Information Services & Use 38 (2018) 187–189
DOI 10.3233/ISU-180022
IOS Press

Blockchain initiatives and implementation

Sonia Mundra*
CPA, President, Chenega Analytic Business Solutions, 10505 Furnace Road, Suite 205, Lorton, VA 22079, USA

Abstract. All professionals should consider the use of blockchain as a new and exciting arrow in their quiver when it comes to program risk management. In fact, even recently as several months ago, The National Institute of Standards and Technology (NIST), published a draft paper discussing and defining blockchain and its role in security. Traditional program structuring and deployment will not work well for blockchain technology. When we implement a new technology, we need to understand first what it is, potential use cases such as tracking the provenance and transfer of a digital asset, what we hope to accomplish, and then how we can implement to reduce the most risk to the organization. This includes determining if blockchain encryption is a good fit for the assets (using a flowchart), determining if the organization is ready for the change (change management) and the role of training as bookends to the program (first initial training, then development of SOPs and user training once the blockchain has been deployed). This paper discusses how to reduce risk to the organization, as a poorly-planned implementation can create turmoil and waste lots of time and money including a loose structure that can be applied as a baseline and then customized based on the needs of the organization.

Keywords: Blockchain, risk-assessment, security

These days, when we turn on the television or listen to the news, we hear about the latest hot topic: blockchain. Typically, a breathless announcer is giving news of the latest ups and downs of the popular cryptocurrencies, such as Bitcoin [1] and Ripple [2]. Our society seems to be mesmerized with the "Bitcoin phenomenon" and its seeming financial volatility. We have also heard the stories of Mt. Gox[3] and other scurrilous entrepreneurs, who have bilked investors out of their hard-earned savings. Due to this type of coverage, cryptocurrencies sound to most like a sham, and something that has nothing to do with the fundamentals of our businesses. However, nothing could be further from the truth. Blockchain, the technology that powers Bitcoin and other cryptocurrencies, has many different use cases, and has the potential to absolutely transform not just information technology (IT), but also identity management, land management, voting, shipping, records management, and nearly every other industry that you can imagine.

Blockchain can essentially be described as the new standard for securing data. Traditionally, data has been stored in a centralized database with a single (human) system administrator or central authority, who gives users access to the database and validates transactions. Centralized data warehouse storage is viewed as inferior to blockchain, because it has a single point of failure that can be penetrated or hacked. Databases with a central authority also require special skills of a system administrator, bank, lawyer or

*E-mail: sonia.mundra@chenegaabs.com.

[1]Bitcoin, Wikipedia, https://en.wikipedia.org/wiki/Bitcoin, accessed September 1, 2018.

[2]Ripple is a company that facilitates global payments for enterprises using blockchain technology (see: https://ripple.com/). Accessed September 1, 2018.

[3]Mt. Gox, Wikipedia, https://en.wikipedia.org/wiki/Mt._Gox, accessed August 31, 2018.

notary, which increases both cost and time-to- market for goods and services. Blockchain, on the other hand, can be defined as a distributed, or decentralized, database. Both physical (tangible) and intangible assets can be digitized, and the digital footprint of the asset can be stored on a blockchain. The digital blockchain that is used to represent the asset in question is stored on multiple systems and computers. Each computer system has a designated user, or administrator. If the owner of the digital asset wishes to make a change to the asset (for example, transfer of ownership), then the change must be approved by all system users, for the change to be validated and subsequently transacted. Every change in the asset becomes another block in the blockchain, with each block having its own special key. Recording of changes provides a clear audit trail for executive leadership, and of course for external audits. Blockchain distributed ledgers provide what is known as "consensus-based permission." If a hacker attempts to alter one blockchain, secure blockchain technology will not permit the change; since all the distributed blockchains must sync or reconcile to each other, for the change to be considered valid. Blockchain databases are considered by technology pundits to be nearly hackproof, through their use of SHA-256 encryption (see: https://www.movable-type.co.uk/scripts/sha256.html), and certainly more secure than traditional centralized databases; allowing only owners of digital assets to alter and make changes to the asset.

