THE INTEGRITY OF ELECTIONS IN THE UNITED STATES: PROTECTING VOTERS FROM SUPPRESSION, TECHNOLOGY, AND PANDEMICS

By Chelsey Gonzalez

TABLE OF CONTENTS

I.   INTRODUCTION

Voter protections have been a basic tenet of society since the Fifteenth Amendment was ratified in 1870.[1] For close to one and a half centuries, United States ("U.S.") citizens have lined up at voting booths to vote.[2] Congress believed voting was so important it created the Fifteenth Amendment to protect voting rights.[3] Along with and following the passage of the Fifteenth Amendment, Congress further created multiple Constitutional amendments to grant voting rights to persons of all races and genders.[4] Yet, voters still face many challenges when they arrive at voting booths to participate in one of the most important elections in the United States: the election to determine who will become President of the United States.[5]

Every four years, citizens across the U.S. generally take part in two important elections: state primary or state caucus and the general election for President of the United States.[6] To vote in both elections, citizens must ensure they are registered to vote, and, if they are registered to vote, they must confirm their registration is valid.[7] In certain states, these registration requirements include voter identification laws.[8] These voter identification laws require voters to provide their state government identification with an additional form of identification before they are able to either register to vote, obtain a ballot, or vote in an election.[9] Voter identification laws were formed to supposedly reduce electoral fraud.[10] However, voter identification laws have created more of a barrier to vote than a protection against voter fraud.[11]

---

[1] *See* U.S. CONST. amend. XV, § 2.

[2] *See* U.S. CONST. amend. XV.

[3] *See id.* § 2.

[4] *See* U.S. CONST. amends. XIV, XIX.

[5] *See* Grace Panetta et al., *The Nineteenth Amendment Passed 100 Years Ago Today. The Evolution of American Voting Rights in 244 Years Shows How Far We've Come—And How Far We Still Have To Go*, BUSINESS INSIDER (Aug. 18, 2020), https://www.businessinsider.com/when-women-got-the-right-to-vote-american-voting-rights-timeline-2018-10#what-voting-rights-issues-remain-today-16.

[6] *See Presidential Election Process*, USA.GOV, https://www.usa.gov/election (last updated Jan. 21, 2021).

[7] *See Voter Registration*, USA.GOV, https://www.usa.gov/voter-registration (last visited Feb. 11, 2021).

[8] *Voter Identification Requirements: Voter ID Laws*, NAT'L CONF. OF STATE LEGISLATURES. (Aug. 25, 2020), https://www.ncsl.org/research/elections-and-campaigns/voter-id.aspx.

[9] *Id.*

[10] *See id.*

[11] *See Oppose Voter ID Legislation – Fact Sheet*, ACLU, https://www.aclu.org/other/oppose-voter-id-legislation-fact-sheet (last visited Feb. 11, 2021).

Coupled with these concerns over electoral fraud are concerns over voter accessibility.[12] To remedy voter obstruction and access, the Federal government created multiple laws that seek to protect voters from all walks of life.[13] These laws have ensured that voters located in the U.S. and overseas have the right to vote in, at the very least, federal elections.[14] In these cases, voters are offered the option of voting by mail or online.[15] Still, voter suppression and accessibility are challenges federal and state governments presently face.[16]

Additionally, anxiety about technical glitches and hackers for those who vote digitally has created doubt in the ability of the U.S. to keep voter information protected and the overall reliability of voter results ensured.[17] These insecurities have prompted our nation to research new avenues to ensure every U.S. citizen can vote through a reliable polling system.[18] Despite the voting pilot programs the U.S. has implemented, there have been no lasting solutions adopted by the federal government to combat voter suppression, accessibility, and reliability.[19]

Notwithstanding the United States' challenges in protecting its voters, both domestic and foreign governments have found success in making voting accessible to all voters through blockchain voting.[20] Blockchain voting is an online voting system that utilizes blockchain to protect data.[21] State governments have used blockchain technology to facilitate voting for persons who would not otherwise have been able to vote.[22] Foreign

---

[12] *See* H.R. Res. 3295, 107th Cong. (2002) (enacted).

[13] *See* 52 U.S.C.A. § 10301.

[14] *See id*.; Nat'l Defense Authorization Act of 2010, Pub. L. 111-84, 123 Stat. 2321 (2009).

[15] Nat'l Defense Authorization Act of 2010, Pub. L. 111-84, 123 Stat. 2321 (2009).

[16] *See* Rebecca Ayala, *Voting Problems 2018*, BRENNAN CENTER FOR JUSTICE (Nov. 5, 2018), https://www.brennancenter.org/our-work/analysis-opinion/voting-problems-2018.

[17] *See* Maura Barrett & Ben Popken, *How the Iowa Caucuses Fell Apart and Tarnished the Vote*, NBCNEWS (Feb. 21, 2020), https://www.nbcnews.com/politics/2020-election/how-iowa-caucuses-fell-apart-tarnished-vote-n1140346; CNN Editorial Research, *2016 Presidential Campaign Hacking Fast Facts*, CNN (Oct. 31, 2019), https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

[18] *See* Nat'l Defense Authorization Act of 2010, Pub. L. 111-84, 123 Stat. 2321§ 579 (2009) .

[19] *See* Susan Greenhalgh et al., *Email and Internet Voting: The Overlooked Threat to Election Security*, ACM (Oct. 9, 2018), https://www.acm.org/binaries/content/assets/public-policy/jtreportemailinternetvoting.pdf.

[20] Reuben Yap, *The Promise and Reality of Blockchain's Role in Global Elections*, COINTELEGRAPH (Mar. 20, 2020), https://cointelegraph.com/news/the-promise-and-reality-of-blockchains-role-in-global-elections; Lucas Mearian, *Utah County Moves to Expand Mobile Voting Through Blockchain*, COMPUTERWORLD (Oct. 21, 2019), https://www.computerworld.com/article/3446836/utah-county-moves-to-expand-mobile-voting-through-blockchain.html.

[21] *See* Mike Orcutt, *Why Security Experts Hate that "Blockchain Voting" Will be Used in Midterm Elections*, M.I.T. TECH. REV. (Aug. 9, 2018), https://www.technologyreview.com/2018/08/09/2425/why-security-experts-hate-that-blockchain-voting-will-be-used-in-the-midterm-elections/.

[22] Mearian, *supra* note 20.

governments have begun integrating blockchain voting into their system of governance.[23] However, insecurities still hang over our legislators as to whether blockchain voting can be trusted.[24] This Article proposes that the U.S. should pass new laws that adopt blockchain voting. Specifically, the U.S. should, subject to certain rules, allow both federal and state governments to allow online voting through blockchain voting on platforms that are reputable, stable, and tested.

