Journal of Health Care Law and Policy

Volume 20 | Issue 1 Article 5

# Exploring Applications of Blockchain in Securing Electronic Medical Records

Bach Nguyen

# EXPLORING APPLICATIONS OF BLOCKCHAIN IN SECURING ELECTRONIC MEDICAL RECORDS

BACH NGUYEN

## I. INTRODUCTION

In the Summer of 2016, a hacker by the name of "thedarkoverlord" stole over 650,000 medical records from the databases of three separate healthcare institutions.[1] The hacker was not only selling the records for hundreds of thousands of dollars online,[2] but may also have been extorting the institutions by demanding money to prevent further attacks and distribution of records.[3] The value of these medical records is ten to sixty times greater than a credit card number on the black market,[4] as the information on the records may be used to perpetrate other types of fraud[5], such as filing fraudulent tax returns, making these records a prime target for malicious hackers.[6]

Unfortunately, this is not an isolated or uncommon incident. In 2015, nearly 100 million healthcare records were compromised.[7] The attacks affect everyone, from everyday people to celebrities such as Kanye West.[8] The combination of the value of medical records and the relatively low cybersecurity of healthcare facilities[9] make healthcare records one of the most lucrative targets for



1. Bradly Barth, *Hacker Purportedly Selling Over 650,000 Stolen Medical Records on Dark Web Marketplace*, SC MAGAZINE, (Jun. 27, 2016), https://www.scmagazine.com/hacker-purportedly-selling-over-650000-stolen-medical-records-on-dark-web-marketplace/article/529296/.

2. *Id.*

3. *Id.*

4. Caroline Humer & Jim Finkle, *Your Medical Record is Worth More to Hackers Than Your Credit Card*, REUTERS, (Sept. 24, 2014), http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924; Jennifer Schlesinger & Andrea Day, *Dark Web is Fertile Ground for Stolen Medical Records*, CNBC, (Mar. 11, 2016), http://www.cnbc.com/2016/03/10/dark-web-is-fertile-ground-for-stolen-medical-records.html.

5. Humer & Finkle, *supra* note 4.

6. Jennifer Schlesinger & Andrea Day, *Dark Web is Fertile Ground for Stolen Medical Records*, CNBC, (Mar. 11, 2016), https://www.cnbc.com/2016/03/10/dark-web-is-fertile-ground-for-stolen-medical-records.html.

7. *Id.*

8. Glenn Minnis, *Kanye West Medical Records Stolen, Heads Set to Roll at UCLA Medical Center*, INQUISITR.COM, (Dec. 21, 2016), http://www.inquisitr.com/3815695/kanye-west-medical-records-stolen-heads-set-to-roll-at-ucla-medical-center/.

9. Humer & Finkle, *supra* note 4.

cybercriminals.[10] According to the Department of Health and Human Services, more than 113 million records were compromised in 2015, and during the first quarter of 2016, the healthcare industry averaged 4 attacks per week.[11] In fact, the 2016 IBM Cyber Security Intelligence Index named the healthcare industry the single most attacked industry.[12] Efforts to modernize healthcare facilities to match the rapidly advancing technological landscape has created and exposed a host of vulnerabilities that are actively targeted by malicious parties.[13]

In the financial world, the rise of Bitcoin,[14] a digital currency, and the underlying technology, the blockchain, has upturned traditional notions of banking and finance,[15] capturing immense attention during its meteoric rise.[16] For the creator of Bitcoin, the decentralized, tamper-proof system was the much-needed alternative to centralized banking following the financial crisis of 2008.[17] The blockchain is a data structure that uses cryptography to allow participants to securely manipulate data without the need for a central authority.[18] The application of blockchain is not limited to Bitcoin, however, with many eager to apply the technology to other areas, such as contracts and business with *Etherium* and the *DAO*.[19]

There have been numerous calls to invest more into improving the state of EMRs, including increased engagement between the public and private sector and a more defined NIST framework to help providers secure their data.[20] This paper seeks to examine the potential applications of blockchain technology to the

10. Schlesinger & Day, *supra* note 6.

11. Nsikan Akpan, *Has Health care Hacking Become an Epidemic?*, PBS (Mar. 23, 2016) http://www.pbs.org/newshour/updates/has-health-care-hacking-become-an-epidemic/.

12. *Expert Tells House Committee: "Healthcare Cybersecurity Is Worse Than Reported"*, BUSINESSWIRE (Apr. 5, 2017) http://www.businesswire.com/news/home/20170405006088/en/.

13. Jonathan H. Lomurro, *Electronic Medical Records: Changing Medical Malpractice Litigation*, 300 N.J. LAW. 36, 37 (2016).

14. Bitcoin is a popular cryptocurrency, which is a digital currency with no central bank and instead is managed by a decentralized network of computers which manage and maintain the transactions that occur on the network. *See infra* § III. A.

15. Michael R. Gordon et al., *Bitcoin to Blockchain: How Laws and Regulations Are Conforming to and Impacting the Use of Virtual Currency*, N.Y.C. B. ASS'N (Apr. 28, 2016), http://www.nycbar.org/cle-offerings/if-i-were-a-virtually-rich-man-developments-in-the-laws-and-regulations-impacting-the-digital-currency-revolution/.

