Science and Technology Law Review

Volume 24 | Number 1 Article 8

2021

Signed, Sealed, Patented?: A Look at the United States Postal Service's Patent Application for Implementing Blockchain Technology in Mobile Voting Systems

Ethan Todd
Southern Methodist University, Dedman School of Law

Signed, Sealed, Patented?: A Look at the United States Postal Service's Patent Application for Implementing Blockchain Technology in Mobile Voting Systems

*Ethan Todd**

I. INTRODUCTION

More Americans used absentee ballots to vote in the 2020 election cycle than ever before. Some 65.5 million absentee ballots were cast in the 2020 general election, while only 24.8 million were cast in the 2016 general election.[1] This increased usage of the United States Postal Service (USPS) for casting ballots is part of a systematic increase in the use of mail-in voting that has been in motion since 1996.[2] While the 2020 election instigated a sharp spike in mail-in voting amid health and safety concerns caused by COVID-19, it also brought about heightened attention to absentee ballots.[3] Because many states tabulate absentee ballots for days following the election, an increase in absentee ballots may create confusion and incite litigation due to delays in counting.[4] While calls for a modernized absentee voting system are legion, the technical hurdles have remained while officials and voters are skeptical of change.

The USPS, however, has recently signaled that the winds of change may soon be upon us. On August 13, 2020, the United States Patent and Trademark Office (USPTO) published Patent Application 16/785,354 (the '354 Application), an application submitted by the USPS, which describes a "vot-

---

* Ethan Todd is a 2022 candidate for a Juris Doctor from SMU Dedman School of Law. He received a Bachelor of Arts in Journalism and Public Relations from the University of Georgia in 2018.

1. *EAVS Deep Dive: Early, Absentee and Mail Voting*, U.S. Election Assistance Comm'n (Oct. 17, 2017), https://www.eac.gov/documents/2017/10/17/eavs-deep-dive-early-absentee-and-mail-voting-data-statutory-overview; Michael McDonald, *2020 General Election Early Vote Statistics*, U.S. Elections Project, https://electproject.github.io/Early-Vote-2020G/index.html (last updated Nov. 23, 2020, 4:21 PM).

2. Hannah Hartig, Bradley Jones, & Vianney Gomez, *As States Move to Expand the Practice, Relatively Few Americans Have Voted by Mail*, Pew Res. Ctr. (June 24, 2020), https://www.pewresearch.org/fact-tank/2020/06/24/as-states-move-to-expand-the-practice-relatively-few-americans-have-voted-by-mail/.

3. Drew DeSilver, *Mail-in Voting Became Much More Common in 2020 Primaries as COVID-19 Spread*, Pew Res. Ctr. (Oct. 13, 2020), https://www.pewresearch.org/fact-tank/2020/10/13/mail-in-voting-became-much-more-common-in-2020-primaries-as-covid-19-spread/.

4. Mark Sherman, *GOP Maneuvers to Challenge Battleground Absentee Ballots*, AP News (Nov. 3, 2020), https://apnews.com/article/election-day-legal-challenges-b85ec8351882d5508fde27e8dd6b251d.

ing system" that "can use the security of blockchain and the mail to provide a reliable voting system."[5] The '354 Application raises many questions, ranging from the viability of the system proposed to whether or not the application will survive its review and prosecution by the USPTO. This Casenote seeks to address these issues in turn and in three parts. In the first part, it will provide a brief explanation of blockchain technologies and analyze the '354 Application to provide a discussion of how the Application would actually work in practice. In the second part, it will discuss how a modernized, electronic absentee voting system would comport with the United States' current election laws. Finally, in the third part, it will discuss the patent law obstacles that the '354 Application may face or be susceptible to in its journey to grant.

II. BLOCKCHAIN TECHNOLOGY, VOTING, AND THE APPLICATION

A. What is Blockchain Technology?

To understand the voting system proposed by the USPS and how it differs from more traditional internet technologies, it is necessary to understand blockchain technology. Described generally, blockchain technology provides a distributed, decentralized public ledger in order to provide a secure method of storing and recording many different forms of transactions.[6] While first described and outlined in 1991 as a system where document timestamps could not be tampered with, blockchain did not manifest a real-world application until the emergence of Bitcoin in 2009.[7] But cryptocurrency applications are just one of the many possibilities that have emerged as potential or current utilizations of this technology. Blockchain is shown to have workable applications to technologies such as smart contracts, licensing, and online banking transactions.[8] Among these newer applications of blockchain technology, the prospect of its use in voting systems provides an attractive alternative for proponents of modernizing election systems in the United States without invoking many of the proven drawbacks of voting in a centralized internet voting system.[9]

5. U.S. Patent Application No. 16/785,354, Publication No. 2020/0258338 A1 (published Aug. 13, 2020) (United States Postal Service, applicant), at [57] [hereinafter '354 Application].

6. Luke Conway, *Blockchain Explained*, INVESTOPEDIA, https://www.investopedia.com/terms/b/blockchain.asp (last updated Nov. 17, 2020).

