Policy Considerations for the Blockchain Technology Public and Private Applications

*Garry Gabison**

I. INTRODUCTION

In 2008, Satoshi Nakamoto—an individual or group of individuals[1]—released a paper that described Bitcoin, a first of its kind, peer-to-peer electronic cash system.[2] Bitcoin relies mostly on existing technology but requires a new invention, a blockchain, to solve an old problem: how do two parties conduct an online transaction without knowing or trusting each other and without the need for a trusted third-party intermediary?[3] Encryption and large-scale redundancy was combined with Nakamoto's blockchain to solve this problem for the first time—the Bitcoin blockchain is the key.[4]

---

* J.D. from the University of Virginia School of Law and Ph.D. in Economics from Yale University. Visiting Assistant Professor Georgia Institute of Technology School of Public Policy. The first draft of this paper was written while I was a Research Fellow at the European Commission Joint Research Centre Institute for Prospective Technological Studies. The content of this article does not reflect the official opinion of the European Commission. Responsibility for the information and views expressed in the article lies entirely with the author. I would like to thank my colleagues in the Information Society Unit for their feedback and suggestions during our lively seminars.

1. *See, e.g.*, Elle Hunt et al., *Bitcoin Creator Satoshi Nakamoto Probably Australian Entrepreneur, Reports Claim*, THE GUARDIAN (Dec. 8, 2015), http://www.theguardian.com/technology/2015/dec/09/bitcoin-creator-satoshi-nakamoto-alleged-to-be-australian-academic; Emin Gün Sirer, *How to Spot Bitcoin Inventor Satoshi Nakamoto*, MIT TECH. REV. (Dec. 10, 2015), https://www.technologyreview.com/s/544431/how-to-spot-bitcoin-inventor-satoshi-nakamoto/ (discussing the true identity of Nakamoto). Recently, Craig Wright has claimed to be Satoshi Nakamoto, but skepticism over his remarks remain. *See, e.g.*, *Craig Steven Wright Claims to be Satoshi Nakamoto. Is He?*, THE ECONOMIST (May 2, 2016), http://www.economist.com/news/briefings/21698061-craig-steven-wright-claims-be-satoshi-nakamoto-bitcoin; *Craig Wright's Claims to be Satoshi Nakamoto Come Under Fire*, THE ECONOMIST (May 2, 2016), http://www.economist.com/news/briefings/21698066-onus-on-craig-wright-provide-better-evidence-satoshi-nakamoto.

2. SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM (2008), https://bitcoin.org/bitcoin.pdf.

3. *Id.*

4. *Id.* (The article summarizes the process through 6 steps: (1) broadcasting the information to the network; (2) each node in the network compiles the information; (3) each node checks the information by solving a complicated process; (4) each node broadcast the proof that it solved the checking process; (5) the nodes accept the broadcast only if the information included is proven to be correct; and (6) the nodes add to the chain the new information, where it is, timestamp, and its location in the chain is contingent on the previous elements of the chain.).

Blockchains are permanently distributed spreadsheets or ledgers where information can only be added—never deleted.[5] The spreadsheet is not in-and-of-itself a novel technology, but blockchain's decentralized attribute and permanency,[6] combined with its incorruptibility (or quasi incorruptibility),[7] makes its applications potentially disruptive.[8] As with most technologies, blockchain technology has several advantages but also significant drawbacks. When considering a switch to this new technology, decision makers need to perform a complicated cost–benefit analysis.

Bitcoin, the blockchain's first application, has been described by some as a virtual currency.[9] Following Bitcoin's lead, the financial industry is now at the forefront of taking blockchain technology mainstream, but likely for different motivations.[10] Banks may have different motivations for taking this technology forward. Some banks may feel threatened[11] because blockchain technology can offer a cheaper alternative to traditional banking and can

5. *Id.*

6. Primavera De Filippi & Aaron Wright, Decentralized Blockchain Technology and the Rise of Lex Cryptographia (Mar. 10, 2015) (unpublished manuscript), https://ssrn.com/abstract=2580664 (describing the process through which blocks are permanently added to the chain in a decentralized manner).

7. The Bitcoin whitepaper describes the likeliness of an attack. NAKAMOTO, *supra* note 2. These attacks have been known as "51% attacks" because they require the attacker to gain control of 51% of the total mining hash rate. Danny Bradbury, *The Problem with Bitcoin*, 11 COMPUTER FRAUD & SECURITY 5 (2013).

8. Bradbury, *supra* note 7.

9. The debate over whether bitcoins qualify as a currency or asset has been investigated by policymakers around the world. *See, e.g.,* Robleh Ali et al., *Innovations in Payment Technologies and the Emergence of Digital Currencies*, BANK OF ENG. Q. BULL. Q3 (2014), http://www.bankofengland.co.uk/publications/Pages/quarterlybulletin/2014/qb14q3.aspx; *Virtual Currency Schemes a Further Analysis*, EUR. CENT. BANK (Feb. 3, 2015), https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf; Dong He et al., *Virtual Currencies and Beyond: Initial Considerations*, INT'L MONETARY FUND (Jan. 20, 2016), http://www.imf.org/external/pubs/cat/longres.aspx?sk=43618.

10. Banks have taken the lead in developing commercial applications of blockchain technology. Forty-two banks (including UBS, Goldman Sachs, and JP Morgan) have invested into a start-up (R3 CEV) that is developing a standardized architecture for private ledgers. Nathaniel Popper, *Funds Roll In for Start-Up Harnessing Bitcoin Tech*, N.Y. TIMES (Jan. 21 2016), http://www.nytimes.com/2016/01/22/business/funds-roll-in-for-start-up-harnessing-bitcoin-tech.html.

11. *See, e.g.,* Cade Metz, *Why Wall Street Is Embracing the Blockchain—Its Biggest Threat*, WIRED (Feb. 16, 2016), http://www.wired.com/2016/02/wall-street-is-embracing-the-blockchain-its-biggest-threat/; Arjun Kharpal & Julia Chatterley, *Blockchain Won't Kill Banks: Brock Pierce*, CNBC (Apr. 11, 2016) http://www.cnbc.com/2016/04/11/blockchain-wont-kill-banks-brock-pierce.html.

reach portions of the population without access to banks.[12] Thus, some of these banks may be trying to preempt the very tool that could doom their future. Some banks may also consider quasi-centralized applications of this technology to represent its best use.[13] Under a quasi-centralized blockchain system, banks and financial institutions envision an opportunity to cooperate and create a common system based on a know-your-consumer business model to take advantage of blockchain technology while satisfying regulatory requirements and ameliorating its drawbacks.

The information recorded on blockchains can, however, go beyond currency and its transfers. Blockchain applications have grown substantially in recent years.[14] Recent projects look to provide services that are traditionally provided by public entities.[15] For instance, in Estonia, the government has teamed up with a private company (Bitnation) to provide e-residency and notarization services through a blockchain.[16] Some other applications of this potentially disruptive technology are discussed below.

Blockchain technology comes with its own challenges. This article discusses the policy challenges that will be presented if blockchain technology becomes widely adopted. The policy ecosystem is not fully adapted to this technology, and rules and regulations would have to be retrofitted. This article first discusses issues presented by *public* blockchains, best analogized as a permanent public ledger. Specifically, privacy breaches and copyright infringement may increase if data recording moves from the current centralized systems to a distributed blockchain system.