Part I of this Article will provide a history of selected issues with voting the United States has faced. Part II will discuss voting laws implemented by Congress to improve voter accessibility and the manner in which new legislation can be drafted to address modern voting concerns. Part III will explain blockchain and the different types of blockchain networks, and it will also examine governments that have either partially, or fully, integrated blockchain voting into their government operations. Part IV will address possible counterarguments to implementing blockchain voting into governance. Part V of the Article is a conclusion restating the reasons why the United States should fully integrate blockchain to implement a technology that fully secures data and data transference.

I.   UTILIZING BLOCKCHAIN FOR VOTER ACCESSIBILITY

On October 31, 2008, an unknown person using the alias Satoshi Nakamoto[25] published a "White Paper" titled "Bitcoin – A Peer-to-Peer Electronic Cash System."[26] The paper suggests creating a system of online payments that would do away with financial institutions all together.[27] Nakamoto's overall goal was to create an electronic system that would allow a person to transfer money to another person, thereby creating a peer-to-peer system of transaction.[28] This electronic currency system became known as cryptocurrency.[29]

Cryptocurrencies are internet-based currencies in which ownership is confirmed using cryptography.[30] These virtual coins have a chain of digital signatures which allow owners to "transfer[] coins 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."[31] Thus,

---

[23] Yap, *supra* note 20.

[24] Greenhalgh, *supra* note 19.

[25] It is unclear whether Satoshi Nakamoto is a group of people or one person.

[26] Satoshi Nakamoto, *Bitcoin: A Peer-To-Peer Electronic Cash System*, BITCOIN, 1 (2008), https://bitcoin.org/bitcoin.pdf.

[27] *Id.*

[28] *Id.*

[29] *Frequently Asked Questions*, BITCOIN, https://bitcoin.org/en/faq (last visited Feb. 11, 2021).

[30] *See id.*; Nakamoto, *supra* note 26.

[31] Nakamoto, *supra* note 26, at 2 (This is the bitcoin blockchain. The electronic currency creates a chain that can be verified due to the chain of ownership.).

Nakamoto utilized two technologies: the cryptocurrency, Bitcoin, and the distributed ledger technology,[32] blockchain.[33] While blockchain is primarily known through Bitcoin, it is the way Blockchain functions to protect user information that makes the technology so revolutionary.[34]

A. HOW BLOCKCHAIN WORKS

Nakamoto explained the manner in which Blockchain can be utilized to facilitate the transactions of virtual currencies.[35] Nakamoto first created a timestamp server by "taking a hash of a block of items" and coding it to include previous timestamps and subsequent timestamps, thereby creating a chain.[36] Nakamoto then created a "proof-of-work system," which works to place a value on a hash and gives the hash[37] the required zero bits to satisfy the proof-of-work.[38] Once the proof-of-work is satisfied, it becomes difficult to tamper with the block without redoing the work.[39] This process is repeated with each hash; thus, the more transactions that occur on a block, the longer the chain becomes.[40] To change the transaction history, each block that exists after the block the person seeks to change must be recoded, and then that person would have to surpass any new work the honest nodes have done.[41]

Additionally, because nodes consider the correct chain to be the longest chain, if two versions of a block are created simultaneously, nodes will attach to the first one it receives.[42] However, nodes will switch to the longest branch after the next proof-of-work is created.[43] Due to the ability to create multiple blocks, there is a possibility a hacker might attempt to create a chain to trick the nodes into attaching to the false chain, instead of the honest chain.[44] Nakamoto, accounting for this possibility, coded the nodes to deny accepting invalid transactions from blocks or to deny blocks containing invalid

---

[32] *See* Sue Troy, *Distributed Ledger Technology (DLT)*, TECHTARGET, https://searchcio.techtarget.com/definition/distributed-ledger (last visited Feb. 17, 2020) (Distributed ledger technology ("DLT") is a "digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time." DLT does not have central data storage or administration functionality.).

[33] *See* Nakamoto, *supra* note 26.

[34] *See* BITCOIN, *supra* note 29.

[35] *See* Nakamoto, *supra* note 26, at 2.

[36] *Id.*

[37] "A hash is a function that converts an input of letters and numbers into an encrypted output of a fixed length." Jake Frankenfield, *Hash*, INVESTOPEDIA (June 30, 2020), https://www.investopedia.com/terms/h/hash.asp.

[38] Nakamoto, *supra* note 26, at 3.

[39] *Id.*

[40] *See id.*

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] *Id.*

transactions all together.[45]

Thus, the only way a person can hack into a chain would be to hack into their own chain.[46] However, even this presents challenges for a hacker. During a transaction, the transaction's receiver generates a public and private key.[47] The public key is shared between the sender and the receiver of the transaction, while the private key remains with the receiver, not the sender, of the transaction.[48] Because the sender no longer has the private key, the sender cannot prepare "a chain of blocks ahead of time," but must wait until the transaction sends to begin altering the chain.[49]

Nakamoto also created a solution to possible problems with disk space by discarding spent transactions.[50] These transactions are discarded and "hashed in a Merkle Tree."[51] The Merkle Tree saves the data onto one hash so that the data may still be accessed, while at the same time taking up less space.[52]

Nakamoto's overall goal of making a peer-to-peer, unregulated electronic exchange was successful.[53] Nakamoto created a technology that supported the transfer of valuable information, without the burden of dealing with constant attacks on security.[54]

B. PUBLIC AND PRIVATE BLOCKCHAIN NETWORKS

Blockchain utilizes two different networks for users: a private blockchain and a public blockchain.[55] The two blockchain networks refer to a person's ability to write, read, or participate on the blockchain or the blockchains ledger.[56] A blockchain can be "public and open, public and closed, private and open, or private and closed, which can determine how the publics access to the blockchain is limited.[57]

Although public blockchains operate with an administrative governance structure,

---

[45] *Id.* at 6.

[46] *Id.*

[47] *See id.* at 7.

[48] *See id.*

[49] *Id.*

[50] *Id.*

[51] *Id.* "Merkle Trees summarize all transactions in a block by producing a digital fingerprint of the entire set of transactions." Shaan Ray, *Merkle Trees*, HACKERNOON (Dec. 14, 2017) https://hackernoon.com/merkle-trees-181cb4bc30b4 (It is created by hashing multiple nodes until there is only one hash leftover. This hash becomes the "root hash" or the "Merkle root.").

[52] *See* Ray, *supra* note 51.

[53] *See* BITCOIN, *supra* note 29.

[54] *Id.*

[55] *See* Jared R. Butcher et al., *Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues: Overview*, PRACTICAL LAW (2021) *available at* WestLaw Practical Law.

[56] Demiro Massessi, *Public vs. Private Blockchain in a Nutshell*, COINMONKS (Dec. 12, 2018), https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f.