16. *See* Paul Vigna, *For Bitcoin, A Year like No Other*, WALL STREET J. (Dec. 31, 2017), https://www.wsj.com/articles/for-bitcoin-a-year-like-no-other-1514721601.

17. Maria Bustillos, *The Bitcoin Boom*, NEW YORKER (Apr. 1, 2013), http://www.newyorker.com/tech/elements/the-bitcoin-boom.

18. Steven Norton, *CIO Explaner: What Is Blockchain?*, WALL STREET J. (Feb. 2, 2016), http://blogs.wsj.com/cio/2016/02/02/cio-explainer-what-is-blockchain/.

19. *See* Joshua Fairfield, *Smart Contracts, Bitcoin Bots, and Consumer Protection*, 71 WASH. & LEE L. REV. ONLINE 35 (Sept. 2014), http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1003&context=wlulr-online (Etherium is a cryptocurrency similar to Bitcoin. The DAO is a decentralized autonomous organization, that takes its name from the concept from which it is derived).

20. *Supra* note 12.

healthcare industry with the goal of securing and maintaining medical records. First, the paper will examine the current state of the healthcare industry, particularly the history and use of electronic medical records ("EMR"), the laws and rules regulating the use of EMR, and the current state of security.[21] Next, the paper will discuss the blockchain, including its application in other contexts.[22] Finally, the paper will analyze the possible applications of the blockchain to the implementation and maintenance of EMR systems, potential security features to accompany the implementation, and the feasibility of those applications.[23] Overall, blockchain technology shows a great deal of promise for information security, however further developments are necessary before it can be adopted for electronic medical records.

## II. THE CURRENT LANDSCAPE OF ELECTRONIC HEALTH RECORDS

The medical field has rapidly adopted new technology in recent decades, from new instruments and tools to improve the care provided, to healthcare information infrastructure and record storage.[24] This shift towards EMR and electronic health records ("EHR") was a method of replacing cumbersome and antiquated paper charts.[25] The rapid adoption, did not adequately address security concerns, leading to exploitable security concerns in an industry ill equipped to deal with the demands of this new technology.[26] To understand this situation, it is important to take a closer look at how the current systems came into place.

### *A. History and State of Electronic Medical Records*

Electronic records generally come in two forms: electronic medical records, and electronic health records.[27] EMR are an electronic version of traditional paper medical charts, filled out and maintained by clinicians, which document

21. *See infra* Part II.

22. *See infra* Part III.

23. *See infra* Part IV.

24. *See* Wynne M. Snoots, *Information Technology and the Medical Profession: A Curse or an Opportunity?*, BAYLOR UNIVERSITY MEDICAL CENTER PROCEEDINGS, (Apr. 15, 2002), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1276501/.

25. Jonathan H. Lomurro, *Electronic Medical Records: Changing Medical Malpractice Litigation*, 300 N.J. LAW. 36, 37 (2016).

26. Lydia J. Andrasz, *HIPAA and Electronic Medical Records: Benefits and Security Issues*, 25 DCBA BRIEF 26, 29 (2012); Lori J. Strauss, *Electronic Medical Records—Benefits and Liabilities, Organizations Must Safeguard Against Risks When Using Electronic Medical Records*, 17 J. HEALTH CARE COMPLIANCE 57, 57-58 (2015); Niam Yaraghi, *A Health Hack Wake-Up Call*, USNEWS (Apr. 1, 2016), https://www.usnews.com/opinion/blogs/policy-dose/articles/2016-04-01/ransomware-hacks-are-a-hospital-health-it-wake-up-call.

27. *What Are the Differences Between Electronic Medical Records, Electronic Health Records, and Personal Health Records?*, HEALTHIT.GOV, (last updated Nov. 2, 2015), https://www.healthit.gov/providers-professionals/faqs/what-are-differences-between-electronic-medical-records-electronic.

the patient's medical history and treatment.[28] By contrast, EHR contains the aforementioned information, in addition to information from all clinicians involved with the patient's care, providing a more comprehensive view of the patient's health.[29] Both types of records are typically stored and managed locally by the healthcare provider, where providers either purchase software from a vendor, or create their own.[30] While there were 632 certified vendors as of July 2016,[31] the lion share of the market is covered by Epic Systems, servicing major medical providers such as Kaiser Permanente, CVS's Minute Clinics, and Johns Hopkins, and covering 56% of Americans' medical records.[32]

In 2004, the Bush administration heavily pushed the adoption of EMR and EHR (herein referred to as "EMR"), with the goal of pushing most American medical records to electronic systems capable also of sharing data between providers and institutions, by 2014.[33] The Obama administration continued with this plan, introducing a five-year plan in 2009, which included financial incentives for adoption and cuts to Medicare payments for non-adopters.[34] Both administrations saw this as a method of improving care and cutting costs.[35] These financial incentives increased enrollment astronomically, from 9.4% of US hospitals using digital systems in 2008, to 75.5% in 2014, just six years later.[36] Because of the rapid adoption, security concerns became a priority.[37] The Department of Health and Human Services ("HHS") issued regulations through the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule, in 2000, and the HIPAA Security Rule, in 2003.[38] These rules set standards for information privacy, namely ensuring the security and integrity of patient

28. Lydia J. Andrasz, *HIPAA and Electronic Medical Records: Benefits and Security Issues*, 25 DCBA BRIEF 26, 26 (2012); *see also What are the Differences Between Electronic Medical Records, Electronic Health Records, and Personal Health Records?*, HEALTHIT.GOV, (last updated Nov. 2, 2015), https://www.healthit.gov/providers-professionals/faqs/what-are-differences-between-electronic-medical-records-electronic; Strauss, *supra* note 26, at 57–58.