7. *Id.*

8. Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park & Kari Smolander, *Where is Current Research on Blockchain Technology?—A Systematic Review*, PLOS ONE (Oct. 3, 2016), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477.

9. *See* DAVID JEFFERSON, AVIEL D. RUBIN, BARBARA SIMONS, & DAVID WAGNER, A SECURITY ANALYSIS OF THE SECURE ELECTRONIC REGISTRATION AND VOTING EXPERIMENT (SERVE) (Jan. 21, 2004), https://classes.cs.uoregon.edu/

In creating this distributed, decentralized public ledger, blockchain uses "blocks" that consist of digital information stored in a "chain" that comprises the public database.[10] The blocks typically comprise three pieces of digital information: (1) transactional information such as date, time, and—in the context of a voting system—ballot selections; (2) a unique digital signature to identify the participant in a transaction; and (3) a unique code, specific to each separate block, called a hash that distinguishes a block from every other block—these are cryptographic codes created by special algorithms that enhance the security and anonymity of any given transaction.[11] It is relevant to note that not every transaction in every situation is given a single block; in many instances, a single block may house thousands of other transactions.[12]

For a transaction to be added to a block, it must first be verified.[13] The verification process is one of the key distinguishing characteristics of blockchain technology as compared to a traditional electronic recording system. Whereas with traditional public records of information, one party is responsible for verifying new data entries, blockchain uses a wide network of computers that rush to incoming data entries to ensure the details of the transaction are consistent with the original data entry.[14] This use of a network of computers to verify a single transaction is what renders blockchain "decentralized."[15] After verification, the transaction is stored in a block with the details of the transaction and the participant's digital signature.[16] Once all transactions in a block have been verified, the block is given its unique "hash," or identifying code, as well as the hash of the most recent block added to the blockchain.[17] The completed transactions in the blockchain become publicly recorded—hence the description of blockchain as a distributed "public key"—while user data remains confidential.[18]

04W/cis607ev/readings/SERVE_paper.pdf; *see also* Scott Wolchok, Eric Wustrow, Dawn Isabel & J. Alex Halderman, *Attacking the Washington, D.C. Internet Voting System*, *in* 16TH CONF. ON FIN. CRYPTOGRAPHY & DATA SEC. (2012), https://core.ac.uk/download/pdf/205222709.pdf (experimenting with a voting system that used a standard internet browser connected to a central server, rather than blockchain).

10. Conway, *supra* note 6.

11. *Id.*

12. *Id.*

13. *Id.*

14. *Id.*

15. *Id.*

16. Conway, *supra* note 6.

17. *Id.*

18. *Id.*

When a computer connects to the blockchain, it receives a copy of the blockchain that is updated automatically when a new block is added.[19] This means that, depending on the size of the network, thousands or millions of copies of the same blockchain are available to all the network computers.[20] This verification system allows for the blockchain to achieve greater security. When the transactions in a block have been verified, the block is then given its own "hash" code and receives the hash of the block before it.[21] Hash codes are created by algorithm and are uniquely created according to the digital information within the block.[22] Therefore, if the digital transaction data of an existing block is edited in any way, the hash code changes as well.[23] Because each block contains the hash of the previous block, if that previous block's hash were to change due to a hacker changing transaction data within the block, the hacker would need to also update the next block, as well as any other subsequent blocks in order to cover their tracks.[24]

While disadvantages to blockchain (which are explored later) certainly exist, blockchain objectively provides a more accurate, secure, and transparent method of inputting and recording digital transactions than traditional centralized systems. Whether these advantages can be used to effectively implement an absentee voting system which accounts for the accuracy, trustworthiness, and anonymity that is axiomatic to the proper functioning of a democratic election process, however, is another question.

B. The USPS Patent Application

The '354 Application claims a voting system comprised of four main components.[25] The following section will discuss these components as described in the claims while utilizing the specification to illuminate the full scope of the terms to explain the ways this system may work. Before that, however, the author will discuss contextually relevant portions of the specification that will aid in understanding the system claimed.

Patents may be broken down into their respective parts to better understand what the proposed invention would entail. The majority of the written portion of the patent and the drawings provided make up the specification, which provides "one of ordinary skill in the art" with a narrative description of the proposed technology in various possible embodiments.[26] The nar-

19. *Id.*
20. *Id.*
21. *Id.*
22. Conway, *supra* note 6.
23. *Id.*
24. *Id.*
25. '354 Application, *supra* note 5, col. 2, at 15.
26. *See* Teleflex, Inc. v. Ficosa N. Am. Corp., 299 F.3d 1313, 1325 (Fed. Cir. 2002).

rower, final portion of the patent—the claims—seeks to precisely define the "metes and bounds" actual invention sought to be patented.[27] While the patent claims themselves narrowly claim the blockchain system to be employed in the voting system and its necessary components, the specification goes further to detail how the system could potentially be employed in a more tangible way.[28] The system largely relies on a "paper ballot that is printed with a QR code, barcode, or other computer or machine readable identifier" that is sent to a registered voter.[29] From there, the '354 Application contemplates many forms for the voting system to embody:

> In some embodiments of the vote by mail system, an election official can create a template ballot for use by potential voters. Voters can then apply to the system to allow them to receive a mailed ballot. The system can verify the identity of the voter and create a pseudo-anonymous token in the form of a unique identifier that represents the voter. In some embodiments, the vote by mail system then generates a paper ballot that is printed with a QR code . . . or other computer or machine readable identifier that represents the token . . . . The paper ballot having the identifier thereon can be mailed to the voter that corresponds with that token. In some embodiments, the voter can receive the paper ballot and use a mobile device or other computer to scan the ballot with a camera. The voter can then use the mobile device to cast digital votes . . . which are then written to a blockchain.[30]

However, the specification also references an embodiment in which "the voter does not vote electronically, but instead fills out the paper ballot and sends it to the registrar."[31] The system would also allow the QR code or other computer readable code to be "used to verify that the ballot was properly submitted by a registered voter."[32] From the registrar's end, they could receive the ballot, scan the QR code, and certify the voter has voted and then ensure that the digital votes are added to the vote tallies of the candidate.[33] As exemplified by these varied embodiments, it is clear that the voting system would be available for states to use in varying degrees—from using the system to more transparently track and verify one's vote to using the full

27. *See id.* at 1324.

28. *See id.* at 1326 ("That claims are interpreted in light of the specification does not mean that everything expressed in the specification must be read into the claims.").

29. '354 Application, *supra* note 5, at [0044].

30. *Id.* at [0044–45].

31. *Id.* at [0045].

32. *Id.*

33. *Id.* at [0046].

capacity of the system to cast a vote electronically and verify its transmission by the registrar.[34]

The '354 Application's specification largely envisions a blockchain system that outlines and accords with the general blockchain technology principles discussed above.[35] However, recall that one of the general traits of blockchain is that it is a public ledger.[36] Interestingly, the '354 Application specification specifically envisions an embodiment in which "the blockchain ledger is not publicly distributed, but is distributed among election authorities for a county, state, country, or any combination thereof."[37] Further, the ledgers would be distributed among nodes which would be maintained "by various election precincts or districts or election systems."[38] Thus, rather than using miners, the ledgers would be distributed in servers and computers directly maintained by election groups or systems.[39]

The specification also envisions a system in which ballots would be mailed with a computer readable code which could be scanned by mail processing equipment throughout its traverse, updating the delivery status of the ballot, allowing for greater transparency of the ballot in the mailing process.[40] The postal service could also gather and compile information and other ballot delivery statistics to create reports for election officials.[41] Once the ballot is received by the voter, the voter could then scan votes on the ballot and submit them to the blockchain; this could "be done by voting in an application or a mobile computing device, by taking a picture of a filled out physical ballot and returning the image, etc."[42]

The "application" envisioned by the USPS is further detailed in the specification and in Figure 14 of the '354 Application.[43] The specification describes a "Vote By Mail" (VBM) application, which would (in some embodiments) require a voter to first register with the appropriate election au-

34. *See id.* at [0044–46].

35. *See supra* Part II(A).

36. *Id.*

37. '354 Application, *supra* note 5, at [0050].

38. *Id.*; Jimi S., *Blockchain: What are Nodes and Masternodes?*, MEDIUM (Sept. 5, 2018), https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f#:~:text=nodes%20form%20the%20infrastructure%20of%20a%20blockchain.&text=they%20store%2C%20spread%20and%20preserve,transaction%20history%20of%20the%20blockchain (explaining that nodes can be any kind of device, but are generally computers, laptops, or even bigger servers).

39. '354 Application, *supra* note 5, at [0050].

40. *Id.* at [0109].

41. *Id.*

42. *Id.* at [0112].

43. *Id.* at [0118].

thority in order to receive authorization to download the application.[44] One form of authorization contemplated is a "ballot access token," which could take the form of a twelve-digit alphanumeric code or a QR code, that would be assigned individually to each voter and would allow voters to access their ballot.[45] Once the VBM application is downloaded, a user could receive a second computer-readable code that would allow the user to actually vote in a specific election.[46] Once a voter has loaded and filled out their ballot in the VBM application, the user could use the application to sign the ballot by using a stylus or finger to record a digitized version of the user's physical signature. Once completed, the application transmits the ballot selections to a blockchain abstraction layer or "blockchain access layer," along with other data which could include an election identifier, ballot identifier, and voter identifier.[47] "[T]he blockchain abstraction layer can be a computer, server, . . . or group of computing devices that coordinate storing information on the blockchain."[48] Once submitted to the blockchain abstraction layer, the voter's entries and data could then be recorded in a voting database and added to a submitted vote blockchain, then can be verified by an election official based on comparing the digital signature to the one on file for that voter.[49] After the voter is approved, the blockchain abstraction layer would then create an entry on an accepted vote blockchain and any remaining links between the actual votes and the identity of the voter can be deleted.[50]

While the specification does not define the claims of a patent, it is clear that the '354 Application contemplates a voting system that is almost entirely electronic and where voters could cast their votes from their smartphone.[51] However, various states may be hesitant to make such a leap; the '354 Application anticipates this as well, and allows for states to use the technology not as a primary voting function but as a secondary verification and tracking function to be used in conjunction with a filled-out physical ballot.[52]

The first component of Claim 1 of the '354 Application's voting system is a "blockchain access layer."[53] This blockchain access layer is configured to "receive input from" both a "user operated mobile computing device" as well

44. *Id.*

45. '354 Application, *supra* note 5, at [0118].

