluating User Privacy in Bitcoin" (Paper delivered at the International Conference on Financial Cryptography and Data Security, 1-5 April 2013) [unpublished], s 4.1.

[78] *Ibid*, s 3.1.

[79] The number of blockchain users can be estimated by the number of blockchain wallets being used, since while users may have more than one wallet, they must have at least one wallet to utilize the system. See "Blockchain Wallet Users" (Graph), online: <https://blockchain.info/charts/my-wallet-n-users>.

blockchain system is secure *because of* its transparency could make it a strong choice as a non-proprietary electronic voting system.

Detection of Problems and Remedial Contingencies

One issue that might arise from the use of bitcoins for voting is if a voting transaction becomes "stuck" in transfer. Because bitcoin miners choose which transactions they process, transactions with higher transaction fees are more likely to get processed quickly, while transactions with lower fees assigned will be processed more slowly, or not at all. This is because transactions without fees are often considered "spam" transactions that will not be approved and added to the blockchain.[80] So long as a transaction fee of at least one satoshi per byte (0.00000001 BTC) is applied, a transaction should go through, though if the transaction fee is lower it may take longer for votes to be registered. Additionally, there is the issue of transaction fees. If a truly immutable blockchain is desired, it should be built on a public blockchain that requires a fee to use – a fee that would need to be borne by the Government of Canada. If the government was to foot the bill for casting bitcoin votes on a public blockchain, questions still arise as to how to distribute the funds required.

Since the registration of votes is of paramount importance, an e-voting system should allow voters themselves to confirm whether their vote has been registered. Should it be decided that voter receipts are a good idea, the provision of such receipts could be done through a bitcoin wallet app (which people would need in order to vote anyway) or through other means – Norway has created a notification system that allows people to verify their votes through verification codes transmitted via text message.[81] This potential delay is also a compelling reason to follow Schwartz and Grice's suggestion of having a week-long voting period that ends prior to the last day of ballot casting. Allowing a buffer period will ensure that votes that get stuck will have extra time to go through, increasing the probability that all votes cast electronically will be counted. Furthermore, if multiple votes were allowed as

[80] Ruben de Vries & Thomas Kerin, "All You Need to Know: Transaction Fees", *BTC.com*, online: <https://blog.btc.com/why-do-we-need-to-pay-transaction-fees-and-what-is-the-right-fee-fcf6ee17c072>; see also *BitcoinWiki*, "Transaction fees", online: <https://en.bitcoin.it/wiki/Transaction_fees> (accessed on 1 May 2017).

[81] Schwartz & Grice, *supra* note 52 at 57-58.

they are in Estonia, having a buffer period of several days before election day would allow officials to reconcile multiple votes.[82]

In terms of remedial contingencies, Schwartz and Grice state that electronic voting should work at most in tandem with physical ballot-casting methods, and non-electronic voting options should be available at all times.[83] Given the permanent nature of blockchain-based transactions, strategies for reconciling multiple votes could be necessary in order to mitigate the risk of failed voting transactions, with the added benefit of reducing the risk of vote coercion. If people can attempt to vote both online and in person, as in Estonia,[84] permitting multiple votes would allow those who attempt to vote online unsuccessfully to still register a vote through traditional voting means. This may require adding a level of electronic oversight to traditional voting methods to determine which vote of many made by an individual is the most recent (i.e. if the latest vote is the only one counted, we must be able to determine which was the latest vote cast). However, given the permanent nature of blockchain transactions the addition of the electronic component may be necessary to mitigate the risk of failed votes by allowing multiple voting opportunities.

Effective and Independent Oversight

One issue that arises is the lack of oversight that necessarily comes with people using internet voting. While the government can create and put out apps to facilitate electronic voting and ensure that everyone is operating on the same base software (e.g. the government could create a bitcoin wallet app specifically for voting), the reality is that unless everyone's personal machine is inspected and secured, there will necessarily be less oversight of the voting process and equipment in an uncontrolled voting environment than in the traditional system where everyone votes in a controlled setting.[85] In order to mitigate risks associated with unobserved voting (such as coercion or the use of malware on voters' devices to interfere with the voting process), Schwartz and Grice recommend stringent testing of the system before voting and auditing afterwards, and suggest that instead of running e-voting as similarly

[82] *Ibid* at 40.
[83] *Ibid.*
[84] *Ibid.*
[85] Schwartz & Grice, *supra* note 52 at 18.

as possible, that special oversight rules be created to reduce risks specifically associated with voting by electronic means.[86]

