NEW KID ON THE BLOCK: HOW BLOCKCHAIN CAN IMPROVE THE UNITED STATES FOOD SECTOR

Kyler Massner†

I. INTRODUCTION

In January 2018, the first transaction of United States soybeans to China took place entirely on the blockchain.[1] Blockchain—a decentralized public ledger—al-

† J.D., Drake University Law School, 2019; B.A. Political Science, University of Iowa, 2012. The author would like to thank his soon to be wife Taylor for being my rock and son Kasch for providing me the inspiration to "go for it." The author would also like to thank the Editorial Board of the *Drake Journal of Agricultural Law* for all their hard work in

lowed the parties to drastically cut costs and increase transaction speed by digitizing the terms of the contract without a third party facilitator.[2] Reductions in cost and improved efficiency are vital for the agricultural industry to turn a profit—hence, the large sums of investment by the industry in blockchain should come as no surprise.[3]

Not only can blockchain cut costs, but it can make the United States food sector safer by permitting unprecedented levels of traceability at a low cost, while also securing valuable intellectual property. Realizing these advantages is currently underway. For example, Walmart announced in September 2018 that it would begin to use blockchain to track every shipment of spinach and lettuce sold in its stores.[4] This announcement was in response to a nationwide contamination of romaine lettuce which caused widespread illness, the removal of suspect inventory, and accounted for millions in lost profit.[5] Many of these consequences can be attributed to the inability to differentiate safe versus contaminated food product, such being the byproduct of a convoluted supply chain and inadequate food monitoring system.[6]

This is all about to change. With blockchain real time management, quality control, and traceability of a product in the supply chain is now becoming a reality.[7] By the fall of 2019, Walmart will require more than 100 farmers to input information about their product into a blockchain developed by IBM.[8] For Walmart, this move fits into a broader strategy of ensuring safe, quality, yet affordable food products for its customers.[9] Blockchain helps accomplish this strategy by providing unprecedented and cost-effective access to information regarding the source and quality of food in the supply chain. In the event of another emergency, this would enable companies to either entirely prevent contaminated product from ever

making this publication possible.

1. *U.S. soy cargo to China traded using blockchain*, REUTERS: MKT. NEWS (Jan. 22, 2018), https://perma.cc/7RQB-AYH2.

2. *Id.* (stating Louis Dreyfus' global head of trade operations, Robert Serpollet, commented that by leveraging blockchain the time spent processing documents and data relating to the transaction was reduced five-fold).

3. *Id.*

4. Michael Corkery & Nathaniel Popper, *From Farm to Blockchain: Walmart Tracks Its Lettuce*, N.Y. TIMES (Sept. 24, 2018), https://perma.cc/P8D7-U3UB.

5. *Id.*

6. *Id.*

7. *Id.*

8. *Id.*

9. *Id.*

reaching the shelves, or alternatively, to make a quick recall of contaminated product with surgical accuracy.[10] These claims were realized when Walmart put blockchain to the test. In its test, it took Walmart seven days to track a piece of fruit to a specific farm using conventional systems, but with blockchain that seven days dropped to only to a matter of seconds.[11]

These advantages are not alone for the private sector to reap. Governments are increasingly looking to blockchain as a way of improving administrative efficiency and effectiveness. The main argument of this note is that both public and private stakeholders in the United States food sector should leverage blockchain to improve the health, safety, and quality of the nation's food product while also ensuring producers remain competitive in the global market. The food sector, from farmers to end user, is critical to both the economic and human health of the nation. If blockchain is leveraged, the sector will not only have a distinct comparative advantage on the international market, but will also help achieve goals laid out by the federal government.

This note will begin with a brief description of what blockchain is and how it provides the advantages discussed. While the discussion and implications of blockchain will be done in depth, it is by no means meant to be an exhaustive examination of the technology.

Part two of the note will focus on the many component parts of the United States food sector. This includes how the sector operates, how it monitors food products for safety, and how the federal government has classified it as critical infrastructure. Finally, I will discuss the hurdles academics and government agencies face when researching or administering the sector, and how these hurdles can be addressed with blockchain.

II. BLOCKCHAIN

A. What is it?

The year was 2008 when a programmer going by the pseudonym Satoshi Nakamoto integrated a host of cryptographic and digital tools to lay the foundation of a new database protocol which became known as blockchain.[12] Blockchain is a distributed immutable ledger, upon which Satoshi Nakamoto built "Bitcoin"—a decentralized digital currency—which ensures the integrity of information without

10. *Id.*
11. *Id.*
12. SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 1, https://perma.cc/JRY7-HRU7 (archived Sept. 5, 2019).

centralized control.[13] Essential to blockchain is a peer-to-peer network of computers that validates, maintains, and records data on an immutable ledger, where security is accomplished by encryption mechanisms built directly into the network.[14] Since Bitcoin's launch in 2009, it has rapidly become one of the largest payment systems in the world.[15]

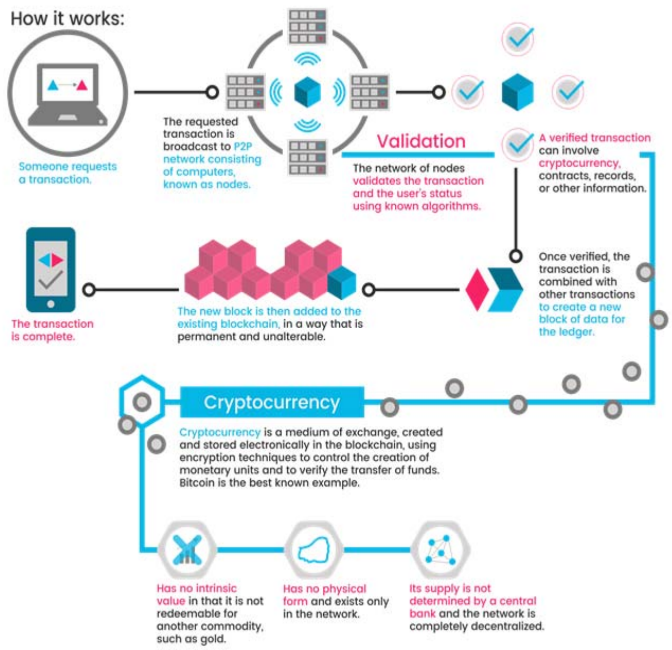
In general, blockchain is a technology which stores information that is highly resistant to modification. Such information is stored on blocks placed into a chronological chain synchronized across multiple computers. While data can be added to the blockchain, no information can be modified retroactively or even deleted without alerting the network. These mechanisms make information on the blockchain highly resistant to malicious attacks or data loss. For a bird's eye view of the process Don and Alex Tapscott summarized it as such,

> Every ten minutes, like the heartbeat of the bitcoin network, all the transactions conducted are verified, cleared, and stored in a block which is linked to the preceding block, thereby creating a chain. Each block must refer to the preceding block to be valid. This structure permanently time-stamps and stores exchanges of value, preventing anyone from altering the ledger. If you wanted to steal a bitcoin, you'd have to rewrite the coin's entire history on the blockchain in broad daylight. That's practically impossible. So the blockchain is a distributed ledger representing a network consensus of every transaction that has ever occurred. Like the World Wide Web of information, it's the World Wide Ledger of value—a distributed ledger that everyone can download and run on their personal computer.[16]

For a visual representation of how the process work FIGURE-1 is provided below.