46. *Id.*

47. *Id.* at [0120].

48. *Id.* at [0121].

49. *Id.* at [0124].

50. *Id.* at [0125].

51. '354 Application, *supra* note 5, at [57].

52. *See id.* at [0060].

53. *Id.* at [0177], at 15.

as an "election official system."[54] From the user-operated mobile device, the blockchain access layer receives input "comprising a computer readable code scanned from a physical ballot, ballot selections, and an electronic signature."[55] From the election official system, the blockchain access layer receives at least a "ballot and an election identifier."[56] The blockchain access layer can be envisioned as the network with which voters' phones and election systems interact, with the network likely being maintained by the election system servers (as described in the specification and discussed above).[57]

A second component of the '354 Application is "a first database in communication with the blockchain access layer, the first database configured to receive and store the ballot selections and the electronic signature from the blockchain access layer." [58] That a voter's electronic signature and their actual ballot selections would be kept in the same database could be a point of concern for voter anonymity. However, Claim 2 also claims the system of Claim 1 "wherein the ballot selections and the electronic signatures are stored in separate structures in the first database."[59] The specification describes this database as a "received ballots database."[60]

A third component of the '354 Application is "a second database in communication with the block chain access layer."[61] When a voter elects to receive their ballot, the blockchain access layer generates a "vote identification" for the ballot and electronic signature associated with the voter.[62] This second database is configured to receive this vote identification from the blockchain access layer and to store a "pointer"—an identifier—to a location of both the ballot selections and the electronic signature in the first database.[63] These pointers are used to correspond the vote identification with the ballot cast by the individual voter.[64]

A fourth component of the '354 Application is a blockchain database.[65] The blockchain database is configured to "receive the vote identification from the second database and to receive the ballot selections from the

54. *Id.*

55. *Id.*

56. *Id.*

57. *See* '354 Application, *supra* note 5, at [0047–50].

58. *Id.* col. 2, at 15.

59. *See id.*

60. *Id.* at [0062].

61. *Id.* col. 2, at 15.

62. *Id.*

63. *See* '354 Application, *supra* note 5, col. 2, at 15.

64. *See id.* at [0123].

65. *Id.* col. 2, at 15.

blockchain access layer" when an election official verifies the ballot by confirming the signature provided.[66]

III. BENEFITS OF THE PROPOSED SYSTEM AND POTENTIAL DRAWBACKS

There are numerous potential benefits of utilizing blockchain technology for voting systems, assuming the technology is used according to plan. However, there are clear concerns with using this technology, especially in an arena such as elections. The purpose of the following sections is to set forth these advantages and disadvantages and contextualize them in the voting arena.

A. Advantages

Earlier discussion highlighted some of the primary advantages of using blockchain technology generally.[67] However, these advantages come with particular allure in a voting system due to the inherent characteristics of voting. One of the main tentpoles of blockchain is transparency—it is generally regarded as open source, with a visible public ledger.[68] Recall, however, that the '354 Application specifically discusses that in some embodiments, the ledger of votes would not be publicly available, but only available to the connected election systems.[69] That does not mean, however, that the '354 Application sacrifices transparency. The '354 Application could increase transparency in the mail-in voting process through the use of computer-readable codes on mailed ballots.[70] By using mail processing equipment to scan these codes throughout their journey to the mailbox and back, the system would enable voters to track their ballots through the delivery process and confirm their delivery and verification status.[71] This differs slightly from the current tracking systems which generally enable absentee voters to see some updates, such as when and if their ballot is received and accepted or rejected, but the current system does not allow voters to track their ballots in a detailed manner and is not a uniform policy among states.[72]

66. *Id.*

67. *See supra* Part II(A).

68. Conway, *supra* note 6.

69. '354 Application, *supra* note 5, at [0050].

70. *See id.* at [0060].

71. *See id.* at [0109].

72. *See* Dave Beaudoin, *Forty-Four States Allow Voters to Check the Status of their Ballot Online*, BALLOTPEDIA NEWS (Oct. 28, 2020, 4:42 AM), https://news.ballotpedia.org/2020/10/28/44-states-allow-voters-to-check-the-status-of-their-ballot-online/.

More security is achieved by blockchain technology through the verification and hashing functions that occur when a transaction is recorded.[73] When a block is completed, it is given a unique hash based upon the information it holds, as well as the hash of the block preceding it.[74] Because the information of a block defines the hash, any change in the data within a block would result in a new hash, which would trigger other computers of the hash's invalidity.[75] This level of security and verifiability of the data entered could be especially helpful in warding off claims, or showing evidence, of instances of voter fraud.