In addition to testing and retesting the technology itself, Schwartz and Grice suggest that a board comprised of members with "technical expertise, independence, reliability and multiparty support" be created in order to oversee the implementation of electronic voting.[87] Given the complexity of the blockchain system, it would be wise to assign a board to direct implementation and oversight of the system.[88] Doing so would ideally "help address concerns that may arise from the novelty and technological complexity of conducting an election partly by Internet".[89] Appointing a board supported by various political parties, members of the judiciary, and experts on the use of blockchain technology would also greatly assist in building Canadians' trust of the internet voting system, which Pieters and Becker say is necessary if online voting methods are to be adopted.[90] It will also ensure that the system as a whole is scrutinized for inconsistencies, errors, and compliance with current election practices and legislation, and make sure that parts of the system do not get overlooked. Since peoples' levels of confidence in electronic voting systems still fall behind their confidence levels in paper-ballot-based voting,[91] having a diverse board is particularly necessary in order to reduce the impression of overreliance on technicians and programmers caused by the complexity of the system, thereby lending the system greater credibility as an alternative voting method.

Cost Justification and Efficiency

The final major factor that would require consideration before implementing a blockchain-based electronic voting system is the overall cost of implementing the system. The type of equipment used in electronic voting greatly impacts the cost to run such a program, and will vary widely depending on whether the program and equipment is run in a controlled or

---

[86] *Ibid* at 62, 65.
[87] *Ibid* at 66.
[88] *Ibid.*
[89] *Ibid.*
[90] Wolter Pieters & MJ Becker, "Ethics of E-Voting: An Essay on Requirements and Values in Internet Elections" Paper in Ethics of New Information Technology: Proceedings of the Sixth International Conference of Computer Ethics CEPE2005 (Enschede, The Netherlands, 17-19 July 2005) at 3, online: <eprints.eemcs.utwente.nl/13894/>.
[91] Smith, *supra* note 69 at 68, 80-81.

uncontrolled voting environment. In a controlled voting environment, all of the machines people use are provided to voters. Before, during, and after the election the machines need to be stored and maintained, adding these costs to the cost incurred when machines were initially acquired. Different machines have different costs related to their upkeep and how they interact with the voting system; for example, depending on what kind and how many machines the e-voting system uses, costs could vary wildly.[92] Further, because the blockchain system requires transactions to be uploaded and disseminated via the internet, taxpayer dollars would also need to be put towards setting up Wi-Fi or mobile hotspots in areas where no internet exists. This would potentially necessitate the purchase or rental of routers and modems, as well as a deal with internet services providers to provide fast, reliable internet to polling sites. Furthermore, once the election ends this equipment would either need to be disposed of or stored and maintained, incurring continuous costs.[93]

In contrast, e-voting in an unsecured environment could cut down on equipment costs, since individuals would be able to use their personal internet-connected devices. While Elections Canada would have the option of developing a special voting app that would act as a bitcoin wallet for transacting votes, it would not be necessary for them to do so as long as they utilized a previously-established cryptocurrency that operated on an existing system (like bitcoins). The purchase, storage and maintenance may still be required; for example, accommodation may be required for individuals without access to internet-linked computers. Furthermore, if people were allowed to cast multiple votes (including at least one paper ballot) in order to mitigate the risk of coercion and votes not being registered in a timely manner, some electronic equipment would have to be purchased in order to keep track of which votes were cast when. Lastly, the implementation of an electronic voting system would require the hiring of various experts in blockchain technology, e-voting systems, computer maintenance, and electronic security. While these costs may decrease once the system is in place and less troubleshooting is needed, one cannot deny that personnel costs associated with developing and implementing an electronic system would likely be high. It is unclear whether the costs of implementing an e-voting system would be outweighed by its utility.

---

[92] SAVEOurVotes, "Cost Analysis of Maryland's Electronic Voting System" (2008), online: <saveourvotes.org/legislation/packet/08-costs-mdvotingsystem.pdf>.

[93] Schwartz & Grice, *supra* note 52 at 19.

Implementation

In brief, blockchain technology is a type of technology for facilitating electronic transactions that has the potential to be used as a platform for electronic voting in Canada. While the technology already exists and is theoretically useable by anyone with internet access, time and patience will be required in order to bring this technology to the point where it could be used elections on a wide-scale.

A major obstacle that would need to be overcome is the opacity of the system. Regardless of one's opinion on the propriety of using an unregulated currency transfer system created by an anonymous originator, the fact remains that the blockchain system of transfer is a fairly abstract concept and may be difficult to comprehend for the average voter. The question that needs to be asked is: do voters care how the system works? The answer for many may be "no", and so long as they are informed enough to use the system and understand that it is secure, that may be sufficient rationale for the majority of the electorate to get behind the technology. For those who want more information on the system and how it factors into the voting process, more information could be provided, particularly on a website or through pamphlets and other advertising. Additionally, telephone or webchat support resources could be created for people who still have questions. The main information to impress upon voters is how the system keeps votes confidential and what the electronic voting process looks like.