13. *Id.* at 4.
14. *Id.* at 8.
15. PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW 20-21 (2018).
16. DON TAPSCOTT & ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION 7 (2016).

FIGURE-1[17]



B. The "Trust Machine"

The advantages of blockchain stem from the ability to trust in a scientific process that is not dependent upon human agency.[18] In an ordinary transaction, trust is derivative of the integrity of the parties involved, and while it is appealing to think people can be trusted, history has shown us as prone to mistake, self-interest, and even fraud.[19] Consequently, a society like ours, which increasingly depends on global relationships, is particularly vulnerable to parties or systems which are beyond our ability to effectively monitor, especially if located in foreign countries.[20] Moreover, these global relationships are often facilitated by third party intermediaries (e.g., Wells Fargo Bank, Citibank, Louis Dreyfus Company, and

17. Max Teodorescu, *Blockchains promise to change the world; here's everything you need to understand*, ELECTRONIC PRODUCTS (Nov. 11, 2016), https://perma.cc/9S5D-2H6E.

18. TAPSCOTT & TAPSCOTT, *supra* note 16, at 10-11.

19. *Id.*

20. *Id.*

Archer Daniels Midland Company, etc.), who—by their position—harvest value for themselves while creating a byzantine system which hinders efficiency and accountability.[21] These intermediaries also collect vast amounts of sensitive data, which are stored in centralized databases and become prime targets for cybercrime.[22] The Federal Bureau of Investigation estimated such cybercrime cost the economy $1.4 billion in 2017.[23]

Blockchain avoids these issues by relying upon a consensus driven cryptographically secured network that cultivates trust and integrity independent of a validating authority and without the need for a centralized database.[24] This was enabled by the creation of a consensus protocol unique to blockchain which distributes such functions to a network instead of by centralizing them.[25]

A consensus protocol can be articulated as the "rules of the road" governing how the network agrees on what information should be recorded on the blockchain versus what information should not be.[26] The collection of all the information forms a data entry, referred to as a "block," which must reference every prior block to be considered an accurate representation of information on the blockchain.[27] It is important to note that information in a block can take many forms, thus making agreement on what information is valid and worthy of being recorded an important issue.[28] Consensus protocols solve this issue and, while many types exist, the original and arguably most secure protocol—Proof of Work (PoW)—is the one which underlies Bitcoin.[29]

In the PoW protocol, the network of computers is incentivized to dedicate computing power, time, and energy to solve a complex algebraic riddle (a process called *hashing*), which ensures the security, confidentiality, and accuracy of data contained on a block.[30] Hashing is the process of taking information and masking it via a cryptographic algorithm which immunizes the information from decoding or tampering.[31] Moreover, since validity requires this process to reference the entire history of the chain, no one actor can rewrite history without such changes

21. *Id.*
22. *Id.*
23. *Latest Internet Crime Report Released*, FBI (May 7, 2018), https://perma.cc/76JU-R46N.
24. TAPSCOTT & TAPSCOTT, *supra* note 16, at 11.
25. *Id.*
26. *Consensus for Kids*, LISK, https://perma.cc/5LPY-NHDN (archived July 11, 2019).
27. *Hashing*, LISK, https://perma.cc/UG2J-6KBG (archived July 11, 2019).
28. *Consensus for Kids*, *supra* note 26.
29. TAPSCOTT & TAPSCOTT, *supra* note 16, at 31.
30. *Id.* at 31-32.
31. *Hashing*, *supra* note 27.

being easily witnessed.[32]

A block is validated once the hash is found via the expenditure of work—i.e., time, energy, computing power.[33] The product of this work is easily verifiable which, combined with the cost required to conduct it, dissuades foul play and proves to the network that the block is accurate and trustworthy.[34] Furthermore, this is where information is time-stamped—creating data that is traceable and immutable from the moment of creation.[35]

To note how excited people are about the potential implications of blockchain, The Economist October 2015 cover story, titled *The Trust Machine*, describing it as having the potential to "change how the economy works."[36] In sum, because the accuracy, security, and validity of information can be realized—not via a centralized actor but instead by a network—blockchain provides the infrastructure to efficiently and securely maintain and distribute information worldwide absent conventional risks.[37] A network which natively ensures trust and integrity regardless of the actions of others.[38]

III. BLOCKCHAIN ADVANTAGES

A. Security and Resiliency via Decentralization

One advantage of blockchain is its decentralization. Since a blockchain can be *bootstrapped*—downloaded and maintained easily by anyone on nearly any computer device—the result is a single database capable of being hosted on thousands of computers worldwide, thus providing a database resilient to hacks or catastrophic system failure.[39] Moreover, because data on the blockchain is constantly broadcast and maintained on thousands of computers within the network, the information is always available and immune to loss.[40] Consequently, as long as there is one computer within the network keeping the blockchain updated, the blockchain survives and with it—your valuable data.[41] FIGURE-2 below depicts this concept of a centralized versus decentralized database.

32. TAPSCOTT & TAPSCOTT, *supra* note 16, at 30-31.

33. *Id.*

34. *Id.*

35. *Id.* at 30-31 (e.g., like a mosquito trapped in amber, so too is information via this hashing process).

36. *Id.* at 8.

37. TAPSCOTT & TAPSCOTT, *supra* note 16, at 31-32; *Hashing*, *supra* note 27.

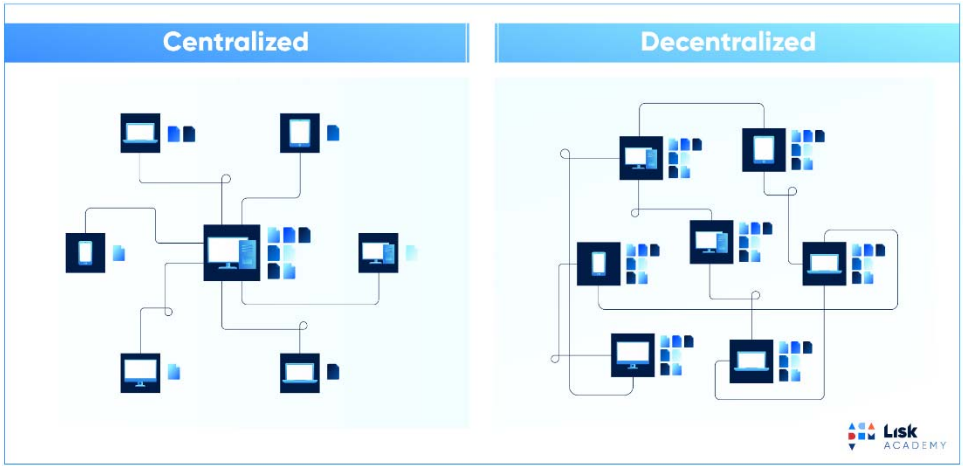
38. TAPSCOTT & TAPSCOTT, *supra* note 16, at 33.