---

12. Brett Scott, *How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?*, UNITED NATIONS RES. INST. FOR SOC. DEV. (2016), http://www.unrisd.org/80256B3C005BCCF9/search/196AEF663B617144C1257F550057887C?.

13. These banks form a consortium with the objective of implementing a private blockchain this year. Kim S. Nash, *Blockchain: Catalyst for Massive Change Across Industries*, WALL ST. J. (Feb. 2, 2016), http://blogs.wsj.com/cio/2016/02/02/blockchain-catalyst-for-massive-change-across-industries/. Other banks partnered (e.g., BNP Paribas, Citigroup, etc.) have invested in blockchain projects targeting, among other things, stocks, derivatives, and loans. Another financial institution alliance (involving Visa, Inc., Nasdaq, etc.) is also backing their own project. Bank of America has already filed numerous patents on Blockchain technology. Arjun Kharpal & Julia Chatterley, *Bank of America is Going Big on Blockchain*, CNBC (Jan. 28, 2016), http://www.cnbc.com/2016/01/28/bank-of-america-is-going-big-on-blockchain-plans-to-file-20-patents.html.

14. Nash, *supra* note 13.

15. Ian Allison, *Bitnation and Estonian Government Start Spreading Sovereign Jurisdiction on the Blockchain*, INT'L BUS. TIMES (Nov. 28, 2015), http://www.ibtimes.co.uk/bitnation-estonian-government-start-spreading-sovereign-jurisdiction-blockchain-1530923.

16. *Id.*

The article then discusses the drawbacks of *private* blockchains. Private blockchains can be implemented in different ways, but current implementations require special equipment that could stifle wide-scale adoption due to the associated switching and operating costs. Furthermore, blockchain algorithms provide no mechanism to correct erroneous recordings within the blockchain. As such, the benefits of blockchain technology may currently be outweighed by drawbacks. This article narrowly considers governmental implementations, but these issues apply to all blockchains.

Finally, this article offers a counter-argument in favor of public entities adopting blockchain technology. The secure nature of this technology allows for easier and broader publication of government data, which could help transparency goals. Furthermore, the mathematical algorithms used in blockchain implementations assure the accuracy and legitimacy of the information stored within. This article is written from the perspective of United States and European Union policymakers, but the arguments within can be further generalized.

II. THE EXPANSION OF PUBLIC BLOCKCHAINS CONSTITUTES A THREAT TO PRIVACY AND COPYRIGHT

Publicly accessible blockchains resemble the current Internet, allowing anyone to view the data.[17] Bitcoin, for example, allows anyone with internet access to view the entire transaction history of every bitcoin in existence.[18] Recording any property transactions (real, intellectual, or intangible) could offer the same benefits.

A public blockchain makes the recorded information readily available and decreases some transaction costs.[19] For instance, if patent ownership was recorded on a blockchain at the national patent office, a technology implementer could locate a patent right holder in order to purchase or license the patent rights. However, such a blockchain with public access has significant drawbacks. This section discusses the policy issues presented by a publicly accessible blockchain where everyone can read and write on the blockchain.

A. Privacy

Public blockchains jeopardize information privacy because of two inherent characteristics. First, blockchain technology relies on an append-only

17. *See generally* Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 837, 843–44 (2015) (discussing Bitcoin and its operation using blockchain technology).

18. *See id.*

19. *See The Great Chain of Being Sure About Things*, THE ECONOMIST (Oct. 31, 2015), http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable [hereinafter *The Great Chain*].

data process; as such, no information can be removed.[20] Second, public blockchains rely on a distributed data storage system where their entire node network records the same information; accordingly, any change requires practically the entire network to agree on the change.[21] Removing information becomes difficult—if not impossible—in blockchains with well-distributed networks.[22]

Controlling information uploaded to a public blockchain is a central issue. If a user uploads sensitive or private information, policymakers who attempt to enforce or encourage privacy may find no way of ameliorating the damage.[23] In the Internet age, privacy has already become a concern.[24] The European Commission and the United States have had different responses to similar issues.

In Europe, policymakers recognized a right-to-be-forgotten in 1995,[25] which entitles European citizens to request the removal of their personal information from searchable internet data stores.[26] The intent and scope of this directive has been defined and reaffirmed by the European Court of Justice (ECJ) in 2014 in *Google v. Agencia Española de Protección de Datos (AEDP)*.[27]

20. *See generally* Katherine Heines, *The Risks and Rewards of Blockchain Technology*, 63 RISK MANAGEMENT 4, 6–7 (Mar. 1, 2016) (discussing blockchain technology and its functionality between various network users).

21. *See id.*

22. *See id.*

23. *See generally* Ronald J. Krotoszynski, Jr., *The Polysemy of Privacy*, 88 IND. L.J. 881 (2013) (discussing the different concepts of privacy and comparing the U.S. and EU approach to privacy).

24. Consumers are often unaware how their information is collected and used. *See* Jai-Yeol Son & Sung S. Kim, *Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model*, 32 MIS Q. 503, 506 (2008), http://www.jstor.org/stable/25148854 (analyzing different information privacy responses once internet users are made aware how their information is used, including not engaging, removing already disclosed information, complaining, spreading negative publicity, etc.).

25. *See generally* Council Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 12, 1995 O.J. (L 281) 31, 42 (establishing the right of an individual to ask for personal data which is incomplete or inaccurate to be deleted).

26. *See generally* Jeffrey Rosen, *The Right to be Forgotten*, 64 STAN. L. REV. ONLINE 88, 92 (2012) (discussing the right to be forgotten and how it will be implemented and criticizing its impact on public speech).

27. *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317, at *21.

In *Google v. AEDP*, a Spanish citizen complained to a search engine, Google, and a newspaper, *La Vanguardia*, that when his name was inputted into the Google search engine, a negative 1998 *La Vanguardia* newspaper story about the man appeared.[28] AEDP, the regulating agency, rejected the complaint with regard to the newspaper, because at the time of publishing the information was free speech protected news; AEDP, however, affirmed the complaint with regard to Google because search results amounted to a provider of content.[29] Google appealed the administrative ruling and the case was referred to the highest European court.[30] The ECJ found that search engines process and present information and, therefore, fall under the authority of AEDP as a content provider.[31] Under the directive, search engines are controllers of information.[32] The Court balanced the interest of free speech against the right to privacy,[33] but this delicate balance remains case specific.[34] The Court ruled that upon a request from an individual, a name-based search might, under certain circumstances (e.g., a lengthy passage of time), warrant enjoining the return of a link to information stored by a third party.[35] In other words, what is secondary content in some contexts can be primary content in others, and citizens have a right to control some primary personal content—the right to be forgotten.[36]

The introduction of a public blockchain could complicate how to implement the right-to-be-forgotten.[37] In a centralized system, a judge can demand that the central server remove the unwanted information.[38] But in a decentralized system, multiple nodes carry identical copies of the same information—nodes that may not even be within a court's jurisdiction.[39] Enforcing a re-

28. *Id.* ¶ 14.

29. *Id.* ¶¶ 15–16.

30. *See id.* ¶¶ 18–20.

31. *See id.* ¶ 30.

32. *See id.* ¶ 38.

33. *See Google Spain SL*, 2014 E.C.R. 317, at ¶ 74.

