Journal of Forensic Sciences And Criminal Investigation
ISSN: 2476-1311

Juniper Publishers key to the Researchers

Review Article
Volume - 10 Issue 1 - July 2018
DOI: 10.19080/JFSCI.2018.10.555780

J Forensic Sci & Criminal Inves
Copyright © All rights are reserved by Nima Zahadat

Blockchain: A Critical Component to Ensuring Data Security

Nima Zahadat* and Whitney Partridge

Department of forensic sciences, University of Baltimore, USA

Submission: July 16, 2018; **Published:** July 25, 2018

***Corresponding author:** Nima Zahadat, Department of forensic sciences, University of Baltimore, School of criminal justice, USA, Email: nzahadat@ubalt.edu

Abstract

Over a decade old, Blockchain, the technology used to facilitate cryptocurrency transactions is beginning to gain traction in other facets of information technology. This decentralized database has applications that extend beyond cryptocurrency use. The increased focus on this technology has highlighted how centralized data management can be replaced through the decentralized nature of Blockchain and disrupt a number of industries that currently rely on centralized data management. This paper will explore the origins of Blockchain from smart contracts through the adoption inside cryptocurrency solutions. In addition to addressing the technology, challenges of Blockchain adoption within existing regulatory and civil law will be explored. Moving toward more future state, this paper will explore the potential impacts of Blockchain on various industries such as healthcare and banking which rely on traditional data management strategies. All of these facets are considered in the discussion of how Blockchain can revolutionize how organizations can manage data. Finally, the facets of Blockchain will be examined in the ability for such structures to have a positive impact on the availability, integrity and confidentiality of data, giving organizations a way to secure confidential information.

Keywords: Blockchain; Cryptocurrency; Confidentiality; Integrity; Availability

Introduction

Cryptocurrency has been in existence for almost a decade and has grown into a five-hundred billion-dollar market [1]. Cryptocurrency, which is synonymous with virtual currency, is based on Blockchain technology. Blockchain is an "immutable public ledger of transactions maintained by a peer-to-peer network through a distributed consensus protocol" [2]. Bitcoin was the first publicly available cryptocurrency to utilize the Blockchain architecture. Hundreds of cryptocurrencies have since been created, some quite different from Bitcoin, but each encompassing the Blockchain methodology. The architecture consists of users storing synchronized blocks of data on their computers. These blocks build upon one another across the Internet and around the globe, forming a chain. When transactions are made, new blocks are added that include this data. This is accomplished through the use of cryptography. Cryptography generates a hash value which is computed from combining the previous block to the new block. This hashing algorithm verifies that modifications to the data has not been made or tampered with without detection [3].

What makes this different from other technology is that the data is not owned by an individual or company. Instead, each individual has access to his or her full transaction history. This contrasts significantly from traditional transactional record keeping by corporations, governments, and other institutions that maintain private records. Typically, a corporation or business has complete control over records pertaining to their customer, client, or patients. However, Blockchain differs in that it records every transaction cryptically since its inception. Every user shares the same list of transactions which is continuously updated in order to keep the transaction ledger current. This keeps all ledgers reconciled with each other as new transactions occur. The advantage of this in relation to Blockchain is that it maintains the integrity of the records because they are distributed on a peer-to-peer network. In order to successfully modify the transaction history, an attacker would need to alter the majority of the data blocks and hash values within the Blockchain. This is would require compromising a substantial portion of computers of the users globally.

Literature Review & Research

With the initial concept of cryptocurrency and Blockchain technology nearing a decade old, there has been an increased focus of research on the topic and a belief in the viability of Blockchain technology as a replacement for traditional record keeping. For example, Tapscott & Tapscott, authors of Blockchain Revolution, believe that "This new digital ledger of economic transactions can be programmed to record virtually everything

of value and importance to humankind: birth and death certificates, marriage licenses, deeds and titles of ownership, educational degree, financial accounts, medical procedures, insurance claims, votes, provenance of food, and anything else that can be expressed in code." The Harvard Business Review's article on The Truth About Blockchain states that Blockchain technology will be a gradual, slow and steady process which will take decades to implement into daily life and the economy [4]. This article referenced two analogies. Their first analogy compared Blockchain to TCP/IP, one of the basic key protocols that governs networking traffic, which took more than thirty years to implement.