39. *Id.* at 34.

40. *Id.*

41. *Id.*

FIGURE-2[42]



B. Security via Encryption

A second advantage of blockchain is that it provides a mechanism for encrypting data and communications against theft and malicious behavior. Encryption devices are embedded at every level in blockchain.[43] In blockchain, opting out is not an option and individual instances of reckless behavior do not affect others on the network.[44] Such lengths means users transacting on blockchain need not concern itself with hackers since the design of the network natively defends itself against such acts.[45]

While encryption processes may vary between blockchains, in Bitcoin there are only two types at work. The first is public key infrastructure (PKI), a type of asymmetric cryptography where users use two keys (one for encrypting and one for decrypting information) in order to interact with the network.[46] Similar to a two-key system required to access a safety deposit box, these keys help guard a user's data against fraudulent activity since nothing can occur without using both keys.[47] Via PKI encryption, Bitcoin has become the second largest deployment of encryption in the world.[48]

42. *Blockchain Network Explained*, LISK, https://perma.cc/FLZ7-7MUZ (archived July 11, 2019).
43. TAPSCOTT & TAPSCOTT, *supra* note 16, at 39-40.
44. *Id.* at 39.
45. *Id.* at 40.
46. *Id.* at 39-40.
47. *Id.* at 6.
48. *Id.* at 39-40.

The second encryption process, SHA-256, is the cryptographic hash function which determines the difficulty of the hashing process on the Bitcoin network.[49] SHA-256 was published by the United States National Institute of Standards and Technology and is accepted as a United States Federal Information Processing Standard.[50] SHA-256 sets the difficulty of the hashing process which secures that information on a block is valid.[51]

By way of these encryption devices, the confidentiality of a communication or validity of a dataset is insulated against the risks associated with centralized data and cybercrime.[52] This means the risks of data being manipulated or falling into the wrong hands is greatly reduced. Additionally, the risk of system failures crippling entire businesses are nearly eliminated, all of which is made possible by a low cost technology that provides the infrastructure for individuals to securely communicate and maintain encrypted, authenticated, and traceable data.[53]

C. The Internet of Things and Traceability

Beyond secure databases possibly the most disrupting advantage of blockchain is the traceability it enables, both on the blockchain itself and in providing the Internet of Things (IoT), smart contracts, and decentralized applications (dApps) a secure place to operate, record information, and conduct automated actions.[54] The IoT is the term used to define the network of internet-connected devices which communicate, sense, and interact with each other and the external world (e.g., drones, soil moisture probes, etc.).[55] Without blockchain, IoT devices lack the infrastructure which allows secure communication and data storage. Blockchain provides this infrastructure and creates a transparent digital record of the information provided by IoT devices. Furthermore, since IoT devices can be placed virtually anywhere, operators are allowed to track and monitor individual products quickly and, since data is timestamped, temporal information is provided which can be analyzed to see how and when a product has changed overtime.[56]

---

49. *Id.* at 40.
50. *Id.* at 40-41.
51. *Id.*
52. *Id.* at 39.
53. *See id.* at 41.
54. *Id.* at 7, 22.
55. *Internet of Things*, GARTNER: IT GLOSSARY, https://perma.cc/53KA-5HUG (archived July 11, 2019).
56. TAPSCOTT & TAPSCOTT, *supra* note 16, at 22, 152-55 (explaining an IoT device could pinpoint where a grain shipment is in a supply chain, what the current temperature or moisture is, while the blockchain provides a look into how such factors have changed throughout the course of that grain shipments life).

With the access to such large yet individualized amounts of information, operators could efficiently prove compliance with regulations, safely distribute information, or quickly optimize their own production lines.[57]

Another potential of blockchain is it enables smart contracts and dApps. A smart contract is a piece of code which executes a set of complex instructions on the blockchain, while dApps are decentralized applications existing on a blockchain instead of an individual's personal device.[58] Together, smart contracts and dApps provide an interface to the blockchain making it easy to interact with and leverage its advantages.[59] For example, it can be used to make a self-executing contract where payments are immediately dispersed once obligations are fulfilled. In farming operations, this can be used to facilitate direct purchasing from producers and eliminate the need for third party brokers. It could also be leveraged to alert an owner and automate operations based upon weather data, soil moisture, or livestock health.[60] Lastly, it could be used by those in the food industry to meet consumer demands to see where and how that product (e.g., beef) was raised (e.g., grass-fed or not) and brought to their local supermarket.[61] These and other features can increase the efficiency and quality of production improving the safety and competitiveness of the sector in the global market.[62] In fact, research and testing of blockchain in this sector is already being conducted by the Blockchain Food Safety Alliance to improve food tracking, safety, and to meet consumer demands for greater transparency.[63]

Not only can the private sector leverage blockchain, but governments can as well. Indeed, governments are increasingly looking to take advantage of these same capabilities as a way of improving a government's response to threats or their administration of oversite and enforcement with regulatory frameworks.[64] For example, because blockchain provides an immutable record that is easily shared, government officials could use blockchain to automate alerts to flag suspicious activity or accumulate better data to create more effective and tailored policies.[65] These

57. *Id.*

58. *Id.* at 47, 101-02, 152-55; Jake Frankenfield, *Decentralized Applications – dApps*, INVESTOPEDIA: CRYPTOCURRENCY (Feb. 6, 2018), https://perma.cc/H9KK-EM3C.

59. TAPSCOTT & TAPSCOTT, *supra* note 16, at 47, 101-02, 120-21, 152-55.

60. *Id.* at 47, 101-02, 152-55.

61. *Blockchain Transparency Explained*, LISK, https://perma.cc/5SNG-LY56 (archived Sept. 18, 2019).

62. TAPSCOTT & TAPSCOTT, *supra* note 16, at 47.

63. TREVOR AMEN & TANNER EHMKE, BLOCKCHAIN: CHANGE IS COMING TO AGRICULTURAL SUPPLY CHAINS 3 (2018), https://perma.cc/G5VC-6BPJ.

