NOTE

VETO THE BLACK-BOX POLITICS: HOW IMPLEMENTING BLOCKCHAIN TECHNOLOGY INTO THE UNITED STATES VOTING SYSTEM WILL GIVE OUR WORLD THE TRANSPARENCY WE DESERVE

I. INTRODUCTION

If our federally elected officials represent the United States on the world stage, why do "We the People"[1] tolerate an antiquated, black-box system of voting to have these officials speak on our behalf?[2] A Gallup World Poll conducted from April to May 2019 found that 59% of Americans do not have confidence in the "honesty of elections."[3] Indeed, the last time a majority of Americans felt confident in the honesty of elections was in 2009, with only 59% of Americans answering in the affirmative, with the "average confidence" from 2006 to 2019 equating to 43.9%, and a record low of 30% in 2016.[4] When compared to the thirty-one other countries included in the 2019 Gallup poll, the United States placed twenty-seventh, behind Hungary at twenty-sixth, and marginally topping Lithuania, Turkey, Latvia, Chile, and Mexico.[5] Following January 6, 2021, the record low was broken

---

1. U.S. CONST. pmbl.

2. *See* Jon Evans, *2020 and the Black-box Ballot Box*, TECHCRUNCH (Aug. 11, 2019, 9:00 AM), https://techcrunch.com/2019/08/11/2020-and-the-black-ballot-box [https://perma.cc/TU39-R8A7].

3. RJ Reinhart, *Faith in Elections in Relatively Short Supply in U.S.*, GALLUP (Feb. 13, 2020), https://news.gallup.com/poll/285608/faith-elections-relatively-short-supply.aspx [https://perma.cc/KXA6-DZAE].

4. *Id.* (finding the average by adding each year's affirmative confidence and dividing the sum by the total number of years (fifteen)).

5. *See id.*; *see also Corruption Perceptions Index*, TRANSPARENCY INT'L, https://www.transparency.org/en/cpi/2021 [https://perma.cc/9SGM-S5LD] (last visited Dec. 2, 2023) (highlighting that "[t]he [Corruption Perceptions Index] ("CPI") ranks 180 countries and territories around the world by their perceived levels of public sector corruption. The results are given on a scale of 0 (highly corrupt) to 100 (very clean)").

when an ABC News Poll found that only one in five, or 20%, of Americans are confident in our election system.[6]

Additionally, the Electoral Integrity Project ("EIP"), an independent study with teams based out of Harvard University and Sydney University, conducted research about the quality of elections around the world.[7] In 2016, the EIP's expert surveys ranked each country's Perceptions of Electoral Integrity ("PEI"), and found that the United States scored a sixty-two out of 100 with Turkey, Mexico, and Hungary scoring a forty-eight, fifty-seven, and fifty-six, respectively.[8] In 2022, the United States scored a 58.78, dropping four points since 2016, with Turkey, Mexico, and Hungary scoring a 51.12, 58.9, and 49.82, respectively.[9] The PEI scores are used to rank 169 countries around the world by their electoral integrity, with scores of sixty and over indicating strong integrity, fifty to fifty-nine indicating moderate integrity, and less than fifty indicating weak integrity.[10] Hence, while the United States placed within the moderate to high integrity range with a score of 58.78, it ranked sixty-fourth worldwide and one of the worst amongst Western Democracies.[11]

Further, the United States, in regard to citizens' perception of corruption, ranks slightly better than Turkey, Mexico, and Hungary, which have Corruption Perception Indexes ("CPIs") of thirty-eight, thirty-one, and forty-three, respectively, compared to the United States at sixty-seven.[12] The CPI ranks 180 countries and territories around the

---

6. Brittany Shepherd, *Americans' Faith in Election Integrity Drops: POLL*, ABC NEWS (Jan. 6, 2022, 11:01 AM), https://abcnews.go.com/Politics/americans-faith-election-integrity-drops-poll/story?id=82069876 [https://perma.cc/55LM-4YBT].

7. PIPPA NORRIS, WHY AMERICAN ELECTIONS ARE FLAWED (AND HOW TO FIX THEM) 1, 25, 69 (2017).

8. *Id.* at 30-31.

9. Holly Ann Garnett et al., *2022 Perceptions of Electoral Integrity, (PEI-8.0)*, HARV. DATAVERSE (May 17, 2022) [hereinafter Garnett et al., *2022 Perceptions of Electoral Integrity*], https://gdcc.github.io/dataverse-previewers/previewers/v1.3/SpreadsheetPreview.html?fileid=6297541&siteUrl=https://dataverse.harvard.edu&datasetid=6290816&datasetversion=1.1&locale=en [https://perma.cc/UQ4T-GQ8S] (select "Access File" then "MS Word" under "Download Options," accept the "Dataset Terms" by selecting "Accept," open the file, then go to page 11 to view "PEIIndexP" under "Survey Variables in PEI 8.0" under "OVERALLINTEGRITY") (cross-referencing the PEI data from column titled "PEIIndexp" that corresponds with an individual country from the column titled "Country"). "PEIIndexp" is the raw PEI index. HOLLY ANN GARNETT ET AL., PERCEPTIONS OF ELECTORAL INTEGRITY (PEI) DATASET 11 (Electoral Integrity Project 2022). This is compared to the "PEIindexI" which is the imputed PEI index that fills in missing values not found in the study. *Id.* at 12 (open the file, then go to page 12 to view "PEIIndexI" under "Survey Variables in PEI 8.0" under "OVERALLINTEGRITY").

10. NORRIS, *supra* note 7, at 30.

11. *See id.* at 2, 66; Garnett et al., *2022 Perceptions of Electoral Integrity*, *supra* note 9.

12. *Corruption Perceptions Index*, *supra* note 5.

world by their perceived levels of public sector corruption, on a scale from zero, or highly corrupt, to 100, or no corruption.[13]

This Note does not propose that citizens' trust in *elections* directly correlates with government corruption.[14] Further, this Note does not suggest that the United States is corrupt or that there have been proven widespread instances of voter fraud.[15] This Note is not even suggesting that *everyone* will feel 100% confident in the outcome of elections.[16] Even Finland, which ranked the highest on Gallup's 2019 poll, with eighty-nine percent of citizens reporting to believe in the honesty of elections,[17] and ranked one of the best countries for lack of corruption with a CPI score of eighty-eight,[18] has not achieved 100% confidence.[19] Several studies demonstrate that political corruption is an inescapable consequence of lacking citizen trust.[20] While one may read this Note with skepticism that the solution presented is based off false claims of voter fraud, or is an attempt to fix an unbroken voting system, the United States cannot remain the "leader of the free world" while simultaneously ranking close to, or behind, highly corrupt, and low-scoring countries like Turkey, Mexico, and Hungary in electoral honesty studies.[21] So, while achieving 100% trust in elections is a pipedream, this should not imply that the United States should ignore the problem altogether.[22]

---

13. *Id.*

14. *See infra* Part III.A.

15. *See* Lee Rainie et al., *Trust and Distrust in America*, PEW RSCH. CTR. (July 22, 2019), https://www.pewresearch.org/politics/2019/07/22/trust-and-distrust-in-america [https://perma.cc/KC5D-DMLH] (discussing how American distrust in federal government and in each other is a deeply rooted problem that gets in the way of finding solutions to key societal issues).

16. *Id.*

17. Reinhart, *supra* note 3.

18. *Corruption Perceptions Index*, *supra* note 5.

19. *See Public Trust in Government: 1958-2022*, PEW RSCH. CTR. (June 6, 2022), https://www.pewresearch.org/politics/2022/06/06/public-trust-in-government-1958-2022 [https://perma.cc/S797-E6H6] (displaying data that demonstrates trust levels below seventy-five percent for Americans even in a time regarded as most trustworthy).

20. *See, e.g.*, Stephen D. Morris & Joseph L. Klesner, *Corruption and Trust: Theoretical Considerations and Evidence from Mexico*, 43 COMPAR. POL. STUD. 1258, 1262 (2010).

21. Venus D., *What Does the "Leader of the Free World" Mean?*, HIST. INDEX, https://www.historicalindex.org/what-does-the-leader-of-the-free-world-mean.htm [https://perma.cc/BKU5-872S] (Aug. 13, 2023) (defining "Free World" as a nation that embodies, *inter alia*, a system where "[r]epresentatives of government are chosen by the people through a fair election process"); *see Corruption Perceptions Index*, *supra* note 5.

22. *See* John Davenport, *11 (Bipartisan) Ways to Improve Voting in the United States*, AM. MAG. (Mar. 1, 2021), https://www.americamagazine.org/politics-society/2021/03/01/election-reform-voting-bill-congress-239992 [https://perma.cc/7BPV-9GQ5].

Additionally, it is misguided to pin all the blame of lacking government trust on the waning trust in elections.[23] Notwithstanding this point, election trust is a major factor in overall government trust,[24] and not only will inaction push the United States to lose its title as "leader of the free world," but governmental action will be stymied, especially when the public believes that the government will "do what is right" only twenty percent of the time.[25]

The distrust of the United States government has increased over the last few years and will continue to corrode the foundation of democracy if we fail to modernize the system used to perform one of our most essential rights as Americans.[26] Change is long overdue, and the public should not tolerate this lack of transparency in the digital age, especially when solutions are available.[27]

Implementing blockchain technology into the United States election system has the power to alleviate some of the grievances present with the current system.[28] The United States must pioneer election change, and push other North Atlantic Treaty Organization ("NATO") countries to join, to allow the global ecosystem to benefit from the transparent relationship our government, and others, can foster across the globe.[29] While NATO rightfully spends a considerable amount of time and money researching and sharing information amongst member states regarding external threats to democracy, they seldom share information regarding internal threats to democracy, which may present greater devastation.[30]

---

23. Rainie et al., *supra* note 15.
24. *See id.*
25. *Public Trust in Government: 1958-2022*, *supra* note 19.
26. *See* Shepherd, *supra* note 6.
27. *See infra* Part IV; *see also* Evans, *supra* note 2.
28. *See* Jacob Beckett, Comment, *Blockchain Voting: WY Not?*, 21 WYO. L. REV. 411, 430 (2021) (discussing the current issues surrounding the United States voting system such as weak security and lacking transparency); *id.* at 427 (detailing how the adoption of blockchain voting nationwide could provide numerous benefits when compared to adoption by just one state). *See generally* HENNING DIEDRICH, ETHEREUM: BLOCKCHAINS, DIGITAL ASSETS, SMART CONTRACTS, DECENTRALIZED AUTONOMOUS ORGANIZATIONS (2016) (exploring the power of blockchain networks and several uses of the Ethereum blockchain in particular and detailing numerous uses and features of a blockchain network, such as creation of audit-friendly government processes, direct democracy via collaborative models, prevention of non-trustworthy data, facilitation of trustless interactions, presentation of freely accessible and visible transactions, prevention of malicious changes in transactions, and prevention of harmless errors).
29. *See 10 Things You Need to Know About NATO*, N. ATL. TREATY ORG., https://www.nato.int/cps/en/natohq/126169.htm [https://perma.cc/P47N-VCGW] (Apr. 13, 2023, 10:47 AM).
30. *See id.* (listing ten missions and goals of the organization, none of which discuss internal threats to democracy).

This Note proceeds in four parts.[31] Part II presents a brief background on blockchain technology and the constitutionality of the federal government implementing a blockchain network for federal elections.[32] Part III opens with a discussion on the allegations of voter fraud in United States federal elections and concludes by demonstrating how five key benefits of blockchain technology from Part II will improve election systems.[33] Lastly, Part IV proposes an exemplary blockchain voting network to be researched and implemented over the next decade and sets forth how the United States can encourage its allies to adopt a similar system for their elections.[34]

II. BRIDGING THE BACKGROUND OF BLOCKCHAIN TECHNOLOGY WITH THE ELECTIONS CLAUSE OF THE CONSTITUTION

One must understand the general foundation of blockchain technology and the dynamic between the federal and state governments to grasp the scope of this Note.[35] Thus, Subpart A will discuss the history, function, and several use-cases of blockchain technology.[36] Thereafter, Subpart B will present a constitutional analysis of the federal government's power under the Elections Clause of the United States Constitution to implement blockchain technology in federal elections.[37]

A. Blockchain Technology

1. Blockchain Basics

A "typical" blockchain is a decentralized[38] public ledger that records digital information.[39] The computers on the network, called

---

31. *See infra* Parts II–V.

32. *See infra* Part II; *see also* Beckett, *supra* note 28, at 427 (discussing Wyoming's implementation of blockchain technology to govern elections).

33. *See infra* Part III; *see also* DIEDRICH, *supra* note 28, at 92-93 (listing several key benefits of a blockchain and different ways to describe blockchain technology relevant to its potential use).

34. *See infra* Part IV; *see also* Beckett, *supra* note 28, at 427 (describing how a federal government-led initiative to implement blockchain voting could lead to adoption in other states other than Wyoming).

35. *See* U.S. CONST. art. I, § 4, cl. 1. *See generally* Uzma Jafar et al., *Blockchain for Electronic Voting System—Review and Open Research Challenges*, SENSORS, Aug. 31, 2021, at 1.

36. *See infra* Part II.A; *see also* DIEDRICH, *supra* note 28, at 92-93 (listing several key benefits of a blockchain).

37. *See infra* Part II.B; *see also* U.S. CONST. art. I, § 4, cl. 1.