The second analogy provided in this article referenced a 2014 study conducted at MIT. Each undergraduate student was given $100 in Bitcoin. Half of the students opted not to partake in this new technology. Of the fifty percent that did not participate, thirty percent did nothing with the Bitcoin and the other twenty percent converted it to cash. Having nearly twenty percent of students converting the Bitcoin to cash speaks volumes as this comes from an institution that focuses on technological innovations. While the idea of Tapscott's vision seems viable, issues such as the prejudice of cash in favor of new currency types will need to be resolved before this can become a reality. One of today's greatest criticisms concerning the Blockchain architecture is its lack of scalability. According to Croman, Bitcoin can handle up to 7 transactions per second and takes 10 minutes or longer to confirm these transactions whereas credit and debit cards can process thousands of transactions per second. Another concern is the amount of electricity required to operate and secure Blockchain [5]. An exorbitant amount of energy is required in order to achieve profitable revenue for mining.

As such, miners are purchasing more powerful hardware and are performing work in countries with the least expensive electricity rates [6]. Another significant challenge that needs to be addressed is coming up with a solution to identify individuals' identities in order to provide authentication [3]. In order to achieve authentication, the user must be able to prove his identity. Companies such as u Port, Sho Card, and Sovrin have created protocols to authenticate identity management for Blockchain; yet none of these platforms has been adopted [7]. Because Blockchain provides confidentiality and does not have a mechanism in place to identify individuals' identities, it is being used by cybercriminals to commit crimes that in most cases cannot be traceable back to the perpetrator [2]. Developers will need to find alternative ways to increase the transaction speed, reduce energy consumption, and implement a protocol to be accepted and utilized by the Blockchain community to verify individuals' identities.

While there is plenty of work to be done to improve Blockchain technology, some of its positive attributes include the confidentiality, integrity, and availability that it provides to its users. Confidentiality is currently the subject of many discussions in the media as several businesses with centralized databases have been subjected to data breaches, resulting in an increase in identity theft and the loss of consumer confidence [7]. The key differentiator with Blockchain is that a wide scale data breach is unlikely due to the decentralized nature of the data. An attacker would have to compromise a substantial portion of the block with a vast number of users' private keys. This decentralized storage system also improves the integrity of the data. By design, Blockchain's availability supersedes that of centralized databases. Centralized databases are subjected to a variety of risks including natural disasters, power outages, technology failures, and ransomware attacks. In any of these scenarios, a network administrator would work to restore lost data from backup servers. In some cases, the data may not be fully restored. Whereas in Blockchain, data is decentralized.

"Distribution and replication intend to ensure availability and survivability of the ledger, in case of a subset of the servers fails." [8]. At the time of the writing of this article, there are no uniform laws in place pertaining to the Blockchain structure. Some legal aspects to take into consideration for Blockchain adoption include jurisdiction, performance, liability, intellectual property, data privacy, enforceability, and compliance. Because Blockchain extends across jurisdictional boundaries around the world and laws vary from state to state and from country to country, legislation is essential to solving these complex issues. Several states including Arizona [9,10]. Colorado [11]. Florida [12]. Hawaii [13]. New York [14]. Tennessee [15]. Vermont [16]. Virginia [17] and Wyoming [18]. have introduced legislation on Blockchain. These bills primarily focus on defining cryptocurrency and proposing taxation on it rather than addressing the complex issues referenced above.

Currently, Blockchain's primary use is the exchange of virtual currency for goods and services. This is just the beginning, as it has the potential to be used for several other purposes in a variety of sectors including but not limited to insurance processing, banking, education, and healthcare. There are many different types of insurance, but they all serve the same purpose: to protect or ensure the functioning of a good or service. This is usually accomplished through the use of a contract. In the 1990s, a new type of contract was developed which became known as a smart contract. These smart contracts have become increasingly popular over the past several years, which is attributed to the Ethereum cryptocurrency. With a smart contract, a legal entity such as a person or company will create a set of rules which rely upon a condition that is recorded in the Blockchain. Once that condition has been met, the funds will be transferred to the intended recipient. For example, a home equipped with sensors could automatically notify the insurance company of damage sustained from a storm and initiate contact with a company to perform the necessary repairs [19]. This is just one way Blockchain and smart contracts can be used to improve customer service and reduce operating costs. Gatteschi also suggests that

How to cite this article: Nima Z, Whitney P. Blockchain: A Critical Component to Ensuring Data Security. J Forensic Sci & Criminal Inves 2018; 10(1): 555780. DOI: 10.19080/JFSCI.2018.10.555780.

smart contracts could be used to conduct risk assessments on individuals. Premiums would be computed based on individuals' habits and behaviors.