64. TAPSCOTT & TAPSCOTT, *supra* note 16, at 66, 203-07.

65. *Id.* at 66; AMEN & EHMKE, *supra* note 63.

advancements were noted by Jesse McWateres, the World Economic Forum's financial innovation leader, who commented, "The most exciting thing about [blockchain] is how traceability can improve systemic stability" thus "allow[ing] regulators to use a lighter touch."[66]

Together, all this data made possible by these various technologies provides a level of identification and traceability previously beyond our grasp.[67] For example, if an outbreak occurred in a group of livestock inside an operation utilizing blockchain, one could protect human lives and economic wealth by quickly tracking the threat to the exact source(s) of contamination (e.g., a single cow), in addition to learning what caused the outbreak, who is at risk, and how this threat began or changed over time.[68] See FIGURE-3 for a representation of the areas which blockchain could connect.

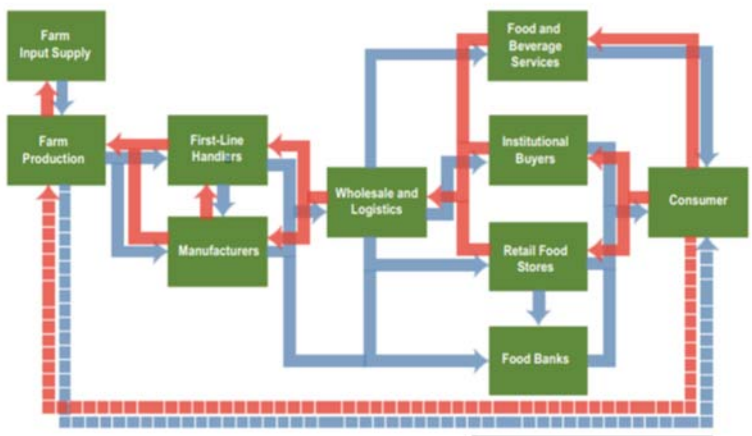
FIGURE-3[69]

66. TAPSCOTT & TAPSCOTT, *supra* note 16, at 66.
67. *Id.* at 22, 152-55.
68. *Id.* at 97-99.
69. AMEN & EHMKE, *supra* note 63, at 2.

IV. INTRODUCTION TO THE UNITED STATES FOOD AND AG SECTOR

The United States food system is a remarkable success, providing unprecedented access to a relatively inexpensive and varied supply of food.[70] The food system has been so successful that it represented approximately 5% of the United States' gross domestic product in 2012, affecting the life of every American citizen while exerting influence around the world.[71] This success has been made possible via a complex and dynamic supply chain composed of many actors operating within broader social, economic, and physical contexts.[72] Because of this complexity, policy decisions regarding this system have implications for a multitude of actors, all with differing interests (e.g., human and environmental health, domestic and international economics, etc.).[73] FIGURE-4 below provides an illustration of the "food supply chain" which is defined as a process through which "raw materials and inputs are turned into edible food products that are consumed by end-users."[74]

FIGURE-4[75]



70. INST. OF MED. & NAT'L RESEARCH COUNCIL, A FRAMEWORK FOR ASSESSING EFFECTS OF THE FOOD SYSTEM 1 (Malden C. Nesheim et al. eds., 2015), https://perma.cc/BXJ2-WJK5.

71. *Id.* at 1, 37.

72. *Id.* at 1, 6.

73. *Id.* at 1.

74. *Id.* at 31.

75. *Id.* at 2.

As presented in the above image primary production of food product often begins in the farm production sector where farmers and ranchers utilize resources to produce raw agricultural commodities (i.e., crops or livestock).[76] Despite some raw food product being sold directly from farmers, the vast majority of it proceeds through several different hands before ultimately being consumed.[77] This process often begins by farmers selling their product to first line handlers or primary processors.[78] This group includes farming cooperatives, commodity traders, bakeries, and meat packers, among others—who either prepare the raw food product or pass it along to wholesalers or other entities with logistic services.[79] Wholesalers purchase this product and store it throughout a network of warehouses and then distribute it to retailers via extensive transportation operations.[80] Logistic firms, in contrast, do not actually take possession of the food product, but instead are paid to provide distribution and inventory coordination services in addition to placing buyers with sellers.[81] Once a buyer is found, the food product is then passed onto the retail food sector which includes grocery stores, retail outlets, and restaurants—where consumers or restaurants ultimately buy the food product for further preparation and consumption.[82]

This most basic description of the process highlights the complexity which characterizes the food supply chain, but also the many points where information can be collected or contamination may occur. If such a system, or even part of it, were to leverage the advantages of blockchain, the safety of food product would rise.

V. Policy Environment of the Food Sector

The United States food system has long been shaped by legislation to address concerns of both environmental and human health.[83] After the events of September 11, 2001, the nation's attention refocused on food security issues relating to bioterrorism and identified the food and agriculture sector as critical infrastructure.[84]

76. *Id.* at 32.
77. *Id.*
78. *Id.*
79. *Id.* at 32-33.
80. *Id.* at 33.
81. *Id.*
82. *Id.* at 33-34.
83. *Id.* at 64-68.
84. K.R. Schneider et al., Agroterrorism in the US 1 (2015), https://perma.cc/M839-U4EH.

Many of the policies seek to ensure the safety of our food by deployment of monitoring systems and periodic testing.[85] By leveraging blockchain, government agencies could track product and accrue vital information which will improve the success rates of such systems.

For environmental concerns, the United States Department of Agriculture (USDA) and the Environmental Protection Agency (EPA) are the two agencies tasked with researching, writing and implementing policy.[86] The USDA has tackled environmental concerns by providing technical and financial assistance to farmers via voluntary programs and public investment.[87] USDA programs include commodity payments to farmers for adopting conservation plans, paying farmers to remove environmentally sensitive areas from active production, and cost-share incentives to install and maintain environmentally sound practices.[88] In conjunction, the EPA creates national policy and guidelines and then delegates to the states the responsibility for addressing specific issues.[89] For both the USDA and EPA programs, the information collected via the deployment of IoT devices secured on the blockchain could be used to efficiently tailor programs, improve accountability, and achieve better results.