Another advantage of using blockchain technology is its decentralized nature, as opposed to storing information in a central location.[76] Because the blockchain is distributed across a network of computers, each updating when new blocks are added, it is more difficult to tamper with the blockchain.[77] Thus, the information is preserved and recorded accurately.

B. Disadvantages

While significant benefits can be realized with blockchain technology, very realistic concerns remain in relying on such a system to be a large factor in a democratic voting process. Blockchain technology is still developing; as with most new technologies, weaknesses will be, and have been, exploited.[78] The '354 Application, in many instances, accounts for these shortcomings.

A key concern with the utilization of blockchain technology in voting is compromised anonymity.[79] It has been shown that blockchain transactions can still be linked to some user information.[80] Further, it has been found that the computer-generated user codes can be linked to IP addresses, even when users are behind firewalls.[81] The '354 Application could seek to solve this potential issue simply: by not allowing the ballot selection ledgers to be publicly accessible, ledgers cannot be linked to individual users unless the servers maintaining the ledgers are infiltrated.[82]

---

73. *See* Conway, *supra* note 6.

74. *Id.*

75. *Id.*

76. *Id.*

77. *See id.*

78. *See* Yli-Huumo et al., *supra* note 8 (noting instances of distributed denial-of-service attacks, fifty-one percent attacks, data tampering, and authentication and cryptography issues).

79. *See id.* at 4.

80. *See id.* at 17.

81. *See id.*

82. *See* '354 Application, *supra* note 5, at [0057].

Newer blockchain networks are also susceptible to what are known as "fifty-one percent attacks."[83] Recall that when a corrupted block is added to a chain, member nodes would cross-check the hash on the block.[84] If the hash is inconsistent with a majority of the nodes, the member nodes flag the block and the transaction will be cancelled.[85] But if attacker nodes collectively control more computational power than the member nodes, the network is susceptible to the fifty-one percent attack.[86] This concern raises significant questions, given the '354 Applications description of the member network of verifiers being closed to outsiders, and thus providing uncertainty with how much computational power this network would hold.[87]

C. Implications of Governmental Ownership of the '354 Application

The '354 Application also presents an interesting question: what are the possible effects and implications of the potential governmental ownership of the voting system envisioned by the '354 Application? While the effects of patent issuance to a governmental agency such as the USPS are largely and likely benign, some of the relevant issues should be discussed.

Congress has made clear that any federal agency is authorized to "apply for, obtain, and maintain patents" in the United States.[88] This authority further allows the agency owning a patent to "grant nonexclusive, exclusive, or partially exclusive licenses under federally owned inventions."[89] This law is undisturbed by the Supreme Court's ruling in *Return Mail, Inc. v. United States Postal Service*,[90] which held that the USPS (or any other federal agency) was not a "person" allowed to challenge the validity of a patent post-issuance.[91] Indeed, in that case, the Court expressly recognized that the USPS or any other agency "may still apply for and obtain patents whether or not it may petition for a review proceeding under the AIA seeking cancellation of a patent it does not own."[92] Thus, it is well-settled that the USPS has the statutory authority to submit for approval the '354 Application.

---

83. Alyssa Hertig, *Blockchain's Once-Feared 51% Attack is Now Becoming Regular*, COINDESK (June 7, 2018, 11:00 PM), https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular.

84. *See* Conway, *supra* note 6.

85. *See id.*

86. *See* Hertig, *supra* note 83.

87. *See* '354 Application, *supra* note 5, at [0111].

88. 35 U.S.C. § 207(a)(1) (2018).

89. *Id.* § 207(a)(2).

90. 139 S. Ct. 1853 (2019).

91. *Id.* at 1867.

92. *Id.* at 1864.

While it is clear that the USPS has the authority to apply for a patent, it may be questioned what the potential benefits or detriments of governmental ownership of the '354 Application may be. One may fear that the federal government may use the exclusionary power of a patent right to hold the invention without ever implementing its use. Indeed, the central right granted by the registration of a patent is the right to exclude others from making, using, selling, or offering for sale the claimed invention for twenty years from the filing of the patent application.[93] And it is also true that a federal agency is "authorized to," but is not required to, grant licenses for the inventions an agency may obtain a patent for.[94] However, the federal government, in obtaining patents for new inventions, serves an important function in "promot[ing] the progress of science and the useful arts"[95] by adhering to the disclosure requirements of the Patent Act. Section 112 of the Act requires that a specification sufficiently disclose the "manner and process of making and using" the invention to enable any person skilled in the art to make and use the invention.[96] This enablement requirement serves to further progress and invention by allowing other inventors to build upon the technology of the claimed invention in novel and useful ways. Additionally, agencies owning patent rights to inventions generally "encourage[ ] the patenting and licensing of the government's intellectual property" to "encourage innovation and promote commercialization of technologies that may be developed using federal resources."[97] In promoting the use of federally funded inventions, agencies may make their patents available for licensing to businesses and other organizations.[98] This seeks to ensure fairness and openness in licensing.[99] This general policy shows that the USPS, in seeking to obtain a patent for the '354 Application, would not likely use the right of exclusion granted by a patent in a malevolent way but as a way to license the technology either exclusively or non-exclusively to entities for implementation in state voting systems.