29. Andrasz *supra* note 28; *see also What are the Differences Between Electronic Medical Records, Electronic Health Records, and Personal Health Records?*, HEALTHIT.GOV, (last updated Nov. 2, 2015), https://www.healthit.gov/providers-professionals/faqs/what-are-differences-between-electronic-medical-records-electronic.

30. *Id.*

31. *Health Care Professional EHR Vendors*, HEALTHIT.GOV (Jul. 2016) https://dashboard.healthit.gov/quickstats/pages/FIG-Vendors-of-EHRs-to-Participating-Professionals.php.

32. Patrick Caldwell, *We've Spent Billions to Fix Our Medical Records and They're Still a Mess. Here's Why*, MOTHERJONES (Oct. 21, 2015), http://www.motherjones.com/politics/2015/10/epic-systems-judith-faulkner-hitech-ehr-interoperability.

33. Andrasz *supra* note 28; *see also* Jonathan H. Lomurro, *Electronic Medical Records: Changing Medical Malpractice Litigation*, 300 N.J. LAW. 36, 36–37 (2016).

34. *See supra* note 33.

35. Andrasz *supra* note 28.

36. *See* Caldwell, *supra* note 32.

37. *See* Andrasz, *supra* note 28; Strauss, *supra* note 28.

38. *See* Andrasz, *supra* note 28.

information especially for EMRs.[39] The Health Information Technology for Economic and Clinical Health ("HITECH") Act was enacted and became effective in 2009, further enforcing these rules.[40]

Despite these efforts, vulnerabilities still exist in current systems, with tens of millions of records having been lost or stolen since 2009.[41] Hackers have regularly been able to compromise the security of these healthcare providers, whether they be state health departments, hospitals, or private practices.[42] Each provider is responsible for ensuring their system, whether they purchase a system from a provider or create their own.[43] The result is widespread inconsistencies in security levels, as well as difficulty communicating across platforms and between providers.[44] To further complicate issues, some providers like Epic have made it more difficult for their system to communicate with other systems.[45] perhaps in an attempt to avoid compromising information to less secure systems or in an effort to lock its providers in its own ecosystem. Cybersecurity is aptly called an arms race between security experts and hackers, and inconsistencies across systems create exploitable vulnerabilities with catastrophic consequences.[46]

### *B. HIPAA Privacy Rule and "Break-the-Glass" Procedure*

There are a few laws that address security issues regarding healthcare information and medical records. Most relevant to EMR are HIPAA and the HITECH act. "Congress enacted HIPAA on August 21, 1996 to 'improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long–term care services and coverage, to simplify the administration of

39. *Id.*

40. *See* Andrasz, *supra* note 28; Lomurro, *supra* note 33.

41. *See* Andrasz, *supra* note 28.

42. *See id.*

43. *See* Andrasz, *supra* note 28; *What Security Safeguards are Designed to Prevent Electronic Health Records from being Hacked?*, HEALTHIT.GOV, (last updated Jan. 15, 2013), https://www.healthit.gov/patients-families/faqs/what-security-safeguards-are-designed-prevent-electronic-health-records-being.

44. *See Health Information Privacy, Security, and Your EHR*, HEALTHIT.GOV, (last updated Apr. 13, 2015), https://www.healthit.gov/providers-professionals/ehr-privacy-security; Leon Rodriguez, *Privacy, Security, and Electronic Health Records*, HEALTHIT.GOV, (Dec. 12, 2011), https://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/privacy-security-electronic-health-records/; Andrasz *supra* note 28.

45. *See* Caldwell, *supra* note 32.

46. *See* Max Taves, *How Fear and Self-Preservation Are Driving a Cyber Arms Race*, CNET.COM, (May 2, 2015), https://www.cnet.com/news/how-fear-and-self-preservation-are-driving-a-cyber-arms-race/.

health insurance, and for other purposes.'"[47] Additionally, Congress instructed HHS to provide recommended standards for the privacy of personal health information.[48] The "Privacy Rule" was promulgated in 2001, allowed 2-3 years for covered entities, including health plans, healthcare clearinghouses, and most healthcare providers, to come into compliance with the rule.[49] In general, the rule defines and limits the ability for covered entities to access patient health information, and also guarantees patients to access his or her own information.[50]

Following initiatives to incorporate technology into healthcare,[51] the HITECH Act was signed into law in 2009.[52] In addition to promoting the use of EMR, the Act also greatly emphasized the importance of information privacy and security by enforcing the prior HIPAA rules.[53]