The Food and Drug Administration (FDA) and USDA both administer policy concerning the health and safety of the nation's food supply.[90] It is important to note FDA and USDA's safety regulations apply only to those products in interstate commerce (which is a vast majority of total food product), while the FDA's Food Code provides only a model for jurisdictions to manage the safety of food in the service and retail sector.[91] Formulating this policy is largely the product of a consensus of government, academic, consumer, and private actors.[92]

Ensuring food safety has largely focused on managing and reducing risks associated with pathogen contaminated food product.[93] Contamination of a food source can originate from sources such as farms and food handlers or can occur when the food is either stored, transported, or processed.[94] The first instance of legislation addressing these concerns began with the Pure Food and Drug Act of

85. *Id.* at 3.
86. INST. OF MED. & NAT'L RESEARCH COUNCIL, *supra* note 70, at 65-66.
87. *Id.* at 66.
88. *Id.*
89. *Id.*
90. *Id.* at 68.
91. *Id.*
92. *Id.*
93. *Id.* at 67.
94. *Id.*

1906 that was subsequently supplemented by later laws which culminated with the Food, Drug, and Cosmetic Act of 1938.[95] Since 1938, other legislation (e.g., Federal Meat Inspection Act, the Poultry Products Inspection Act, the Egg Products, and Inspection Act) have worked to protect consumers and is administered by the USDA's Food Safety and Inspection Service.[96]

It was in response to substantial outbreaks and public concern that the Hazard Analysis and Critical Control Points (HACCP) approach to food safety began in the 1960s.[97] Originating within the United States space program, HACCP is a risk-based prevention-focused approach for pathogen, chemical, and physical hazards.[98] Based upon HACCP assessments, regulations have emerged including the FDA's Low Acid Canned Food, the USDA's Pathogen Reduction/HACCP rule, and the FDA's HACCP regulations concerning seafood and juice.[99] Most recently, the Food Safety Modernization Act (2010) expanded the preventative HACCP strategy for food safety to products not covered by current regulations and places the responsibility for recording and reporting food safety issues increasingly on food companies.[100]

In addition to the aforementioned policies, two major policies were signed in the wake of September 11, 2001. The first policy, the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (the Act), recognized that the agriculture and food production sector was at particular risk for bioterrorism (the use of biological agents as weapons to advance personal or political goals), and was implemented to increase the nation's ability to prevent and respond to bioterrorist attacks or other public health emergencies.[101] Pursuant to the Act, the FDA is charged with developing and implementing regulations to increase security which include: registration of food facilities, notification of imported food, establishment and maintenance of records, and administrative detentions.[102] The Act empowers the FDA by leveraging the capabilities of United States Customs

95. *Id.*
96. *Id.*
97. *Id.* at 67-68.
98. *Id.*
99. *Id.* at 68.
100. *Id.*
101. Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Pub. L. No. 107-188, § 101, 116 Stat. 594, 596 (2002); SCHNEIDER ET AL., *supra* note 84; *Gateway to Health Communication & Social Marketing Practice*, CENTERS FOR DISEASE CONTROL & PREVENTION, https://perma.cc/59CV-5JTY (archived July 11, 2019).
102. SCHNEIDER ET AL., *supra* note 84.

and Border Protection (CBP).[103] Under this agreement, "specially trained CBP personnel at ports of entry can inspect cargo and perform other examinations, while also having authorization to hold suspected cargo for further testing."[104]

To enable the agency to "quickly identify and locate affected food processors and other establishments in the event of deliberate or accidental contamination of food" the FDA makes nearly all domestic and foreign actors involved in the food supply chain register with the FDA.[105] The Act also requires parties importing food product to notify the FDA of impending arrival to provide the agency with "advance information," thus allowing the FDA "to target potentially high-risk shipments" which threaten the security of the sector.[106] Placing this register of food processing facilities on the blockchain could help effectuate the Acts goals and improve the speed of which high-risk shipments are identified.

VI. Policy of Critical Infrastructure

A. The Food and Agriculture Sector

After the attacks on September 11, 2001, the Homeland Security Act of 2002 was signed into law establishing the Department of Homeland Security (DHS) and tasking it with securing and making resilient our Nation's critical infrastructure.[107] Critical infrastructure is defined as the Nation's "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[108] Future use of "critical infrastructure" in this note will be referring to the food and agriculture sector.

Pursuant to this responsibility, DHS is required to develop a comprehensive plan for securing the Nation's critical infrastructure.[109] The first comprehensive plan, the *National Infrastructure Protection Plan* (*National Plan*), was completed

103. Public Health Security and Bioterrorism Preparedness and Response Act § 331; *The Bioterrorism Act*, U.S. CUSTOMS & BORDER PROTECTION (Jan. 27, 2014), https://perma.cc/KTF7-RGMF.

104. *The Bioterrorism Act*, *supra* note 103.

105. Rhona S. Applebaun, *Protecting the Nation's Food Supply from Bioterrorism*, FOOD SAFETY MAG. (Feb./Mar. 2004) (emphasis omitted), https://perma.cc/WE6Z-2BNW.

106. *The Bioterrorism Act*, *supra* note 103.

107. Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, 2135 (2002); *see also* U.S. DEP'T OF HOMELAND SEC., NIPP 2013: PARTNERING FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE 4 (2013), https://perma.cc/88XV-UUYM.

108. USA Patriot Act of 2001, Pub. L. No. 107-56, § 1016(e), 115 Stat. 272, 401 (2001).

109. U.S. DEP'T OF HOMELAND SEC., *supra* note 107, at 8-9.

in 2006 and updated in 2013.[110] The policy of the United States regarding the food and agriculture sector as critical infrastructure is a culmination of new understandings and past federal directives that include: Executive Orders, Presidential Policy Directives, the *National Strategy for Information Sharing and Safeguarding* (NSISS), and the *National Plan*.[111] The forthcoming paragraph will briefly describe how these directives combine to define United States policy reflected in the *National Plan*, setting goals concerning the food and agriculture sector as critical infrastructure.

VII. PREVIOUS DIRECTIVES INFLUENCING THE NATIONAL PLAN

Presidential Policy Directive 8: *National Preparedness* aims at strengthening the United States through systematic preparation for threats which include acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters which might affect our food systems.[112]

Presidential Policy Directive 21 (PPD-21): *Critical Infrastructure Security and Resilience* commits the federal government to pursue an integrated approach with the private sector to address both physical and cyber threats.[113] To effectuate these goals, PPD-21 identifies sixteen critical infrastructure sectors and establishes Sector-Specific Agencies (SSAs) to oversee and provide knowledge and technical expertise for their respective sectors.[114] These SSAs are tasked with coordinating and collaborating with stakeholders, while also serving to carry out incident management responsibilities in a time of crisis.[115] Of these sixteen critical infrastructure sectors, the Food and Agriculture sector is overseen by co-SSAs, including the USDA and the Department of Health and Human Service (HHS).[116]

Executive Order 13636: *Improving Critical Infrastructure Cybersecurity* calls for the development, and implementation of a "technology-neutral cybersecurity framework" to reduce cyber risk and promote the "adoption of strong cybersecurity practices" to increase information sharing with privacy protections.[117]

---

110. *Id.* at 9.

111. *Id.* at 7-9.

112. *Presidential Policy Directive / PPD-8: National Preparedness*, U.S. DEP'T HOMELAND SEC. (Mar. 30, 2011), https://perma.cc/KG6H-GEM7.