34. *See id.* ¶ 81.

35. *See id.* ¶¶ 88, 99.

36. Google evaluates about 572 requests a day and grants about half of them. In spite of the processing volume, the Google process has been criticized for its opacity; and the policymakers have been criticized for leaving Google to adjudicate the right to be forgotten requests. *See* Mark Scott, *Europe Tried to Rein In Google. It Backfired*, N.Y. TIMES (Apr. 18, 2016), http://www.nytimes.com/2016/04/19/technology/google-europe-privacy-watchdog.html.

37. *See* Jeni Tennison, *What is the Impact of Blockchains on Privacy?*, THE OPEN DATA INSTITUTE (Nov. 12, 2015), https://theodi.org/blog/impact-of-blockchains-on-privacy.

38. *See id.*

39. *See id.*

moval order becomes complicated, if not impossible.[40] If unwanted information is placed on a public blockchain, the blockchain's immutable design may require the information to remain.[41]

In the United States, some of the privacy debate revolves around "revenge porn."[42] Revenge porn refers to the nonconsensual distribution of media depicting consensual intimacy.[43] Victims of revenge porn may use different strategies to address this kind of privacy breach. First, they may initiate private actions seeking damages in tort law or an injunction against the person who spread the material.[44] Second, if there is proof of who took the photos, victims can turn to copyright infringement.[45]

Civil recourse often falls short, failing to provide enough incentive to prevent revenge porn from spreading.[46] To address this inefficiency, the majority of U.S. jurisdictions have criminalized the intentional distribution of revenge porn,[47] but only a minority of states have comparable civil remedies.[48] An important civil remedy is the possibility of obtaining an injunction to prevent further distribution.[49] Even if a victim is successful, however, in the current system, the unwanted information can live beyond the original posting.[50]

---

40. *See id.*

41. *See id.*

42. Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, at 345 (2014).

43. *Id.* at 359.

44. *Id.*

45. *Id.* at 359–60.

46. *Id.* at 357 (arguing for the introduction of criminal penalties to effectively address nonconsensual porn).

47. *See State Revenge Porn Laws*, C.A. GOLDBERG LAW, http://www.cagoldberglaw.com/states-with-revenge-porn-laws/ (last visited Nov. 10, 2016) (reporting that as of March 20, 2016, twenty-seven states and the District of Columbia have criminalized revenge porn, whereas only nine states have civil remedies for revenge porn); *see, e.g.*, CAL. PENAL CODE § 647(j)(4) (criminalizing the intentional distribution of material that was produced "under circumstances in which the persons agree or understand that the image shall remain private as a misdemeanor and fineable offense).

48. GOLDBERG LAW, *supra* note 47.

49. Citron & Franks, *supra* note 42, at 358–59; *see, e.g.*, CAL. CIV. CODE § 1708.85(d) (allowing specifically for injunctive relief for victims of revenge porn).

50. Citron & Franks, *supra* note 42, at 349 (explaining once information reaches the internet, a downloader of the media can report the document; once information is disclosed, the media spreading would require further litigation of subsequent posters).

Aware of the remaining gaps, private companies have attempted to provide a solution.[51] Specifically, search engines, like Google, offer services akin to the right to be forgotten.[52] This is offered to revenge porn victims who request images not to appear in searches anymore.[53] However, removing search results from Google does not remove the information from the Web.[54]

Policymakers face a constant struggle to balance the freedom of expression with the right of privacy.[55] Europe's right to be forgotten is criticized as a heavy infringement on the right of expression[56] that provides insufficient protection of privacy for consensually taken but non-consensually distributed intimate photographs.[57]

In a blockchain world, deleting information generally becomes more complicated than in a centralized system. Some have used this particular characteristic to create a censor-resistant social media system.[58] For example, Twister is a micro-blog application in the image of Twitter, but Twister relies on blockchain technology to avoid censorship.[59] In such a system, defamatory statements could permanently exist with no regulatory means of removal. This distinction between the current centralized system and a blockchain system may, however, be only minimally consequential, because in current systems all information can simply be downloaded and disseminated again, making it still difficult to remove defamation from the internet.

Under current technology, blocking searches offers the only feasible avenue to limit this dissemination, but it does not prevent access if the direct

51. Dino Grandoni, *Google to Remove 'Revenge Porn' Images From Search Results*, N.Y. TIMES (June 19, 2015), http://bits.blogs.nytimes.com/2015/06/19/google-to-remove-revenge-porn-images-from-search-results/.

52. Amit Singhal, *"Revenge Porn" and Search*, GOOGLE PUB. POL'Y BLOG (June 19, 2015), http://googlepublicpolicy.blogspot.com.es/2015/06/revenge-porn-and-search.html.

53. Grandoni, *supra* note 51.

54. *Id.*

55. Citron & Franks, *supra* note 42, at 374–77.

56. Jimmy Wales, the co-founder of Wikipedia, has criticized the EC rule and the EJC ruling on privacy and right to be forgotten as censorship of history. *See, e.g.*, Natasha Lomas, *Jimmy Wales Blasts Europe's "Right To Be Forgotten" Ruling As A "Terrible Danger"*, TECHCRUNCH (June 7, 2014), http://techcrunch.com/2014/06/07/wales-on-right-to-be-forgotten/; Joe Miller, *Wikipedia Link Hidden By 'Right To Be Forgotten'*, BBC (Aug. 4, 2014), http://www.bbc.com/news/technology-28640218.

57. Citron & Franks, *supra* note 42, at 357 (arguing that civil penalties do not provide a sufficient deterrent for individuals to post these photos).

58. Klint Finley, *Out in the Open: An NSA-Proof Twitter, Built with Code from Bitcoin and Bittorrent*, WIRED (Jan. 13, 2014), http://www.wired.com/2014/01/twister/.

59. *Id.*

link is provided.[60] Policymakers need to reinvestigate this issue even within the current state of technology and even more with the advent of blockchain technology. The next section discusses a different approach with regard to copyrighted material.

B. Copyright

Copyrighted materials face similar problems when published without authorization; a copyrighted work of art could be published on a public blockchain—permanently and unlawfully.[61] Once a copyrighted work of art is recorded on the ledger, it will become virtually impossible to take down because no central server can be disconnected and the individual cannot be stopped.[62] Further mitigation by injunction would be impossible to enforce, leaving victims with recovery for damages as their only possible recourse.[63]

In order for copyright holders to recover damages, they must decide from whom to collect.[64] Copyright holders already face this question under the current system, and as copyrighted material is published on blockchains, holders will turn to one of four entities: the original poster of the copyrighted material; the Intermediary Service Providers (ISP)[65]; the public blockchain's creator; or the subsequent downloaders.[66]

A copyright holders' first stop ought to be the original infringer.[67] Even if an individual owns the right to enjoy a copyrighted work of art (e.g., a legally purchased a copy of a movie), uploading the work onto a webhost or blockchain is unlawful and subjects the individual to liability.[68] But these infringers might often prove judgment-proof in most cases and are not a good avenue for recovery. If a copyright holder attempts to recover for every download and for each upload, the original infringer quickly becomes judg-

60. Grandoni, *supra* note 51.

61. Nick Vogel, Comment, *The Great Decentralization: How Web 3.0 Will Weaken Copyrights*, 15 J. MARSHALL REV. INTELL. PROP. L. 135, 148 (2015).