93. 35 U.S.C. § 154(a)(1)–(2).

94. *Id.* § 207(a)(2).

95. U.S. CONST. art. I, § 8, cl. 8.

96. 35 U.S.C. § 112(a).

97. *Technology Transfer Activities*, U.S. DEP'T INTERIOR, https://www.doi.gov/techtransfer/patents (last visited June 16, 2021).

98. *See* WALTER G. COPAN, U.S. DEP'T COM., NAT'L INST. OF STANDARDS & TECH., FEDERAL LABORATORY TECHNOLOGY TRANSFER FISCAL YEAR 2016: SUMMARY REPORT TO THE PRESIDENT AND CONGRESS 6 (Sept. 2019), https://www.nist.gov/system/files/documents/2019/10/30/fy2016_fed_lab_tech_transfer_rept_fina_9-10-19.pdf.

99. *Id.* at 6–7.

IV. LEGAL ISSUES ENCOUNTERED BY THE PROPOSED SYSTEM

Blockchain technology, if used effectively, has the potential to change the way Americans think about voting and elections.[100] It has the potential to allow secure and anonymous digital voting from one's phone or tablet.[101] In order for implementation of such a system, however, it must be able to comport with the current voting laws and constitutional requirements. Further, because the USPS seeks to protect their proposed voting system with a patent, the USPS will face the obstacle of receiving registration of the patent, which is a far cry from a guarantee.[102] This section will briefly discuss the relevant legal hurdles to which a blockchain technology-based voting system would be subject.

In large part, the United States Constitution grants states a "broad power to prescribe the 'Times, Places, and Manner of holding Elections for Senators and Representatives,' Art. I, § 4, cl. 1, which power is matched by state control over the election process for state offices."[103] This broad power also includes the ability to determine election administration structure and procedures, with the result being that no state administers elections exactly the same way as another state.[104] The Constitution, however, instructs Congress to determine the time and day of general elections, and further gives Congress the power to "at any time by Law make or alter" states' election regulations except as to the places of choosing Senators.[105] While this grant of authority may seem omnipotent, principles of federalism have prevented Congress from wielding the Elections Clause with unbridled authority.[106] Thus, Congress has historically only infrequently exercised its constitutional authority to regulate state election systems.[107] Notable among these are the Voting Rights Act of 1965, the National Voter Registration Act of 1993, and the Help America Vote Act of 2002 (HAVA).[108]

100. Conway, *supra* note 6.

101. *See id.*

102. *See* '354 Application, *supra* note 5.

103. Tashjian v. Republican Party of Conn., 479 U.S. 208, 217 (1986) (quoting U.S. CONST. art. I, § 4, cl. 1).

104. *Election Administration at State and Local Levels*, NAT'L CONF. ST. LEGISLATURES (Feb. 3, 2020), https://www.ncsl.org/research/elections-and-campaigns/election-administration-at-state-and-local-levels.aspx.

105. U.S. CONST. art. I, § 4.

106. *See* Shelby County v. Holder, 570 U.S. 529, 542–44 (2013) (discussing the balance between federal and state control of elections).

107. *Election Administration at State and Local Levels*, *supra* note 104.

108. Voting Rights Act of 1965, Pub. L. No. 89-110, 79 Stat. 437 (codified as amended in scattered sections of 52 U.S.C. (Supp. III 2016)); National Voter Registration Act of 1993, Pub. L. No. 103-31, 107 Stat. 77 (codified as

Of these congressional enactments, HAVA presents the greatest regulatory framework with which a blockchain voting system must comport.[109] Congress passed HAVA in 2002 following the issues surrounding the controversial 2000 election and similar problems which persisted after the election.[110] HAVA presented a comprehensive set of regulations to address problems with certain voting systems, such as those using a punch card system.[111] HAVA granted federal funds to states for, among other things, modernizing voting equipment and systems.[112] This receipt was conditioned on states' compliance with standards set forth by Congress.[113] These standards require a modernized voting system: (1) permit the voter to independently verify the votes selected by the voter on the ballot before the ballot is cast; (2) allow the voter the opportunity to change or correct their ballot before it is cast; (3) notify voters who have selected more than one candidate for an office and give them a chance to rectify the error while preserving confidentiality; (4) produce a permanent paper record of the votes within audit capacity; (5) be accessible and private for individuals with disabilities; (6) be accessible for voters who speak minority languages; (7) comply with an error rate no greater than that in 2002; and (8) adopt a uniform definition of what constitutes a vote.[114]

HAVA defines a "voting system" as including the "total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used" to define ballots, cast and count votes, report or display election results, and maintain and produce any audit trail information.[115] HAVA does not, however, provide or note specific systems that are permitted within its framework; rather, a new voting system would need to fit within the definition of "voting system" and comply with the standards set forth.[116] Instead, HAVA established the Election Assistance Commission (EAC), an independent federal agency authorized to adopt voluntary voting system guidelines and provide testing for national certification of hardware and software.[117]

---

amended at 52 U.S.C. §§ 20501–20511 (Supp. III 2016)); Help America Vote Act of 2002, Pub. L. No. 107-252, 116 Stat. 1666 (codified as amended at 52 U.S.C. §§ 20901–21145 (Supp. III 2016)).