113. Press Release from the Office of the Press Sec'y, The White House, Presidential Policy Directive – Critical Infrastructure Security and Resilience (Feb. 12, 2013) [hereinafter Critical Infrastructure Security and Resilience] (on file at https://perma.cc/XRL2-FRJU).

114. *Id.*

115. *Id.*

116. *Id.*

117. U.S. DEP'T OF HOMELAND SEC., *supra* note 107; *see also* Exec. Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

Presidential Policy Directive 41: *United States Cyber Incident Coordination* recognizes networked technology is especially vulnerable to "malicious activity, malfunction, human error, and acts of nature . . . ."[118] Where effective responses to such threats supports an "open, interoperable, secure, and reliable information and communications infrastructure" which promotes trade and commerce, international security, free expression, and the privacy and security of the citizenry.[119]

The NSISS identifies the need to establish "information-sharing processes and sector-specific protocols with private sector partners, to improve information quality and timeliness and secure the Nation's infrastructure."[120]

VIII. THE NATIONAL PLAN

National policy regarding the food sector as critical infrastructure is a culmination of the aforementioned directives and to fulfill this vision the *National Plan* lays out goals representing the direction strategic action should be focused.[121] These goals are to:

> [1] Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities;
> [2] Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments;
>
> [3] Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, and employing effective responses to save lives and ensure the rapid recovery of essential services;
>
> [4] Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making; and
>
> [5] Promote learning and adaptation during and after exercises and incidents.[122]

The goals of the *National Plan* "elevate security and resilience as the primary aim of critical infrastructure homeland security planning efforts" and calls for collaborative efforts between government and private actors to integrate both cyber,

118. Press Release from the Office of the Press Sec'y, The White House, Presidential Policy Directive – United States Cyber Incident Coordination (July 26, 2016) (on file at https://perma.cc/4SNM-83TN).

119. *Id.*

120. U.S. DEP'T OF HOMELAND SEC., *supra* note 107, at 9.

121. *Id.* at 1, 5.

122. *Id.* at 5.

physical, and resilience efforts.[123] The *National Plan* does so by breaking down critical infrastructure into three parts: the risk environment, the operating environment, and partnership structure.

A. Risk Environment

The *National Plan* recognizes threats to the food sector are complex and constantly evolving (e.g., terrorism, pandemics, technical failures, etc.), while acknowledging global supply chains and trans-national infrastructure are increasingly vulnerable to cyber-attacks due to the growing integration of information and communication technologies.[124]

B. Operating Environment

The *National Plan* recognizes the operating environment of the food sector is characterized by interdependency and interconnectedness which will only increase as cloud computing, mobile devises, and wireless connectivity becomes the norm.[125] The physical and digital exchange of information, products, and services of the food sector cross jurisdictional boundaries are characteristics which only heightens the need for joint planning and investment.[126] Vulnerabilities to unauthorized access affects the confidentiality, integrity, and availability of information required to operate in the food sector poses a challenge to actors who must be allowed to confidently use and protect their critical information.[127]

In recognition of these challenges, the *National Plan* calls for transparent information-sharing practices which protect and enable law enforcement investigations while still ensuring privacy and the protection of civil liberties.[128]

C. Partnership Structure

The *National Plan* recognizes the federal government must partner with the private sector since, in this digital age, the increase in connectivity often makes private actors the "front lines of national defense," thus necessitating a sustainable partnership between private and government actors which "precludes any one entity from managing risks entirely on its own . . . ."[129] Additionally, the *National Plan* recognizes all partners within the risk environment will benefit from sharing

123. *Id.* at 4.
124. *Id.* at 8.
125. *Id.* at 9.
126. *Id.* at 10.
127. *Id.*
128. *Id.*
129. *Id.*

each other's knowledge and capabilities to produce a better understanding of risks posed which allows a more effective and accurate response.[130]

In sum, the policy environment's mission is to ensure the safety of the United States food sector. It is the result of a myriad of legislation and actors, often with overlapping jurisdictions, who encounter difficultly in carrying out their objectives by the sheer volume and complexity which characterizes the sector. Moreover, the *National Plan* and other directives recognize much of the information collected by one agency could be readily used by another if given the ability to efficiently and securely share that information.[131] Here is an area where blockchain could be used.

A food sector built upon the blockchain would allow these various government and private actors to securely collect, share, and analyze information in real time. Information can create more effective policy and response by autonomously alerting the appropriate authority at the start of an emergency instead of the end. To ensure our agencies have the capabilities and resources to fulfill the aforementioned goals, it would benefit the nation to have a system which can confidently store and efficiently share information across appropriate authorities. Blockchain could be this resource.

IX. Surveillance of the Food System

A. Foodborne Disease and Illness

Data regarding the safety of our food and foodborne illnesses is collected by a myriad of active and passive surveillance programs administered by the government, academic, and private sectors.[132] One of these programs, the National Outbreak Reporting System (NORS), passively monitors outbreaks concerning two or more people who become ill after ingesting the same food.[133] Research has shown of these outbreaks 50% were due to viruses, 42% to bacteria, 7% to chemical or toxic agents, and 1% to parasites.[134] In outbreaks which cause hospitalization, 61% involved Salmonella, 13% involved Escherichia coli, and 8% involved noroviruses.[135] However, these statistics are thought of as only representing the "tip of the iceberg" since many foodborne illnesses go undetected, reflecting the current inadequacies of conventional reporting systems and the need for something

130. *Id.*
131. *Id.*
132. Inst. of Med. & Nat'l Research Council, *supra* note 70, at 101-02.
133. *Id.* at 102.
134. *Id.*
135. *Id.*

new.[136]

The other program, FoodNet, is an active surveillance program that monitors and estimates foodborne illness in the United States.[137] FoodNet is considered to provide better estimates of foodborne illness since it normalizes data to the actual population size of an incident site, thus allowing monitoring of year to year trends.[138] Based upon data FoodNet provided, for the years between 2000 and 2008, the Centers for Disease Control and Prevention (CDC) estimates foodborne disease causes 47.8 million illnesses, 127,839 hospitalizations, and 3,037 deaths every year which translates to "1 in 6 Americans becoming ill . . . from consuming contaminated food."[139] An even more frightening statistic, this same study cited that out of the 47.8 million illnesses, only 9.4 million of these could be accounted for by a *known* pathogen, highlighting the frightening reality that much of what is causing us to get sick is currently unknown.[140]

Despite these best efforts, investigations into foodborne illnesses are complicated by the nature of the subject of study. Contaminates can come from unknown nonfood sources and the temporal relationship between consumption and symptoms of contaminated food can vary making it difficult to fully capture.[141] Previous publications have noted many of these shortcomings are the result of conventional data collection and attribution systems which either underreport outbreaks, monitor only a small fraction of the food system, or attribute an outbreak to an unspecified source or pathogen.[142] Risk assessments of the food system are dependent on complex associations between various actors and sources, making research resource intensive and incomplete under conventional methods.[143] Furthermore, while FoodNet and NORS surveillance systems have helped to build our understanding of the problem, they still do not capture the real cost of foodborne disease; the chronic or congenital disease which impacts the productivity and quality of an individual's life are not reflected.[144]