62. *Id.* at 141.

63. *Id.* at 148.

64. *See id.* at 146.

65. Intermediary service providers include internet service providers, web content hosts, and caching. *See* Online Copyright Infringement Liability Limitation Act, 17 U.S.C. § 512(a), (b) (2010).

66. Vogel, *supra* note 61, at 143–47.

67. *Id.* at 146.

68. *See, e.g.*, 17 U.S.C. §§ 501–04 (mandating a copyright can obtain an injunction against an infringer and request damages); British Acad'y of Songwriters, Composers and Authors v. Sec'y of State for Bus. Innovation & Skills [2015] EWHC 1723, Case No: CO/5444/2014 (holding that making a copy for its own use can also be construed as unlawful copying and lead to liability).

ment-proof.[69] This issue will continue under a blockchain technology recording system.

Second, the copyright holder may decide to go after wealthier entities—ISPs.[70] In Europe and the United States, ISPs face limited liability for internet content uploaded by their users. In the United States, the Digital Millennium Copyright Act (DMCA) and the Online Copyright Infringement Liability Limitation Act have become the principle tools for online copyright enforcement.[71] Under these acts, ISPs can face liability for the unlawful dissemination of copyrighted material.[72] However, the DMCA creates a safe harbor against liability for internet service providers and webhosts if, "upon notification of claimed infringement . . . , [the ISP] responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity."[73]

In Europe, the EU Copyright Directive[74] and the E-Commerce Directive[75] offer comparable guidelines for the implementation of digital copyright holder rights and limitations of ISP liability.[76] Among other things, a copy-

69. Vogel, *supra* note 61, at 148.

70. *Id.* at 144–45.

71. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) [hereinafter DMCA] (codified as amended in sections of 17 U.S.C., 28 U.S.C., & 35 U.S.C.); Online Copyright Infringement Liability Limitation Act, 17 U.S.C. § 512 (2010); Ryan Bates, *Communication Breakdown: The Recording Industry's Pursuit of the Individual Music User, a Comparison of U.S. and E.U. Copyright Protections for Internet Music File Sharing*, 25 NW. J. INT'L L. & BUS. 229 (2004).

72. DMCA, *supra* note 71, § 1203(c).

73. *Id.* at § 512 (c)(1)(C).

74. Directive 2001/29/EC, of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, 2001 O.J. (L 167), 10.

75. Directive 2000/31/EC, of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1 [hereinafter E-Commerce Directive].

76. *See, e.g.*, Yaman Akdeniz, *To Block or Not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression*, 26 COMPUT. L. & SEC. REV. 260 (2010), https://ssrn.com/abstract=1906712 (comparing the DCMA and the E-commerce Directive); Bates, *supra* note 71; Stephen E. Blythe, *The U.S. Digital Millennium Copyright Act and the E.U. Copyright Directive: Comparative Impact on Fair Use Rights*, 8 TUL. J. TECH. & INTELL. PROP. 111 (2006); Lucie Guibault et al., *Study on the Implementation and Effect in Member States' Laws of Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society*, INST. FOR INFO. LAW, UNIV. OF AMSTERDAM (Feb. 2007), http://ec.europa.eu/internal_market/copyright/docs/studies/infosoc-study_en.pdf.

right holder can file a notice to a webhost and the webhost can avoid liability if "the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."[77]

Recent European court decisions have provided copyright holders another tool in the fight against copyright infringement.[78] Even though ISPs can avoid liability and have no duty to monitor their customers,[79] copyright holders can request an injunction to make ISPs block their customers' access to copyright infringing websites. These types of injunctions can prove useful for copyright holders if the webhost is not within the court's jurisdiction. However, more savvy ISP customers have means of circumventing the ISPs through virtual private networks, proxy servers, onion routing, etc.[80]

In a blockchain world, webhosting could become decentralized; removing content from a public chain within one jurisdiction does not affect the chain in another jurisdiction.[81] Blockchain technology undeniably affects the way copyright holders can use the DMCA and the E-Commerce Directive to take down copyright-infringing content. Copyright holders may have to file more injunctions to block access to links rather than having the content removed; nonetheless, going after every ISP, even in a single jurisdiction (e.g., Germany), could prove prohibitively complicated and expensive.

Third, copyright holders can attempt to recover from a public blockchain's creators. In the past, companies that created software that enabled and incited infringement have been held liable for inducing infringement.[82] After a blockchain matures to decentralization, the original software

77. E-Commerce Directive, *supra* note 75, art. 14.

78. In 2014, the Court of Justice of the European Union held that ISPs could be ordered to block access to websites carrying copyright-infringing materials. Case C-314/12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, 2014 E.C.R. I. In 2015, the Germany Supreme Court ruled and reaffirmed a similar case in Bundesgerichtshof [BGH] [Federal Court of Justice] Nov. 26, 2015, Gesellschaft für musikalische Aufführungs, Case ZR 3/14.

79. E-Commerce Directive, *supra* note 75, art. 15.

80. *See 5 Ways to Bypass Internet Censorship and Filtering*, How-To Geek, http://www.howtogeek.com/167418/5-ways-to-bypass-internet-censorship-and-filtering/ (last visited Nov. 10, 2016).

81. A copyright holder can recover from an ISP if it has knowledge that it is enabling infringement. An ISP may claim they have no knowledge of what their users post. With blockchain technology, it could become complicated to identify all the ISP hostings required to prove that each individual ISP had knowledge of the content of the blockchain. For instance, Bitcoin has several thousand reachable nodes hosting and validating exact replicas of its blockchain. *See* Global Bitcoin Nodes, https://bitnodes.21.co (last visited Nov. 10, 2016).

82. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 919 (2005) ("hold[ing] that one who distributes a device with the object of promot-

creators remain the only "centralized" avenue of damage recovery when unauthorized material is appended to the blockchain. In some situations, this recovery avenue will fail because public blockchains, like Bitcoin's, are usually created and developed as an open source project, allowing the creators and developers to remain anonymous.[83] And even if known, the software designers may not even profit from their creation, making them judgment-proof.

Finally, copyright holders can attempt to recover from the subsequent infringers—individuals who downloaded their work unlawfully. The copyright holder needs to find creative ways to defeat the numerosity of infringers; a copyright holder would need to identify a large number of individuals, each liable for a small amount, and sue them, possibly collectively, in order to take advantage of economies of scale.

For instance, in *Voltage Pictures, LLC v. Does*,[84] a film producing company filed a suit against thousands of infringers over a copyrighted film. As part of the case, the company filed subpoenas with ISPs to obtain user records.[85] The company later dismissed the case but showed how identifying users can be used to recover damages. Some companies specialize in tracking infringement and enforcing copyrighted works.[86]

In a blockchain, identifying infringers can prove difficult because the cryptography associated with most blockchain protocol masks identities and IP addresses; nonetheless, anonymity in a public chain may only be superfluous. Researchers have showed how to use data publicly published on a blockchain in order to track individuals as well as their activities, accounts, and other information.[87]

In other words, based on current technology, copyright enforcement is already complicated and often unfruitful. Retrofitting current regulation to

---

ing its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties").