[57] *Id.*

public blockchains do not have a central authority.[58] Since no single person controls a public blockchain, anyone can join public blockchain networks.[59] However, public blockchains are still considered secure because public blockchains do not allow data to be tampered with once it has been validated.[60] Due to public blockchains' accessibility, it presents many risks to business transactions.[61] Bitcoin, and other cryptocurrencies, are examples of the risks public blockchains pose.[62]

To combat security issues, public blockchains were made to rely on incentives to ensure "everybody in the system behaves honestly and according to the rules."[63] These incentives were first proposed by Nakomoto in proposing bitcoin's blockchain.[64] Nakomoto promised more bitcoin to users who mined bitcoin and added their transactions to blockchain.[65] The overall goal was to award honest participants economically and dissuade dishonest participants by threatening them economically taking away their ability to recoup any losses they may suffer while trying to hack the system.[66]

While public blockchains are permission-less networks, private blockchains are permissioned.[67] Thus, access to the blockchains ledger is limited to trusted parties who must use their "true verified identities."[68] Private blockchains are often equipped with identity management tools that allow users to plug in identity management solutions so organizations can determine what users are accessing its blockchain and determine what data each user may access on its blockchain.[69] Due to its permissions, private blockchains are used by organizations and businesses that want to collaborate "without exposing their transactions and business processes."[70]

Where public blockchains, such as bitcoin, use consensus mechanisms[71] such as a proof-of work, private blockchains use less complicated consensus mechanisms, such as

---

[58] Butcher, *supra* note 55.

[59] Massessi, *supra* note 56.

[60] *Id.*

[61] Butcher, *supra* note 55.

[62] *Id.*

[63] Massessi, *supra* note 56.

[64] *See* Nakomoto, *supra* note 26, at 6.

[65] *See id.*

[66] Massessi, *supra* note 56.

[67] Butcher, *supra* note 55.

[68] *Id.*

[69] Massessi, *supra* note 56.

[70] Butcher, *supra* note 55.

[71] A consensus mechanism is a "fault-tolerant mechanism" used by blockchain systems to achieve "the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems." Jake Frankenfield, *Consensus Mechanism*, INVESTOPEDIA (July 29, 2020), https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp.

a "proof-of-authority, which verifies a node's identity."[72] Thus, instead of nodes solving difficult mathematical problems within the proof-of-work framework, the nodes use a set of authorities that allow the nodes to create new blocks and secure the blockchain.[73]

Blockchain voting companies, such as Voatz, use permissioned blockchain on its blockchain voting systems.[74] Voatz authenticates voters through its permissioned blockchain before it allows voters to cast their ballot.[75] Voatz chose permissioned blockchain because permissioned blockchain "emulates" United States elections and decreases the chances of hackers disguising themselves as verifiers.[76] Permissioned blockchain allows administrators to "increase the number of nodes and designate which organizations . . . can participate in the blockchain network as verifiers."[77] Administrators create elections and decide when the election begins and ends, configure ballots, and register voters.[78] Voters can cast their ballots and verify their votes through blockchain voting.[79] Thus, blockchain voting on permissioned networks gives both administrators and voters a way to confirm the voting system is yielding safe and accurate results.[80]

C. GOVERNMENT MODELS FOR BLOCKCHAIN VOTING

Digital democracies are not a revolutionary discovery.[81] A digital democracy was utilized to create new regulations in Taiwan.[82] While blockchain voting is a different type of digital democracy than what governments are accustomed to, implementing a blockchain voting system has proven itself successful.[83] Presidential candidate Andrew Yang campaigned to integrate blockchain voting during his run in the 2020 democratic primary.[84] Multiple governments, both domestically and internationally, have either utilized blockchain voting for elections or began implementing plans to integrate

---

[72] Butcher, *supra* note 55.

[73] *See* Anastasiia Lastovetska, *Blockchain Architecture Basics: Components, Structure, Benefits & Creation*, MLSDev (Jan. 5, 2021), https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture.

[74] Denise Tambanis, *Blockchain Applications: Election Voting*, BLOCKCHAIN PHILANTHROPY FOUND. (Feb. 5, 2019), https://medium.com/bpfoundation/blockchain-applications-election-voting-a1436e7d10cb.

[75] *See id*.

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] *See id*.

[81] *See* Chris Horton, *The Simple but Ingenious System Taiwan Uses to Crowdsource its Laws*, M.I.T. TECH. REV. (Aug. 21, 2018), https://www.technologyreview.com/s/611816/the-simple-but-ingenious-system-taiwan-uses-to-crowdsource-its-laws/.

[82] *Id.*

[83] *See* Larry Moore & Nimit Sawhney, *Under the Hood: The West Virginia Mobile Voting Pilot*, VOATZ (Feb. 11, 2019), https://sos.wv.gov/FormSearch/Elections/Informational/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf.

[84] *See Modernize Voting*, YANG 2020, https://www.yang2020.com/policies/modernize-voting/ (last visited Jan. 26, 2021).

blockchain voting into its voting system.[85]

For example, in 1998, Utah created a state Uniformed and Overseas Citizens Absentee Voting Act ("UOCAVA"), section 20A-6-103, which allowed persons with disabilities, military, military spouses and dependents, and overseas voters, to vote electronically.[86] Utah has since developed an app using blockchain-based technology to allow disabled voters who meet UOCAVA's requirements to cast ballots via their smartphones.[87] Utah partnered with Tusk Philanthropies to create the app.[88] The app relied on permissioned blockchain and required voters to scan their identification, take a portrait, and then scan their fingerprint to tie a smart device to a specific voter.[89]

In its November 2018 primary elections, the Thailand Democratic Party used blockchain technology to nominate its party leader.[90] More than 120,000 citizens voted in the primary.[91] Voters who used the blockchain voting app submitted photo identifications to verify their identities.[92] The voting app itself encrypted and stored the voting data on the InterPlanetary File System, which stored its hashes on the Zcoin blockchain.[93] Multiple private keys were required to access the voting data to ensure security.[94] Once the election was completed, only five people were needed to decrypt the voting data and obtain the results.[95]

India's Chief Election Commissioner ("The Commissioner"), Sunil Arora, is seeking to implement blockchain voting to increase voting accessibility to those voters who cannot physically reach a voting both on election day or who are not physically present where they are registered to vote.[96] The developing blockchain system is being formatted

---

[85] *See* Lucas Mearian, *Utah County Moves to Expand Mobile Voting Through Blockchain*, COMPUTERWORLD (Oct. 21, 2019), https://www.computerworld.com/article/3446836/utah-county-moves-to-expand-mobile-voting-through-blockchain.html; TNN, *Working on Tech Solution for 'Lost Votes', Says CEC*, TIMES OF INDIA (Feb. 13, 2020), https://timesofindia.indiatimes.com/india/working-on-tech-solution-for-lost-votes-says-cec/articleshow/74109019.cms; Moore & Sawhney, *supra* note 83.