In recognition of current analytical shortcomings and the complex character

136. *Id.*
137. *Id.*
138. *Id.*
139. *Id.*
140. *Id.* at 102-03.
141. *Id.* at 113.
142. *Id.*
143. *Id.* at 116.
144. *Id.* at 103 (explaining that quality adjusted life year (QALY) analysis estimates economic and social costs of foodborne illnesses. Researchers utilizing QALY estimate that of the fourteen *recognized* pathogens which cause foodborne illness, the annual cost ranges for these illness's is between $4.4-$33 billion).

of the food supply system, researchers have worked to develop a framework that can identify research and development needs for government agencies.[145] When formulating this framework researchers highlighted the need for new data collection systems to make this framework more successful.[146] Researchers noted that because the collection of data is dispersed and controlled between local, state, federal, and private actors, the access and analysis of such data can be difficult.[147] For example, on the federal level alone datasets regarding the food supply systems are dispersed between the USDA's Food Availability Data System, the CDC's National Health and Nutrition Examination Survey, the United States Department of Labor and several more.[148] Because of this siloed data, researchers recommend the federal government fund and create new data collection programs in order to provide a comprehensive understanding of the nation's food system across all domains.[149] Specifically, researchers note government, academic, and private actors all recognize the need to efficiently share data, and prioritize the development of a government-industry collaboration mechanism makes data readily available to be used in research and policy analysis.[150]

X. Why the United States Should Adopt Blockchain

Due to the complexity and importance the United States food and agriculture sector holds for the nation's economic and human health, the sector should consider leveraging blockchain technology to improve the collection, security, and sharing of data. In turn, adopting blockchain would increase the safety of our food and the sector's competitiveness on the global stage. The forthcoming sections will be a brief overview of the benefits which blockchain could provide when applied to the sector and why such an endeavor would not only be congruent with existing policy but would help achieve those federal goals.

XI. The Food Supply Chain

As previously discussed, the United States food system is a remarkable success which is made possible by a complex supply chain composed of various actors.[151] However, this complexity creates challenges for researchers and those in charge of monitoring and responding to foodborne illnesses. The complex web of

145. *Id.* at 15, 16.
146. *Id.* at 16.
147. *Id.*
148. *Id.* at 16-17.
149. *Id.* at 17.
150. *Id.*
151. *Id.* at 1, 6, 37.

actors which make up the food sector also place communication of sensitive information at risk; a risk that was exposed in 2013 when Chinese nationals were arrested for stealing trade secrets of American agricultural companies.[152] But a food and agriculture sector which leverages the capabilities of blockchain could make strides in eliminating these problems. These problems could be eliminated because blockchain and the technologies made possible by it (i.e., IoT, Smart Contracts, dApps) would enable the sector to efficiently trace product and encrypt data, thus securing it against malicious actors and allowing it to be confidently shared to authorized individuals around the world.[153]

Particularly, traceability might be the most disrupting aspect of blockchain. The ability to track a product along every stage in the supply chain and see exactly what has happened to it and how it has changed over time, means both public and private actors could quickly respond to a threat with surgical accuracy.[154] As the Walmart example showed, such traceability reduces the time it takes to find a contaminated product from days to seconds, which means both money and lives can be saved. Furthermore, with IoT devices, smart contracts, and dApps, whose potential is realized once it is secured with blockchain, stakeholders in the food sector are enabled a level of control previously impossible due to the level of information now available.[155] Information which can then be used to tailor a product to consumer taste, provide users with information they desire, monitor product quality, or effectively reconfigure supply chains.[156]

Not only can blockchain provide traceability, but it also provides the ability for parties to transact business directly with each other without a third-party intermediary. Transactions have already occurred on blockchain; for example the Grain Discovery platform was used by two Canadian farmers in January of 2019 to find a buyer, sell their corn, and receive payment instantly.[157] One of the farmers was quoted saying, "If blockchain technology means a few extra dollars in my pocket and a few hours less trucking, then that's a win."[158]

152. *Verdict in Seed Espionage Case*, AGWEB (Oct. 22, 2016), https://perma.cc/S3N9-GZFT.

153. DELOITTE, CONTINUOUS INTERCONNECTED SUPPLY CHAIN 11, 14 (2017), https://perma.cc/WZP3-5NC3.

154. *See* Corkery & Popper, *supra* note 4.

155. AMEN & EHMKE, *supra* note 63, at 2-3.

156. *Id.*

157. Laurie Bedord, *Grain Discovery Executes Corn Transaction Using Blockchain*, SUCCESSFUL FARMING (Jan. 22, 2019), https://perma.cc/D2K7-3KY7.

158. *Id.*

XII. BLOCKCHAIN IS CONGRUENT WITH FEDERAL POLICY

Federal investment into a sector blockchain would also be in line with several existing government initiatives.[159] Beginning with United States policy concerning critical infrastructure, the *National Plan* and previous presidential directives recognize that the interdependency and connectedness of the food sector make it increasingly vulnerable to both malicious attacks and catastrophic disasters.[160] The food sector also operates in an environment that is increasingly being characterized by the exchange of information and products across jurisdictional bounds, thus elevating the possible consequences of a physical or cyber-attack.[161] Furthermore, such risks raise the importance of partnering with the private sector since many modern threats places them on the "front lines of national defense."[162] To improve national security, federal policy seeks to improve assessment systems, secure critical infrastructure, minimize adverse consequences, and encourage sharing of information across the food sector.[163] Blockchain technology could be a tool to satisfy these objectives within the food and agriculture sector.

First, as discussed, blockchain is a distributed ledger not requiring a centralized authority to operate or maintain information on the network.[164] The fact the blockchain protocol is technology neutral and can be easily bootstrapped to virtually any computer, it is congruent with Executive Order 13636, and results in a database which is decentralized; thus resilient against a targeted attack or catastrophic event which would otherwise compromise the system.[165] Moreover, because blockchain is encrypted on various levels, users can be sure their private data will be kept secure, accomplishing the goal of increasing adoption of information sharing with privacy protections laid out in Executive Order 13636.[166]

Second, the *National Plan* creates SSAs to oversee and administer their respective sector which blockchain could improve. The food sector is administered by both USDA and HHS who are tasked with collecting information, collaborating with stakeholders, and carrying out incident responses in a time of crisis.[167] However, as the *National Plan* and researchers of the sector recognize, the food sector

159. *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 107.

160. *See Presidential Policy Directive / PPD-8: National Preparedness*, *supra* note 112.