The implementation of Blockchain in the banking industry has the potential to overcome logistical inadequacies and reduce overhead and transaction costs. This protocol diminishes the likelihood of human error and fraud in that smart contracts can perform the majority of this work without human involvement Blockchain has the capability to reduce or nearly eliminate the need for third-parties to affirm the accuracy of financial transactions [20]. Legal settlements could be expedited as the transfer of money would no longer take days. Blockchain would have the ability to manage land records and verify deeds of ownership with transaction timestamps [21]. In education, Blockchain could be used to verify and confirm student attendance, grade point averages, and diplomas and degrees awarded. This would save time and money for the purpose of validating the applicant's credentials. According to Kuvshinov et al., the Blockchain architecture in education should be divided into public and private layers. The public layer would include the information necessary to prove the authentication and integrity of the user, and the private layer would include the student's grades, courses taken, and degrees earned [22]. This protocol would ensure confidentiality and integrity of this data.

The healthcare sector has made improvements in recent years through the implementation of patient portals. Patients can now use this platform to communicate with their physician, request prescription refills, schedule appointments, and view their visit summaries. The risk associated with this technology is that it is being stored on a centralized database, making it a prime target for cybercriminals and hackers. Furthermore, it does not store the patient's complete medical record, which must be requested by the patient and which is oftentimes accompanied by a fee for retrieval and printing. As such, most patients are not in possession of their medical records and are not able to easily share their documented medical history with other providers [23]. Yu, Wang, Jin, Li, and Jang created a mobile app called the Healthcare Data Gateway that allows patients to manage and control what healthcare data they elect to share with each provider. Being able to share healthcare data with multiple providers offers a "better understanding of patterns and trends in public health and disease to ensure better quality care, better recommendations for exercising or doctors, and plan services that make the best of limited national health service budgets for the health and wellbeing of everyone, and so on. [24].

Key Findings

The previous section explored various ways in which Blockchain technology can be implemented into day-to-day lives. The potential impact is beyond the scope of imagination and surpasses the areas that were highlighted in this paper. Researchers will continue to find new ways to utilize this budding technology. As previously mentioned, Blockchain encompasses confidentiality, integrity, and availability which should help drive this technology from its infancy stage to a broader use of acceptance. In order for Blockchain to gain acceptance, its shortcomings need to be addressed. The most important of these shortcomings is how to inform and socialize the core concepts of Blockchain technology and how it secures transaction information to the general public. Having a well-informed public is critical for the widespread adoption of this emerging technology [25].

Once more research has been conducted and the general public has been educated, the advantages of using a decentralized database to store and access information should be more apparent. Provided that Blockchain will be able to maintain privacy, security, and availability, this technology should flourish, and centralized databases may become obsolete. Today, when searching for answers to questions or learning how to perform a particular task, individuals no longer refer to an encyclopedia. Google and YouTube are preferred methods as they have better search functionality, are up-to-date, and provide users with instantaneous answers and solutions. It is likely that one day, as Blockchain becomes more ubiquitous through research, adoption, and commercialization, individuals will become as comfortable with Blockchain technology as they are with Google and YouTube.

Conclusion

Blockchain technology has the capability to transform and improve individuals' day-to-day lives and the way companies conduct business. While Blockchain is still in its infancy and has not yet gained widespread adoption around the globe, the benefits this technology can provide outweigh the current use of centralized databases. To move forward with this innovation, researchers will need to figure out a solution to increase transaction speed, reduce energy consumption, and implement protocols to be accepted and utilized by the Blockchain community to verify individuals' identities. Lawmakers must establish responsible parties to ensure the Blockchain is properly functioning and determine jurisdiction, liability, enforceability, and compliance. Ultimately, this immutable decentralized record database will benefit both consumers and businesses. Consumers will retain ownership of their records, and businesses will benefit from reduced overhead costs associated with information being stored and maintained on a decentralized database. This will produce a self-monitoring and recording of activity that will create a system that ensures transparency, confidentiality, integrity, and availability of records. As a result, consumers should no longer fear for the loss of their data arising from risks such as ransomware attacks and natural disasters. In essence, Blockchain can provide a solution to combatting some of today's most challenging cybersecurity attacks by providing confidentiality through cryptography, integrity through self-validation, and availability through redundancy.