[86] UTAH CODE ANN. § 20A-6-103 (West 2018).

[87] Mearian, *supra* note 85.

[88] *Id.*

[89] *Id.*

[90] Bitcoin Magazine, *Thailand Uses Blockchain-Supported Electronic Voting System in Primaries*, NASDAQ (Nov. 13, 2018), https://www.nasdaq.com/articles/thailand-uses-blockchain-supported-electronic-voting-system-primaries-2018-11-13.

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] TNN, *Working on Tech Solution for 'Lost Votes', says CEC*, TIMES OF INDIA (Feb. 13, 2020), https://timesofindia.indiatimes.com/india/working-on-tech-solution-for-lost-votes-says-cec/articleshow/74109019.cms.

to allow citizens to vote from anywhere in the country.[97] The commissioner also plans to link voter identifications with an identification number, known as Aadhaar, to authenticate voters.[98]

The United States can analyze governmental models for blockchain voting systems that were implemented by domestic and international governments to determine the safest way to create a blockchain voting system. Blockchain's "true verified identity" can fulfill the identification requirements that voter identification laws require of its citizens without placing a heavy burden on voters,[99] while the ease of using an app would most likely increase voter turnout.[100]

II.   CHALLENGES TO THE IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY IN ELECTIONS

Despite the promise of blockchain voting, it has yet to be used on a large scale.[101] The elections which have utilized blockchain voting in the U.S. have only allowed a limited number of people to use the app to vote.[102] Thus, it is unclear how successful wide-scale implementation of blockchain voting would be without more research. However, research has found several issues that blockchain voting systems must address before it is rolled out across the United States.[103]

Voter fraud is one concern governmental officials hold.[104] While blockchain encryption is reliable, researchers found that blockchain encryption did not resolve all the security risks online voting encounters.[105] Blockchain does not protect ballots from malware that is already present on voters' computers.[106] Thus, attackers may "'rent'" malware-infected computers on the Black Market and manipulate ballots to modify votes.[107] Attackers may do this while presenting a false screen on the voter's computer to make the voter believe he or she is submitting a ballot reflecting their vote, when the voter is actually submitting the manipulated ballot.[108]

---

[97] *Id.*
[98] *See id.*
[99] *See* Voter ID Requirements, USA.GOV, https://www.usa.gov/voter-id (last visited Jan. 26, 2021).
[100] YANG 2020, *supra* note 84.
[101] *See* Moore, *supra* note 83.
[102] *Id.*
[103] *See* Greenhalgh, *supra* note 19.
[104] *Id.*
[105] *Id.* at 13.
[106] *Id.* at 10.
[107] *Id.*
[108] *Id.*

The U.S. intelligence community is also concerned over disruption attacks.[109] Disruption attacks are attacks that create distrust in the voting system.[110] Disruption attacks breach voting systems by either infecting the voting system with ransomware or deleting submitted votes altogether.[111] Because blockchain cannot mitigate every disruption attack, there is a fear that blockchain voting could further public distrust in the United States voting system.[112]

Government officials who regulate blockchain voting would also have to screen for collusion attacks.[113] Collusion attacks are attacks by the administrators of the blockchain voting system.[114] The concern over collusion attacks is that administrators of the blockchain voting system could rig the election in favor of a specific candidate.[115]

Despite the concerns over blockchain voting, blockchain voting does not present the new concerns about voting insecurities the U.S. currently faces with traditional voting systems.[116] During the 2016 elections, Russia attempted to access the United States voting systems.[117] While the Select Committee on Intelligence ("Select Committee") did not find evidence that the votes casted on voting machines were manipulated, the Select Committee found evidence of data exfiltration.[118]

Ultimately, the government will always need to protect voters from attackers who seek to effect U.S. elections. The real issue is finding equilibrium between creating a voting system that is accessible to all voters under all circumstances and ensuring that the voting system is secure. While concerns over voter system security are real, blockchain voting still presents a solution to voter accessibility that should be adopted once the government discovers a manner in which to harness blockchain technology.

III. PERVASIVENESS OF VOTER SUPPRESSION, TECHNOLOGICAL ISSUES, AND LIMITED ACCESSIBILITY

---

[109] *Id*. at 10.
[110] *Id*.
[111] *Id*.
[112] *Id*.
[113] *Id*. at 13.
[114] *Id*.
[115] *Id*.
[116] *Id*.
[117] David E. Sanger & Catie Edmondson, *Russia Targeted Election Systems In All 50 States, Report Finds*, N.Y. TIMES (July 25, 2019), https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html.
[118] S. REP. NO. 116-xx, at 3, 6 (2019).

The traditional voting system used in the United States has operated under multiple threats involving systemic suppression, technology issues, and accessibility issues.[119] As a result of these threats, voters across the United States are being negatively affected.[120] Although traditional voting allows voters who cannot attend in-person voting to cast absentee mail-in ballots, absentee voting does not address concerns over voter suppression.[121] Despite voting concerns, no measures to secure voter data and decrease voter suppression through blockchain voting have been codified.[122]

The following are three examples reflecting the manner in which voting systems in the United States have been harmful to voters.

A. ARIZONA VOTER SUPPRESSION

On March 22, 2016, voters in Maricopa County, Arizona, arrived at their polling places to place their votes in the state's Presidential primary election.[123] However, voters were soon hit with the realization that Maricopa County did not have the infrastructure to ensure every citizens vote was counted.[124] Maricopa County only had "one site per every 21,000 voters."[125] Due to Maricopa County's limited voting sites, voters were forced to cast their ballot after 11:00 p.m., some waiting more than four hours to exercise their democratic franchise.[126]

---

[119] *See* Anne Ryman, Rob O'Dell, & Ricardo Cano, *Arizona Primary: Maricopa County Had One Polling Site For Every 21,000 voters*, AZCENTRAL (Mar. 22, 2016), https://www.azcentral.com/story/news/politics/elections/2016/03/22/live-arizona-primary-coverage-presidential-preference-election/82096726/.

[120] *See* Kevin Freking, Colleen Long, & Nicholas Riccardi, *Democrats Want To Provide Mail-In Ballots Amid Covid-19. Republicans Don't*, CHICAGO TRIBUNE (Apr. 4, 2020), https://www.chicagotribune.com/election-2020/ct-coronavirus-mail-ballots-20200404-kdvbtbaexffnnhypukvzyy53km-story.html.

[121] *See* Danielle Root & Aadam Barkley, *Voter Suppression During the 2018 Midterm Elections*, AM. PROGRESS (Nov. 20, 2018), https://www.americanprogress.org/issues/democracy/reports/2018/11/20/461296/voter-suppression-2018-midterm-elections/.