109. *See id.*

110. *See* 52 U.S.C. §§ 20901–20902 (2002).

111. *Id.* § 20901.

112. *Id.*

113. *Id.* § 21081.

114. *Id.* § 21081(a)(1)(A–C).

115. *Id.* § 21081(b).

116. 52 U.S.C. § 21081(a–b).

117. *Id.* §§ 20921–20922.

Looking to the '354 Application's specification, it is clear that a voting system utilizing blockchain could easily satisfy the standards required of a voting system under HAVA. Some of the standards, such as the ability to independently verify one's vote and auditability of the permanent record, are specifically described as a benefit of the USPS's proposed voting system.[118] Others, such as privacy and accessibility for disabled voters and language flexibility, are inherent to a voting system using a personal computing device.

Another significant indicator of the '354 Application's cogency with HAVA is the recent election guideline compliance report issued for Voatz, a mobile blockchain voting platform, which determined that the system meets the applicable requirements for voting systems in the United States.[119] The testing was performed by Pro V&V, one of two testing labs certified by the EAC as a Voting System Testing Laboratory.[120] Thus, while not yet officially certified by the EAC, the Pro V&V report concluded that the Voatz system "meets the applicable requirements set forth for voting systems in the U.S. Election Assistance Commission (EAC) 2015 Voluntary Voting System Guidelines (VVSG), Version 1.1, with the clarifications or exceptions noted in Section 4.0."[121]

The technology behind the Voatz system is not published or patented, but it has been in use since 2018 when it was first tested in the West Virginia election for use by overseas military voters.[122] This raises an interesting question: whether the '354 Application could be rendered invalid because the same or equivalent technology is already in use. Without knowing the actual source code and system that Voatz uses, the USPS could find itself subject to a patent infringement or invalidation proceeding.[123]

Apart from the requirement of the proposed voting system comporting with current election laws, the '354 Application must also face the scrutiny of the patent prosecution process of the USPTO in order to be registered and

118. '354 Application, *supra* note 5, at [0044–46].

119. *Test Report for Test and Evaluation of the Voatz Remote Accessible Ballot Delivery, Marking and Return (RABDMR) System*, PRO V&V (July 17, 2020), https://voatz.com/wp-content/uploads/2020/07/VOATZ_Final_Test_Report_Revision_02.pdf [hereinafter *Test Report*].

120. Certificate of Accreditation to Pro V&V, Inc., U.S. ELECTION ASSISTANCE COMM'N (Feb. 24, 2015), https://www.eac.gov/sites/default/files/voting_system_test_lab/files/Pro_VandV_accreditation_certificate_2015.pdf.

121. *Test Report*, *supra* note 119, at 14.

122. *Warner Pleased with Participation in Test Pilot for Mobile Voting*, W. VA. OFF. SEC'Y STATE (Nov. 16, 2018), https://sos.wv.gov/news/Pages/11-16-2018-A.aspx [hereinafter *Test Pilot*].

123. 35 U.S.C. § 102(a)(1) (2018) ("A person shall be entitled to a patent unless the claimed invention was . . . in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention . . . .").

protected.[124] In undergoing this process, there are many requirements which any patent application must show, and a failing on any one of these fronts may render a rejection for the application.[125] These requirements will be discussed in the following paragraphs.

To obtain a patent, an application must meet four primary requirements: (1) the invention must cover eligible subject matter; (2) the invention must be novel; (3) the subject matter must be "useful"; and (4) the invention must not be "obvious."[126] In order for the '354 Application to be approved, it is necessary for these requirements to be met. While the subject matter and usefulness requirements are likely to be met by the '354 Application, the novelty and nonobviousness requirements may present a greater challenge, and thus will be discussed in more depth.

The voting system claimed in the '354 Application will likely have little trouble with meeting the subject matter requirement. Section 101 of the Patent Act provides that "process[es], machine[s], manufacture[s], or composition[s] of matter" are patentable.[127] If an invention fails to fall into one of these four categories, the invention is not patentable.[128] At a quick glance, it is clear that a voting "system" or "method," as described in the '354 Application does not envision a machine, article of manufacture, nor a composition of matter.[129] Thus, to be patentable subject matter, the voting system would need to qualify as a "process."[130] Further, a patentable invention must also fall outside one of the three judicially created exceptions to patentable subject matter: "laws of nature, natural phenomena, and abstract ideas are not patentable."[131] This abstract idea exception presents a particularly relevant inquiry when it comes to patents using computer technology when the computer technology does nothing more than implement the mental steps required of a claimed method or system.[132] Were the '354 Application to somehow be determined to merely be claiming an abstract idea, it must show that it contains an inventive concept sufficient to transform it into patent-

124. *Id.* § 131.

125. *Id.* § 101–03.

126. *Id.*

127. *Id.* § 101.