83. For example, Bitcoin's creator, the pseudonymous Satoshi Nakomoto, remains unmasked. Emin Gün Sirer, *How to Spot Bitcoin Inventor Satoshi Nakamoto*, MIT TECH. REV. (Dec. 10, 2015) https://www.technologyreview.com/s/544431/how-to-spot-bitcoin-inventor-satoshi-nakamoto/.

84. 818 F. Supp. 2d 28 (D.D.C. 2011).

85. Matthew Sag, *Copyright Trolling, an Empirical Study*, 100 IOWA L. REV. 1105, 1115 (2015).

86. *Id.*

87. *See, e.g.*, Malte Möser, Anonymity of Bitcoin-Transactions: An Analysis of Mixing Services (July, 2013) (unpublished manuscript), https://www.wi.uni-muenster.de/sites/wi/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf; *see also* Fergal Reid & Martin Harrigan, *An Analysis of Anonymity in the Bitcoin System*, *in* SEC. AND PRIVACY IN SOC. NETWORKS 197 (Yaniv Altshuler et al. eds. 2013), https://arxiv.org/pdf/1107.4524.pdf.

blockchain technology could provide some temporary relief. But policymakers may face the need to readdress the DMCA and E-Commerce Directive in the near future in order to find a more suitable solution. Copyright holders may also find a way within blockchain technology to better enforce their rights.[88]

This section focused on the private incentives of private individuals to censor information about themselves or their intellectual creations. The government may also wish to censor a wide variety of other types of information (e.g., child pornography, terrorist propaganda, etc.), and blockchains may make this censorship far more difficult.

While the incentives differ, the conversations and conclusions remain valid; the permanency of a blockchain creates problems. The decentralized nature of blockchains could also create additional problems that will require revisiting: since all the nodes in a public blockchain carry the same information, if unlawful information has been uploaded and if possession of the information exposes the node owner to liability (e.g., "owning" child pornography), a public blockchain could, theoretically, expose all node owners to liability (criminal and civil).[89]

Arguably, node owners could avoid liability by being classified as an ISP; clarification may, therefore, be necessary in view of this new technology with particular emphasis on how much control over a server is necessary to create liability. Alternatively, server owners can avoid having unwanted information by controlling who can write the information on their servers. The next section investigates such a server system; a private network. Specifically, the next two sections investigate how governments can use private blockchain for record keeping.

III. PRIVATE GOVERNMENTAL BLOCKCHAINS CURRENTLY INCREASE RECORD-KEEPING COSTS WITHOUT OFFERING SUFFICIENT BENEFITS

A blockchain where only authorized individuals have access to the recorded information resembles most private networks or Internet sites where

88. In the blockchain, the music/movie industry can find a solution: blockchain technology makes very small-valued transactions more affordable. Copyright holders could make their digital art freely available, but with embed codes that meter usage and charge (very small amounts) accordingly. Similarly, newspapers may switch to a freemium basis. *See* Laura Shin, *Hate Online Ads? A New Product Offers An Alternative: Micropayments*, FORBES (Feb. 9, 2016), http://www.forbes.com/sites/laurashin/2016/02/09/hate-online-ads-a-new-product-offers-an-alternative-micropayments/.

89. This issue already exists when looking at cloud technology. *See, e.g.*, Audrey Rodgers, *From Peer-to-Peer Networks to Cloud Computing: How Technology is Redefining Child Pornography Laws*, 87 ST. JOHN'S L. REV. 1013, 1045 (2013) (discussing the question of who possesses the child pornography in a cloud computing system).

information access requires credential input. While this type of blockchain creates similar issues, such as privacy and copyright infringement, these blockchains also present a possible opportunity for policymakers; governments could benefit from implementing private blockchain technologies for their record keeping. This section discusses the policy issues presented by a private access blockchain where only authorized individuals can read and write to the blockchain.

A. Cost–Benefit Analysis and the Environmental Impact of Blockchains

Concerns have been raised about both the cost to switch to a blockchain system and its environmental impact. These two issues usually go hand-in-hand to some extent, but not always, as is proven by Bitcoin.

Policymakers have looked at blockchain technology and how to efficiently implement it. For instance, the state of Vermont investigated the upsides and downsides of the technology.[90] Vermont researchers performed a cost–benefit analysis of a switch to a blockchain recording system. The state concluded that the current technological cost of switching to a blockchain did not outweigh the added security it provided.[91]

In the case of Bitcoin, the system costs are shared between all the node owners since each must purchase its own equipment to maintain the node.[92] Nakamoto originally envisioned that all nodes would also be "miners," but this is not a requirement; the functions can be separated.[93] Many nodes merely validate blocks and distribute the blockchain among other nodes; this is relatively inexpensive.[94] On the other hand, some nodes—"miners"—compete with each other to obtain a reward for "finding" a block.[95] The reward for finding a block is newly minted bitcoins, distributed only when there is consensus among the nodes that the miner has found the block.[96] Mining nodes find blocks by computing random numbers against selected transactions (hashes) until a solution is found to a complex math problem that can

90. *See* JAMES CONDOS ET AL., BLOCKCHAIN TECHNOLOGY: OPPORTUNITIES AND RISKS Ch. 5 (2016) (discussing the cost involved in setting up a mining center in order to process bitcoin data and profit).

91. "[T]he benefits of adoption of blockchain technology by state agencies is, at this time, not outweighed by the costs and challenges of such implementation." *Id.* at 20.

92. *See* NAKAMOTO, *supra* note 2, at 3.

93. *See id.* ("Each node works on finding a difficult proof-of-work for its block.).

94. Simon Barber et al., *Bitter to Better How to Make Bitcoin a Better Currency*, FIN. CRYPTOGRAPHY AND DATA SEC. 399, 401 (2012) ("Bitcoin nodes can be divided into broadly two classes, verifiers and clients.").

95. *See* NAKAMOTO, *supra* note 2, at 4.

96. *See id.* at 3–4.

only be solved by trial and error.[97] This trial and error method of problem solving requires astronomical amounts of computations, i.e. computer work.[98] Accordingly, the provision of a solution is "proof-of-work."[99] All the transactions used in finding the solution make up the next "block" of transactions in the blockchain.[100] This required work from miners is what secures the bitcoin blockchain, and the reward, along with transaction fees, is what incentivizes mining node owners to dedicate resources to doing this.[101] Because there is only one reward given per block (rather than being distributed among all miners) an arms race type scenario where mining node operators are continually adding more and faster equipment to be the first to find a block.[102] In order to assure block solutions are found at an average of ten minutes, the network periodically adjusts the difficulty of finding a solution.[103] This is designed to regulate the supply of bitcoins, but it also perpetuates the arms race scenario.[104] For this reason, the equipment and electricity costs required to profitably mine bitcoins is already enormous and ever increasing.[105]

For a private blockchain to emulate Bitcoin's, its system must also include encryption and redundancy of checking the information.[106] Without these redundancies, it would simply amount to an encrypted centralized system.[107] In other words, these processes create an even larger need for hardware, because instead of having one centralized center (and a backup), a blockchain requires a distributed system with multiple hardware centers.[108] But these redundancies are present in Bitcoin in order to verify and validate transactions without the need of a trusted party. In a private blockchain, trusted parties are necessarily present. Accordingly, in a private blockchain, the redundancies may add no utility over current centralized systems; rather, they only encumber the system.

97. *See id.* at 3.

