ARIZONA STATE UNIVERSITY

CORPORATE & BUSINESS LAW JOURNAL FORUM

VOLUME 5 MARCH 2024 NUMBER 10

COMMENTARY

A Blockchain World: How Businesses Can Use Blockchain to Reduce Cybersecurity Issues and Legal Liability

BY KIKI OWENS*

Data breaches and cyber-attacks continue to increase, ultimately causing severe informational exposure and substantial monetary loss. From a business' standpoint, these incidents negatively affect their customers and open the door to excessive legal claims against their business. As of 2023, there have been 953 incidents resulting in 5.36 billion breached records.[1] Although this is a decrease from the 1,063 incidents in 2022, the incidents in 2023 have led to far greater breached records.[2] An overwhelming amount of these incidents have occurred due to lack of or deficient cybersecurity systems. Subsequently, businesses and agencies continue to struggle with implementing a hack proof system. As states continue to adopt stricter privacy regulations, it becomes more imperative for businesses to adopt an improved system. While it is important to recognize that there will never be a completely secure system, there are ways that the system can be less susceptible and more resistant to infiltrations.

The blockchain system is certainly a viable solution to reduce data breaches and cyber-attacks. A blockchain system is unique because it can be "private" and "permissioned," meaning it is accessible only to certain users, while providing transparency of transactions to its select users.[3] This is applicable in the cybersecurity

[*] J.D. Candidate, Class of 2024, Sandra Day O'Connor College of Law at Arizona State University.

[1] Neil Ford, *List of Data Breaches and Cyber Attacks in 2023*, IT GOVERNANCE BLOG (Nov. 3, 2023), https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023#:~:text=According%20to%20our%20research%2C%20there,total%20to%20over%205%20billion.

[2] Luke Irwin, *Data Breaches and Cyber Attacks in 2022: 480 Million Breached Records*, IT GOVERNANCE BLOG (Jan. 10, 2023), https://www.itgovernance.co.uk/blog/data-breaches-and-cyber-attacks-in-2022-408-million-breached-records.

[3] Bryce Suzuki et al., *Blockchain: What It Means for Clients, Contracts, and Law Practice*, ARIZ. ATT'Y (Feb. 2018), www.azbar.org/AZAttorney.

context because the blockchain ensures the information on the blockchain is secure and allows for any attacks or hackers to be traceable. Further, the blockchain has no single point of failure which is common in most data breaches because data is encrypted across different nodes.

Blockchain is a digital ledger that attaches and records data across computers in a network.[4] These computers are referred to as nodes that can store a copy of the blockchain—creating a peer-to-peer network.[5] To keep the blockchain secure, cryptography is utilized to string the digital "blocks" together.[6] The blocks are commonly used to store information such as transactions, ownership records, and agreements.

Typically, individuals need a trusted intermediary to ensure records are stored properly between parties.[7] Common intermediaries are banks and government agencies. However, blockchains are unique because they eliminate the need for an intermediary through an agreement between users called a "consensus protocol."[8] This protocol ensures data validation and resistance to any impermissible modifications—virtually being resistant to any hacking.[9]

Blockchain is capable of being used to reduce cybersecurity threats. Businesses can utilize a permissioned private blockchain to prevent severe data breaches and cyber-attacks. In fact, blockchain can aid in preventing fraud, securing data storage, tracing threats and attacks, and creating a tamper proof system.

First, blockchain can prevent fraud by securing and managing digital identities. To accomplish this, a permissioned private blockchain should be utilized so the network can only be accessed by specific individuals.[10] This prevents fraud because the blockchain must confirm the individual's identity, making the blockchain restrictive.

Second, blockchain can securely store data. The decentralization of data means data is stored across multiple nodes in the blockchain, thereby making it difficult to steal or encrypt a single point of data.[11] This feature addresses public concern that mass amounts of data are stored in one place and can be intercepted in one fatal attack.[12] Blockchain does not have a single point of failure, such as a single vulnerable computer or a user who mistakenly lets a hacker infiltrate a company's entire system.

Third, blockchain serves as a reliable way to trace threats and attacks. In a blockchain, transactions are time stamped after they are verified, thus creating a record of all transactions.[13] This time stamp process is crucial because the records can be audited at

[4] *ITIF Technology Explainer: What Is Blockchain?*, INFO. TECH. & INNOVATION FOUND. (Oct. 3, 2018), https://itif.org/publications/2018/10/03/itif-technology-explainer-what-blockchain/.

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] Suzuki, *supra* note 3.

[9] *Id.*

[10] *ITIF Technology Explainer*, *supra* note 4.