[122] *See* Greenhalgh, *supra* note 19.

[123] Ryman, *supra* note 119; Dan Merica, Jeff Zeleny, & Adam Levy, *DNC, Iowa Democrats Point Fingers as Contract for Caucus App Revealed*, CNN (Feb. 14, 2020), https://www.cnn.com/2020/02/14/politics/iowa-democratic-party-shadow-contract-dnc/index.html; Nick Corsaniti & Stephanie Saul, *Ohio's Governor Postpones Primary as Healthy Emergency Is Declared Over Virus*, N.Y. TIMES (Mar. 16, 2020), https://www.nytimes.com/2020/03/16/us/politics/virus-primary-2020-ohio.html?te=1&nl=on-politics%20with%20lisa%20lerer&emc=edit_cn_20200317.

[124] Ryman, *supra* note 119.

[125] *Id.*

[126] *Id.*

Other voters faced challenges with being automatically removed from voter rolls.[127] A voter roll is a list of registered voters who are eligible to vote in an electoral district.[128] Voter rolls are typically purged to remove names of people who have moved out of the district, died, or have become ineligible to vote.[129] Despite these policies, Maricopa County's policy purges voters whose ballots have been returned undelivered, who do not update their registrations after two elections, and after the government has deemed the voter "inactive."[130] Maricopa County created the policy to prevent voter fraud.[131] However, Maricopa County has disproportionately purged more lower-income, minority households.[132]

After the 2016 Arizona primary, the Department of Justice ("DOJ") began investigating voter suppression in Arizona.[133] The DOJ investigated reports of voters being turned away at the polls because voters' party registrations were switched to another political party due to a computer glitch.[134] In *Democratic National Committee v. Hobbs*, the Ninth Circuit held that an Arizona voting policy constituted impermissible voter denial in violation of section 2 of the Voting Rights Act.[135] The Voting Rights Act prohibits procedures that discriminate against a specific class of people.[136] This ruling is significant given Maricopa County's history with a police force well-known for violating the Latino community's constitutional rights.[137] The ruling casts a hopeful light on the future of voter accessibility in Maricopa County.

B. THE DEBACLE OF THE IOWA DEMOCRATIC CAUCUSES IN 2020

---

[127] Dianna M. Nanez & Agnel Philip, *Maricopa County Residents Purged from Voter Rolls More than 1 Million Times in Past Decade*, AZCENTRAL (Nov. 4, 2018), https://www.azcentral.com/story/news/politics/elections/2018/11/04/minorities-poor-areas-most-affected-maricopa-county-voter-purges/1855248002/.

[128] *See Access To and Use Of Voter Registration Lists*, NAT'L CONF. OF STATE LEGISLATURES (Aug. 5, 2019), https://www.ncsl.org/research/elections-and-campaigns/access-to-and-use-of-voter-registration-lists.aspx.

[129] *See id.*

[130] Nanez & Philip, *supra* note 127.

[131] *See id.*

[132] *Id.*

[133] Eugene Scott, *DOJ Looking Into Voter Suppression Claims In Arizona*, CNN (Apr. 5, 2016), https://www.cnn.com/2016/04/05/politics/justice-department-investigation-arizona/index.html.

[134] *See* Samantha Lachman & Ryan J. Reilly, *The DOJ Is Investigating Arizona's Election Mess*, HUFFPOST (Apr. 5, 2016), https://www.huffpost.com/entry/justice-department-arizona_n_5702b720e4b083f5c6085933.

[135] Democratic Nat'l Comm. v. Hobbs, 948 F. 3d 989, 999 (2020).

[136] *See* 52 U.S.C. § 10101(a)(2).

[137] *See* Mihir Zaveri, *Joe Arpaio Says He Will Run Again For Maricopa County Sheriff*, N.Y. TIMES (Aug. 7, 2020), https://www.nytimes.com/2019/08/25/us/joe-arpaio-sheriff.html.

To fight voter suppression and make its caucus more accessible, Iowa Democrats used a mobile application ("app") to report presidential caucus results.[138] A caucus is a private event run by the political parties themselves, as opposed to being run by the state and local governments.[139] Iowa Democrats believed in using a reporting app to "modernize the process."[140] Thus, on February 3, 2020, the world tuned into the opening night of the Presidential race.[141]

The Iowa caucus is known to upstart the momentum for presidential campaigns, which stays with American voters until election season ends.[142] However, in 2020, the caucus failed to bring their typical momentum and instead became a nationally renowned meltdown.[143] The cause of this meltdown was a glitch in the Democratic National Committee ("DNC") mobile app created to report the caucus results.[144] The glitch made it impossible to "calculate and submit data from more than 1,700 Iowa caucus sites."[145] Iowa Democrats developed the app over the course of seven months; however, the DNC expressed doubt about the virtual caucus in August of 2019 due to security concerns.[146] Despite the DNC's doubts, Iowa Democrats moved forward with the app.[147] Iowa citizens were still awaiting final results from the Iowa caucus two weeks after the caucus took place.[148]

Ultimately, the app itself was found to be in working condition, and the issues were with the coding on the back end.[149] Two major blockchain voting startups, Voatz and Votem, confirmed the app utilized in the Iowa caucuses did not use a blockchain voting system.[150] The app also faced challenges with accessibility for voters who were not familiar with technology and had trouble accessing the app.[151] The app developers required users to download a "helper app and change advanced settings" to access the

---

[138] *See* Maura Barrett & Ben Popken, *How the Iowa Caucuses Fell Apart and Tarnished the Vote*, NBCNEWS (Feb. 21, 2020), https://www.nbcnews.com/politics/2020-election/how-iowa-caucuses-fell-apart-tarnished-vote-n1140346.

[139] *See What's The Difference Between "Caucus" vs. "Primary"?* DICTIONARY.COM, https://www.dictionary.com/e/caucus-vs-primary/ (last visited Jan. 27, 2021).

[140] Barrett & Popken, *supra* note 138.

[141] *See id.*

[142] *See* Rick Sobey, *Iowa Caucuses Will Give Candidates 'Momentum' for New Hampshire: Pollster*, BOS. HERALD (Feb. 3, 2020), https://www.bostonherald.com/2020/02/03/iowa-caucuses-will-give-candidates-momentum-for-new-hampshire-pollster/.

[143] *See* Merica, *supra* note 123.

[144] *See id.*

[145] *Id.*

[146] *See* Barrett & Popken, *supra* note 140.

[147] *Id.*

[148] *See id.*

[149] *Id.*

[150] *See* Helen Partz, *App Used In Iowa Caucus Isn't Mobile Voting, Blockchain Voting App Says*, COINTELEGRAPH (Feb. 5, 2020), https://cointelegraph.com/news/app-used-in-iowa-caucus-isnt-mobile-voting-blockchain-voting-app-says.