On the opposite end of the increased privacy and security protections are "break-the-glass" procedures. "Break-the-glass"—or "break glass"—procedures are mechanisms to provide access of personal health information to otherwise non-authorized parties in the event of an emergency.[54] Examples of where "break glass" procedures may be necessary range from a mundane forgotten password or username, to more extreme situations where a provider who otherwise does not have access to a particular patient's records is nonetheless thrust into an emergency medical situation where access to the patient's information is necessary for treatment.[55] One common solution is to use a generic "emergency" user account that enables access to otherwise restricted personal health information, where access to the user account is overseen by some reasonable administrative measures.[56] Use of the account is also subject to audit, further minimizing risk of abuse through reprimand.[57]

### *C. The Current Security Protocol for Healthcare Systems*

The HIPAA "Security Rule" requires "specific measures to safeguard [patients'] electronic protected health information to ensure its confidentiality,

47. Deborah F. Buckman, *Validity, Construction, and Application of Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Regulations Promulgated Thereunder*, 194 A.L.R. Fed. 133, §2 (Originally published in 2004); *See also* Andrasz, *supra* note 28.

48. Buckman *supra* note 47; *see also* Andrasz, *supra* note 28.

49. *Id.*

50. *Id.*

51. *See supra* Part II.A.; *see also* Andrasz, *supra* note 28.

52. *See* Andrasz, *supra* note 28.

53. *Id.*

54. *Break Glass Procedure: Granting Emergency Access to Critical ePHI Systems*, YALE.EDU, (Dec. 2004), http://hipaa.yale.edu/security/break-glass-procedure-granting-emergency-access-critical-ephi-systems.

55. *Id.*

56. *Id.*

57. *Id.*

integrity, and security."[58] Beyond that, however, the statute does not offer much guidance, suggesting features including "access controls" such as passwords or encryption.[59] The specifics are largely left to the provider and their capabilities and budget, which is the reason why there are such broad discrepancies in security across the healthcare industry.[60] Where cybersecurity is a fast moving field, this means many providers may be operating on outdated software, leaving vulnerabilities especially exposed.[61] As of July 2016, 75% of providers using certified technology were still using technology that met HHS's 2014 certification requirements, where the remaining providers were still using 2011 certified technology.[62] This does not include providers that are using uncertified technology, or none at all.[63] Given the current state of healthcare cybersecurity, it is clear that far more needs to be done to secure patient information.

## III. AN OVERVIEW OF THE BLOCKCHAIN

A blockchain, a technology originally developed with Bitcoin[64], is a peer-to-peer network where each computer in the network verifies and records every transaction on the network, and transactions are only recorded on the ledger once the network confirms the validity of the transaction, thus preventing third party manipulation and streamlining the record.[65] Every modification to the ledger is autonomously reviewed and verified against the ledger recorded on each computer in the network, so if there is an illegitimate change on any single computer, or node, in the network, the change is invalid and will not be recorded.[66]

. Imagine a single parent preparing a grocery list. This parent has a child with a particular affinity for sweets. As a comparison to a traditional computer

58. *What Security Safeguards are Designed to Prevent Electronic Health Records from being Hacked?*, *supra* note 43.

59. *Id.*

60. *See supra* Part II.A.

61. *See* Feisal Nanji, *Security Challenges of Electronic Medical Records*, COMPUTERWORLD.COM (Feb. 9, 2009), http://www.computerworld.com/article/2531320/security0/security-challenges-of-electronic-medical-records.html (discussing vulnerabilities in modern health systems, including having equipment with inadequate protection, and having equipment connected to the web for convenience, leaving that equipment vulnerable to attack).

62. HEALTH CARE PROFESSIONAL EHR VENDORS, HEALTHIT.GOV (Jul. 2016) https://dashboard.healthit.gov/quickstats/pages/FIG-Vendors-of-EHRs-to-Participating-Professionals.php.

63. *Id.*

64. Bitcoin is a popular cryptocurrency, which is a digital currency with no central bank and instead is managed by a decentralized network of computers which manage and maintain the transactions that occur on the network. *See infra* Part III.A.

65. Nicolette De Sevres, Bart Chilton & Bradley Cohen, *The Blockchain Revolution, Smart Contracts and Financial Transactions*, 21 CYBERSPACE LAW. NL 3, 3 (2016).

66. Michele D'Aliessi, *How Does the Blockchain Work?*, MEDIUM (Jun. 1, 2016), https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae.

system, suppose the parent writes his grocery list and leaves the list on the refrigerator to take to the store at a later date.[67] Also suppose the parent periodically revises the list, crossing off unnecessary items and adding new items.[68] Knowing this, the child can then go to the refrigerator and modify the grocery list to include her favorite sweets or exclude her least favorite foods.[69] Assuming the child is skillful in her modifications, the handwriting for the changes would be indistinguishable from the parent's, and the parent could go on to buy items according to the modified list, and not according to the untampered, accurate list.[70] Because the parent is prone to revising the list, even if a modification was detected, it would be difficult to distinguish a legitimate modification (made by the parent) from an illegitimate modification (made by the child).[71] Additionally, even supposing there was a record of each iteration of the list, it would be difficult to isolate exactly when the illegitimate modification occurred without additional information, and so it would be difficult to revert to the most recent legitimate form of the list.[72] The parent could revert to the first iteration of the list, thus guaranteeing that no modifications have been made, but this risks losing all the legitimate modifications the parent made at later dates.[73] The parent could revert the list to a more recent version of the list, but it would be difficult to be certain that this eliminated the illegitimate modifications, as the child may have made the modification in an earlier version. This is analogous to many modern information storage systems, where information is stored at a single location, so if an attacker is able to access the system and modify the information undetected (such that, to the system, the attacker is indistinguishable from a legitimate user), it becomes very difficult to identify and reverse the illegitimate modification without either losing valuable data or risking not eliminating the modification.[74] Most modern cybersecurity measures revolve around developing more sophisticated methods of detecting and reversing unauthorized access or developing more secure methods of granting and denying access, resulting in a race with attackers who develop more sophisticated means of bypassing these security features.[75]