38. *See* Sam Daley et al., *Blockchain. What Is Blockchain Technology? How Does It Work?*, BUILT IN (Aug. 31, 2022), https://builtin.com/blockchain [https://perma.cc/R2MP-E37V]. *See generally* Jafar et al., *supra* note 35 (discussing decentralization and focusing solely on decentralization for blockchain voting networks). Decentralization, one of the most important concepts in blockchain technology, is a network organizational structure where no one individual,

"nodes," work together to verify a proposed transaction by using brute force algorithms to solve the "nonce," or the "number used only once" randomly chosen based on network difficulty, appended to the hash of a transaction.[40] A hash involves a mathematical function (i.e., a hash function) that converts an arbitrary length of data transacted into an encrypted output of a fixed length, whereas the nonce is used to later validate this data and maintain the difficulty of the system.[41] In simple terms: a hash function can take any amount of data, no matter how large or small, and convert that data into an output of fixed length, typically 256-bits, that the nodes will attempt to decode.[42] As an example, the input "the quick brown fox jumped over the lazy dog" when transformed by algorithm 256 ("SHA-256") will give an output of:

> 20c1892df4e665666558289367ae1682d1f93bc5be4049627492cdb5a4
> 2635e4.[43]

Additionally, a hash is deterministic, meaning that the input may always be derived from the output, and any change in the input will render a different output; theoretically, no two inputs will have the same output.[44] This meaning, even a slight change in the input, such as capitalizing the "b" in "the quick *B*rown fox jumped over the lazy dog" gives an entirely different output:

> 81d819e4c5087bca0e261dac7b1205d94ed86c31458b6b3df29e7e4ba6
> e01012.[45]

After the hash is solved by the computer, the hash is placed on a "block," which is a collection of all the transaction data, and is linked

---

organization, or computer is the bearer of authority; rather, authority is distributed to several points, any of which may act as an independent central point, yet the network as a whole maintains no central point of control. Daley et al., *supra* note 38.

39. DIEDRICH, *supra* note 28, at 94-95.

40. *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN 1, 3, https://bitcoin.org/bitcoin.pdf [https://perma.cc/YQ2B-HMUC] (last visited Dec. 2, 2023); Jake Frankenfield et al., *Nonce: What It Means and How It's Used in Blockchain*, INVESTOPEDIA, https://www.investopedia.com/terms/n/nonce.asp [https://perma.cc/VTD8-G7ZK] (June 12, 2022).

41. Jake Frankenfield et al., *What Is a Hash? Hash Functions and Cryptocurrency Mining*, INVESTOPEDIA, https://www.investopedia.com/terms/h/hash.asp [https://perma.cc/24XR-QE45] (Feb. 12, 2023).

42. *See* DIEDRICH, *supra* note 28, at 106-07 (describing the use of SHA-256, which is a hash algorithm that converts input data into a fixed 256-bit output).

43. *Generate SHA256 Hash*, DIGITALOCEAN: TIMESTAMP GENERATOR, https://timestampgenerator.com/generate-hash/sha256 [https://perma.cc/67TM-AGXS] (last visited Dec. 2, 2023) (using input under "Enter Text" as "the quick brown fox jumped over the lazy dog").

44. DIEDRICH, *supra* note 28, at 109.

45. *Generate SHA256 Hash*, *supra* note 43 (emphasis added) (using input under "Enter Text" as "the quick Brown fox jumped over the lazy dog").

together, by hash, to the block before it.[46] This forms a "chain" of blocks in a successive, single list that is disseminated throughout the entire network.[47]

Solving a hash using brute force, or continuous trial and error, is known as proof-of-work.[48] This name derives from the "work" that computers on the network are required to perform to verify each transaction.[49] Each node on the network has an opportunity to compete to be the first node to finish the work required, or in this case, solving the hash first to earn a monetary reward.[50] While proof-of-work is the dominant means of verifying transactions, the use of brute force algorithms consumes massive amounts of energy, making such a system unsustainable.[51] For this reason, a new method for verifying transactions has surfaced, known as proof-of-stake.[52] This name derives from the "stake," typically cryptocurrency, that computers put into the network for an opportunity to verify a transaction.[53] Successful verifications are monetarily rewarded, while unsuccessful verifications are penalized by the network, reducing the amount of the cryptocurrency staked by that computer.[54]

Thus, rather than the proof-of-work "race" to solve a highly complex algorithm amongst millions of computers, a proof-of-stake protocol allows computers, known as transaction validators, to be randomly selected based on the proportion of their staked currency on the blockchain.[55] The greater the validator's stake, the higher the chance of being selected by the network to validate a transaction.[56] However, several blockchains that utilize proof-of-stake are a bit more complex and take into account the "staking age," or the amount of time the currency has been staked; randomization; and the "node's wealth," or the total amount of currency staked, to select a validator to "forge" the

46. *See* Nakamoto, *supra* note 40, at 3.
47. *See id.*
48. Laura M., *Proof of Work VS Proof of Stake: Which One Is Better?*, BITDEGREE, https://www.bitdegree.org/crypto/tutorials/proof-of-work-vs-proof-of-stake [https://perma.cc/2V94-GWEF] (Feb. 16, 2023).
49. *See id.*
50. *See id.*
51. *See Proof-of-Work, and Its Flaws, Explained*, HEDERA, https://hedera.com/learning/consensus-algorithms/proof-of-work-and-its-flaws-explained [https://perma.cc/75XJ-AHPW] (last visited Dec. 2, 2023).
52. *See* Laura M., *supra* note 48.
53. *See id.*
54. *See id.*
55. *See* @LucaPennella, *Proof-of-Stake (POS)*, ETHEREUM (Mar. 1, 2023), https://ethereum.org/en/developers/docs/consensus-mechanisms/pos [https://perma.cc/V9XT-B9TS].
56. *See id.*

next block.[57] The two most popular selection mechanisms include the Randomized Block Selection and Coin Age Selection.[58] Randomized Block Selection selects validators with the lowest hash value and the greatest number of cryptocurrency staked.[59] The lowest hash value is calculated by the validator encrypting the hash of the previous block using their private key.[60] Since each validator's private key is unique, and every block's hash is different, the use of a private key generates a unique hash value for each validator in the network that is compared to find the lowest value.[61] Coin Age Selection selects validators based on the highest "coin age," or the amount of time that their tokens have been staked, and resets the validator's age every time a block has been forged.[62] The coin age is "determined by multiplying the number of coins at stake with the number of days the coins has been held at stake."[63]

A validator is rewarded in transaction fees if they have verified the transaction accurately, which is monitored by the entire network.[64] Hence, staking creates a financial motivator to ensure the integrity of the system: as long as the penalty or amount staked is larger than the transaction fee to be earned, passing a fraudulent transaction will cost the validator a substantial amount of money.[65]

Ethereum integrated a proof-of-stake consensus protocol in September 2022 and has adopted a unique implementation procedure to ensure network immutability and the validity of blocks.[66] The Peercoin Blockchain on the other hand has been utilizing proof-of-stake since 2012 with a selection mechanism that is computing power agnostic when solving a hash for block validation; this meaning, even those with a

---

57. Slance, *What Is Proof-of-Stake – Explained in Detail (Animation)*, YOUTUBE (Nov. 23, 2021), https://www.youtube.com/watch?v=YudpU58uYuM [https://perma.cc/TXT8-ZUKT].

58. *Id.*

59. Techskill Brew, *Proof of Stake in Blockchain (Part 8 – Blockchain Series)*, MEDIUM: BLOCKCHAIN 101 (Jan. 27, 2022), https://medium.com/techskill-brew/proof-of-stake-or-pos-in-blockchain-part-8-blockchain-basics-32d461232e1c [https://perma.cc/L4B3-TP4X].

60. *Id.*

61. *Id.*

62. Someshwaran M., *What Is Proof of Stake in Blockchain? Is It the Best Consensus Algorithm?*, MEDIUM: CAP. PLATFORM (Aug. 11, 2019), https://medium.com/the-capital/what-is-proof-of-stake-in-blockchain-is-it-the-best-consensus-algorithm-d5571de9c368 [https://perma.cc/599Y-YZ46].

63. Techskill Brew, *supra* note 59.

64. Slance, *supra* note 57.

65. *Id.*

66. *See* @LucaPennella, *supra* note 55 (describing the selection of validators using the native function RANDAO); @corwintines, *Proof-of-Stake (POS)*, ETHERUM (July 25, 2023), https://ethereum.org/en/developers/docs/consensus-mechanisms/pos [https://perma.cc/EK7U-JGLR].

personal computer can solve for a hash with relatively low computing power.[67] While Ethereum's more complex system has yet to be proven on the large network, considering the high minimum staking amount of thirty-two Ether,[68] there are notable downsides to the Peercoin model as well.[69] The most concerning is the "nothing at stake" problem, where validators do not lose any of their staked tokens if a fraudulent transaction is passed, leading to no monetary repercussions.[70] Additionally, the need to lock up assets for a set period of time and the high staking value needed to participate may dissuade individuals from staking their currency, and push them towards investing in staking pools, which are centralized entities that combine assets from many individuals and allow for investors to withdraw their stake earlier then required by the network.[71] In effect, this would create the same concern facing proof-of-work models, which is the rise of centralized mining pools, and potential accumulation of fifty-one percent of the network computing power, which can erode the network's decentralized framework; however, this concern is far less likely on a proof-of-stake protocol when considering the amount of stake needed to acquire fifty-one percent of the network.[72]

2. Types of Blockchain Networks and the Central Use-Case

Blockchains can be public or private, and the implementation of a proof-of-work or proof-of-stake consensus protocol will depend on the type and use of the blockchain.[73] Public blockchains allow anyone to join and access the network to participate in verifying or sending transactions.[74] The most well-known example of a public blockchain is

---

67. *Proof-of-Stake*, PEERCOIN DOCS, https://www.peercoin.net/docs/proof-of-stake [https://perma.cc/72G8-WKK5] (last visited Dec. 2, 2023).

68. *See* @LucaPennella, *supra* note 55. One Ether, at the time of writing, is valued at $1,973.84. *Ethereum Price — ETH Price Index & Real-time Charts*, ETHEREUMPRICE, https://ethereumprice.org [https://perma.cc/KS66-8FZH] (last visited Dec. 2, 2023). Accordingly, 32 Ether equates to $63,179.52. *See id.* (equating 1,973.84*32 = 63,162.88).

69. *See* Vitalik Buterin, *Proof of Stake FAQ*, VITALIK BUTERIN'S WEBSITE: PROOF STAKE FAQ (Dec. 31, 2017), https://vitalik.ca/general/2017/12/31/pos_faq.html [https://perma.cc/2KFN-Y94V].

70. *See id.*

71. *See id.*

72. *See id.*; *see also* Griffin Mcshane, *What Is a 51% Attack?*, COINDESK: TECH., https://www.coindesk.com/learn/what-is-a-51-attack [https://perma.cc/U6KZ-HD59] (last visited Dec. 2, 2023).

73. Shobhit Seth & Erika Rasure, *Public, Private, Permissioned Blockchains Compared*, INVESTOPEDIA, https://www.investopedia.com/news/public-private-permissioned-blockchains-compared [https://perma.cc/AHS3-SVLA] (July 28, 2022).

74. *Id.*

Bitcoin, which was created to establish an alternative payment system free from central government control.[75]

For instance, let's consider a hypothetical where user A wants to send $50 to user B; in our current, centralized[76] economy, if user A's cash is deposited with a bank, then user A would need to contact the bank to retrieve their $50 before sending this money to user B.[77] On the blockchain, user A would send a request to the network in the form of a hash; for purposes of this hypothetical, the request "A wants to send $50 to user B" will become the hash:

> fc5c4666fcd96b4e8072571b4de7c84729aadbd280d5fdbe75854548e8c2763a.[78]

Once the hash has been sent to the network, the computers will race to solve the hash for a monetary reward,[79] with the first computer to solve correctly receiving the reward after the entire network verifies the answer.[80] Upon consensus, a new block is formed with (1) the hash of the previous block; (2) the transaction data; and (3) the hash of the current block.[81]

Some blockchains are considered a hybrid between public and private, otherwise referred to as a permissioned blockchain, which grants general public access to the blockchain while reserving, for some users, certain permissions to edit transactions.[82] This contrasts with a purely private blockchain, which only allows for selected users to participate in verifying or sending transactions.[83] A private blockchain is generally owned by an operator who is given the rights to override, edit, and delete entries on the blockchain.[84]

---

75. *See* Nakamoto, *supra* note 40, at 2.

76. *See id.*; James McWhinney et al., *Can Bitcoin Kill Central Banks?*, INVESTOPEDIA, https://www.investopedia.com/articles/investing/050715/can-bitcoin-kill-central-banks.asp [https://perma.cc/EJ7J-DMVH] (May 30, 2022).

77. *See* DIEDRICH, *supra* note 28, at 63 (detailing the use of blockchain in FinTech, or financial technology, and how the transparent and trustless transactions provided for by blockchain removes the need for middlemen working at the banks that are currently employed to ensure validity).

78. *See id.* at 107 (displaying examples of hashed outputs); *see also Generate SHA256 Hash*, *supra* note 43 (using input under "Enter Text" as "A wants to send $50 to user B").

79. *See* Nakamoto, *supra* note 40, at 4.

80. *See id.* at 3.