161. U.S. DEP'T OF HOMELAND SEC., *supra* note 107, at 9-10.

162. *Id.* at 10.

163. *Id.* at 5.

164. TAPSCOTT & TAPSCOTT, *supra* note 16, at 33-34.

165. *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 107; *see also* Exec. Order No. 13636, 78 Fed. Reg. at 11,739.

166. *See* TAPSCOTT & TAPSCOTT, *supra* note 16, at 10-11; U.S. DEP'T OF HOMELAND SEC., *supra* note 107; *see also* Exec. Order No. 13636, 78 Fed. Reg. at 11,739.

167. Critical Infrastructure Security and Resilience, *supra* note 113.

is characterized by complex relationships which frustrate these abilities to provide effective oversite and administration.[168] Here, leveraging IoT devices, smart contracts, and dApps on the blockchain could allow the collection of highly individualized data points which can result in better communication and analysis within the sector.[169] For example, a dApp could be developed incentivizing stakeholders to register and contribute to data collected by the USDA or HHS which would facilitate these SSAs in developing relationships or pushing out urgent information to their private partners. Another example would be in the event of a potential outbreak where a response could be carried out quickly since SSAs and concerned parties would have access to a database which permits greater analysis of the complex relationships which define the sector; thus minimizing consequences to both human health and profit margins.

XIII. CONGRUENT WITH LEGISLATIVE POLICY

A food and agriculture sector that leverages blockchain could also help meet the goals of current federal legislation or even highlight areas where new legislation is necessary. For instance, the 2010 Food Safety Modernization Act placed increased responsibility on food companies for safety and contamination reporting, a responsibility which could be better fulfilled if the company had the advantages of a blockchain.[170] In addition, pursuant to the Act, the FDA is tasked with registering food facilities and maintaining databases to prevent against a bioterrorism event, while also committing the CBP agency to inspect cargo and perform other examinations.[171] Unfortunately for inspectors, approximately 11 million shipping containers enter United States ports each year,[172] while in 2018 agricultural imports were valued at approximately $120 billion, making physical inspection nearly impossible without disrupting the flow of international trade.[173]

The problems presented by such volume could be reduced if actors were encouraged to implement blockchain into their operations. Due to the traceability made possible with blockchain, these private actors could track a product from its

168. INST. OF MED. & NAT'L RESEARCH COUNCIL, *supra* note 70, at 102-03.

169. THARUN MOHAN, IMPROVE FOOD SUPPLY CHAIN TRACEABILITY USING BLOCKCHAIN 54 (2018), https://perma.cc/27GS-CE5L ("it is evident that blockchains can be more efficient in tracking food provenance, preventing substantial scale contamination of food products, identify and remove the source of foodborne illness within seconds while the contemporary systems could take as much as weeks").

170. *See* INST. OF MED. & NAT'L RESEARCH COUNCIL, *supra* note 70, at 68.

171. *The Bioterrorism Act*, *supra* note 103.

172. *Cargo Security and Examinations*, U.S. CUSTOMS & BORDER PROTECTION (June 15, 2018), https://perma.cc/FD2T-CSAC.

173. *Agricultural Trade*, ECON. RES. SERV. (Apr. 22, 2019), https://perma.cc/TD54-2ATZ.

international source to the cargo ship.[174] Additionally, since the blockchain creates an immutable digital record that permits analysis of change overtime, such an actor can ensure a food product did not spoil or that a shipping container was not tainted in anyway.[175] Moreover, due to blockchain cultivating trust as a part of its programming, neither the government nor private actors need to concern themselves about whether the information has been manipulated since it would be easy to verify; thus resulting in increased efficiency for both government inspectors and private actors trying to maintain compliance.[176]

In fact, the United States had already begun to experiment with blockchain in this very realm. In June of 2018, the DHS awarded Factom Inc. nearly $200 thousand to begin beta testing a blockchain to secure CBP devices (cameras, sensors, etc.) to ensure the integrity and authenticity of the data collected.[177] Since the United States government already recognizes the benefits of blockchain in regards to the CBP it should not be a stretch for officials to see the efficacy of blockchain within the food sector to allow the FDA and CBP to operate efficiently with greater success at identifying agricultural product which are potentially harmful.

XIV. MEETING THE CALL TO ACTION

Lastly, a food sector blockchain can help fulfill the need of better data for government officials, researchers, consumer advocates, and boardrooms by supplying such actors with access to individualized data. Currently, data regarding the safety of our food supply is collected by a myriad of surveillance programs administered by many different actors.[178] While each program operates differently, the resounding conclusion is current statistics only represent the tip of the iceberg since many foodborne illnesses go undetected and where much of what is causing us to get sick is largely unknown.[179] Researchers note these consequences are the result of inefficient and expensive data collection practices which is further hindered by data being siloed within private databases—all of which prevents analysis across such a dynamic sector.[180] It is due to these shortcomings researchers have

174. AMEN & EHMKE, *supra* note 63, at 2-3.

175. *See* TAPSCOTT & TAPSCOTT, *supra* note 16, at 97-99; CONG. BUDGET OFFICE, SCANNING AND IMAGING SHIPPING CONTAINERS OVERSEAS: COSTS AND ALTERNATIVES 1 (2016), https://perma.cc/52M4-GNGP.

176. TAPSCOTT & TAPSCOTT, *supra* note 16, at 10-11, 203.

177. Press Release, Dep't of Homeland Sec. Sci. & Tech., DHS Awards Austin-Based Factom, Inc. $192k for Blockchain Tech (June 15, 2018) (on file at https://perma.cc/BWV9-5BCX).

178. INST. OF MED. & NAT'L RESEARCH COUNCIL, *supra* note 70, at 101-02.

179. *Id.* at 102-03.

180. *Id.* at 113.

called for collaboration between government and private sector actors to develop better data collection services.[181] Blockchain could provide this service.

Blockchain could be the database these researchers are looking for due to many of the reasons previously highlighted. The fact the blockchain can be installed cheaply on many computers and leverage the capabilities of IoT devices, smart contracts, and dApps means the "database" these researchers desire would encompass a large swath of the country and reduce research costs.[182] Moreover, because of such capabilities, researchers could receive unique, individualized data points allowing better analysis of the complex relationships which define the sector.[183] Blockchain also sidesteps the problems of siloed data since the ledger can be shared and is always up to date.

Blockchain is a disrupting technology which will have various implications across the economy. The described benefits are just the beginning. As the understanding of and technology of blockchain becomes more mature, the benefits will only continue to grow. It is because of these benefits the United States food sector should embrace blockchain technology. Not only to improve the sectors bottom line, but to improve upon an already sterling history.

181. *Id.* at 17.
182. *See* TAPSCOTT & TAPSCOTT, *supra* note 16, at 33-34.
183. *See id.* at 7, 22.