The blockchain takes a different approach to solving this problem. Continuing with the analogy, suppose the parent instead keeps multiple copies of the list around the house and other locations, such in his car and on his cell phone. Instead of maintaining the list in series, that is, keeping copies of each

67. *See generally Id.*
68. *Id.*
69. *Id.*
70. *Id.*
71. *Id.*
72. *Id.*
73. *Id.*
74. *Id.*
75. *Id.*

iteration of the list, the lists themselves self-maintain in parallel, meaning whenever the parent legitimately modifies one list, every other list verifies the authenticity of this modification and updates to reflect the change.[76] Suppose the child now were to illegitimately modify the list on the refrigerator; the parent would easily be able to discover not only that this particular list was modified, but also what was modified by comparing the list to every other list.[77] This allows the parent to correct the list, and also to evaluate flaws with that particular list.[78] An important conceptual point is that there is no master grocery list.[79] The parent is not modifying one list and then merely copying the information from that list onto every other list as, the child could then identify which list was the master list, modify that list, resulting in the parent copying that information onto every other list. Instead, each list is equally legitimate, therefore the child would have to modify every list in the network of lists without being detected, which is far more difficult to accomplish than modifying one list.[80]

While the process of simultaneously updating lists may be difficult for a single parent to accomplish, the task is far easier for a computer network, where each computer in the network contains a "list" and can go through the updating and verification process without a centralized "parent" figure.[81] More accurately, each "list" or system containing the "list" is able to self-monitor and regulate modifications, and verify the modifications independent of a third party, such as the parent or the child, making the network peer-to-peer, where each peer is a "list" or system containing the "list."[82] This is the key difference that makes networks and systems operating with a blockchain structure far more difficult to tamper with and modify without authorization.[83]

### *A. Bitcoin and Other Applications of Blockchain*

For Bitcoin and similar cryptocurrencies, blockchain is used as a ledger to record transactions.[84] The basic set-up is such: there is a network of computers on which this ledger exists.[85] When an individual makes a purchase using Bitcoin, that transaction occurs instantaneously across two nodes, or "blocks," in the network, or "chain."[86] Because the transaction occurred across two nodes at the exact same time, there was a legitimate exchange, and this transaction is

76. *Id.*
77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*
81. *Id.*
82. *Id.*
83. *Id.*
84. Norton, *supra* note 18.
85. *See generally How Does Bitcoin Work?*, BITCOIN.ORG, https://bitcoin.org/en/how-it-works.
86. *See generally id.*

recorded on the ledger of every computer in the network in an updating process.[87] On the other hand, if the ledger on one node changes without any others, as is the case when a hacker makes a unilateral change on one node, the change is cross-referenced with every other system in the network, and because the ledgers no longer match, the change is illegitimate and is undone.[88] The verification process is completed through "mining," an autonomous process where computers in the network "donate" computing power used to verify transactions.[89] As compensation and incentive, "miners" generate new Bitcoin (at very low rates to avoid inflation), which stimulates the Bitcoin economy and facilitates further transactions.[90]

Another notable application of blockchain is in "The DAO." "The DAO" (not to be confused with a decentralized autonomous organization, of which "The DAO" is one, and from which "The DAO" takes its name) is a collection of smart contracts built on the Ethereum blockchain, which sets the rules for and collects money from investors and invest that money based on how the investors vote.[91]

"The DAO" operates on Ethereum, a decentralized cryptocurrency similar to Bitcoin, but, which can run smart contracts.[92] A smart contract is created by encoding the terms of a traditional contract and uploading the smart contract to the blockchain.[93] "Contractual clauses are automatically executed when pre-programmed conditions are satisfied," and because the transactions are monitored, validated, and enforced by the blockchain, there is no need for a trusted third party, such as an escrow agent.[94] "Where a smart contract's conditions depend upon real-world data (e.g., the price of a commodity future at a given time), agreed-upon outside systems, called oracles, can be developed to monitor and verify prices, performance, or other real-world events."[95]

"A standard DAO framework has been written by Slock it and can be found on its GitHub. This framework is written. . .to run on the Ethereum blockchain. It has been developed free and open source, so everyone can reuse it to create its

87. *Id.*

88. *Id.*

89. *Id.*

90. *Id.*

91. Michael del Castillo, *The DAO: Or How A Leaderless Ethereum Project Raised $50 Million*, COINDESK.COM, (May 12, 2016), http://www.coindesk.com/the-dao-just-raised-50-million-but-what-is-it/.