128. *See id.*

129. '354 Application, *supra* note 5, at [0014], at 1.

130. *See* 35 U.S.C. § 101.

131. Alice Corp. v. CLS Bank Int'l, 573 U.S. 208, 216 (2014) (citing Ass'n for Molecular Pathology v. Myriad Genetics, 569 U.S. 576, 589 (2013)).

132. *See id.* at 225.

eligible subject matter.[133] Applications of such abstract ideas to a new and useful end remain eligible for patent protection.[134]

Section 101 also specifies that the subject matter sought to be patented must be "useful."[135] In order to satisfy this requirement, a claimed invention must have both "substantial" and "specific" utility.[136] To have substantial utility, a claimed invention must have a "real-world" value which provides some immediate benefit to the public.[137] To have specific utility, the claimed invention must disclose a use which is not so vague as to be meaningless.[138]

Further, for an invention to be patentable, it must be considered new or "novel."[139] This means that an invention cannot be patented if prior public disclosures of the invention have already been made prior to the filing of the application.[140] While the public disclosure analysis is somewhat complicated, the primary rules show that an invention will not be patentable if: (1) the invention was known to the public before the applicant filed the application; (2) the invention was described in a printed publication before the applicant filed the application; or (3) the invention was described in a published patent application or issued patent that was filed before the applicant filed for patent protection. [141] Thus the examiner of the '354 Application will search prior publications to see if the claims of the Application have been disclosed either in other sources or patent applications prior to the time the USPS filed the '354 Application. Further, Section 102 also makes clear that a patent application may be denied if the claimed invention was "in public use, on sale, or otherwise available to the public before the effective filing date of the claimed invention."[142] This provision may prove to be a point of contention in the prosecution of the '354 Application in light of the existence of other blockchain voting technologies already in existence such as the Voatz application. Voatz utilizes blockchain technology for a voting system and has been used in West Virginia since at least 2018, prior to the filing of the '354 Application.[143] Notably, Voatz has not sought or obtained a patent for their technology. However, in the prosecution of the '354 Application, it may be considered whether the Voatz technology renders the '354 Application not

133. *Id.* at 217.

134. *Id.* (citing Gottschalk v. Benson, 409 U.S. 63, 67 (1972)).

135. 35 U.S.C. § 101.

136. *In re* Fisher, 421 F.3d 1365, 1371 (Fed. Cir. 2005).

137. *Id.*

138. *Id.*

139. 35 U.S.C. § 102.

140. *See id.*

141. *See id.*

142. *Id.* § 102(a)(1).

143. *Test Pilot, supra* note 122.

novel.[144] For the Voatz (or another similar) technology to anticipate the '354 Application, the similar technology would need to disclose every element of what the patentee claims as his invention, a difficult hurdle.[145]

Finally, Section 103 of the Patent Act requires that an invention be a non-obvious improvement over prior art.[146] Thus, even if an invention is not exactly the same as prior products or processes—rendering the invention novel—it may still be denied protection if it is determined that the invention would have been obvious to one "having ordinary skill in the art to which the claimed invention pertains."[147] This means that an examiner will compare the invention to prior art (already established inventions in the field) to determine whether the differences in the new invention would have been obvious to one having ordinary skill in the type of technology used in the invention.[148] This determination is made more difficult by *KSR International v. Teleflex*,[149] where the Supreme Court held that "obvious" combinations of multiple prior art sources may be a bar to the granting of a patent.[150] Meaning that, in prosecution of the '354 Application, the question may arise whether the patent sought is rendered obvious due to it merely being an obvious combination of existing technologies which one skilled in the art would contemplate. Recall that the '354 Application consists of some elements, such as a voting system based on blockchain technology and a computer readable code, which are currently known and in use.[151]

V. CONCLUSION

Based upon the preceding discussion, it is clear that blockchain voting technology could bring about a major change in the way Americans are able to vote. Accessibility to the ballots continues to be a driver for many in their determination of whether to vote or not.[152] Blockchain technology could serve to increase this accessibility through the implementation of a simple and expedient method of voting. With this understanding in mind, the USPS set forth a patent application for a secured voting system using blockchain technology which could utilize the technology to varying degrees, within the determinations of the states. It is also likely that such a system would be able to comport with existing election laws already in place. However, a patent

144. *See* 35 U.S.C. § 102.

145. *See id.*

146. *Id.* § 103.

147. *See id.*

148. *Id.*

149. 550 U.S. 398 (2007).

150. *Id.* at 417–18.

151. '354 Application, *supra* note 5, at [0004].

152. Certificate of Accreditation to Pro V&V, Inc., *supra* note 120.

application does not come with a guarantee of patent granting. The '354 Application will be required to cover the hurdles inherent to patent granting, and the current existence of similar technologies may present a potential obstacle in this process. Further, while the advantages of using such technology are legion, legitimate concerns about voter anonymity, election security, and technological scalability remain. Thus, while it is apparent that the USPS is interested in utilizing revolutionary technology for elections, such a utilization is still in its fledgling stages and subject to significant barriers before a universal adoption of this technology—which is not a given—can even be contemplated.