[151] *See* Barrett & Popken, *supra* note 123.

voting app because the app was not available in official app stores.[152] Additionally, the instructions voters received on the manner in which to download the app created challenges for voters who were unfamiliar with technology.[153]

Overall, the Iowa caucus furthered the doubt voters held about using technology to vote.[154] The end of the caucus left Iowa voters with no real winner due to inconsistent results.[155] The caucus fiasco even led the Iowa Democratic Party chairman to resign from his position due to the failures of the voting app.[156] In an email to Cointelegraph, the Chief Executive Officer ("CEO") of Votem stated while Blockchain could not have fixed the issues the app had, it could have identified the problem early on.[157] Logically, it follows that if the app had used blockchain, the caucus could have had a better outcome because the problems could have been identified and remedied earlier on.[158]

C. INTERNATIONAL PANDEMIC

In March of 2020, the United States was hit with an international pandemic that caused the President of the United States to shutdown borders to foreign countries and call a state of emergency.[159] The Centers for Disease Control and Prevention ("CDC") advised against events of more than 250 people and recommended keeping a distance of at least six feet from other people.[160] Due to the pandemic, many states postponed their 2020 Democratic Primary Elections to protect public health.[161] Ohio Governor Mike DeWine filed a lawsuit to delay elections until June 2, 2020 due to public health concerns.[162]

---

[152] *Id*.

[153] *Id*.

[154] *See id*.

[155] *See* Dareh Gregorian & Maura Barrett, *Iowa Democratic Party Chair Resigns After Caucus Fiasco*, NBCNEWS (Feb. 12, 2020), https://www.nbcnews.com/politics/2020-election/iowa-democratic-party-chair-resigns-after-caucus-fiasco-n1136126.

[156] *Id*.

[157] Partz, *supra* note 150.

[158] *See id*.

[159] Donald J. Trump, *Letter from President Donald J. Trump on Emergency Determination Under the Stafford Act*, WHITE HOUSE (Mar. 13, 2020), https://trumpwhitehouse.archives.gov/briefings-statements/letter-president-donald-j-trump-emergency-determination-stafford-act/.

[160] *Considerations for Events and Gatherings*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/coronavirus/2019-ncov/community/large-events/mass-gatherings-ready-for-covid-19.html?te=1&nl=on-politics%20with%20lisa%20lerer&emc=edit_cn_20200317 (last visited March 2020).

[161] Nick Corasaniti & Stephanie Saul, *16 States Have Postponed Primaries During the Pandemic. Here's a List.*, N.Y. TIMES (Aug. 10, 2020), https://www.nytimes.com/article/2020-campaign-primary-calendar-coronavirus.html?te=1&nl=on-politics%20with%20lisa%20lerer&emc=edit_cn_20200317.

[162] *See* Ben Axelrod, *Ohio Department Of Health Director Orders Polls Closed Due To 'Health Emergency'*, WKYC (Mar. 17, 2020), https://www.wkyc.com/article/news/health/coronavirus/gov-mike-dewine-to-file-lawsuit-to-delay-ohio-primary/95-d8688879-ec84-444a-944e-e94f087652a3.

However, Ohio state Judge, Richard Frye, denied the Ohio Governor's request to delay voting.[163]

State officials who decided to move forward with the primary election reasoned that counties had already received millions of ballots and forecasted huge voter turnout.[164] Florida's Governor, Ron DeSantis, voiced his belief that voting could still be done "in a way where you're not going to have crowds."[165] However, concerns over voter turnout mounted due to voters who did not have mail-in ballots choosing to stay indoors instead of driving to their polling place to cast their ballot and risk the possibility of contracting the respiratory virus.[166] Due to these concerns, several states researched alternative ways to conduct their voting processes to ensure voter turnout without putting public health at risk.[167] Three states determined the best way to ensure public health was to cancel in-person voting and only allow mail-in voting for state and local elections as well as the Democratic primaries.[168]

Following various states cancelling their elections, members of Congress discussed the manner in which they could make voting accessible to citizens during the pandemic.[169] The Speaker of the United States House of Representatives, Nancy Pelosi, suggested funding mail-in voting for all citizens so every voter would have a safe way to vote.[170] However, government leaders refused Pelosi's suggestion due to concerns over voter fraud and voting becoming too accessible to all U.S. citizens.[171] While Congress did not agree on a mandated mail-in election system for the 2020 elections, the economic aid package allocated $400 million to the Election Assistance Commission.[172] The commission provided grants to States during the 2020 election cycle.[173]

---

[163] Nick Corasaniti & Stephanie Saul, *Ohio's Governor Postpones Primary As Health Emergency Is Declared Over Virus*, N.Y. TIMES (Mar. 16, 2020), https://www.nytimes.com/2020/03/16/us/politics/virus-primary-2020-ohio.html?te=1&nl=on-politics%20with%20lisa%20lerer&emc=edit_cn_20200317.

[164] *Id.*

[165] *Id.*

[166] *See* Chicago Tribune Staff, *Illinois Primary Results: Marie Newman Ousts U.S. Rep. Dan Lipinski; Cook County State's Attorney Kim Foxx Survives*, CHICAGO TRIBUNE (Mar. 17, 2020), https://www.chicagotribune.com/election-2020/ct-illinois-primary-election-day-updates-20200317-gf5morm2gzbc5j3laniwpr5kx4-story.html.

[167] Corsaniti, *supra* note 163.

[168] Susan Cornwell, *Pelosi Wants 'Vote By Mail' Provisions In Next U.S. Coronavirus Bill*, REUTERS (Apr. 1, 2020), https://www.reuters.com/article/us-health-coronavirus-usa-vote/pelosi-wants-vote-by-mail-provisions-in-next-coronavirus-bill-idUSKBN21J6D0.

[169] *Id.*

[170] *Id.*

[171] Steve Benen, *Trump Says More Than He Should've About Voter Turnout, GOP Losses*, MSNBC (Mar. 31, 2020), https://www.msnbc.com/rachel-maddow-show/trump-says-more-he-should-ve-about-voter-turnout-gop-n1172881 (citing President Donald J. Trump as stating the aid package democrats proposed would increase voting to a point where Republicans would no longer become elected officials).

[172] Coronavirus Emergency Supplemental Appropriations Act, 2020., H.R. 6074, 116th Cong. (2020).