92. Rob Price, *A 3-Minute Guide to Ethereum, the Crazy Digital Currency that was Just Rocked by a $50 Million Hack*, BUS, INSIDER, (Jun. 17, 2016), http://www.businessinsider.com/what-is-ethereum-decentralised-digital-currency-hit-by-50-million-hack-the-dao-smart-contracts-hard-fork-2016-6?r=UK&IR=T.

93. De Sevres et al., *supra* note 65.

94. *Id.*

95. *Id.*

own Decentralized Autonomous Organization."[96] Slock.it is a for-profit company registered in Germany, which developed the basic framework for a DAO blockchain.[97] The project is open-source, which means that anyone can access and change the framework. However, "The DAO" runs on a particular client or version, which is downloaded by members,[98] where users on a different or modified version are limited or unable to communicate with users on the main distribution.[99]

There have been multiple other explorations and proposals for the capabilities that blockchain offers, generally leveraging the tamper-proof nature of the ledger or the decentralized and peer-to-peer characteristics of the technology, notably in the works of Joshua Fairfield, Victor Li, Tom Bell, Nick Vogel, and Michael Abramowicz.[100]

### *B. Blockchain and Privacy*

While blockchain technology is very effective at facilitating and maintaining records for peer-to-peer, tamper-proof transactions, it is not innately designed with information privacy in mind.[101] Being fundamentally open, a basic blockchain allows anyone on the network to read the contents on the network;[102] the writing or modification process is what is secured.[103] Returning briefly to the grocery list analogy, the child is able to read what is on the grocery list without much issue, but has far more difficulty modifying the grocery list without detection.

There have been a number of recent projects aimed at utilizing blockchain technology to secure privacy. Mooti CEO Brad Chun recently unveiled the company's first project, Mootipass, which provides a cryptographic

96. *What is the DAO?*, THEDAOWIKI, (last updated Jun. 29, 2016), https://daowiki.atlassian.net/wiki/display/DAO/Introduction+to+the+DAO; *see also* Castillo, *supra* note 91.

97. *The DAO Framework, Slock.it FAQ*, SLOCK.IT, https://slock.it/index.html.

98. Vitalik Buterin, *Onward from the Hard Fork*, ETHERIUM.ORG, (Jul. 26, 2016), https://blog.ethereum.org/2016/07/26/onward_from_the_hard_fork/.

99. *Id.*

100. Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, (2016) (discussing numerous applications for blockchain); Michael Abramowicz, *Cryptoinsurance*, 50 WAKE FOREST L. REV. 671 (2015) (discussing applications for insurance); Tom Bell, *Copyrights, Privacy, and the Blockchain*, 42 OHIO N. U. L. REV. 439 (2016) (discussing applications for copyright and privacy); Fairfield, *supra* note 19; Joshua Fairfield, *Bitproperty*, 88 S. CAL. L. REV. 805 (May, 2015) (discussing applications for property records); Victor Li, *Bitcoin's Useful Backbone*, 102 A.B.A. J. 31 (Mar. 2016) (discussing applications for private record keeping); Nick Vogel, *The Great Decentralization: How Web 3.0 will Weaken Copyrights*, 15 J. MARSHALL REV. INTELL. PROP. L. 136 (2015) (discussing consequences for copyright law).

101. *See* Vitalik Buterin, *Privacy on the Blockchain*, ETHERIUM.ORG (Jan. 15, 2016) https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/.

102. D'Aliessi, *supra* note 66.

103. *Id.*

identification and validation service.[104] The service uses technology developed by the company,[105] called "Identity Chains," which builds off of blockchain technology to allow for identification without divulging personal information.[106] Customers could entrust their personal information to the company, which would then secure the personal information using cryptography across a blockchain, and then provide only as much information as necessary to other vendors to verify the customer's identity.[107] For example, if bank asks whether a customer is old enough to open an account, Mooti could confirm that the customer was of age without revealing the customer's exact age.[108] Other companies, such as tech giant Microsoft, have also been working on blockchain based identity systems.[109]

Another project from bitcoin experts and researchers at MIT, dubbed Enigma, was revealed in June of 2015,[110] tackles the problem differently. The technique, called "secure multiparty computation," is a method of encryption that divides data into hundreds of indecipherable chunks and distributes those chunks randomly across hundreds of computers in the network.[111] Computations can be performed on the chunks of data without revealing the contents of the data to external observers or even the computers performing the computations.[112] The Enigma network also stores the record of who owns the data on a blockchain, where the owner can reassemble the pieces of data in order to decrypt the information.[113] Only when all the pieces are assembled correctly can the data be read; this allows data to be shared online while still keeping the data private.[114] By utilizing the blockchain, Enigma is able to perform encrypted computation at several orders of magnitude faster than previous encryption schemes, though still ten to a hundred times slower than performing the computation without encryption.[115] Additionally, as with all computations on blockchain, the system requires a fairly large network to operate, and the security of the system increases with the number of computers in the network, but the speed decreases with the

104. Brady Dale, *Microsoft and Mootipass Bet Identity could be Blockchains' Killer App*, OBSERVER.COM, (Aug. 18, 2016), http://observer.com/2016/08/mootipass-blockchain-identity-brad-chun/; *See also* MOOTIPASS.COM, http://mootipass.com/.