81. *See id.*

82. Seth & Rasure, *supra* note 73.

83. *Id.*

84. *Id.*

3. The Evolution from Monetary Transactions to Digital Asset Transactions

The evolution of blockchain technology has allowed for other types of transactions, such as transferring ownership of digital items in the form of non-fungible tokens ("NFTs") and decentralized autonomous organizations ("DAOs") that allow users to establish an independent entity exclusively governed on the blockchain.[85] The Ethereum Network[86] pioneered this evolution with the integration of smart contracts onto the blockchain.[87] Smart contracts are analogous to traditional written contracts, but they are not legally binding.[88] Smart contracts consist of code written by software engineers that is interpreted and executed by the Ethereum Virtual Machine to perform some function.[89]

For example, consider the hypothetical where user A sells a digital portrait to user B after user B transfers $100 to user A's account in monthly installments of $10.[90] The smart contract would automatically transfer the portrait once all payments are received.[91] Although this is a very simplified example, the utility of smart contracts extends beyond the scope of this Note.[92] A notable downside, however, is that there is no interpretation beyond the written code;[93] the contract will execute

---

85. *See* DIEDRICH, *supra* note 28, at 180; Rakesh Sharma et al., *Non-Fungible Token (NFT): What It Means and How It Works*, INVESTOPEDIA, https://www.investopedia.com/non-fungible-tokens-nft-5115211 [https://perma.cc/BE6B-4CR4] (Apr. 6, 2023).

86. *See What Is Ethereum?*, ETHEREUM, https://ethereum.org/en/what-is-ethereum [https://perma.cc/VY35-9JVN] (last visited Dec. 2, 2023) (describing smart contracts as "computer programs living on the Ethereum blockchain"). Smart contracts and their function are attributable for the flexibility offered by the Ethereum Network. *Id.*

87. *See* DIEDRICH, *supra* note 28, at 169-70, 180-81 (describing the background of smart contracts, their prominence on the Ethereum Network, and how smart contracts interplay with DAOs).

88. *See id.* at 167-69.

89. *See* @wackerow, *Anatomy of Smart Contracts*, ETHEREUM: INTRO TO ETHEREUM (Aug. 15, 2022), https://ethereum.org/en/developers/docs/smart-contracts/anatomy [https://perma.cc/M78D-N3DQ] (explaining how the code creates a call to the EVM to perform some function, this being, executing the smart contract).

90. *See* DIEDRICH, *supra* note 28, at 169 (detailing the use of smart contracts to transfer digital assets).

91. *See id.* at 169-70.

92. *See id.*; Cryptopedia Staff, *Real-World Use Cases for Smart Contracts and dApps*, CRYPTOPEDIA, https://www.gemini.com/cryptopedia/smart-contract-examples-smart-contract-use-cases [https://perma.cc/9MMM-ULR5] (Dec. 23, 2021).

93. *See* Nathaniel Popper, *A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency*, N.Y. TIMES: DEALBOOK (June 17, 2016), https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html [https://perma.cc/Q99Z-UJA8] (describing

exactly as written and cannot be changed.[94] While this may conversely serve as a benefit, any poorly programmed smart contract could have serious ramifications that cannot be rectified after signing.[95]

Consider this hypothetical: user B made five payments, lost his job, and can no longer afford the portrait.[96] If there is no code that allows for automatic returns, he is out of luck unless user A sends the money back.[97] Such a feature, however, will not always be a negative consequence.[98] For example, smart contracts have been utilized by private blockchain networks to establish a system of voting.[99] If written correctly, smart contracts that allow for a rigid allocation of ballots, and maintain an immutable record of transactions, have proven successful when tallying votes.[100]

4. States Utilizing Private Blockchain Networks in Voting

Private blockchains have mostly emerged in domestic and international business, but other uses, such as voting, have become more prevalent.[101] In 2018, West Virginia launched the nation's first mobile, blockchain-based voting program for "military personnel, their families, and civilians stationed or working abroad."[102] The city of Denver and

---

how computer scientists attempted to alter the code *ex post*). Nevertheless, the code of a smart contract will run as written with no third-party interpretation to rectify a bug. *Id.*

94. *See* DIEDRICH, *supra* note 28, at 168.

95. *See* Cryptopedia Staff, *What Was the DAO?*, CRYPTOPEDIA, https://www.gemini.com/cryptopedia/the-dao-hack-makerdao [https://perma.cc/PQZ8-Y6PV] (Mar. 16, 2022) (discussing a flaw in a smart contract is what allowed a hacker to steal $60 million worth of Ether). Eventually, there was a hard fork which resulted in the creation of two blockchains: Ethereum and Ethereum Classic. *Id.*

96. *See* DIEDRICH, *supra* note 28, at 168.

97. *See id.*

98. *See What Is a Smart Contract, and How Does It Work?*, COINTELEGRAPH, https://cointelegraph.com/learn/what-are-smart-contracts-a-beginners-guide-to-automated-agreements [https://perma.cc/NZS5-VN6V] (last visited Dec. 2, 2023) (describing how automatic execution removes the requirement for a third-party intermediary).

99. *See* Larry Moore & Nimit Sawhney, *Under the Hood: The West Virginia Mobile Voting Pilot*, VOATZ, INC. 1, 4, 6 (2019), https://sos.wv.gov/FormSearch/Elections/Informational/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf [https://perma.cc/456L-5ZQG]. The technology behind the blockchain infrastructure for the Voatz project included the open-source Hyperledger blockchain software build with programming documentation capable of supporting smart contracts. *See Smart Contracts and Chaincode*, HYPERLEDGER, https://hyperledger-fabric.readthedocs.io/en/release-2.5/smartcontract/smartcontract.html#smart-contracts-and-chaincode [https://perma.cc/CM6H-VHE5] (last visited Dec. 2, 2023).

100. *See* Moore & Sawhney, *supra* note 99, at 4.

101. *See* Beckett, *supra* note 28, at 425-26 (describing Voatz, a private blockchain system used in other state elections but detailing why Wyoming should not implement a centralized blockchain for blockchain voting).

102. *See* Moore & Sawhney, *supra* note 99, at 1.

Utah County have similarly launched pilot programs for blockchain-voting in elections.[103] Denver, Utah County, and West Virginia implemented their blockchains using the privately held company Voatz.[104] While these localities are certainly leaders in the space, reliance on a single private entity is ripe for abuse, which is discussed in greater detail in Part IV.[105]

B. United States Voting Laws: The Dynamic Between the Federal and State Governments

Article 1, Section 4, Clause 1 of the United States Constitution states: "The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each state by the legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the Places of chusing Senators."[106] The Framers "understood the Elections Clause as a grant of authority to issue procedural regulations, and not as a source of power to dictate electoral outcomes, to favor or disfavor a class of candidates, or to evade important constitutional restraints."[107] The Clause "gives [the] States authority [] to enact numerous requirements as to [the] procedure and safeguards" necessary to enforce the right to vote, and the "power to regulate the time, place, and manner of elections does not justify, without more, the abridgment of [this] right[]."[108] Hence, states are entitled to "adopt 'generally applicable and evenhanded restrictions that protect the integrity and reliability of the electoral process itself'" with an emphasis on the states' interest in "having orderly, fair, and honest elections," while Congress may introduce legislation to mandate a uniform medium to foster voting.[109]

III. FROM SUPREME COURT INVOLVEMENT, TO MILLION-DOLLAR INVESTIGATIONS, TO VIOLENCE: HOW BLOCKCHAIN TECHNOLOGY CAN ALLEVIATE VOTER DISTRUST, DIVISION, AND UNCERTAINTY

Whether one personally agrees with the recent questioning of election integrity, it is uncontested that the past two decades have demonstrated numerous claims of fraud percolating in the court system

---

103. Beckett, *supra* note 28, at 413-14, 425.
104. *See id.* at 425.
105. *See id.* at 426; *see infra* Part IV.
106. U.S. CONST. art. I, § 4, cl. 1.
107. U.S. Term Limits, Inc. v. Thornton, 514 U.S. 779, 833-34 (1995).
108. *Id.* at 834.
109. *See id.* at 834.

and media.[110] For a quintessential democratic right to be continuously questioned, and eighty percent of Americans demonstrating concerns, a change is more than deserved.[111] Subpart A will give an overview of the history of voter fraud allegations in the United States since 2000.[112] Subpart B will discuss the questions and concerns arising from the upcoming 2024 presidential election.[113] Lastly, Subpart C will demonstrate how blockchain technology can alleviate or prevent further questioning or allegations of election misconduct.[114]

A. The Uncertain History of United States Elections

The fact of the matter is that *all of the previous challenges concerning election outcomes have been mere allegations*.[115] So why is a change warranted if there has been no evidence of widespread fraud?[116] While some pundits have masqueraded the issue as the "sore-loser effect"[117] and others have characterized it as "[international] attack[s] on U.S. democracy[,]"[118] the underlying reality is that citizens will always

---

110. *See infra* Part III.A; *see also* Shepherd, *supra* note 6 (discussing election distrust after the January 6, 2021 attack on the United States Capitol).

111. *See* Shepherd, *supra* note 6.

112. *See infra* Part III.A; *see also* Jessica Reaves, *Counting the Lost Votes of Election 2000*, TIME (July 17, 2001), http://content.time.com/time/nation/article/0,8599,167906,00.html [https://perma.cc/3SEA-TAV3].

113. *See infra* Part III.B; *see also* Michael Waldman, *How Bad Could the 2024 Election Be?*, BRENNAN CTR. FOR JUST. (Feb. 1, 2022), https://www.brennancenter.org/our-work/analysis-opinion/how-bad-could-2024-election-be [https://perma.cc/ET9T-NFUV].

114. *See infra* Part III.C. *See generally* Alexander Daniels, *Blockchain & Shareholder Voting: A Hard Fork for 21st-Century Corporate Governance*, 21 U. PA. J. BUS. L. 405 (2018) (hypothesizing different phases of blockchain evolution in the realm of shareholder voting and how the benefits of a blockchain network will eventually replace the existing, traditional forms and mediums for shareholder voting in a manner that presents promising benefits and improvements).

115. *See* Daniel Funke, *Fact-Checking False Claims About the 2020 Election*, POLITIFACT (Nov. 19, 2020), https://www.politifact.com/article/2020/nov/20/fact-checking-false-claims-about-2020-election [https://perma.cc/5PF8-DNH4] (responding to over eighty misleading or false claims about voter fraud in the 2020 election, sixteen days after Election Day, or five false claims a day); *see also* Philip Bump, *The 2020 Election Was Neither Stolen Nor Rigged: A Primer*, WASH. POST: POL. (Sept. 15, 2022, 5:09 PM), https://www.washingtonpost.com/politics/2022/09/15/2020-election-trump-false-fraud-claims [https://perma.cc/FC6X-LZSU].

116. Bump, *supra* note 115 (explaining the lacking evidence behind claims of the 2020 presidential election being stolen, yet half of Republicans stating they have "no confidence at all that votes were cast legitimately and counted accurately").

117. James Piazza, *The 'Sore Loser Effect': Rejecting Election Results Can Destabilize Democracy and Drive Terrorism*, CONVERSATION (Sept. 7, 2022, 11:56 PM), https://theconversation.com/the-sore-loser-effect-rejecting-election-results-can-destabilize-democracy-and-drive-terrorism-171571 [https://perma.cc/WT7Q-WL8Z].

118. James Lamond, *The Origins of Russia's Broad Political Assault on the United States*, CTR. FOR AM. PROGRESS (Oct. 3, 2018), https://www.americanprogress.org/article/origins-russias-broad-political-assault-united-states [https://perma.cc/4W5L-YVYS].

be upset if their desired candidate does not win; it's the unfortunate nature of our two-party system.[119] However, constantly questioning the validity and integrity of our election system has generated dangerous consequences, such as Supreme Court involvement and national uncertainty,[120] $32 million of taxpayer money spent on investigations,[121] and the continual narrative of unproven election fraud[122] that resulted in violence and death.[123] These three consequences tell the story of how even *mere allegations* have led to more damaging results over time.[124] So, the question isn't why a change is warranted based off allegations: the question is, when is our breaking point?[125]

1. 2000 Election: Bush v. Gore

"Counting the Lost Votes of Election 2000."[126] The main issue involved in the 2000 presidential election was whether voting punch cards were counted by the card-reading machines.[127] One of the most prominent complaints was that the card-reading machines did not register punch holes that were incompletely compressed.[128] While a bulk of the attention was focused on Florida and the Supreme Court,[129] a study by social scientists at the Massachusetts Institute of Technology ("MIT") and the California Institute of Technology ("Caltech") found as many as four to six million votes were lost in the 2000 election due to voting machine issues, lost absentee votes, and improper voter

---

119. *See* PEW RSCH. CTR., PARTISANSHIP AND POLITICAL ANIMOSITY IN 2016: HIGHLY NEGATIVE VIEWS OF THE OPPOSING PARTY – AND ITS MEMBERS 1 (2016), https://www.pewresearch.org/politics/wp-content/uploads/sites/4/2016/06/06-22-16-Partisanship-and-animosity-release.pdf [https://perma.cc/9FS4-7PB5] (describing the animosity between voters of the Republican and Democrat party).

120. *See* Reaves, *supra* note 112.

121. Kevin Breuninger, *Robert Mueller's Russia Probe Cost Nearly $32 Million in Total, Justice Department Says*, CNBC: POL. (Aug. 2, 2019, 6:30 PM), https://www.cnbc.com/2019/08/02/robert-muellers-russia-probe-cost-nearly-32-million-in-total-doj.html [https://perma.cc/Y4QU-TQBL].

122. *See* Lindsay Wise & Andrew Duehren, *Woman Is Killed By Police; Members Evacuated*, WALL ST. J., Jan. 7, 2021, at A1; *see also* Funke, *supra* note 115.

123. *See* Wise, *supra* note 122, at A1; *see also* Gerald F. Seib, *Political Violence Shakes Country*, WALL ST. J., Jan. 7, 2021, at A1.

124. *See* Davenport, *supra* note 22.