98. *See id.*

99. *See id.* at 5.

100. *See id.* at 3.

101. *See* NAKAMOTO, *supra* note 2, at 3.

102. Morgan E. Peck, *The Bitcoin Arms Race Is On!*, IEEE SPECTRUM (May 6, 2013), http://spectrum.ieee.org/computing/networks/the-bitcoin-arms-race-is-on.

103. *See* NAKAMOTO, *supra* note 2, at 3–4.

104. *See* Peck, *supra* note 102.

105. ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES 131 (2016).

106. *See* Condos et al., *supra* note 90, at 6–7.

107. *See id.* at 7.

108. *See id.*

The fixed cost of implementing a blockchain may not be the largest roadblock. The energy consumption associated with a blockchain and its redundancy can accumulate quickly.[109] In its current Bitcoin implementation, no single entity carries the costs of running a blockchain ledger, thus it is quite difficult to estimate its true costs.[110] Nonetheless, the range of estimations show that maintaining the Bitcoin blockchain is very costly.[111] For example, the Bitcoin blockchain can require as much energy as a small town of 150,000 habitants to a country of 10 million habitants depending on the efficiencies of the machines that store and process the ledger.[112]

A private, government controlled blockchain may not require a network as large as Bitcoin and could be cheaper to run.[113] Nevertheless, due to the redundancies of a blockchain system, it would be more costly to operate than the current centralized system.[114] Furthermore, switching all recording systems to a blockchain and scaling them to the level required to serve large populations could become quite expensive and damaging to the environment.[115]

Even though proponents would argue that a governmental blockchain would be more efficient or the heat created by the blockchain could be recycled,[116] a blockchain system would remain more environmentally demanding than the current centralized system.[117] In a post-COP21 world,[118] energy consumption may become a priority for policymakers.[119] Within the current state of computing power and energy consumption, policymakers may find it difficult to argue in favor of a private blockchain for public records. Because

109. *The Great Chain*, *supra* note 19.

110. *See id.*

111. *See id.*

112. *See id.*

113. *See* DELOITTE LLP, BLOCKCHAIN ENIGMA. PARADOX. OPPORTUNITY (2016), http://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf.

114. *Id.* at 11.

115. *The Great Chain*, *supra* note 19.

116. Condos et al., *supra* note 90.

117. *The Great Chain*, *supra* note 19.

118. Coral Davenport, *Nations Approve Landmark Climate Accord in Paris*, N.Y. TIMES (Dec. 12, 2015), http://www.nytimes.com/2015/12/13/world/europe/climate-change-accord-paris.html. COP21 was the twenty-first annual session of the Conference of Parties to the United Nations Framework Convention on Climate Change (UNFCCC) that concluded on December 12, 2015. COP21 resulted in a global agreement on the reduction of climate change. *See UN Climate Change Conference Paris 2015*, UNITED NATIONS, http://www.un.org/sustainabledevelopment/cop21/ (last visited Nov. 14, 2016).

119. *Id.*

the redundancy serves little purpose in a private blockchain (which is not trustless), it may be more reasonable to simply continue using centralized databases for most government recordkeeping.

B. Trusting the Gatekeeper

In their report, Vermont policymakers identified one glaring downside to the blockchain: the technology does not guarantee content accuracy.[120] Even if a blockchain is used to keep public records, the secured information will only be as good as the human entering the information.[121] Vermont's original application protocol, however, relied on multiple human inputs in order to assure accuracy: multiple individuals agree to the transaction and the algorithm only verifies and transfers the funds.[122] The permanency of a blockchain can make record-keeping more complicated than the current system[123] because multiple trusted individuals would be required to assure the accuracy of permanent entries.[124] And the use of trusted individuals seemingly undermines the primary purpose of blockchain technology, which is to make an accurate and publicly accessible immutable record of transactions without the need for concentrating trust in third parties in order for individuals to conduct and publicly record such transactions.[125]

Furthermore, blockchains make correcting mistakes difficult because transactions are not reversible.[126] Blockchain technology was created to allow individuals who do not know or trust each other to transact together online without the need for a trusted intermediary.[127] Irreversibility ensures the reliability of transactions.[128] Accordingly, reversing blockchain transactions in order to correct mistakes defeats the purpose and design of the technology, which is why correcting mistaken entries is prohibitively difficult.

Hypothetically, a government could deploy a blockchain to maintain public real estate records.[129] Under such a system, a property purchaser could record the deed from the seller by going down to city hall, no differently than

120. Condos et al., *supra* note 90, at 19–20.

121. *Id.* at 20.

122. Anton I. Badev & Matthew Chen, Bitcoin: Technical Background and Data Analysis, Board of Governors of the Fed. Res. Sys. Fin. and Econ. Discussion Series, 11–12, (2014) (unpublished working paper).

123. *Id.* at 12.

124. *Id.*

125. *See* Condos et al., *supra* note 90, at 15.

126. *See id.*

127. *Id.*

128. *See id.*

129. *See generally* Barber et al., *supra* note 94, at 401 (discussing how this can already occur within small bitcoin transactions).

is currently done.[130] But if the transaction is recorded on a blockchain, if the human entering the transaction makes a mistake, and the buyer does not notice it, the property owner may lose the right to the property or face a lengthy legal battle.[131] In other words, a blockchain algorithm checks that the transaction can occur, but it does not check its content for accuracy. For a real estate transaction,[132] it could ensure that the seller can sell, but it does not ensure that the "correct" buyer receives the title.

Potential risks with land titles already exist and these risks have led to the creation of the title insurance market.[133] Switching to a blockchain would raise similar issues and continue the need for such risk absorbing businesses.[134] However, because blockchains timestamp any changes, if a mis-

130. Blockchain systems could provide for an opportunity to standardize recording methods across U.S. states and EU member states. *See generally* Tanya D. Marsh, *Foreclosures and the Failure of the American Land Title Recording System*, 111 COLUM. L. REV. 9 (2011) (discussing the need for a standardization of land recording across the United States and need to the move to a computer based system that would facilitate searches); De Filippi, *supra* note 6 (discussing possible applications of the blockchain technology including smart property that can be transferred within a few click thanks to their registration on a blockchain).

131. If the property is misattributed, the rightful owner would need to enjoin the misattributed owner through a court system to transfer the property to him. Any court intervention increases inefficiencies.

132. Land mapping and ownership recording has been one of the first non-financial blockchain application. Honduras and Greek politicians have expressed interest in using a form a Blockchain ledger to keep track of property ownership. *See The Trust Machine*, THE ECONOMIST (Oct. 31, 2015), http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine. A pilot of the Honduras project has allegedly provided positive results, but the project also seems to have stalled beyond these initial results. *See* Gertrude Chavez-Dreyfuss, *Honduras to Build Land Title Registry Using Bitcoin Technology*, REUTERS (May 14, 2015), http://www.reuters.com/article/usa-honduras-technology-idINKBN0O01V720150515; Peter Kirby, *A Humble Update on the Honduras Title Project*, FATCOM (Dec. 24, 2015) https://factom.com/blog/a-humble-update-on-the-honduras-title-project. An on-going project in Ghana is also mapping out all the property through a blockchain registry. Falila Gbadamassi, *Le Blockchain, La Technologie Qui Pourrait Donner Vie à Des Cadastres Virtuels*, FRANCE TV INFO. (Feb. 9, 2016) http://geopolis.francetvinfo.fr/le-blockchain-la-technologie-qui-pourrait-donner-vie-a-des-cadastres-virtuels-95941.