105. Dale, *supra* note 104.

106. Andrew Egbert et al., *Identity Chains*, IACR.ORG, https://eprint.iacr.org/2016/469.pdf (last visited Jan. 1, 2018).

107. Dale, *supra* note 104.

108. *Id.*

109. *Id.*

110. Andy Greenberg, *MIT's Bitcoin Inspired 'Enigma' Lets Computers Mine Encrypted Data*, WIRED.COM, (Jun. 30, 2015), https://www.wired.com/2015/06/mits-bitcoin-inspired-enigma-lets-computers-mine-encrypted-data/.

111. *Id.*

112. *Id.*

113. *Id.*

114. *Id.*

115. *Id.*

increasing size of the network.[116] Both Mooti and Enigma are still in early stages of development, however, and still need to be completed and tested.[117]

Another security measure is multi-factor authentication.[118] This security measure has already been offered by popular services such as Google and Facebook since 2011, requiring both a password and a security code sent to the account owner's cell phone in order to log in.[119] This principle is more flexible, and generally revolves around authentication using two or more different verification methods, commonly referred to by "something you know (such as a password), something you have (a trusted device that is not easily duplicated, like a phone), something you are (biometrics [such as a fingerprint])."[120] Securing information through this extra level makes it far more difficult for unauthorized attackers to access an account.[121] . For example, if an attacker acquires a patient's password through a computer scam, phishing, or other method, it is unlikely that they are also able to steal a physical object from the patient, and furthermore acquire the patient's fingerprint.[122] Where blockchain typically is secured by a private cryptographic key known only to the owner,[123] a multi step authentication process could further secure the owner's information.

## IV. APPLICATION OF BLOCKCHAIN TO ELECTRONIC MEDICAL RECORDS

Given the dynamic uses of blockchain technology, EMR can utilize the technology in several ways to increase security. One method is similar to the model presented by Mooti, where data is stored securely on the blockchain, and access to that information is granted as necessary to authorized parties.[124] A second method is similar to Enigma, where the entire medical record, including private information, is distributed in cryptic chunks across a network and is only assembled and decrypted for the owner.[125] Both models provide advantages and present challenges, however, as technology advances, both show promise for the future of medical record security.

116. *Id.*

117. Dale, *supra* note 104; Greenberg, *supra* note 110.

118. Kelly Gremban et al., *What is Azure Multi-Factor Authentication?*, MICROSOFT AZURE, (Dec. 8, 2016), https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication.

119. Alex Wawro, *How to Set-Up Two-Factor Authentication for Facebook, Google, Microsoft, and More*, PCWORLD, (Apr. 25, 2013), http://www.pcworld.com/article/2036252/how-to-set-up-two-factor-authentication-for-facebook-google-microsoft-and-more.html.

120. Gremban et al., *supra* note 118.

121. Wawro, *supra* note 119.

122. Gremban et al., *supra* note 118.

123. *How Does Bitcoin Work?, supra* note 85.

124. *See supra* Part III.B.

125. *See supra* Part III.B.

### *A. EMR Using the Mooti Model*

Using a service similar to Mooti, a patient's health record could be held securely on a blockchain network.[126] Upon visiting a healthcare center, the patient could verify her identity, allowing the physician to access the patient's medical record.[127] Further security measures could require the patient to perform a multi-step authentication,[128] which could take many forms including using the patient's health information that is already on record as a method of identity verification. Additionally, given the current proliferation of fingerprint scanners on smartphones and other devices, there are many different avenues to pursue in implementing multi factor authentication.[129] This way, access to the patient's information is limited where the patient is not present. A concern is that the service too strictly regulates the information to which the physician has access, where a physician should be granted broad access to the patient's medical record to consider potential health conflicts and interactions between treatments and conditions, and to work on the patient's case where the patient is not present.

A nuance of HIPAA worth noting is that de-identified health information is not covered by the Act.[130] What this means is that the health information and personally identifiable information can be provided separately.[131] Using a similar service as Mooti, personally identifiable information may be provided separately to a full medical record, or not provided at all and merely used to verify the identity of the patient and grant access to the medical record.[132] The fact that de-identified health information is not covered by HIPAA also means that physicians may still work on a patient's case without the patient's presence by merely working with the de-identified file.[133] This file would still be protected from tampering thanks to the blockchain, and the personal information would be even more secured from unauthorized viewers by the service.[134]

One major difficulty arises with "break glass" procedures. Due to the increased security measures, access to health information in emergency

126. *See supra* Part III.B.

127. *See supra* Part III.B.

128. *See supra* Part III.B.

129. *See* Gremban et al., *supra* note 118.

130. Buckman *supra* note 47.

131. *Id.*

132. Buckman *supra* note 47; Dale, *supra* note 104.

133. *See* Buckman, *supra* note 47 (Encryption can be realized in several different ways to achieve security; one additional way worth further exploration is utilization of the patient's personally identifiable information to generate a security key that would link the protected, personally identifiable information with the non-protected medical history. In separating the personally identifiable information with the medical information, EMR providers would be able to hold the personal information in strict protection, while allowing more ease of access to the medical information to which physicians need more immediate access. In a similar model as Mootipass, the record could simply verify the identity of the patient without revealing more sensitive personal information that is not relevant to the practice of medicine, allowing physicians to perform their duties.); Dale, *supra* note 104.