125. *See id.*

126. Reaves, *supra* note 112.

127. *Id.*

128. *See id.*

129. *See* Bush v. Gore, 531 U.S. 98, 144 (2000) (Breyer, J., dissenting) ("The political implications of this case for the country are momentous.").

registration.[130] In 2001, Steve Ansolabehere, a political scientist at MIT, offered a new method of voting:

> In the long run, I think touch screen computing will be important. But for the moment, paper ballots do the best. This is something people are familiar with—unlike punch cards. I mean, where else in your life do you use punch cards? Nowhere. And we vote infrequently enough that punch cards are really strange to many of us; they can be really confusing.[131]

In 1999, at the time of the 2000 election, six different methods of voting were prevalent in the United States, including electronic machines, lever machines, paper ballots, optical scanners, punch cards, and other mixed systems.[132] While the 2001 MIT and Caltech study concludes that optical scanning, or the use of paper ballots in tandem with electronic machines, was the best means to conduct elections at the time, the study also proposed to, "[d]elay Internet voting until suitable criteria for security are put in place."[133] Indeed, the report stated that:

> First, there are concerns of coercion if Internet voting is done from remote locations, such as the voter's home computer. Second, large-scale fraud is more likely because it is easier to hack the entire system if it is on the Internet, than it is to coordinate many millions of voters voting at precincts or thousands of poll workers. Third, many people do not have computers at home or are sufficiently intimidated by computers that Internet voting (either from home or at the precinct) might create a further obstacle to voting for millions of voters.[134]

However, the report did conclude that "[i]nternet voting does hold immediate promise for lowering the obstacles experienced by some voters[,]" but July 2001 was not the time to implement such a change.[135] Twenty-two years later, a change is overdue, and blockchain technology can adequately address the concerns of the past.[136]

---

130. CALTECH/MIT VOTING TECH. PROJECT, VOTING: WHAT IS, WHAT COULD BE 8 (2001).
131. Reaves, *supra* note 112.
132. *See* CALTECH/MIT VOTING TECH. PROJECT, *supra* note 130, at 88.
133. *Id.* at 42.
134. *Id.* at 15-16.
135. *Id.* at 16.
136. *See* Moore & Sawhney, *supra* note 99, at 1.

2. 2016 Election: Trump v. Clinton

"U.S. Sanctions Russia Over Election Hacking; Moscow Threatens to Retaliate."[137] After several allegations of Russia meddling in the 2016 presidential election, the Senate Intelligence Committee conducted a $32 million investigation, and found:

> [T]he Russian Government conducted an unprecedented, coordinated cyber campaign against state election infrastructure. Russian actors scanned databases for vulnerabilities, attempted intrusions, and in a small number of cases successfully penetrated a voter registration database. This activity was part of a larger campaign to prepare to undermine confidence in the voting process. The Committee has not seen any evidence that vote tallies were manipulated or that voter registration information was deleted or modified.[138]

Thus, while the 2016 election focused mostly on voter interference in regard to email phishing attempts that degraded Democrat Nominee Hillary Clinton, these attacks still brought into question election infrastructure and the integrity of our vote, to the point where it cost millions of taxpayer dollars to determine whether any interference occurred after the fact.[139]

3. 2020 Election: Trump v. Biden

"MOB STORMS CAPITOL."[140] The numerous falsehoods about the 2020 presidential election have led to investigations costing roughly $519 million in taxpayer dollars, about sixteen times the amount spent on the 2016 election investigation.[141] But far worse than expenses, the January 6th attack on the Capitol cost the lives of seven individuals: one

---

137. Carol E. Lee & Paul Sonne, *U.S. Sanctions Russia Over Election Hacking; Moscow Threatens to Retaliate*, WALL ST. J., https://www.wsj.com/articles/u-s-punishes-russia-over-election-hacking-with-sanctions-1483039178 [https://perma.cc/SU9K-P88R] (Dec. 29, 2016, 8:42 PM).

138. *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations*, U.S. SENATE SELECT COMM. ON INTEL.: PUBL'NS (May 8, 2018), https://www.intelligence.senate.gov/publications/russia-inquiry [https://perma.cc/LK7Y-VXDB].

139. *See* Lee & Sonne, *supra* note 137.

140. *Mob Storms Capitol: Lawmakers Reject Voiding Two States' Votes After Pro-Trump Riot Disrupts Congress*, WALL ST. J., Jan. 7, 2021, at A1.

141. *See* Sarah Al-Arshani, *Trump's Attempts to Overturn the Election Have Cost Taxpayers More Than $519 Million So Far, Washington Post Finds*, BUS. INSIDER: POL. (Feb. 7, 2021, 3:05 AM), https://www.businessinsider.com/trumps-baseless-election-fraud-claim-cost-taxpayers-over-519-million-2021-2 [https://perma.cc/V9GC-29QB]; Breuninger, *supra* note 121 (calculating increase in spending by dividing $519 million (2020 election) by $32 million (2016 election) to get approximately sixteen).

fatally shot, one by heart attack, one by stroke, one being crushed to death by a stampede, one attacked by the mob, and two suicides following the attack.[142] All of these deaths could have been avoided, and while it is easy to say that January 6th would have never happened if everyone listened to the facts instead of following unreasonable beliefs, this position does not address the root cause of the issue: *how is it possible that thirty-five percent of Americans (about 115,990,000 people)*[143] *believe that the 2020 election was stolen after overwhelming evidence refutes such a claim?*[144]

B. Future Election Allegations: 2024 Presidential Election

"The next presidential election could trigger a constitutional crisis."[145] Following the tragedies of the 2020 presidential election, several pundits are confident that conversations regarding election fraud will resurface.[146] A holistic view of the past elections demonstrate common, underlying issues or concerns with our current election system: questions of security, concerns of vote tampering, and pleas for greater transparency.[147] In combination with previous election issues, record-low trust in election integrity, and the trend towards more violent, expensive, and continuing chaos surrounding election outcomes, the benefits of a blockchain network can help alleviate the pains that derive from the pitfalls that plague the United States election system.[148]

C. The Five Key Benefits of Blockchain Technology

Albeit complex, blockchains offer several benefits that can mitigate the apprehensions of our current election system.[149] Five benefits, such as (1) security, (2) anonymity, (3) time-stamped data, (4) immutability,

---

142. Chris Cameron, *These Are the People Who Died in Connection with the Capitol Riot*, N.Y. TIMES (Oct. 13, 2022), https://www.nytimes.com/2022/01/05/us/politics/jan-6-capitol-deaths.html [https://perma.cc/9WV7-UC7M].

143. Sarah Longwell, *Trump Supporters Explain Why They Believe the Big Lie*, ATL. (Apr. 18, 2022), https://www.theatlantic.com/ideas/archive/2022/04/trump-voters-big-lie-stolen-election/629572 [https://perma.cc/2L8Z-PCZC]. This number is an approximate value based on the 2020 census data finding a population of 331,449,281 people in the United States on April 1, 2020. *QuickFacts*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/US [https://perma.cc/BQ48-Y8BH] (last visited Dec. 2, 2023).

144. Longwell, *supra* note 143.

145. Waldman, *supra* note 113.

146. *See id.*

147. *See* Jane Susskind, Comment, *Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System*, 54 SAN DIEGO L. REV. 785, 794-95 (2017).

148. *See supra* Part III.A; *see also infra* Part III.C.

149. *See infra* Part IV.C; *see also* Evans, *supra* note 2.

and (5) transparency, represent a few important features that a blockchain network can provide to modernize the current election system.[150]

1. Security

A blockchain provides a trustless environment that is not controlled by a central authority.[151] In the example from Part II.A using a bank, both users must trust a single entity, the bank, to store and transfer their money.[152] Contrast this with a blockchain, where transactions are verified by an entire network composed of several entities.[153] This means that one would need to control more than fifty percent of the computers on the network to commit fraud, rather than attack a single point of control.[154] Though theoretically possible, control over the network in this manner is economically infeasible when considering the resources required.[155]

Aside from the structure of the network, there are two important cryptographic concepts that work in the background to provide robust protection: hashing and cryptographic signatures.[156] To recap, hashing, as part of the consensus mechanism, provides a means for everyone on the blockchain to agree on proposed and current blocks.[157] Hashing involves input data and a hash function to produce an output,[158] with input data of any size returning an output of equal size based on the hash function.[159] Blockchains like Bitcoin use SHA-256, which takes any size input and converts it into a 256-bit string.[160] The hash function must be

---

150. *See* Evans, *supra* note 2; Jafar et al., *supra* note 35, at 2.

151. *See* Nakamoto, *supra* note 40, at 2.

152. Steven Young, *Changing Governance Models by Applying Blockchain Computing*, 26 CATH. U. J.L. & TECH. 53, 54 (2018); *see supra* Part II.A.2.

153. Young, *supra* note 152, at 54.

154. Mcshane, *supra* note 72.

155. *See id.*

156. *See* JEFF REED, BLOCKCHAIN 21-23 (2016) (formulating the basic building blocks to implement a blockchain network—that being, digital encryption verified by signatures and hash functions that make transactions nearly impossible to change).

157. *See Explained: What Is Hashing in Blockchain?*, BYBIT LEARN (Dec. 17, 2020), https://learn.bybit.com/blockchain/what-is-hashing-in-blockchain [https://perma.cc/BCB7-99FH].

158. *See What Is a Hash Function in a Blockchain Transaction?*, BITPANDA [hereinafter BITPANDA], https://www.bitpanda.com/academy/en/lessons/what-is-a-hash-function-in-a-blockchain-transaction [https://perma.cc/YB4N-C3HW] (last visited Dec. 2, 2023).

159. *See* @ritesh_nehru, *Blockchain Hash Function*, GEEKSFORGEEKS, https://www.geeksforgeeks.org/blockchain-hash-function [https://perma.cc/8Y5B-KJMW] (Oct. 13, 2022).

160. *See* Ameer Rosic, *What Is Hashing? [Step-by-Step Guide-Under Hood of Blockchain]*, BLOCKGEEKS, https://blockgeeks.com/guides/what-is-hashing [https://perma.cc/4JY8-XFPD] (May 4, 2020).

deterministic, which means that the same input will give you the same output every time.[161] Thus, hashing allows the network to fingerprint the data to ensure that no one has tampered with the transaction prior to being received.[162]

Not only is the entire network secure, but each transaction is secure through digital signatures, which consist of a user's public and private key.[163] The input data typically includes a user's public key, previous hash data, and transaction data.[164] A public key is a string of letters and numbers that is made public for anyone to use, while the private key is a secret string of letters and numbers that would serve as the user's "password."[165] Put another way, public and private keys are analogous to physical keys with a universal lock.[166] The only difference is that the public key may only be used to close the lock, while the private key may only be used to open the lock.[167] This dynamic results in the public key encrypting the transaction data with the private key decrypting the transaction data.[168] Hence, when sending transactions over a blockchain network, the public key is used to encrypt the transaction data that *only*

161. *See* REED, *supra* note 156, at 23. This concept is important not only for security but also when mining or validating blocks and placing them on the blockchain. *See* BITPANDA, *supra* note 158. If the hash is not deterministic, it will not reveal the proper block number, time and date of signing, or the contents within the block. *See id.*

162. *See* REED, *supra* note 156, at 21, 23.

163. *See* DIEDRICH, *supra* note 28, at 104.

164. *See* Cryptopedia Staff, *What Are Public and Private Keys?*, CRYPTOPEDIA, https://www.gemini.com/cryptopedia/public-private-keys-cryptography [https://perma.cc/WYV3-HPFS] (June 28, 2022). The three steps in a transaction include: (1) encryption with a public key; (2) signature using the private key, which proves the transaction has not been modified; and (3) verification of the transaction data. *Id.*

165. *See* Benedict George, *A Crypto Must-Know: Public vs. Private Keys*, COINDESK, https://www.coindesk.com/learn/a-crypto-must-know-public-vs-private-keys [https://perma.cc/G858-ST6W] (Aug. 5, 2022, 4:09 PM).

166. *See* Kirsty Moreland, *What Are Public Keys and Private Keys?*, LEDGER ACAD. (Feb. 15, 2023), https://www.ledger.com/academy/blockchain/what-are-public-keys-and-private-keys [https://perma.cc/D4RQ-B52D].

167. *See* Ayushi Abrol, *Private Key Vs Public Key – How They Work?*, BLOCKCHAIN COUNCIL (July 27, 2022), https://www.blockchain-council.org/blockchain/private-key-vs-public-key [https://perma.cc/TX55-CAQ4]. The function of public and private keys work as two distinct keys: the public key is used to encrypt the data and the private key is used to decrypt the data. *Id.*

168. *See What Is a Private Key?*, KRIPTOMAT: BLOCKCHAIN, https://kriptomat.io/blockchain/what-is-a-private-key [https://perma.cc/HFX9-GXYZ] (last visited Dec. 2, 2023).

the specific private key can decrypt.[169] Without knowing another's private key, there is no means to decrypt another's transaction.[170]

The manner in which we currently cast ballots is very similar to the method of digitally signing on the blockchain.[171] A registered voter will appear at the polling place, where the poll worker will ask for their signature.[172] If a signature is incorrect, the poll worker will flag this as potential fraud.[173] If the signature is sufficient, the voter receives a ballot and places the ballot into a machine that will read and tally the vote.[174] With public and private keys, the proposed solution suggests changes mostly to the median in which votes are cast.[175]

2. Anonymity

A blockchain's anonymity stems from the use of encryption in the form of digital signatures that derive from the interaction between public and private keys.[176] Secret messages can be sent by a digital signature that allow for minimal oversight, since the public ledger will only display the user's public key,[177] rather than any personal information.[178] This makes it very difficult to determine who was involved in the transaction without knowing any other information.[179]

Such a system is defined as "asymmetric encryption," which can be analogized to a voicemail inbox: anyone in the public can access and leave a voicemail for the owner of the phone number, but only the owner

---

169. *See What Are Public and Private Keys and How Do They Work?*, BLOCKCHAIN.COM, https://support.blockchain.com/hc/en-us/articles/4417082520724-what-are-public-and-private-keys-and-how-do-they-work [https://perma.cc/899S-3CQS] (last visited Dec. 2, 2023).