[173] *Id.*

Although Congress did not agree on a solution for U.S. voters, Congress debated voter accessibility for Congressional members.[174] Congressman Vicente Gonzalez suggested that Congress should establish a remote voting system and limit its use to Congress members only.[175] Gonzalez noted that the voting system would be similar to West Virginia's remote voting system, which is limited to service members of the Armed Forces.[176] Gonzalez sought to create the remote voting systems so Congress could continue voting on bills while protecting their health.[177]

Lastly, in a 5-4 decision, the United States Supreme Court granted an order requested by the Republican National Committee to stay a preliminary injunction safeguarding the availability of Wisconsin's absentee voting in its spring election.[178] The preliminary injunction extended the deadline for voters to request absentee ballots from April 2, 2020 to April 3, 2020 and allowed election officials to accept completed ballots until April 13, 2020, "regardless of the postmark date."[179] The Supreme Court's order required absentee voters to postmark their ballots by April 7, 2020, despite the fact that most voters had not received their ballots due to a backlog in sending out absentee-ballots caused by a surge in absentee-ballot requests.[180] In her dissent, Ruth Bader Ginsburg wrote that the Supreme Court's decision would "result in massive disenfranchisement" and require voters to choose between "endangering their own and others' safety" or "los[ing] their right to vote."[181]

IV. VOTER ACCESSIBILITY AND VOTING LAWS

Multiple laws have been passed to make voting accessible to voters from all walks of life. For example, Congress enacted the National Voter Registration Act of 1993 ("NVRA") to make voting accessible to every American.[182] NVRA's purpose was to make it easier for Americans to register to vote and enhance voter participation.[183]

Voter accessibility laws were also passed for the elderly and handicapped to make polling places "physically accessible for people with disabilities during federal

---

[174] Vicente Gonzalez, *It's Time To Consider Creating A Remote Voting System For Congress*, THE HILL (Mar. 17, 2020), https://thehill.com/blogs/congress-blog/politics/488081-its-time-to-consider-a-remote-voting-system-for-congress.

[175] *Id.*

[176] *Id.*

[177] *Id.*

[178] Republican Nat'l Comm. v. Democratic Nat'l Comm., 140 S.Ct. 1205, 1208 (2020).

[179] *Id.* at 1209. (Ginsburg, J., dissenting).

[180] *Id.* (Ginsburg, J., dissenting).

[181] *Id.* (Ginsburg, J., dissenting).

[182] *See* 52 U.S.C. § 20501(b)(1)-(2) (1993).

[183] *See id.*

elections."[184] If physical accessibility is not possible, then the federal government requires the polling place to provide alternative ways to vote.[185] Moreover, in 1986, Congress enacted the Uniformed and Overseas Citizens Absentee Voting Act ("UOCAVA") to allow military, military spouses and dependents, and "citizens residing outside of the United States" to cast absentee ballots in federal elections.[186]

With each accessibility law Congress passed, Congress has continued to uphold section 1 of the Fifteenth Amendment's purpose in giving every United States citizen the right to vote.[187] Despite the previous voter accessibility laws, which have evolved with technology to ensure every American's Fifteenth Amendment right is respected, Congress has not established any real federal standards to support Internet blockchain voting.[188] However, Congress can implement new legislation through section 2 of the Fifteenth Amendment.[189] Section 2 of the Fifteenth Amendment grants Congress power to create legislation to enforce the Fifteenth Amendment.[190] Thus, Congress could use its power to implement a blockchain voting system that can be used to fix the United States' current voting defects.[191] Congress can create and pass legislation similar to the National Defense Authorization Act's Military and Overseas Voter Empowerment Act ("MOVE Act").[192] This Article will focus primarily on creating legislation through section 2 of the Fifteenth Amendment to allow for online, blockchain voting.

A. MILITARY AND OVERSEAS VOTER EMPOWERMENT ACT

The MOVE Act is a subsection of the National Defense Authorization Act of 2010.[193] The MOVE Act amended UOCAVA to include electronic voting.[194] This Article focuses on two sections within the MOVE Act, Section 578 and 579. Section 578 states:

(1) In General. —Each State shall establish procedures—

(A) to transmit blank absentee ballots by mail and electronically (in accordance with the preferred method of transmission designated by the absent uniformed

---

[184] *A Guide to Disability Rights Laws*, U.S. DEP'T OF JUSTICE (2020), https://www.ada.gov/cguide.htm#anchor64292.
[185] *Id.*
[186] *The Uniformed and Overseas Citizens Absentee Voting Act*, U.S. DEP'T OF JUSTICE (2020), https://www.justice.gov/crt/uniformed-and-overseas-citizens-absentee-voting-act.
[187] *See* U.S. CONST. amend. XV, § 1.
[188] Jane Susskind, *Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System*, 54 SAN DIEGO L. REV. 785, 816 (2017).
[189] *See* U.S. CONST. amend. XV, § 2.
[190] *See id.*
[191] Susskind, *supra* note 188.
[192] *See* Nat'l Def. Authorization Act of 2010, *supra* note 19.
[193] *See id.*
[194] *See id.* § 578.

services voter or overseas voter under subparagraph (B)) to absent uniformed services voters and overseas voters for an election for Federal office; and

(B) by which the absent uniformed services voter or overseas voter can designate whether the voter prefers that such blank absentee ballot be transmitted by mail or electronically.[195]

Section 579, subsection (b) states:

(1) In General. -The Presidential designee may establish 1 or more pilot programs under which the feasibility of new election technology is tested for the benefit of absent uniformed services voters and overseas voters claiming rights under the Uniformed and Overseas Citizens Absentee Voting Act....
(c) Considerations. - In conducting a pilot program established under subsection (b), the Presidential designee may consider the following issues:
(1) The transmission of electronic voting material across military networks.
(2) Virtual private networks, cryptographic voting systems, centrally controlled voting stations, and other information security techniques.[196]

Section 578 of the Move Act requires states to provide blank ballots to UOCAVA voters in "at least one electronic format—email, fax, or an online delivery system."[197] However, section 578 is only intended to "be used as a back-up ballot for voters who do not receive a ballot from their state" and it does not require states to accept electronic ballots.[198]Additionally, while section 579 of the MOVE Act only allows for pilot programs, pilot programs are often conducted to determine whether the methods used during the program can be used on a larger scale.[199] While multiple pilot programs have been conducted by the U.S., none of the online voting pilot programs have been adopted by the federal government.[200]

Despite the MOVE Act's innovation in making voting accessible, the Act still has significant limitations.[201] Although Sections 578 and 579 of the Act allows for electronic voting, it only allows for electronic voting under narrow circumstances.[202] Thus, a

---

[195] *Id.*
[196] *Id.* § 579.
[197] *Electronic Transmission of Ballots*, NAT'L CONF. OF STATE LEGISLATURES (Sept. 5, 2019), https://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx.
[198] *Id.*
[199] *See* Lehana Thabane et. al., *A Tutorial on Pilot Studies: The What, Why and How*, 10 BMC MED. RSCH. METHODOLOGY 1 (2010).
[200] *See* Greenhalgh, *supra* note 19.
[201] *See* NAT'L CONF. OF STATE LEGISLATURES, *supra* note 197.
[202] *See* Nat'l Def. Authorization Act of 2010, *supra* note 19, §§ 578-79.

broader law should be drafted by Congress that is similar to the MOVE Act.[203] This law should include three new provisions. First, it should include all voters, instead of voters that only fit within UOCAVA's narrow characteristics. Second, the law should require states to accept electronic ballots from voters from secure sites that utilize blockchain voting, instead of accepting ballots through email, fax, or an unsecure online delivery system. Lastly, the law should allow states to implement laws that adopt successful voting pilot programs—specifically blockchain voting pilot programs—into their respective constitutions.