134. *Id.*

situations may become prohibitively difficult.[135] Emergency situations may arise where patients are unable to provide the necessary multi-factor authorization, in which case some remedial procedure would need to be available.[136] A simple solution would be to scrap the multi-factor authentication and verification, however this invites abuse and unnecessarily sacrifices security for the sake of convenience and accessibility.[137] Reintroduction of an auditing process could dissuade abuse and encourage diligence,[138] and could operate in conjunction with proactive measures to maintain security and privacy. In a "break glass" situation, the authentication requirements could be relaxed in proportion to the circumstances. Because the current system requires at least some personally identifiable information to retrieve the relevant medical records,[139] that information could be the basis of a "break glass" authentication. In fact, having a multi-factor authentication scheme in place allows for alternative avenues for "break glass" authentication, for example if a patient does not have identification but is still able to provide a fingerprint, or vice versa. Certain aspects of a patient's medical record, such as dental records or DNA information, can be incorporated into a remedial, "break glass" multi-factor authentication scheme in order to provide multiple, robust avenues for emergency situations.[140]

One criticism of the Mooti model is that the information is still somewhat centralized, where the Mooti service serves as a gatekeeper, and a successful attack on the service could reveal information that would compromise all the patients served by the service.[141] The second option of the Enigma model provides a more decentralized system, and may be able to leverage more of the security provided by blockchain.

### *B. EMR Using the Enigma Model*

Under an Enigma-style service, the patient's entire medical record would be divided and distributed in cryptographically secured chunks of data, which could be reassembled and decrypted with proper authentication.[142] Although there is the option of having the patient authenticate an interaction using a personal device interfacing with the provider's device, this would disadvantage patients who either do not use or do not have access to a portable computer or

135. *See Break Glass Procedure: Granting Emergency Access to Critical ePHI Systems*, YALE.EDU, (Dec. 2004), http://hipaa.yale.edu/security/break-glass-procedure-granting-emergency-access-critical-ephi-systems.

136. *See id.*

137. Wawro, *supra* note 119.

138. *Break Glass Procedure: Granting Emergency Access to Critical ePHI Systems*, *supra* note 135; Rodriguez, *supra* note 44.

139. *Id.*

140. *See* Gremban et al., *supra* note 118.

141. *See generally* Dale, *supra* note 104.

142. *See supra* Part III.B.

smartphone. A more elegant solution, therefore, would be to use multi-factor authentication.[143] Having a similar security protocol for the physician would ensure that the patient's file could only be accessed and modified by the authorized physician.[144] Similar to the discussion of the Mooti system above, information could also be separated such that the patient's authentication only allows access to the medical record, and no personally identifiable information. The personally identifiable information could remain encrypted in the way Enigma allows where no outside party nor the computer could access the information.[145]

Another benefit of blockchain worth noting is that the peer-to-peer capabilities would allow physicians to collaborate in determining the best course of treatment for a patient. Similar to the voting process on "The DAO,"[146] physicians collaborating on a case could offer their medical judgment in a fast and reliable way. Furthermore, the autonomous programs could present patient information devoid of any personally identifiable information, such that it would be a simple matter of sharing the patient's condition without violating HIPAA.[147] This would make it a simple task to obtain a second opinion, should the patient or physician seek a second opinion.[148]

One drawback of the Enigma system in comparison to existing databases is speed.[149] In some medical contexts, minor delays may not be a concern, however in emergency "break-the-glass" situations, the time taken to decrypt the information may be intolerable. While the speed of the system is improving,[150] the delay is nonetheless a factor worth scrutiny when evaluating the viability of the system.

### *C. Other Considerations*

Blockchain technology as a whole is relatively new, and remains in testing.[151] As with any new technology, caution must be taken, especially when valuable information is at stake.[152] Additionally, the technology remains very demanding both in terms of computing power and raw energy investment,[153] and

143. *See supra* Part III.B.

144. *See supra* Part III.B.

145. *See supra* Part III.B.

146. *See* Castillo, *supra* note 91("anyone around the world who has bought DAO tokens with ethers—votes on decisions, allocates resources and in theory, creates a wide-range of possible returns.")

147. Buckman *supra* note 47.

148. *See generally supra* Part III.A.

149. *See supra* Part III.B.

150. Greenberg, *supra* note 110.

151. Greenberg, *supra* note 110.

152. *Id.*

153. Sebastiaan Deetman, *Bitcoin Could Consume as much Electricity as Denmark by 2020*, VICE.COM, (Mar. 29, 2016), https://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020.

hospital systems may be hesitant to invest so heavily into a security system, especially where many hospitals currently struggle to pay for existing, less elaborate security systems.[154]

## V. CONCLUSION

Security and privacy remain a massive concern for the healthcare industry. While blockchain technology is still in development and undergoing testing, many recent developments show a great deal of promise in terms of securing information and valuable data. Data breaches have only become more severe as technology has advanced, and with the current organization of security solutions, this trend seems unlikely to change in meaningful ways. With blockchain comes a fundamental reorganization of how data is stored and secured, and is worth serious consideration as medical providers and security experts look for solutions to secure patient information.

154. Nanji, *supra* note 61.