170. *See What Are Public and Private Keys in Crypto?*, BLOCKCHAIN.COM, https://support.blockchain.com/hc/en-us/articles/360000951966-What-are-public-and-private-keys-in-crypto- [https://perma.cc/6W4K-ZABQ] (last visited Dec. 2, 2023).

171. *See* Young, *supra* note 152, at 68 (describing the use of digital signatures for governance).

172. *See Election Security Rumor v. Reality*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/rumorcontrol [https://perma.cc/BKS3-2MMV] (last visited Dec. 2, 2023).

173. *See How Do Election Workers Match Signatures? (2020)*, BALLOTPEDIA, https://ballotpedia.org/how_do_election_workers_match_signatures%3F_(2020) [https://perma.cc/QG8E-JR7B] (last visited Dec. 2, 2023); *see also* Sophie Bushwick, *An Expert on Voting Machines Explains How They Work*, SCI. AM. (Nov. 3, 2020), https://www.scientificamerican.com/article/an-expert-on-voting-machines-explains-how-they-work [https://perma.cc/ES85-V6HM].

174. *See* Bushwick, *supra* note 173.

175. *See* Young, *supra* note 152, at 68.

176. *See* Nakamoto, *supra* note 40, at 2.

177. *See id.*

178. *See How Private Is the Blockchain?*, BITSTAMP (Aug. 10, 2022), https://www.bitstamp.net/learn/security/how-private-is-blockchain [https://perma.cc/L5G9-Y6M9].

179. *See id.*

of the number has the ability to unlock the voicemail box to listen to the messages left for him.[180] In other words, while you may know who owns the phone number, there is no possible way for you to derive the contents of the voicemail just by having the phone number.[181] The only possible way for this to happen would be for the user to tell you the contents of the conversation.[182] So, translated into the blockchain, user A would share their public key with user B.[183] User B would use user A's public key to encrypt the message to be sent, and user A will be allowed to unlock this message with his private key.[184] Additionally, public keys have the ability to change over time or expire with each transaction, giving another layer of protection to ensure secrecy.[185]

3. Time-Stamped Data

Data on the blockchain includes a timestamp to demonstrate when such a transaction occurred.[186] While the importance of a timestamp may seem benign, timestamps allow for robust security and immutability as

180. *See* Cryptopedia Staff, *What Is Asymmetric Encryption?*, CRYPTOPEDIA, https://www.gemini.com/cryptopedia/symmetric-vs-asymmetric-encryption [https://perma.cc/32T5-E72V] (June 22, 2021); REED, *supra* note 156, at 21-22; Benjamin P., *Asymmetric Encryption*, MEDIUM (Dec. 22, 2017), https://medium.com/@benameji/mailbox-encryption-7687e0574164 [https://perma.cc/Z9TZ-B7PC]. The "public key" would be akin to a phone number, with the "private key" as the password to provide a digital signature. *See* REED, *supra* note 156, at 21-22. Anybody can call the phone number, but only the holder of the password can access the voicemail. *See id.* While the fact that a voicemail is sent to a particular phone number would be visible on the blockchain, the contents of the voicemail itself, that being, its data, are encrypted and can only be decrypted by use of the password. *See id.*

181. *See id.* at 22.

182. *See* Everything Blockchain, *The Basics of Blockchain Privacy: How to Remain Anonymous on the Blockchain*, MEDIUM: COINMONKS (Aug. 3, 2022), https://medium.com/coinmonks/the-basics-of-blockchain-privacy-how-to-remain-anonymous-on-the-blockchain-3f1cef44ad63 [https://perma.cc/UBF5-5EVN] (enumerating numerous actions a user may take to maintain anonymity).

183. *See* Toshendra Kumar Sharma, *How Is Blockchain Verifiable by Public and Yet Anonymous?*, BLOCKCHAIN COUNCIL (July 11, 2018), https://www.blockchain-council.org/blockchain/how-is-blockchain-verifiable-by-public-and-yet-anonymous [https://perma.cc/35CB-6EG4].

184. *See How Anonymous Is Cryptocurrency?*, ACUANT (Dec. 9, 2020), https://www.acuant.com/blog/how-anonymous-is-cryptocurrency [https://perma.cc/WU36-K6BB]. The "pseudonym" here is in reference to a user's public key which yields no identifying information on its face. *See id.*; *see also* Abrol, *supra* note 167.

185. *See How Anonymous Is Cryptocurrency?*, *supra* note 184 ("As an additional firewall, a new (address) should be used for each transaction to keep them from being linked to a common owner . . . .").

186. *See* Nakamoto, *supra* note 40, at 2.

time is an important input when creating a successive list of blocks on the chain.[187]

4. Immutability

Blockchains are also immutable: altering a transaction would require changing the hash of all the blocks on the chain with consent of the network.[188] As stated before in Section 1,[189] input data includes the hash of the previous block, as well as the transaction data and the user's public key.[190] As an example, take three blocks with the following vote data:

Genesis Block	Block Two	Block Three
Hash: 4jf9d8 Transaction: cda83r sends R vote to USAUSA Previous-Hash: 000000	Hash: f9d02j Transaction: 6f5sd1 sends D vote to USAUSA Previous-Hash: 4jf9d8	Hash: 9gdal Transaction: 9540sa sends I vote to USAUSA Previous-Hash: f9d02j

The first string of six letters and numbers in the "Transaction" denotes the voter's public key, and the "USAUSA" string denotes the government's public key.[191] Suppose that someone wished to change the vote of Block Two to change the transaction of "D vote" to "R vote." The change is reflected as follows, with the italicized and bolded text indicating the changes:

Genesis Block	Block Two	Block Three
Hash: 4jf9d8 Transaction: cda83r sends R vote to USAUSA Previous-Hash: 000000	Hash: *kfod01* Transaction: 6f5sd1 sends *R* vote to USAUSA Previous-Hash: 4jf9d8	Hash: *z4fs3r* Transaction: 9540sa sends I vote to USAUSA Previous-Hash: *f9d02j*

187. *See Blockchain-Based Timestamping: The Complete Guide for Beginners*, LIFEHASH, https://www.lifehash.com/post/blockchain-based-timestamping-the-complete-guide-for-beginners [https://perma.cc/K9LW-FAAV] (last visited Dec. 2, 2023).

188. *See* Nakamoto, *supra* note 40, at 2.

189. *See supra* Part III.C.1.

190. *See* DIEDRICH, *supra* note 28, at 104-05.

191. *See generally* Young, *supra* note 152, at 71, 76-77 (discussing individualized tokens and government tokens used in governance).

Changing anything within the transaction will alter the hash of the current block, thus altering the hash of the next block, and so on.[192] This is because a block's hash is deterministic from (1) the transaction data, and (2) the previous hash.[193] Thus, any change will ripple throughout the network.[194] If the network notices such a disturbance, the change will not be registered, and, assuming a proof-of-stake protocol is used, the person who sought to verify such a transaction will lose some or all of their stake.[195]

So, not only must a potential hacker alter numerous blocks to tamper the system, they must convince 51% of the network that such a change is correct; this is known as a "51% attack,"[196] the success and practicality of which is dependent on whether a blockchain utilizes a proof-of-work or a proof-of-stake consensus algorithm.[197] A 51% attack on a proof-of-work blockchain will require 51% of the *computing power* on the blockchain, which during blockchain's inception, was quite infeasible.[198] However, the prevalence of mining pools, or conglomerates of people joining together to combine network power, has allowed groups of miners to inch closer to the 51% mark.[199] Using the proof-of-stake protocol, performing a 51% attack becomes much more infeasible, and practically impossible.[200] Instead of garnering 51% of the computing power on the network, one would need to attain 51% of the *staked currency* on the blockchain.[201] Additionally, staked currency acts as a collateral on the network, thus any attempt to alter a transaction through a 51% attack could backfire and cause one to lose their entire stake.[202] This creates the monetary incentive to provide network security in good faith, where any foul play becomes too costly to benefit from.[203]

---

192. *See* REED, *supra* note 156, at 23.
193. *See id.*
194. *See id.*
195. *See id.*
196. *See* Laura M., *supra* note 48.
197. *See id.*
198. *See id.*
199. *See id.*
200. *See id.*
201. *See* Murtuza Merchant, *What Is a 51% Attack and How to Detect It?*, COINTELEGRAPH (Nov. 12, 2022), https://cointelegraph.com/news/what-is-a-51-attack-and-how-to-detect-it [https://perma.cc/MWF5-HH5D].
202. *See id.*
203. *See id.*

5. Transparency

Lastly, blockchains allow for a transparent record of every transaction that has occurred.[204] In reference to the chart above in Section 4, such a display would represent the public view of all participants in the election, through a display of public keys and associated votes.[205] It should be noted that this feature is closely linked to the anonymous nature of the blockchain,[206] and that only transactions, rather than "state" data, are shown.[207] Using the bank account example, an investigation into someone's public key will not show how much money the user has in their wallet, i.e., the state data, but will only show their transactions.[208] Of course, one may calculate how much money is in an account by searching for every single transaction that has been completed, but this becomes impractical once a certain number of transactions have been registered, or a public key has changed.[209] Regardless, considering that the only transaction on a voting blockchain would be a transfer of a ballot, and there is only one ballot per public key that would change annually, this issue becomes irrelevant.[210]

IV. IMPLEMENTING THE BLOCKCHAIN AND THE GLOBAL DOMINO EFFECT

Given the myriad of benefits provided by blockchain technology and the concerns with the current voting system in place, the United States Congress must act to adopt a blockchain voting system for future elections.[211] Admittedly, this solution will not occur overnight: years of testing and investment are required to perfect the system so it may not relapse to the pitfalls of the current system.[212] Additionally, to ensure the network is as robust as citizens deserve, implementation on a global level is pivotal for the future of global democracy to provide all citizens

---

204. Linda Orenes-Lerma, *How Does a Blockchain Transaction Work?*, LEDGER ACAD. (Oct. 25, 2022), https://www.ledger.com/academy/how-does-a-blockchain-transaction-work [https://perma.cc/LKL8-QS2N].

205. *See* REED, *supra* note 156, at 23 (describing the data that is visible on the blockchain and how "visible" such data is); *supra* Part III.C.4.

206. *See* REED, *supra* note 156, at 23.

207. *See* DIEDRICH, *supra* note 28, at 94.

208. *See id.* at 95.

209. *See id.*

210. *See id.*

211. Brianna Bogucki, *Buying Votes in the 21st Century: The Potential Use of Bitcoins and Blockchain Technology in Electronic Voting Reform*, 17 ASPER REV. INT'L BUS. & TRADE L. 59, 66-68, 70 (2017).

212. *See* Moore & Sawhney, *supra* note 99, at 1.

a transparent means to exercise their rights.[213] Subpart A will provide a brief, mechanical overview of the current federal election system.[214] Subpart B will propose a blockchain voting system to be researched and implemented over the next decade, with Subpart C illustrating the characteristics of the proposed system.[215] Thereafter, Subpart D will discuss the benefits of all nations implementing a blockchain network to conduct elections, with Subpart E addressing the critics who may challenge the change proposed within this Note.[216]

A. The Current United States Federal Election System

Methods of ballot marking and tabulation vary in the United States, with no uniform procedure in place: some jurisdictions use electronic devices and more modern technology, while others continue to rely on paper.[217] As of 2020, three types of voting equipment have been used in the United States: Optical Scan Paper Ballot Systems, where voters "mark their votes by filling in an oval, box, or similar shape on a paper ballot" which is "scanned . . . at the polling place"; Direct Recording Electronic Systems, where "computers . . . record votes directly into the computers' memory" through a digital interface with an option for Voter-Verified Paper Audit Trail printers to produce "paper records . . . [to] be preserved . . . [for] tabulat[ion] in [the] case of an audit or recount"; and Ballot-Marking Devices and Systems, which allow for the "electronic presentation of a ballot, electronic selection of valid contest options, and the production of a human-readable paper ballot" that makes no listings other than the voter's selections.[218] Most states use a combination of one or more of the available technologies, and every state incorporates mail-in ballots for early and absentee

---

213. *See* Beckett, *supra* note 28, at 427 (detailing how adoption of blockchain initiatives on a national level could provide greater benefits).

214. *See infra* Part IV.A.

215. *See infra* Part IV.B–C; *see also* Moore & Sawhney, *supra* note 99, at 2 (illustrating the mobile voting process used in West Virginia).

216. *See infra* Part IV.D–E; *see also* Beckett, *supra* note 28, at 427 (detailing how nationwide adoption could provide numerous benefits when compared to adoption by just one state).

217. *Voting Methods and Equipment by State*, BALLOTPEDIA, https://ballotpedia.org/Voting_methods_and_equipment_by_state [https://perma.cc/GHM8-TPEE] (last visited Dec. 2, 2023).