B. GRAPPLING WITH CURRENT VOTING LAWS

Currently, there are two voting laws that blockchain voting must satisfy before it can be legitimized: the Help America Vote Act's ("HAVA") voting standard and section 2 of the Voting Rights Act.[204] HAVA was implemented to assist with the administration of Federal election laws and establish "minimum election administration standards for States and units of local government."[205] Whereas, section 2 of the Voting Rights Act prohibits state voting practices that discriminate against a class of people.[206]

First, to address HAVA's concerns, HAVA requires every new voting system to "fit within the definition of voting system to be used in an election for federal office."[207] One legal scholar has suggested that Congress amend HAVA's definition of voting system to include internet voting to allow for blockchain voting.[208] However, subsection (b) of section 301 states the following:

the term ''voting system'' means—

(1) the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used—

(A) to define ballots;
(B) to cast and count votes;
(C) to report or display election results; and
(D) to maintain and produce any audit trail information.[209]

---

[203] *See id.* §§ 578-79.
[204] *Id.* § 578.; 52 U.S.C.A. § 10303(f)(2) (West 2014).
[205] H.R. Res. 3295, 107th Cong. (2002) (enacted).
[206] 52 U.S.C.A. § 10303(f)(2) (West 2014).
[207] Susskind, *supra* note 188, at 805.
[208] *Id.* at 816.
[209] H.R. Res. 3295-41, 107th Cong., § 301(b) (2002) (enacted).

Blockchain voting can fit under HAVA's definition of voting system because HAVA's definition is broad enough that it allows for Congress to create new legislation that is not limited to solely paper ballots.[210] Thus, while amending HAVA to include internet voting would further legitimatize online voting, it is not necessary to implement a blockchain voting system.

   Additionally, HAVA includes two sections that address online voting.[211] Section 20985 of the United States Code requires the Election Assistance Commission ("The Commission") to conduct studies on voting issues.[212] A majority of the issues HAVA outlines for The Commission to study concern online voting.[213] The issues range from studying potential voter fraud through the use of technology to the impact that Internet technology would have on voter participation.[214] Moreover, one subsection states the following:

> The Commission may include in the study conducted under paragraph (1) an examination of…
> (G) identification of current and foreseeable online and Internet technologies for use in the registration of voters, for voting, or for the purpose of reducing election fraud, currently available or in use by election authorities.[215]

   The second Section within HAVA addresses how the Technical Guidelines Development Committee ("Development Committee") assists The Committee in developing voluntary voting system guidelines.[216] Part of the Development Committees job is to request technical support from the Director of the National Institute of Standards and Technology.[217] This technical support is meant to assist the Development Committee in researching and developing voluntary voting system guidelines, such as guidelines for internet voting.[218] It is clear Congress foresaw a future with online voting. However, it is unclear as to whether Congress intended to only grant access to online voting to the persons outlined within the Uniformed and Overseas Citizens Absentee Voting Act.

   Second, the Voting Rights Act of 1965 "must be considered before altering state voting systems."[219] The act invalidates any state law that results in discrimination, "regardless

---

[210] Susskind, *supra* note 188, at 816.
[211] *See* 52 U.S.C. § 20985; 52 U.S.C. § 20961.
[212] 52 U.S.C. § 20985(a)(1).
[213] *See* 52 U.S.C. § 20985(a)(2).
[214] *See* 52 U.S.C. § 20985(a)(2)(A); 52 U.S.C; § 20985(a)(2)(C).
[215] 52 U.S.C. § 20985(a)(2)(G).
[216] *See* 52 U.S.C. § 20961(b)(1).
[217] *See* 52 U.S.C. § 20961(e)(1).
[218] *See* 52 U.S.C. § 20961(e)(1)(E).
[219] Susskind, *supra* note 188, at 806.

of discriminatory intent."[220] The act is violated if the claimant proves the voting practice has a "racially discriminatory effect when viewed under the 'totality of the circumstances.'"[221] The same legal scholar who proposed an amendment to HAVA, also suggested that blockchain voting systems would only have a discriminatory effect if the United States did away with every other voting system and only permitted blockchain voting.[222] Additionally, because society relies so heavily on technology, and there are public facilities, such as the public library and Internet cafes, that provide computers and free Internet to the public, voters are less likely to face difficulties in accessing the Internet.[223] Thus, blockchain voting is unlikely to violate section 2 of the Voting Rights Act.[224]

Ultimately, blockchain voting can satisfy both the Voting Rights Act and HAVA. However, there is no current legislation that makes online, blockchain voting accessible to every voter. Thus, Congress should create new legislation that will codify blockchain voting into Federal law and offer states the option of adopting blockchain voting into their constitutions.

V.   CONCLUSION

This Article began by acknowledging the difficulties the United States has faced in creating secure voting systems that are accessible for every voter. Failing to consider blockchain voting as a voting system that can be adopted throughout the United States due to the hackability issues blockchain voting faces is flawed. Voting is a franchise that should be accessible to every United States citizen. Implementing a blockchain voting system would serve a vital role in making voting accessible to every citizen.

The vulnerability of blockchain voting to hackers overlaps with the issues current voting systems face with attackers. To address the hackability issues, the Federal government should create comprehensive solutions to address gaps in security with blockchain voting. In the absence of reform, the United States could not utilize blockchain voting without risking data exfiltration from attackers.

The United States Federal government should acknowledge that blockchain voting is a lasting solution that could address the problems traditional voting systems face. The United States has a long history of denying citizens their franchise, whether due to their race, gender, or due to frivolous voter identification laws.[225] Once the Federal government addresses the issues blockchain voting faces, blockchain voting should be

---

[220] *Id.*

[221] *Id.*

[222] *Id.* at 809.

[223] *Id.*

[224] *See id.*

[225] *See* U.S. CONST. amends. XIV, XIX; *Voter Identification*, NAT'L CONF. OF STATE LEGISLATURES (Aug. 25, 2020), https://www.ncsl.org/research/elections-and-campaigns/voter-id.aspx.

adopted into law as it is a lasting solution to address voter suppression and accessibility in the United States.