In addition to support available before voting, technical support must be available at the polls as well. Given the digital divide precluding some people from accessing the internet, Elections Canada may feel the need to provide Wi-Fi zones or even internet access points (computers connected to the internet) at polling stations for those individuals who wish to vote online but would not otherwise have internet access. Providing these kinds of resources (as well as resources to accommodate individuals who may be housebound or otherwise unable to go to the polls) will require purchase, maintenance, and storage of physical equipment (such as modems, wireless routers, and computer equipment), as well as the purchase of internet access from a local service provider sufficient to meet the demand of voters. Ideally the temporary strain of an election on the wireless network could be reduced by allowing internet voting over a period of time, somewhat like early polling stations provide now. Other electronic voters using personal devices should also be able to vote for a period of time from anywhere with internet access, both to make voting more convenient and to reduce the stress on provided internet connections. Of course, if Elections Canada decides that it cannot

justify the expense of outfitting polling stations with internet access, they could simply specify electronic voting may only be done at home or with one's own personal device, and all voting at the polls will be done with traditional paper ballots; however, this may run afoul of accessibility requirements.

Possibly the most important aspect of the voting system would be independent oversight. The entire process would have to be supervised by neutral people from varying political parties, academics, members of the judiciary who can interpret whether sufficient accommodations are being made and whether the voting process complies with current election guidelines, and, in this case, individuals familiar and comfortable enough with blockchain technology to monitor the system and troubleshoot technical issues. This oversight board would likely be assembled by a committee dedicated to its creation, in order to ensure a balanced representation of all interests. Further, the board would likely be involved in all aspects of the process to bring blockchain voting to Canadian elections, from alpha and beta testing of the system, to use of the chosen technology in an election, troubleshooting, and reviewing both voting data and results (in an ongoing process throughout the election) as well as the operation (and efficiencies and inefficiencies) of the system itself. The board would also have to analyze issues and present potential solutions for the next election; as such, it may be an idea to have board terms overlap, so that each member sees at least two elections and can compare the results of and improve upon the processes used during each. If the public feels that it can trust the oversight board, ideally they will also develop confidence in the voting system the board represents.

Lastly, and perhaps most obviously, there are considerable technical considerations that will need to be addressed in order to introduce blockchain-based voting as a viable voting option. These considerations may include the development and testing of new or existing wallet apps, testing of various data encryptions methods, determining whether to allow individuals to vote in uncontrolled environments and, if so, how to maximise their voter security and minimize the potential for coercion. Testing will need to be done to determine whether individuals who already have bitcoin accounts can use their current wallet apps, whether it is possible to allow individuals multiple votes despite blockchain transactions being irreversible, and whether current theoretical models of blockchain voting systems could actually be put into

practice.[94] In short, the main implementation obstacles are likely to be public confidence (in the system and the oversight board), technical issues pertaining to the use and development of the voting technology itself, and the purchase, maintenance and storage of equipment.

Conclusion

This paper has described an electronic voting system that operates on the blockchain. Essentially, in order to adopt such a system, voters would be registered to vote and would be assigned a random key pair. It is possible that speciality software would need to be used to ensure that voters are eligible to vote, since otherwise anyone with bitcoins could vote by sending small transactional amounts to the address affiliated with their desired candidates. In the end, votes will be visible and a tally will be computed. While the blockchain system has several advantages in terms of security and transparency, criticisms are warranted given the vital importance of the voting system in allowing Canadians to exercise their *Charter*-enshrined right to vote. Implementing an electronic voting system operating on blockchain technology will incur upfront and continuing costs, require independent oversight by a multi-disciplinary and multi-party board to ensure the system's integrity, and would likely require accommodation for voters who do not have access or knowledge of how to use electronic voting technology. Additionally, the system would have to run alongside the paper balloting system, and it is yet undetermined whether the utility and potential convenience of an electronic voting system would outweigh concerns about system security and the accuracy and promptness of results.

Nonetheless, if appropriately applied, blockchain technology would be an excellent method of transmitting vote information, as it is specifically designed to maintain transaction anonymity and fairness. Its two main advantages are its ability to entirely anonymize and protect voter identities, and the fact that it is relatively tamper-proof with strong inherent safeguards in place to prevent hacking and interference by individuals with less-than-honourable intentions. While blockchain technology remains a potential solution to many of the issues that arise in a centralized e-voting system, much consideration is still needed if Canada wants to take advantage of this decentralized transaction system as a possible avenue to electronic voting in the future.

---

[94] See e.g. Lee, *supra* note 34.