218. *Id.*

voters,[219] but differ on when processing and counting the mail-in votes begin.[220]

The United States' poor ranking amongst Western democracies in regard to electoral integrity,[221] and the downgrade from a "high electoral integrity" score to a "moderate electoral integrity" score between 2016 and 2022[222] is due, in part, to many of the existing voting machines purchased following the Helping America Vote Act of 2002 that have "never [been] subsequently overhauled or replaced."[223] This aging equipment and outdated software, in combination with the lack of sophisticated security, allow these machines to become particularly vulnerable to external cyberattacks by foreign, domestic, or terrorist groups.[224] However, one of the touted benefits of the current election system that prevents complete collapse is the "decentralized nature of [the United States] electoral administration" where security is maintained by 8,000 jurisdictions, "limiting the penetration" efforts by attackers who seek to manipulate the entire system.[225] However, even this major benefit falls short, since even a "minor security breach[]" may reduce the credibility of American elections and trigger doubts about the legitimacy of the eventual winner.[226]

B. The Election Revitalization Act of 2023

The Election Revitalization Act is this Note's proposed piece of legislation to introduce blockchain technology into federal elections.[227] Given Congress's broad authority under the Elections Clause, the bill would detail important procedure and the technological structures of a blockchain voting system.[228] The proposed bill is featured below,

---

219. *Table 16: When Absentee/Mail Ballot Processing and Counting Can Begin*, NAT'L CONF. STATE LEGISLATURES, https://www.ncsl.org/research/elections-and-campaigns/vopp-table-16-when-absentee-mail-ballot-processing-and-counting-can-begin.aspx [https://perma.cc/JR3G-HVV9] (Jan. 18, 2023).

220. *Id.* (providing a table of each state and their respective allowable times to process and count ballots).

221. NORRIS, *supra* note 7, at 2, 18-20.

222. *Compare* NORRIS, *supra* note 7, at 31 (recording the United States with a PEI score of sixty-two in 2016), *with* Garnett et al., *2022 Perceptions of Electoral Integrity*, *supra* note 9 (recording the United States with a PEI score of 58.78 in 2022). A PEI score below sixty indicates "moderate electoral integrity." NORRIS, *supra* note 7, at 30.

223. NORRIS, *supra* note 7, at 15-16.

224. *Id.*

225. *Id.* at 16.

226. *Id.*

227. *See infra* Part IV.B–C. Part IV.B presents the language of a proposed bill, and Part IV.C gives greater detail into the language of the proposed bill. *See infra* Part IV.B–C.

228. *See* U.S. CONST. art. I, § 4, cl. 1.

however it should be noted that the proposed bill is underinclusive to ensure brevity of this Note:

A BILL

To modernize the nation's election systems for Federal elections, by establishing a United States Decentralized Autonomous Organization ("USDAO") for the purposes of hosting, operating, and maintaining federal elections, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE. This Act may be cited as the "Election Revitalization Act of 2023."

SECTION 2. FINDINGS AND PURPOSE.
(a) Findings. – The Congress finds that –[229]

(1) the right of citizens of the United States to vote is a fundamental right;[230]
(2) it is the duty of the Federal, State, and local governments to promote the exercise of that right;[231]
(3) Congress has explicit authority to regulate the time, place, and manner of Federal elections under the Elections Clause, by establishing standards for impartial and uniform administration of Federal elections;[232]
(4) the Elections Clause grants Congress a plenary right to preempt State regulation. This grant of congressional authority was meant to "insure free and fair elections," promote the uniform administration of Federal elections, and "preserve and restore to the people their equal and sacred rights of election";[233]
(5) the Elections Clause grants Congress broad authority over Federal elections to check any "abuses that might be made of the discretionary power" to regulate the time, place, and manner of elections granted the States. As the Supreme Court has recognized, the Elections Clause empowers Congress to "protect the elections on which its existence depends";

229. Substantial portions of this Note's proposed bill, "The Election Revitalization Act of 2023," specifically Section 2(a), took inspiration from, and replicated in some instances, the following House and Senate bills: National Voter Registration Act of 1993, Pub. L. No. 103-31, § 2, 107 Stat. 76, 77 (codified as amended at 52 U.S.C. §§ 20501–20511); Help America Vote Act of 2002, Pub. L. No. 107-252, § 101, 116 Stat. 1666 (codified as amended at 52 U.S.C. §§ 20901–21145); Freedom to Vote Act, S. 2747, 117th Cong. § 3001 (2021).

230. § 2(a)(1), 107 Stat. at 77.

231. *Id.* § 2(a)(2), 107 Stat. at 77.

232. S. 2747, § 3001(a)(1); *see* U.S. CONST. art. 1, § 4, cl. 1.

233. S. 2747, § 3001(a)(2); *see* U.S. CONST. art. 1, § 4, cl. 1.

(6) the Elections Clause grants Congress "plenary and paramount jurisdiction over the whole subject" of Federal elections, and the authority to compel States to alter their regulations even if these alterations would impose additional costs on the States to execute or enforce;[234]
(7) the Elections Clause grants Congress the ultimate authority to ensure "equitable and uniform administration" of Federal elections;[235]
(8) a blockchain-based election system comprised of a decentralized autonomous organization of local election boards provides the needed security, anonymity, and immutability required for an election system.

(b) Purposes. – The purposes of this Act are –

(1) to establish procedures that will modernize the national systems for Federal elections;[236]
(2) to restore the trust and integrity of the electoral process in a manner that provides enhanced security, maintains anonymity, establishes time-stamped data, ensures immutability, and increases transparency;[237]
(3) to make it possible for Federal, State, and local governments to implement this Act in a manner that enhances the participation of eligible citizens as voters in elections for Federal office;[238]
(4) to protect and enhance the integrity of the electoral process;[239] and
(5) to ensure that accurate and current voter registration rolls are maintained and modernized.[240]

SECTION 3. DEFINITIONS.
As used in this Act –

(a) the term "Election" has the meaning stated in section 301(1) of the Federal Election Campaign Act of 1971;[241]

---

234. S. 2747, § 3001(a)(3)–(4); *see* Ass'n Cmty. Org. for Reform Now v. Miller, 129 F.3d 833, 837 (6th Cir. 1997).
235. S. 2747, § 3001(a)(13); *see* U.S. CONST. art. 1, § 4, cl. 1.
236. *See* § 2(b)(1), 107 Stat. at 77 (detailing the purpose of the article, namely, to establish procedures to increase voter turnout).
237. *See id.* § 2(b)(3)–(4), 107 Stat. at 77 (detailing the purpose of the article, namely, to protect the integrity of the electoral process and ensure accuracy in voter registration logs).
238. *Id.* § 2(b)(2), 107 Stat. at 77.
239. *See id.* § 2(b)(3)–(4), 107 Stat. at 77.
240. *Id.* § 2(b)(4), 107 Stat. at 77.
241. *See* 2 U.S.C. § 431(1) (2017); *see also* § 3(1), 107 Stat. at 77.

(b) the term "Federal office" has the meaning stated in section 301(3) of the Federal Election Campaign Act of 1971;[242]
(c) the term "Voter" means a citizen qualified to vote pursuant to Amendment XXVI of the Constitution and the appropriate Congressional legislation;[243]
(d) the term "State" means a State of the United States and the District of Columbia;[244] and
(e) the term "USDAO" means United States Decentralized Autonomous Organization.

SECTION 4. FEDERAL, STATE, AND LOCAL GOVERNMENT PROCEDURES AND ENHANCEMENTS TO NATIONAL ELECTION SYSTEMS FOR FEDERAL ELECTIONS.
(a) In General. – Notwithstanding any other Federal or State law, each State shall establish, with given monies allocated by Congress, Federal election systems within each county board of elections capable of transacting data on a blockchain network, pursuant to the guidance granted by the Office of Science and Technology Policy.[245]
(b) Pre-Election and Election Day Procedure. – Notwithstanding any other Federal or State law[246]:

(1) each State shall issue to each Voter:

(i) a public key, set to expire upon casting a vote or after the Election, whichever is sooner; and
(ii) a private key, stored on a decentralized wallet owned and operated by the USDAO, including an e-ballot token at least one month prior to Election Day of that given year.

(2) each State shall receive a particular amount of monies from Congress based on the proportion of electoral votes that a State has, that is subject to:

(i) a locking period governed by the USDAO; and
(ii) several conditional security and blockchain maintenance requirements set by the Office of Science and Technology Policy, including but not limited to:

---

242. 2 U.S.C. § 431(3); § 3(2), 107 Stat. at 77.
243. *See* U.S. CONST. amend. XXVI; *see also* 52 U.S.C. § 10101(a)(1) (Supp. IV 2012).
244. 52 U.S.C. § 20502(4).
245. *See* Help America Vote Act of 2002, Pub. L. No. 107-252, § 101(b)(1)(A)–(F), 116 Stat. 1666, 1669 (codified as amended at 52 U.S.C. §§ 20901–21145) (detailing how states may use the funds provided to carry out, *inter alia*, improvements to voting systems).
246. *See id.* § 303(a)(1), 116 Stat. at 1708 (delegating pre-Election Day and Election Day duties to state officials to ensure conformity with the law).

a. active validation of e-ballots;
b. proper and correct validation of e-ballots; and
c. proper and correct review of previously validated e-ballots,

the violation of which is subject to the penalties listed in subsection (d).

(c) Post-Election Day Procedure. – No board of elections may execute a transaction after the end time mandated by State law on Election Day, or after 10:00 PM local time, whichever is latest on Election Day. After such time, each board of elections must download and save all transactions committed and validated from the first e-ballot received.[247]
(d) Penalties. – Any violation of the above will subject the State to deductions from the staked amount on the network, in proportion with any programmed variables set by the Office of Science and Technology Policy. The State is subject to such penalties at any time once the Election has commenced, until completion of electoral review.[248]

SECTION 5. VOTER, STATE, AND LOCAL GOVERNMENT PROCEDURES AND ENHANCEMENTS TO NATIONAL ELECTION SYSTEMS FOR FEDERAL ELECTIONS.
(a) In General. – Notwithstanding any other Federal or State law, in addition to any other method of voter registration provided for under State law, each State shall establish procedures to register to vote in Elections for Federal office. Upon lawful registration, each Voter shall receive from their county election board[249]:

(1) a public key, set to expire upon casting a vote or after the election, whichever is sooner; and
(2) a private key, stored on a decentralized wallet owned and operated by the USDAO, including an e-ballot token.

247. *See id.* §§ 241, 245, 302, 116 Stat. at 1686-87, 1690, 1708 (mandating studies and reports regarding the implementation of new voting measures, establishing a time when polls close, and general procedures regarding each).
248. *See id.* § 904, 116 Stat. at 1729 (detailing penalties generally in depriving voters of a fair election).
249. *See id.* §§ 241, 245, 302, 702, 116 Stat. at 1686-87, 1690, 1708-09, 1723 (detailing voter registration procedures and information regarding voting remotely).

(b) Pre-Election Day Procedure. – Notwithstanding any other Federal or State law[250]:

(1) each Voter will receive their public and private key at least one month prior to Election Day of that given year; and

(i) may fill out and complete an e-ballot; and
(ii) cast an e-ballot

at any time up until the time specified in subsection (d).

(c) Election Day Procedure. – Notwithstanding any other Federal or State law[251]:

(1) each Voter may cast their e-ballot token using a personal cellular device, computer, or other technology capable of connecting to the USDAO network; or

(2) if a Voter:

(i) does not have access to a phone, computer, or other device connected to the network; or
(ii) does not know how to access the network from their phone, computer, or other device

this Voter may report to a designated voting area to cast an e-ballot, through either their own personal device at the location, or through an established State-provided device.

(d) Post-Election Day Procedure. – No Voter shall cast an e-ballot at any time past the given end time mandated by State law on Election Day, or after 10:00 PM local time, whichever is latest on Election Day.[252]
(e) Penalties. – Any violation of the above will subject the Voter to penalties previously established by law. The Voter is subject to such penalties at any time once the Election has commenced, until completion of electoral review.[253]

---

250. *See id.* § 303(a)(1), 116 Stat. at 1708-09 (delegating pre-Election Day duties to state officials to ensure conformity with the law).
251. *See id.* (delegating Election Day duties to state officials to ensure conformity with the law).
252. *See id.* § 302(c), 116 Stat. at 1708 (establishing procedures for when polls close).
253. *See id.* § 904(a), 116 Stat. at 1729 (detailing penalties generally in depriving voters of a fair election).

C. Characteristics of a United States Voting Blockchain

1. General Overview

At a broad level, the blockchain voting system will consist of a private blockchain with each county election board serving as a validator.[254] Each election board is responsible for verifying random "e-ballots" on the network.[255] The e-ballots received may come from any state, and all e-ballots will be encrypted on arrival, making it impossible to guess the candidate selected, the name of the voter, or the state of origin.[256] To delegate the e-ballots, the blockchain will implement a proof-of-stake consensus protocol, rather than a proof-of-work protocol to avoid the toll on the environment and the massive electrical expense.[257] Once an e-ballot has been received and verified by both the designated board and the network, the e-ballot will be "cast" on the blockchain network, with a running total of votes for each candidate updated live, sorted by state, county, and more.[258]

2. How Are Votes Delegated?

Looking further in depth, the proof-of-stake consensus system will work as follows: Congress, pursuant to its Spending Power, will grant each state a particular amount of funds based on the proportion of electoral votes that a state has, with a condition tied to the funds.[259] For example, suppose Congress set aside $1 billion[260] to be divided amongst the states for complying with a new, federally regulated election system.[261] If New York opts in, with twenty-eight electoral votes,[262] it

254. *See generally* Moore & Sawhney, *supra* note 99, at 2 (detailing the West Virginia blockchain voting process).

255. *See id.*

256. *See* Beckett, *supra* note 28, at 431.

257. *See id.*; Laura M., *supra* note 48.

258. *See* Beckett, *supra* note 28, at 430, 432.

259. *See* Rachel Orey et al., *The Path of Federal Election Funding*, BIPARTISAN POL'Y CTR. (June 16, 2022), https://bipartisanpolicy.org/explainer/federal-election-funding-path [https://perma.cc/B677-Y3J7] (detailing the process of Congress appropriating federal funds to the states).

260. *Id.* ("Congress has appropriated nearly $5 billion to support state election efforts since 2003.").