How to cite this article: Nima Z, Whitney P. Blockchain: A Critical Component to Ensuring Data Security. J Forensic Sci & Criminal Inves 2018; 10(1): 555780. DOI: 10.19080/JFSCI.2018.10.555780.

References

1. Eskandari S, Leoutsarakos A, Mursch T, Clark J (2018) A first look at browser-based cryptojacking.
2. Bartoletti M, Pes B, Serusi S (2018) Data mining for detecting Bitcoin Ponzi schemes.
3. Pisa M, Juden M (2017) Blockchain and Economic Development: Hype vs. Reality. CGD Policy Paper, Washington, DC: Center for Global Development.
4. Iansiti M, Lakhani K (2017) The Truth About Blockchain: It will take years to transform business, but the journey begins now Harvard Business Review 95(1): 118-127.
5. Mainelli M, Milne A (2016) The Impact and Potential of Blockchain on the Securities Transaction Lifecycle. Swift Institute Swift Institute Working Paper No. 2015-0007.
6. Giungato P, Rana R, Tarabella A, Tricase C (2017) Current Trends in Sustainability of Bitcoins and Related Blockchain Techology. Sustainability 9(12): 2214.
7. Dunphy P, Petitcolas F (2018) A First Look at Identity Management Schemes on the Blockchain.
8. Anta A, Georgiou C, Konwar K, Nicolaou N (2018) Formalizing and Implementing Distributed Ledger Objects.
9. (2018) Income tax payments; bitcoin, HB 1091, 53rd Arizona Legis, 2nd session.
10. (2018) Income tax; virtual currency SB 1145, 53rd Arizona Legis, 2nd session.
11. (2018) Concerning the Use of Cyber Coding Cryptology for State Records, and, in connection therewith, making an appropriation, SB 18-086, 71st Colorado Legis, 2nd session.
12. (2018) HB 1357 Florida.
13. (2018) Relating to Virtual Currency, S.B. 3082, Hawaii, USA.
14. (2018) Open Blockchain tokens-exemptions, HB 0070, Wyoming.
15. (2017-2018) HB 1507 110th General Assembly, Tennessee, USA.
16. (2018) An act relating to Blockchain, cryptocurrency, and financial technology, SB 269 Vermont.
17. (2018) Cryptocurrencies; State Corporation Commission to study, SB 864, Virginia, USA.
18. (2018) Open Blockchain tokens-exemptions, HB 0070, Wyoming.
19. Gatteschi V, Lamberti F, Demartini C, Pranteda C, Santamaria V (2018) Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? Future Internet 10(2): 20.
20. Cocco L, Pinna A, Marchesi M (2017) Banking on Blockchain: Cost Savings Thanks to the Blockchain Technology. 9(3).
21. Kuvshinov K, Nikiforov I, Mostovoy J, Mukhutdinov D, Andreev K, et al. (2018) Disciplina: Blockchain for Education.
22. Raju S, Rajesh V, Deogun J (2017) The case for a data bank: An institution to govern healthcare and education. ICEGOV'17 Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance.
23. Yue X, Wang H, Jin D, Li M, Jiang W (2016) Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. Journal of Medical Systems 40(10): 218.
24. Croman K, Decke C, Eyal I, Gencer AE, Juels A, et al. (2016) On Scaling Decentralized Blockchains (A Position Paper). In 3rd Workshop on Bitcoin and Blockchain Research.
25. Croman K, Decke C, Eyal I, Gencer AE, Juels A, et al. (2016) On Scaling Decentralized Blockchains (A Position Paper). In 3rd Workshop on Bitcoin and Blockchain Research.

This work is licensed under Creative Commons Attribution 4.0 License
DOI: 10.19080/JFSCI.2018.10.555780

Your next submission with Juniper Publishers will reach you the below assets

- Quality Editorial service
- Swift Peer Review
- Reprints availability
- E-prints Service
- Manuscript Podcast for convenient understanding
- Global attainment for your research
- Manuscript accessibility in different formats
  (Pdf, E-pub, Full Text, Audio)
- Unceasing customer service

Track the below URL for one-step submission
https://juniperpublishers.com/online-submission.php

How to cite this article: Nima Z, Whitney P. Blockchain: A Critical Component to Ensuring Data Security. J Forensic Sci & Criminal Inves 2018; 10(1): 555780. DOI: 10.19080/JFSCI.2018.10.555780.