133. *See generally* Jean-Bernard Wurm, *How US-style Title Insurance is Transforming Risk Management in European Real Estate Markets*, 20 HOUSING FIN. INT'L 16 (2006) (noting that title insurance protect against defective titles linked to "include a gap in the chain of recorded ownership, missing documents or invalid signatures" and that Europe has adopted U.S. title insurances).

134. *See generally* Condos et al., *supra* note 90, at 9–10.

take occurs then the mistake's origin (input date, time, identity) can be traced more easily than traditional system.[135] This idiosyncrasy could ease the evidentiary issues with identifying mistakes and accelerate redressing proceedings.[136] Additionally, it can help restore records after cyber-attacks because the record could be returned to any point in time before it was changed.[137]

Alternatively, the Bitcoin protocol also enables some embedded software write-around to ensure the correct distribution of coins: its blockchain allows for "smart contracts" or software enforced contracts where a transaction occurs when some conditions are fulfilled.[138] A recordkeeping blockchain could use a similar "escrow" system where the recording is put on hold by the recorder until an interested party checks its content or time passes.[139] For instance, a birth recording could be inputted at the registry office and put in "escrow" until a parent checks the content of the registry and triggers the record permanency.

This section argues that the current computing power and protocol do not rationally support the switching of public records to a blockchain system. The marginal benefits cannot justify the costs of switching technology. The next section investigates how blockchain systems would benefit governments by providing transparency and legitimacy.

IV. GOVERNMENTS CAN ADVANCE TRANSPARENCY AND LEGITIMACY GOALS WITH BLOCKCHAIN RECORD KEEPING

While the previous sections discuss the drawbacks of blockchain technology, this section supports its adoption. The discussion in section II focused on a complete public blockchain and how policymakers need to adapt to the demand of this technology to combat old foes. The discussion in section III focused on governmental records where the records in question were only writable and accessible to governmental employees; however, this need not be the case. This section investigates the upside of adopting a different kind of blockchain: (i) a blockchain where only governmental entities can write but all can read and (ii) a blockchain where only governmental entities can read but all can write.

A. Transparency

Policymakers can implement many different types of blockchains depending on who can write and who can read the information on the ledger. A blockchain with private access for writing and public access for reading en-

135. *See generally id.*

136. *See generally id.*

137. *See generally id.*

138. *See, e.g.*, De Filippi, *supra* note 6, at 10–11.

139. *See id.* at n.52.

sures that only individuals with permission can write on it, and as such, unwanted information cannot find its way onto the chain. In general, because governmental records need to be trusted, they often fall into this category and leave individuals with rare opportunities to change their own records for things even as simple as an address change.

Over the years, policymakers have encouraged more transparency as a means to provide more accountability. For instance, the United States' Freedom of Information Act (FOIA) requires that federal agencies and departments provide public information upon request without undue delays.[140] The European Commission also has a similar legislation.[141]

Despite the legislatures' good intentions, these types of legislation often fail to fulfill their goals. First, the information requests are resource intensive: they require government employees who do not specialize in answering these kinds of requests to decide what information should or should not be disclosed.[142] While court decisions have offered some guidelines,[143] new issues constantly arise. Second, since they are so resource intensive, FOIA requests waste government resources and involve potentially large delays, depending on the nature of the information.[144]

Making public records fully accessible in a blockchain could improve transparency while also addressing some of the aforementioned shortcomings of lawmakers. Moving public records to a blockchain could remove delays because it would circumvent the need for FOIA requests. Public access for reading need not breach individual privacy: a well-designed system ensures anonymity and saves the government from expending substantial resources in collecting and recording each document multiple times for individual govern-

140. *See generally* Freedom of Information Act (FOIA), 5 U.S.C. § 552 (2012). Several states have equivalent acts. *See, e.g.*, CONN. GEN. STAT. §§ 1-200 to 259 (2015); D.C. CODE §§ 2-531 to 540 (2015); VA. CODE ANN. §§ 2.2-3704 to 3714 (2016).

141. "Any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, has a right of access to European Parliament, Council and Commission documents." Charter of Fundamental Rights of the European Union art. 42, 2000 O.J. C 364/01, at 19.

142. FOIA requests have a list of exemptions and among them, trade secrets, commercial or financial information, confidential information, etc. *See* Dep't of Justice, *Guide to the Freedom of Information Act* (2015), https://www.justice.gov/oip/doj-guide-freedom-information-act-0.

143. *Id.* All the explanations are accompanied by court decision supporting inclusion and exclusion of information. *See id.*

144. The Department of Justice reported that for 2015, its average number of days of delay was 30 days for simple requests and 174 days for complex requests, whereas the Department of State reported 111 days and 511 respectively, respectively, for the same year. *See Annual FOIA Reports*, DEP'T OF JUSTICE, https://www.justice.gov/oip/annual-foia-reports-fy-2015 (last visited Nov. 10, 2016) (Separate agency reports are found within the page).

mental agency; these documents could be recorded automatically with an appended version where the predesigned forms already hide the sensitive information.[145]

In 2016, the government of the United Kingdom (U.K.) published a report in favor of implementing this technology for specific cases.[146] Among the potential applications laid out in that report, the U.K. Chief Scientific Adviser discussed how to apply blockchain to pensions, foreign aid, and general governmental expenditures.[147] The governmental entities can write all of their expenses on a public ledger and the ledger could be available for all to see. These measures would encourage transparency and accountability because any fraud could be fully observed by the public and the press.

B. Legitimacy

This section discusses the upside of having blockchains with public access for writing and private access for reading. These types of ledgers may be even more rare than those discussed in the previous section. In general, information on the distributed ledger remains encrypted; thus, unless the information writer wishes, the information cannot be publicly accessed even if it is completely decentralized.

This type of blockchain could become central to e-voting. For instance, a system could be created where each voter has a private key that they can use to vote on a public ledger (which guarantees single entry[148]) and only the individuals running the chain can access the results (that can only be read in an aggregated manner to ensure anonymity[149]). Various implementations have been put forward to this effect.[150]

Policymakers would gain more legitimacy by using these kinds of incorruptible ledgers. Any changes in the ledger would be recorded, and any fraud

145. A large portion of governmental data comes from information collected in forms. A system could be designed to have the redacting occur *ex-ante*: on each form, individual boxes could be marked publicly visible or not.

146. *See generally* Mark Walport, *Distributed Ledger Technology: Beyond Block Chain*, U.K. GOV'T OFF. FOR SCI. (Jan. 19, 2016), https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review.

147. *Id.* at 68–71.

148. The Bitcoin protocol was designed to prevent double spending of Bitcoins. Similarly, a blockchain used for voting would prevent the possibility of double voting. Once a vote has been cast, the blockchain appending protocol would deny attempts to cast additional votes using the same blockchain token. *See* NAKAMOTO, *supra* note 2, at 3 (discussing the prevention of double spending with through the use of a "proof-of-work" mining algorithm).

149. *See id.* at 6.