261. *Id.* ("Election officials use federal election dollars to upgrade voting systems, maintain voter registration databases, provide provisional and convenience voting options, train election officials and poll workers, and bolster election administration infrastructure across the country.").

262. *See Distribution of Electoral Votes*, NAT'L ARCHIVES, https://www.archives.gov/electoral-college/allocation [https://perma.cc/36ZA-CMPL] (last visited Dec. 2, 2023). The United States has 538 electoral votes in total. *Id.* Hence, New York has 28/538 electoral votes, or 5.2% of the total number of electoral votes. *See id.*

will have an opportunity to receive a maximum of 5.2%, or $52,000,000 of the federal funds reserved to support the state's election efforts.[263] The funds will be given to the state immediately to be used as "stake" on the blockchain network.[264]

After the election, each state will have the opportunity to withdraw all funds staked if voting verification is successful.[265] On the other hand, any flags or fraud tracked by the rest of the network has the potential to strip a proportion of the stake, thereby allowing the state to collect fewer funds at the end of the election cycle.[266] Hence, not only will proof-of-stake give the states an incentive to diligently monitor the network and verification process, but it will place the state's taxpayers on notice regarding whether officials are tampering with the election and wasting tax money.[267]

Proof-of-stake also gives states with a greater number of electoral votes more opportunities to verify transactions.[268] This is because states with greater electoral votes will have more funds designated as stake, which will increase the likelihood that the network will select that state to verify a random e-ballot.[269] This system is analogous to a raffle where one may purchase multiple tickets: the more tickets you have, the better the chance of winning.[270] Keep in mind, however, if a state continues to

---

263. *See id.* Taking 5.2% of the $1 billion dollar budget equates to $52,000,000. *See id.*

264. *See generally* DIEDRICH, *supra* note 28, at 152-53 (detailing the mechanisms of a proof-of-stake network).

265. *See id.* at 153.

266. *See id.*

267. *See* Roberto de Isidro et al., *Proof of Work vs. Proof of Stake: Why Their Differences Matter*, GLOB. X BY MIRAE ASSET (Oct. 5, 2022), https://www.globalxetfs.com/proof-of-work-vs-proof-of-stake-why-their-differences-matter [https://perma.cc/TK9K-QPAK] (describing how proof-of-stake is easier to recover upon an attack when compared to proof-of-work since it is possible to fork the chain and slash the attacker along with the initial large cost of ushering an attack). Considering the large amount of assets and the quick ability to recover, proof-of-stake offers the best option for putting taxpayers on notice of fraud. *See id.*

268. *See* E. Napoletano & Benjamin Curry, *Proof of Stake Explained*, FORBES ADVISOR, https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-stake [https://perma.cc/6VYH-J74C] (Feb. 16, 2023, 4:29 PM).

269. *See* Lyle Daly, *What Is Proof of Stake (PoS) in Crypto?*, MOTLEY FOOL, https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/proof-of-stake [https://perma.cc/3W3Z-3FLZ] (Dec. 12, 2022, 2:44 PM).

270. *See* @LucaPennella, *supra* note 55 (describing proof-of-stake as a lower barrier to entry when compared to proof-of-work). However, when considering the high costs associated with becoming a validator (32 ETH) and the fact that depositing more than 32 ETH will give one a higher chance at being selected to validate, while the cost is surely less than the mining equipment required for proof-of-work, the barriers to entry are still relatively high on the Ethereum Network. *See id.*

lose its stake by attempting to pass fraudulent votes, its stake will decrease to a lower percentage than that of its electoral vote count.[271]

E-ballots are delegated to states in a pseudorandom, proportional manner, meaning that one or more statistical tests for randomness are implemented to produce the results, based upon the number of electoral votes assigned to the state.[272] As an example, while New York has a 5% chance of receiving an e-ballot, each county within New York has a 1/62,[273] or a 1.6%, chance of being selected to verify the e-ballot.[274]

3. What Is the Network Layout? Who Is in Charge?

To eliminate a single point of control, the federal government will be split into fifty different "owners"—these owners being the states.[275] The best way to implement this approach is a government-established decentralized autonomous organization, where each state will serve as a member of the DAO.[276] For this election system, the DAO will be called the USDAO.[277] The USDAO will emulate the decentralized nature of a typical blockchain system while ensuring a collective entity overlooks the process.[278] More importantly, however, this structure will increase the points of contact needed for a hack.[279] Thus, while there remains a "central owner," that owner is essentially fifty different owners, who each have an equal vote in the DAO's approval process.[280] So, for one to hack the USDAO by injecting a malicious smart contract onto the network, twenty-six states would need to pass the invalid code for the

---

271. *See* Jake Frankenfield et al., *What Does Proof-of-Stake (PoS) Mean in Crypto?*, INVESTOPEDIA, https://www.investopedia.com/terms/p/proof-stake-pos.asp#:~:text=Proof [https://perma.cc/T5ZY-GBZA] (May 31, 2023).

272. *See* Onomy Protocol, *Proof of Stake & Validators: An Overview*, MEDIUM (Dec. 27, 2021), https://medium.com/onomy-protocol/proof-of-stake-validators-an-overview-d152fafde499 [https://perma.cc/2EGG-8SQM].

273. *See New York Counties by Population*, N.Y. DEMOGRAPHICS BY CUBIT, https://www.newyork-demographics.com/counties_by_population [https://perma.cc/E5XV-JH4Q] (last visited Dec. 2, 2023) (listing the sixty-two counties in New York).

274. *See id.* If there exist sixty-two counties in total, each county has a 1/62, or 1.6%, chance of being selected at random. *See id.*

275. *See* DIEDRICH, *supra* note 28, at 180-81 (detailing the mechanisms of a DAO).

276. *See id.* at 181. ("A DAO could deal in anything and it could also be a regular, legal business entity one day. It could live longer than its creator.").

277. *See What Is a Decentralized Autonomous Organization, and How Does a DAO Work?*, COINTELEGRAPH, https://cointelegraph.com/daos-for-beginners/what-is-a-dao [https://perma.cc/3MEF-DQWY] (last visited Dec. 2, 2023) (explaining how the DAO structure can be used for corporate governance and voting).

278. *See id.*

279. *See* DIEDRICH, *supra* note 28, at 180 (detailing the programmable and contractual provisions of a DAO that can live on numerous computers to form one organization).

280. *See id.* at 180-81.

hack to be successful—something that is arguably as hard as getting thirty-eight states to ratify an amendment![281]

4. How Are Votes Placed? Will This Be Difficult?

Each voter is given a public and private key by their county election board, set to expire upon the vote being cast or after Election Day, whichever is sooner.[282] The issuance of the keys will follow a similar procedure for voter registration: the key-pair may be used for eligible local elections, primary elections, or general elections.[283] The voter's private key will be stored on a decentralized wallet,[284] owned and operated by the USDAO.[285] Preloaded onto the wallet will be a quasi-Soulbound Token,[286] which, unlike a typical Soulbound Token that cannot be sent to anyone, this token may only be sent to the USDAO (hence, "quasi").[287] This token will represent an e-ballot.[288] The e-ballot may be filled out by phone, computer, or any device connected to the network.[289] While Soulbound Tokens are "soul" "bound," meaning forever with the person, the "person" here would be the USDAO, and considering that they own the wallets, they are merely allowing a brief license to each user to hold onto the token in the form of an e-ballot; these tokens will only ever be minted and issued by the USDAO and will serve as an additional verification layer to determine where an e-ballot has come from.[290] After a vote has been cast, a voter

281. *See Constitutional Amendment Process*, NAT'L ARCHIVES: OFF. FED. REG., https://www.archives.gov/federal-register/constitution [https://perma.cc/XRY4-9Q43] (last visited Dec. 2, 2023).

282. *But see* DIEDRICH, *supra* note 28, at 104 (describing the typical process for creating and issuing public and private keys).

283. *See id.* (describing the versatile use of public and private key pairs).

284. *Cf. id.* at 167, 170 (explaining how smart contracts can trigger the delivery of tangible services virtually). The issuance of public and private keys will be akin to the "service" of issuing voter registration permissions. *Id.* at 104-05.

285. *See id.* at 180-81 (detailing generally how a DAO establishes an entity dictated by smart contracts).

286. *See What Are Soulbound Tokens (SBT)?*, BINANCE ACAD. (Nov. 11, 2022), https://academy.binance.com/en/articles/what-are-soulbound-tokens-sbt [https://perma.cc/4XET-NKR5].

287. *See id.*

288. *See id.*

289. *See* DIEDRICH, *supra* note 28, at 93 (associating blockchains with the transfer for digital assets, transaction data, and cryptography). The transfer of digital assets via the blockchain in a robust voting system will require access to the network itself digitally, by any means, to register newly validated blocks. *See id.* As technology progresses, other means are contemplated for accessing the blockchain network. *See id.*

290. *See What Are Soulbound Tokens (SBT)?*, *supra* note 286 (discussing how the use of Soulbound tokens in DAO governance may improve the integrity of asset-based voting).

may view their e-ballot on the blockchain by locating their public key.[291] This will give voters the ability to recognize that their e-ballot was actually cast and counted; a voter may see which number vote they were and all other votes in real time.[292] Additionally, all public keys will remain anonymous, so unless someone tells you their public key, a voter will not know which vote belongs to whom.[293]

If a citizen (1) does not have access to a phone, computer, or other device connected to the network, or (2) does not know *how* to access the network, this individual may go to their typically designated polling place to cast an e-ballot on a voting station equipped to communicate with the network.[294] These accommodations will ensure that everyone, even those who do not understand the technology, has the means of casting their e-ballot.[295]

It must be noted that for such a system to garner any traction, the graphical user interface of the blockchain voting system must be highly user-friendly.[296] The capital spent on heuristics and human-interface design cannot be understated and must ensure that *everyone*, from a highly sophisticated computer scientist to an uneducated individual, may cast their e-ballot with *little to no difficulty*.[297] Ideally, the network will aim to be as simplistic as a car: a user may not understand what happens under the hood, but if there is a steering wheel and a gas pedal, that user can drive.[298]

D. The Global Impact of Domestic Adoption

Global blockchain implementation will allow anyone around the world to idly monitor international elections.[299] The importance of

291. *See generally* DIEDRICH, *supra* note 28, at 100 (detailing the visibility of a blockchain).

292. *See id.*

293. *See id.* at 104.

294. *See* Beckett, *supra* note 28, at 430 (outlining the general mechanics of a blockchain voting system and detailing how security concerns may dissuade individuals from utilizing the system). User concerns about security, interoperability, and overall technological knowledge gaps alike are factors which may dissuade voters from accepting a change in the means of voting. *Id.* at 431.

295. *But see id.* at 430 ("Perhaps the biggest benefit of a blockchain voting system is simply the fact that voters would not be voting solely on the current voting systems."). While the voting machines certainly would not be the same, for some voters, the method of voting would have to be similar in order to foster comfort with change. *See id.*

296. *See id.* (detailing the need for easily accessible methods for an individual to self-audit their vote).

297. *See id.* ("[O]nce a voter casts a ballot, the voter must place their trust in the election system that that vote will be counted—and counted properly.").

298. *See id.* (highlighting the importance of trust and simplicity when considering new methods of voting).

299. *See* Moore & Sawhney, *supra* note 99, at 3 (discussing the security and allowed transparency of ballots).

global transparency is paramount when considering a world leader can unilaterally create global uproar.[300] Indeed, this situation is not far-fetched when considering how World War II came to fruition.[301] All countries are stakeholders in elections, with leaders having a substantial impact on war, energy, the supply chain, and more.[302] Transparent elections are pivotal to ensuring robust democracies across the globe.[303] The United States must emerge as the leader by ushering engineering and optimal user studies.[304] Small implementations will demonstrate the system's robustness and detect errors before a full-scale system can be integrated abroad,[305] and the United States should be open to both concurrent and pre-research meetings with NATO countries to prompt others to invest in research and development.[306]

Transparency does not mean direct involvement in elections, but merely acting as an observer.[307] Allied countries exchange vital national security information, and have a great stake in member country elections.[308] NATO countries also share the taxing burden of defending member countries with these tough decisions coming from elected officials.[309] Hence, this is not to say that NATO members should get a vote, but it begs the question of why NATO members have not held themselves accountable on the homefront like they hold others accountable worldwide.[310] Especially in the United States, where the

---

300. *See* Marc von Lüpke-Schwarz, *Last 'Free' Vote*, DEUTSCHE WELLE (Mar. 5, 2013), https://www.dw.com/en/voting-in-the-midst-of-nazi-terror/a-16646980 [https://perma.cc/9XN8-X9ZL].

301. *See id.*

302. *See id.*

303. *See id.*

304. *See* Moore & Sawhney, *supra* note 99, at 4 (discussing the post-election audit process).

305. *See id.* at 5.

306. *See id.* (concluding how the success with the small subset of military and overseas voters can be expanded).

307. *See supra* Part IV.B. This Note does not suggest that foreign countries should get a say in the election of officials abroad. *See supra* Part IV.B. Rather, merely acting as an observer by reviewing the results of an election through the visibility of a blockchain would allow global leaders to make more informed decisions and better understand their allies or adversaries. *See* Robbie Gramer, *Trump Can't Do That. Can He?*, FOREIGN POL'Y (Jan. 17, 2019), https://foreignpolicy.com/2019/01/16/trump-cant-do-that-can-he-nato-russia-congress [https://perma.cc/RHX3-GDNF] (describing how the President is given broad power in foreign affairs).