[11] LOUISE AXON ET AL., PRIVACY REQUIREMENTS IN CYBERSECURITY APPLICATIONS OF BLOCKCHAIN, 229, 236 (2018).

[12] *Id.*

[13] *Id.* at 234.

any given time.[14] Further, when new transactions are added, the information and previous block are stored on a new block.[15] A hash pointer is used on each block to point to the previous block. If information in a block is altered, the hash will also be altered, making the other subsequent blocks incorrect. With this structure, the blockchain addresses the frequent issue of individuals being unable to detect and trace any changes of data alteration.

Finally, the blockchain is transparent, which is advantageous for businesses in the cybersecurity context. Approved users can view all transactions that occur and maintain copies of the blockchain.[16] Because these actions are transparent, users can identify any fraudulent behavior. Overall, the system instills confidence in the businesses that use blockchain. In turn, this also promotes trust with the business' customers because the actions are transparent and reduces the fear that information will be improperly accessed by an intermediary.

When a business is subject to a data breach, a business should be capable of identifying the breach and the hacker's presence.[17] Failure to identify the breach, could lead to legal liability. In *In re Equifax, Inc.*, the defendant, Equifax, a consumer reporting agency, suffered from one of the largest data breaches ever, affecting almost half of the American population.[18] The breach occurred from May to July 2017, and resulted in about 150 million Americans' personal and financial information being stolen.[19] Equifax utilized the Apache Struts software program.[20] This program was vulnerable, and the hackers were able to access Equifax's systems by using simple maneuvers to figure out the credentials of the network accounts, thereby giving them access to the consumers' confidential information.[21]

Because Equifax failed to identify the breach and the hacker's presence, the hacker was able to continually extract private information from their servers.[22] The information that the hacker was able to obtain was severe. "The hackers stole at least 146.6 million names, 146.6 million dates of birth, 145.5 million Social Security numbers, 99 million addresses, 17.6 million driver's license numbers, 209,000 credit card numbers, and 97,500 tax identification numbers."[23] This is problematic because the hackers can then use the information to "fraudulently obtain loans and tax refunds, and destroy a consumer's credit-worthiness."[24] The court found that the consumers had made sufficient claims under state data breach notification statutes and unfair deceptive trade practices.[25]

[14] *Id.* at 236.

[15] *Id.*

[16] *Id.*

[17] In re Equifax, Inc., 362 F. Supp. 3d 1295 (N.D. Ga. 2019).

[18] *Id.* at 1309.

[19] *Id.*

[20] *Id.* at 1311.

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.* at 1308.

[25] *Id.* at 1338.

Consequently, Equifax globally settled with the federal agencies such as the Federal Trade Commission and Consumer Financial Protection Bureau for $425 million.[26] This settlement was used to aid those consumers who suffered from the breach.

The key point of *In re Equifax, Inc.*, is that the hackers were unknown to Equifax from May to July 2017.[27] If Equifax implemented a permissioned private blockchain system, the breach may have been less substantial. The blockchain system would have easily identified the hacker. Because the permissioned private blockchain is restricted to certain users, the hacker would have more difficulty obtaining access to the network. Even if the hacker was able to obtain access, any transactions of information would have been time stamped and the hacker's modified copy of the blockchain would have been immediately apparent to all nodes on the blockchain. The hacked copy would be apparent because it would differ from the rest. Once it is apparent, the hacked copy can be ignored and shut down quickly. While the blockchain makes this possible, this would not be achieved with traditional computer software which has a single point of failure.

Although the blockchain system does not notify users when the hacker obtains access, the users should implement a constant monitoring system. Constant monitoring would ensure that the business can pinpoint a breach in the system. If this protocol was implemented, Equifax would have been on notice substantially earlier and able to take preventative measures. Moreover, this would have allowed Equifax to notify the breach to the consumers, potentially negating a future claim under state data breach notification statutes.[28] Thus, Equifax could have avoided such a large data breach if a permissioned private blockchain system was implemented to identify the breach and the hacker at an early stage.

Based on the above, it appears that a permissioned private blockchain system should be implemented by businesses to reduce data breaches and cyber-attacks. Under a permissioned private blockchain system, businesses would have control of their own system, grant access only to certain users, and have encrypted data across nodes—providing for long term protection and avoiding single point failures. Ultimately, the blockchain system provides a variety of solutions for businesses to reduce cybersecurity threats, potential legal liabilities, while simultaneously ensuring confidence in their customers that their data will be protected.

[26] *Equifax Data Breach Settlement*, FED. TRADE COMM'N (Dec. 2022), https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.

[27] *In re Equifax, Inc.*, 362 F. Supp. 3d at 1311.

[28] *Id.* at 1338.