150. *See, e.g.*, Guy Zyskind et al., *Decentralizing Privacy: Using Blockchain to Protect Personal Data*, 2015 IEEE COMPUTER SOC'Y SEC. AND PRIVACY WORKSHOPS 180, 183 (2015).

would be observed and traceable to whomever entered the fraudulent entries: blockchains need not rely on the honesty of the implementer but instead on mathematic accuracy to ensure every single vote is casted by the live voting population.

First, this kind of e-voting would avoid issues of hanging chads.[151] It would remove ambiguity about the intent of the voters when casting ballots in some jurisdictions. For example, the 2000 U.S. presidential election exemplifies how a system can fail, removing a candidate's aura of legitimacy. During these elections, counting issues arose because of the uncertainties about the vote casting and these issues lead to delays; this ultimately required the U.S. Supreme Court to intervene.[152] The courts' involvements have arguably tainted the elections.[153] Relying on a foolproof blockchain could redress some of these issues and reestablish voters' faith in the system.

Second, switching to secured blockchain e-voting could increase legitimacy. Voters could cast their votes from smartphones or home computers, or still go to a public election booth, and these votes would be recorded on a secured blockchain. Easier means of voting could help voter turnout, increase the feeling of democracy, and bestow any elected candidate with more legitimacy.

Finally, blockchain technology could be used to avoid fraudulent voting. For example, blockchain e-voting could avoid ghost voting fraud. Ghost voting is the practice of voting for individuals who are not present or do not exist.[154] A smart blockchain could contain a protocol automatically to check birth and death registries.[155] A smart blockchain could also record the location of individuals when they vote through their phone's GPS, computer IP address, or voting booth.

---

151. *See* Frederick G. Conrad et al., *Electronic Voting Eliminates Hanging Chads but Introduces New Usability Challenges*, 67 INT'L J. HUMAN-COMPUTER STUD. 111 (2009) (arguing in favor of e-voting, but also recommending a better interface).

152. Bush v. Gore, 531 U.S. 98 (2000).

153. Adam Cohen, *Has Bush v. Gore Become the Case That Must Not Be Named?*, N.Y. TIMES (Aug. 15, 2016), http://www.nytimes.com/2006/08/15/opinion/15tues4.html (arguing that "Bush v. Gore was not a legal decision but a raw assertion of power").

154. Brian Kim, *Help America Vote Act*, 40 HARV. J. ON LEGIS. 579, 599 (2003).

155. While its name has been associated with voter fraud, ghost voting also occurs at the legislative level. Ghost voting in parliamentary chambers has recently raised problems on both sides of the Atlantic. *See In European Parliament, Probe Into Ghost Voting for Far-right's Le Pen*, DEUTSCHE WELLE (Oct. 30, 2015), http://www.dw.com/en/in-european-parliament-probe-into-ghost-voting-for-far-rights-le-pen/a-18816733; George Spencer, *NBC10 Investigators Uncover Allegations of Voter Fraud in Harrisburg*, NBC 10 PHILA. (Feb. 18, 2016) http://www.nbcphiladelphia.com/news/local/voter-fraud-ghost-voting-harrisburg-369312361.html.

V. CONCLUSIONS

In general, while considering a switch to blockchain technology, policymakers need to reinvestigate a number of laws and rights. Privacy rights and copyrights have suffered in the Internet age, and blockchain technology may not ease this issue, even if it was created with privacy in mind.

Government may not find the need to switch to a blockchain technology for record keeping just yet. Its implementation involves switching and variable costs that are not justified by the marginal improvement in record keeping; nonetheless, the policy and political push for more transparency could prove to be the deciding factor.

This article does not directly address the financial sector. The blockchain applications to this sector open a host of new questions for policymakers, and policymakers may need to address financial regulation in the view of blockchain technology becoming more mainstream in financial markets. Bitcoin and other virtual currencies have been categorized as the currency of criminals, and Silk Road has been used as the prime example of how Bitcoin can be used in nefarious ways.[156]

Anti-money laundering and counter-terrorist financial measures have become a talking point for policymakers. As recently as June 2015, the European Parliament has passed a new regulation and amended a directive to address money laundering.[157] These new legislations increase the "Know-Your-Customer" requirements for payment service providers.[158] The directive and regulation are broad enough to include digital instruments, but they focus on third-party intermediaries and their duties.[159] As such, a decentralized currency system based on blockchain technology could still avoid this regulation because no payment service provider exists *per se*. However,

156. Jared A. Kleiman, *Beyond the Silk Road: Unregulated Decentralized Virtual Currencies Continue to Endanger US National Security and Welfare*, 4 NAT'L SEC. L. BRIEF 59, 60 (2013), http://digitalcommons.wcl.american.edu/nslb/vol4/iss1/5/.

157. Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, 2015 O.J. (L 141/1) [hereinafter Council Regulation 2015/847 (EU)]; Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, 2015 O.J. (L 141/73) [hereinafter Council Directive 2015/849 (EU)].

158. *See* Council Regulation 2015/847 (EU), *supra* note 157; Council Directive 2015/849 (EU), *supra* note 157.

159. *See id.*

policymakers may decide to target what the IMF describes as "gatekeepers" or virtual currency intermediaries.[160]

Even though the system is decentralized, some chokepoints remain: the currency exchanges, the currency holding service providers, etc. Some of these services could already qualify for regulation. For instance, a currency holding apparatus (known as virtual wallet) could be considered a deposit, and the wallet providers could be considered banks for the purpose of the regulation; nonetheless, most of these chokepoints fall outside current regulation, and need not keep nor provide a record of their transactions to the authorities.[161] The lack of accountability to a policing authority leaves users exposed to attacks without potential remedies and allows potential transfers that finance criminal activities.

From identity recording to wills and testaments,[162] blockchain technology has untapped potential, and entrepreneurs continue finding new applications that will require the participation of policymakers for proper implementation.

160. He et al., *supra* note 9.

161. For example, governments like the Isle of Man have recognized these issues and implemented measures in the form of a regulatory framework where cryptocurrency exchanges must register and abide by the island's anti-money laundering and know-your-customer requirements. Jeremy Khan, *Greetings From Bitcoin Island: No Place on the Planet Has Welcomed Digital Currencies as Warmly as the Isle of Man*, BLOOMBERG (Sept. 8, 2015), http://www.bloomberg.com/news/features/2015-09-07/isle-of-man-tax-haven-with-tailless-cats-becomes-bitcoin-hub. The issue remains the same if the exchange is not located on the island.

162. A blockchain system could be applied to property transfers. Wills and testaments are a specific form of property transfer: a property transfer triggered by the death of the original interest holder. Wills recorded in a blockchain have one major upside—they are timestamped. A constant recording of all wills and the time-stamping of all wills would reduce disputes over the validity a purported will. In other words, the blockchain can carry out the function of a trustless and always accurate notary to prove the time of the document's existence, not necessarily that it represents the true will of the deceased. *See* Trevor I. Kiviat, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569 (2015). Beyond the recording of wills upon a blockchain ledger, smart wills could involve the automated transfer of a smart property upon the death of its owner when the ledger automatically checks the death registry and finds that the writer of the will passed away. Instead of relying on human input, the algorithm can find and retrieve the information from other records. Transfers could include land titles and currency already registered in a blockchain. Trusts could be automated as well. For instance, an inheritance could automatically divest when the beneficiary turns 18, gets married, has children, etc.