308. *See id.*

309. *See id.*

310. *See* Jonathan Masters, *U.S. Foreign Policy Powers: Congress and the President*, COUNCIL ON FOREIGN RELS., https://www.cfr.org/backgrounder/us-foreign-policy-powers-congress-and-president [https://perma.cc/E3D9-E3S7] (Mar. 2, 2017, 2:28 PM) (detailing the powers granted to the President under the Constitution including, *inter alia*, the role of commander-in-chief of the Army and Navy and powers to use military force and collect foreign intelligence).

President has substantial foreign powers, the actions of one official could alter the global dynamic between allies.[311] Thus, international transparency provides a minimal, yet powerful bridge of trust to ensure that the lives of citizens globally are treated by fairly elected officials who dictate international relationships.[312]

E. Addressing the Critics of Change

Discussions of election integrity and implementing change to our election system has been one of the most hotly contested topics since 2020.[313] Indeed, this Note would likely have garnered more support if written prior to 2020.[314] Two major criticisms of change are worth addressing: (1) blockchains and the internet are too flawed to be trustworthy for elections,[315] and (2) the current United States election system is not broken, so it should not be fixed.[316] Both points certainly have merit, and while a blockchain voting system is not a cure for all of the country's issues, it provides a needed step in the right direction.[317]

1. "Blockchain and the Internet Are Too Flawed to Be Trustworthy for Elections"

Most critics of internet voting imagine a non-blockchain system, which surely would present several risks.[318] Yet there are those that do criticize blockchain-based systems, and claim there are many similar cybersecurity risks or allege that blockchain has not been tested

311. *See id.*

312. *See id.*

313. *See* PIPPA NORRIS ET AL., CONTENTIOUS ELECTIONS: FROM BALLOTS TO BARRICADES 7-9 (Electoral Integrity Project ed., 2015) (discussing how election disputes can either be settled through legal appeals and electoral reforms or, in the worse cases, bloodshed and government downfalls and military coups). For a discussion on the 2020 election and future concerns for the upcoming 2024 election cycle, see *supra* Part III.A.3–B.

314. *See id.* ("In particular, a pervasive belief that the election outcome is fraudulent, rigged, or stolen, as well as a lack of confidence in the impartiality, honesty, or independence of electoral authorities (whether true or false), provides a climate of public opinion that facilitates direct political actions mobilized by anti-government forces, notably opposition boycotts, political strikes, and peaceful or violent mass demonstrations and rallies protesting against the process and outcome.").

315. *See 8 Cybersecurity Reasons Why Online Voting May Never Happen*, CYLUMENA: INSIGHT, https://www.cylumena.com/insights/8-cybersecurity-reasons-online-voting-never-happen [https://perma.cc/MYD9-H2V6] (last visited Dec. 2, 2023).

316. Funke, *supra* note 115 (detailing false claims regarding fraudulent tabulation errors with current voting machines).

317. *See* Evans, *supra* note 2.

318. *See 8 Cybersecurity Reasons Why Online Voting May Never Happen*, *supra* note 315.

rigorously or long enough to be secure.[319] This Note would be remiss not to acknowledge this grave concern, especially in light of major cyberattacks, such as the DAO, or fraud by individuals, like the collapse of FTX.[320]

The general concerns surrounding voting over the internet, and adding another "layer of uncertainty" with a blockchain, echo the concerns of the internet in the 1990s and early 2000s.[321] Several critics who warned of the "consequences of digital cash"[322] in the mid-'90s are certainly part of the $2,041,000,000 in projected United States digital payment transactions for 2023[323] or 65.3% of Americans who store their hard-earned cash digitally with banks today.[324] This is not even mentioning that an overwhelming majority of these digital transactions constitute non-blockchain based systems, even though blockchain technology has since proven to be much more secure.[325] The risk of cyberattacks will certainly not fade soon;[326] there will always be someone attempting to undermine a large bank, hospital, or government entity.[327] But threats of attacks have not, and should not, stop innovation.[328] This is not to say that a blockchain voting system should be implemented immediately—there needs to be small test groups and

---

319. *See id.*

320. *See* Cryptopedia Staff, *supra* note 95; *see also* Q.ai, *What Happened to Crypto Giant FTX? A Detailed Summary of What We Actually Know So Far*, FORBES: MONEY (Dec. 13, 2022, 12:48 PM), https://www.forbes.com/sites/qai/2022/12/13/what-happened-to-crypto-giant-ftx-a-detailed-summary-of-what-we-actually-know-here/?sh=119b08a260fa [https://perma.cc/F7Y5-5SZZ].

321. *See* Alexis C. Madrigal, *The People Who Hated the Web Even Before Facebook*, ATL.: TECH., https://www.theatlantic.com/technology/archive/2019/03/people-who-hated-web-even-before-facebook/584932 [https://perma.cc/6BVC-NHG5] (last visited Dec. 2, 2023).

322. *See* Tatsuo Tanaka, *Consequences of Digital Cash*, FIRST MONDAY (Aug. 1996), https://firstmonday.org/ojs/index.php/fm/article/view/474/830 [https://perma.cc/2T5E-T4P6] (explaining how electronic payment systems present issues of security, limited functionality, costly fees, and threats of money laundering).

323. *Digital Payments – United States*, STATISTA, https://www.statista.com/outlook/dmo/fintech/digital-payments/united-states#users [https://perma.cc/UQF5-3639] (last visited Dec. 2, 2023).

324. *Share of Population Using Digital Banking in the United States from 2018 to 2022*, STATISTA, https://www.statista.com/statistics/946109/digital-banking-users-usa [https://perma.cc/AS9W-NSKK] (last visited Dec. 2, 2023).

325. *But see 8 Cybersecurity Reasons Why Online Voting May Never Happen*, *supra* note 315.

326. *See* Erica Louise, *Why Our World Would End If Cyber Security Disappeared?*, TECHAHEAD (Aug. 4, 2017), https://www.techaheadcorp.com/blog/world-end-cyber-security-disappeared [https://perma.cc/VYU6-NQT7].

327. *See id.*

328. *See id.* ("With constant technical innovation, new dangers are continually coming to the surface. Cybersecurity is all about building confidence and safety for the IT world.").

years of testing involved—but the threat of attacks should not deter the country from technological advancements.[329]

2. "The United States Election System Is Not Broken, So Why Fix It?"

While there have not been any proven instances of widespread voter fraud,[330] this does not mean that *mere allegations of voter fraud* do not equally undermine the system.[331] History has proven that some changes to the election system were needed to alleviate concerns, such as the changes since the 2000 election to replace punch cards with paper ballot machines.[332] The main difference today is the political debates that this topic has spurred, but political views about the integrity of the election system are irrelevant.[333] The fact is that (1) both the 2016 and 2020 elections called into question the integrity of the election system, allowing overall trust to slip to twenty percent;[334] (2) over half a billion dollars of taxpayer money was spent defending the "unbroken system" that could have been used to implement substantial and meaningful change elsewhere;[335] and (3) distrust in elections escalated to deadly violence.[336]

Of course, the rebuttal is that such sweeping change is only addressing a small subset of people who continually perpetuate lies and create this violence.[337] However, the same can be said for Congress: why have they expensed half of a billion dollars defending an "unbroken system" for a small majority?[338] The answer is because general concerns do not derive solely from a small subset: *eighty percent of Americans* have some level of distrust in election integrity.[339]

An additional rebuttal to this point is that such a small subset of people incite violence out of the eighty percent, and we will not reach

---

329. *See id.*

330. *See* Funke, *supra* note 115.

331. *See id.*; *see also* Shepherd, *supra* note 6.

332. *See* Help America Vote Act of 2002, Pub. L. No. 107-252, §§ 101, 301, 116 Stat. 1666, 1669, 1704.

333. *See* PEW RSCH. CTR., *supra* note 119, at 1 (describing the animosity between the parties and the passions that derive from the two-party system).

334. Shepherd, *supra* note 6.

335. *See* Al-Arshani, *supra* note 141.

336. *See* Cameron, *supra* note 142.

337. *See id.* (describing the violent group as a "pro-Trump protest"); *see also* Olivia Rubin et al., *By the Numbers: How the Jan. 6 Investigation Is Shaping Up 1 Year Later*, ABC NEWS (Jan. 4, 2022, 7:23 PM), https://abcnews.go.com/US/numbers-jan-investigation-shaping-year/story?id=82057743 [https://perma.cc/K4A2-79K2].

338. *See* Al-Arshani, *supra* note 141.

339. *See* Shepherd, *supra* note 6.

100% trust anyway, so why even bother?[340] This point is weakest: 2,000 people stormed the Capitol Building on January 6th, and seven people were killed.[341] It is true that we will likely never reach 100% trust, and it would be silly to make large expenditures every time a group acted lawlessly,[342] but when eighty percent of Americans question the integrity of a quintessential right; three elections over two decades are questioned at a half-billion dollar cost; 2,000 people attempt to obstruct justice; and seven people die, urgent change is needed.[343]

V. CONCLUSION

The time to act is now.[344] A black-box system of voting cannot remain for another decade if "We the People"[345] expect our democracy to remain fortified.[346] The global economy cannot withstand the existing system of governance.[347] Accountability is required, solutions are on the horizon,[348] and blockchain technology has the power to restore democratic order.[349]

A federally implemented private blockchain for use in voting, monitored by the USDAO, is the best means of modernizing elections.[350] The shared responsibility between all election boards for verifying e-ballots and the fiscal implications of each state will ensure that the system is secure, while generating stability through a minor degree of centrality given to the federal government.[351] The implications of public-private key pairs will provide privacy for citizens, enable anonymous transparency when viewing the ledger's time-stamped data, and develop an immutable ledger of votes to be counted instantaneously with real time statistical data.[352]

---

340. *Compare* PEW RSCH. CTR., *supra* note 19, *with* Shepherd, *supra* note 6 (demonstrating that even at a time of high confidence, citizens' trust for the United States government only reached a level of seventy-five percent, compared to eighty percent of citizens today having some level of distrust in election integrity).

341. *See* Cameron, *supra* note 142; Rubin et al., *supra* note 337.

342. *See* Al-Arshani, *supra* note 141.

343. *See* NORRIS ET AL., *supra* note 313, at 7; *see also* Rubin et al., *supra* note 337.

344. *See* Davenport, *supra* note 22.

345. U.S. CONST. pmbl.

346. *See* Shepherd, *supra* note 6.

347. *See id.*

348. *See* Beckett, *supra* note 28, at 425.

349. *See id.* at 429.

350. *But see* Evans, *supra* note 2 ("A solution to this black-box problem is to either tabulate by hand, or instantiate a separate audit process after each election.").

351. *But see id.*

352. *See 3 Benefits and Limitations of Private and Public Keys Need to Know [sic] Cryptocurrency Investors Need to Know to Secure Their Crypto*, SEC. PILGRIM,

Of course, this solution will be presented with its own flaws; voter suppression can occur digitally by weak internet connection to disadvantaged communities, people can steal mail, and people can use another's phone in an attempt to vote twice.[353] There will always be malicious actors that break the law to prevent someone or some group from voting, but this concept is not new.[354] So, while a blockchain network cannot solve every existing or future issue with the election system, a blockchain can establish a system of transparency to deter bad actors, minimize concerns over election integrity, and put an end to the black-box system of voting that Americans currently suffer from when voting for their elected officials.[355]

*John J. Healy Jr.**

---

https://securitypilgrim.com/3-benefits-limitations-of-keys [https://perma.cc/K4H3-RGYD] (last visited Dec. 2, 2023).

353. *See* CALTECH/MIT VOTING TECH. PROJECT, *supra* note 130, at 16 (discussing past security risks concerning voting infrastructure, how those flaws will be prevalent in internet voting, and how society has continually adapted in response to remedying these concerns).

354. *See id.* at 80 ("[W]e must not be deterred by these risks, because there is an even greater risk that inertia might leave us in our current dilemma.").

355. *See* Evans, *supra* note 2.

* J.D. Candidate, 2024, Maurice A. Deane School of Law at Hofstra University; B.S. Industrial & Systems Engineering, 2021, The Ohio State University. I am beyond grateful for the innumerous friends and colleagues to whom I wish to express my appreciation—a footnote will hardly do it justice, but here is an attempt. First and foremost, thank you to my good friend Emanuele Putrino, Managing Editor of Articles. To him I am indebted for the diligent, thorough, and profound support he has provided since the day I submitted for publication; you are an indispensable component of this Note's success. Many thanks to my friends Alexa Torrens, Editor-in-Chief, and Paul Sessa, Managing Editor of Staff, for their unwavering support and tireless effort in ensuring this Note's excellence. Thank you to my incredible Notes Editor, Owen Daly, for your guidance throughout the writing process. A very special thank you to my accomplished Faculty Advisor Irina Manta. Your thought-provoking considerations and expertise were invaluable to this Note. Furthermore, thank you for your continuous mentorship throughout my time at Hofstra Law School—from working under your leadership on compelling research projects to advice on careers, courses, and so much more. Thank you to Theresa Kelley, Volume 51 Editor-in-Chief, for believing in this Note from the start and for your preliminary support. Thank you to my friends and esteemed Notes and Articles Editors, Victoria Mascia and John Lanka, for your keen editorial support. Thank you to the *Hofstra Law Review* Volume 51 and Volume 52 for your time preparing this Note and adding the meticulous final touches. Thank you to the *Journal of International Business & Law* Volume 22 Staff for your continued encouragement throughout the Note-writing and publication processes. I greatly appreciate everyone who dared to pick up this Note and read to this point. I hope you learned a great deal and now appreciate the topic as much as I do. The contents of this Note and its solution are a culmination of ideas and thoughts inspired from a college presentation I delivered on blockchain voting in 2018. I hope this Note provides the foundation for meaningful change in our country. Lastly, thank you to my dear friends, and most importantly, my loving family: my parents John and Rosanna Healy and my sister Jessica Healy. This one's for you.