The implications of a more secure, more efficient way of tracking and storing digital assets and transactions are astounding. It helps to begin with an example. One of my favorite movies is The Thomas Crown Affair. If you remember the plot of the movie: a very valuable painting is stolen from an art museum. The insurance agent, whose employer does not want to pay the insurance settlement for the stolen painting, is very keen to track down the painting, which is the main asset in question. She proceeds to take a series of different actions to accomplish her mission. First, she tries to retrace the crime by visiting the art gallery. She spends time with the police and watches the surveillance videos. She then busies herself by contacting art dealers, looking for any signs that the asset may have changed ownership - in other words, been sold and changed its state from one asset into another more liquid asset (painting has been sold for cash). Well, that was a lot of work for her, and made for a highly-entertaining plotline. However, suppose the painting has been turned into a digitized asset and secured using a blockchain. As soon as the thief attempted to monetize the asset by transferring ownership, the transaction would immediately pop up on the blockchain. Those administrators who have a copy of the blockchain on their system would need to verify and all reach consensus, that: (1) the person attempting to make the transaction is a valid or authorized user, and (2) the transaction itself is valid and authorized. In the case of the painting, as soon as that thief went to sell the painting, the authorized parties with the blockchain would know about it and be able to deny the transaction. The attempt to create that transaction, even though it did not actually happen, would be memorialized, in other words, recorded, on the blockchain itself. Therefore, the person in question (who was trying essentially to serve as a bad actor) would not be able to later deny her involvement in the attempted fraudulent act. That characteristic of the blockchain is known as *immutability*. One might stipulate that if a thief knows that this is going to happen and she won't be able to monetize the transaction, it might prevent her from stealing the asset, or attempting to make the fraudulent transaction in the first place. The interesting characteristic of blockchain is that this verification happens on the spot, so it's not a situation where we go back to audit something six months or a year later, and see that there has been a bad actor, or find a material misstatement. At that point, the horse is already out of the barn. Even if something is caught in an audit later, the reputational and financial damage to a company can be massive - just ask anyone who worked at Enron or Arthur Andersen in 2002.

Some might wonder if blockchain is redundant compared to current checks and balances already in place. For example, we already use title and insurance intermediaries to verify asset ownership and

provide third party validation, prior to the sale of an asset, such as a house. However, it takes time for title companies to verify a title. It also, like nearly everything in life, costs money. Therefore, we can use other methods besides a blockchain to verify ownership and authorize transactions. However, is our current system the most efficient and effective method of verifying a title? With the advent of blockchain, the answer is: probably not. When choosing a method of verification, we want to achieve at least one objective: either reduce costs, reduce time or reduce risk. Blockchain is fascinating because it has the potential to achieve all three objectives. In an ideal world using the blockchain, we are reducing time involved in completing the transaction; we are reducing costs by eliminating the third-party verifier; and we are potentially also reducing the risk of fraudulent transactions or major errors much, much sooner in the business cycle - versus after the fact, like the way we would with a traditional audit.

However, before we begin our journey into a blockchain-filled utopia, we need to also consider the barriers to implementation. Blockchain is a new technology, requires an extraordinary amount of compute power, and is (right now), very expensive. Therefore, when considering whether to implement a blockchain, one must look first at the Return on Investment (ROI). Blockchain ought to pay for itself, otherwise there is no point in having one. The most risk-averse way to implement would be to start with a Minimum Viable Product (MVP) or Proof of Concept (POC) using a sample size of digitized assets - whether those assets are real property, like land or houses, or intangible assets, like patents or intellectual property. By going through this process, it allows us to look at all our data or assets, and decide which is most valuable. This would be a good practice in any environment, not just a blockchain implementation. At the end of the day we must secure our data; either through some sort of data warehouse, SharePoint system, cloud or blockchain. Therefore, the first question we ought to always ask is: what is the most valuable data, what are the "crown jewels" of the organization? Once identified, we need to focus on securing that first. This topic deals more with data security in general, but it is important to touch on it, since it is the foundation on whether an organization should implement a blockchain, and for what data. Storing and securing data, via any method, is not cheap. No matter what the organization ends up using, the executives in charge should make sure that the Return on Investment (ROI) on that security method is high - in other words, that the money they are paying to protect that data is warranted and costs less than the actual value of the data itself.

About the Author

Sonia Mundra is the President of Chenega Analytic Business Solutions, an Alaska Native Corporation (ANC). She specializes in alpha contracting acquisitions, to create win-win results for Chenega's customers and employees. Ms. Mundra is a Certified Public Accountant (CPA), Project Management Professional (PMP) and a certified Government Blockchain Consultant. Phone: +1 (202) 527-2511; E-mail: sdmundra@chenega.com.

References

[1] CompTIA, 2018. Building a Culture of Cybersecurity: A Guide for Corporate Executives and Board Members. Available online at: https://www.comptia.org/resources/building-a-culture-of-cybersecurity-a-guide-for-corporate-executives-and-board-members.

[2] Blockchain Working Group, ACT-IAC Emerging Technology Community of Interest, 2018. Blockchain Playbook for Federal Government. Available online at: https://www.actiac.org/act-iac-white-paper-blockchain-playbook-us-federal-government.