



Stan Mierzwa

ICIT Fellow & Director and
Adjunct Professor, Center
for Cybersecurity, Kean
University

An Overview of the Potential for Blockchain Technology to Improve Cybersecurity

AN ICIT FELLOW PERSPECTIVE
JANUARY 2022

Introduction

The purpose of this short research commentary is to provide a focused, semi-deep dive into the effort the industry places on cybersecurity defense and operations and the potential to integrate blockchain technology. As cybersecurity threats and incidents continue to rise, better procedures and strategies to protect our organizations' data and systems are crucial to sustaining viable operations. Given that blockchain technology can potentially disrupt other industries (Moore, 2020), it is imperative to examine how it may improve our cybersecurity.

Cybersecurity is an ever-evolving activity. Understanding the role blockchain may play is critical for those responsible for providing technological solutions or introducing technologies to protect their organizations. Thus, this document will outline cybersecurity advancements, associated challenges, and the future impacts blockchain may have moving forward.

Industry Advancement with Blockchain

The use of information technologies can be traced through almost every type of organization, industry, and business. However, if connected to the internet, technology creates the potential for cyber threats. Technology is being rapidly implemented with Internet of Things (IoT) devices, particularly in the manufacturing and the industrial sectors. A report from Cisco Systems indicated upwards of 50 billion Internet-connected items or devices in use as of 2020, and this number is likely growing (Alotaibi, 2019). With IoT devices, communications between the components and other integrated systems are considered standard operation. However, securing network communication traffic between IoT devices is critical to prevent man-in-the-middle or other attack vectors. Improvements to IoT using blockchain can secure information and communication shared amongst IoT devices and improve the confidentiality, integrity, and availability of data information systems (Alotaibi, 2019).

Industrial control systems (ICS) and technologies are critical for maintaining the infrastructure necessary to preserve modern life, including the energy sector and power distribution. Crucial infrastructure can include ICS technology like sensors, smart grid infrastructure, and other mechanisms to maintain operation, availability, and reliability. Unfortunately, threat actors and cybercriminals, including nation-state hackers, are now targeting industrial and critical infrastructure systems in an attempt to harm nations.

Industry History Without Blockchain Use

Historically, computer viruses and other types of malware helped inspire, create, and generate the antivirus and anti-malware industry. Some of the earliest challenging virus attacks occurred in 1998, shocking many in the technology world and creating greater awareness of these types of incidents (Vidyapeeth, 2014). In the continued pursuit to protect assets and information

from security breaches, new technologies add new protection, often referred to as multi-layered security.

Blockchain could be one of the tools for protecting information, computer communication flow, and technology systems from cyber threats. Utilizing a defense-in-depth principle, blockchain can add an additional layer of protection by defending the privacy and security of important data, application programs, and information. For example, a healthcare company is responsible for the privacy and security of patient health-related information. Blockchain might positively contribute to these organizations' layered defenses.

Highlighted Advancements Due to Blockchain

The areas that provide value to cybersecurity defenses are varied. In one aspect, threat intelligence sharing is critical to proactively protect organizations. The inclusion of blockchain technology to safeguard the sharing of essential cyber threats is one advancement in the cybersecurity. One proposed exchange system is the Structured Threat Information Exchange which uses Ethereum, an open-source blockchain, as a threat intelligence sharing mechanism. Here, blockchain technology offers accounting, availability, identity management, decentralization, and privacy (Riesco, Larriva-Novo & Villagra 2019). Sharing knowledge and cyber situational awareness is of daily importance in many organizations. For example, consider the value of knowing about new phishing emails with links to malware, or even worse, ransomware. Sharing potential threats with end-users in any organization can minimize human-centered breaches and incidents.

Potential Resiliency of Blockchain

Preventing cybercriminals from breaching cybersecurity and information security is no easy task. If leveraging the technology used in cryptocurrency transactions can complement the existing solutions, it is worth exploring since it is near impossible to hack into a blockchain or tamper with it to access data. This is because getting the network to accept a new block requires hackers to simultaneously access all the blocks (Moradi, 2019). Maintaining data security via blockchain can be a viable method to add another layer of protection. As new technology solutions evolve and appear on the market, it is important to consider if and how such solutions can be useful in industries. In this example, using blockchain, a new paradigm solution, can have the potential to integrate a resilient transaction-based function.

Using Big Data and Blockchain to Protect Against Cybercrime

Understanding the new and emerging trends every year cannot be overlooked, given the potential for great harm to an industry or organization. Big data and blockchain are two such emerging trends that cannot be ignored, particularly in the areas of cybersecurity and cyber protection. Collecting data from various sources can help organizations spot trends or alert them to data that may need further analysis to protect against cyber threats. For example, INTERPOL's collaborative cybercrime detection system, called ROXANNE, is used to help discover and identify criminal activities by capturing and monitoring real-time text, audio, video, and data feeds (INTERPOL, 2019). Such a system relies on large amounts of combined data and security to ensure the transmitted information is secure. The use of blockchain technologies could assist this system with the coordination, transfer, and storage of such data to ensure privacy. In this instance, the combination of big data, analytics capabilities, and blockchain could notably decrease the ever-growing amount of cybercriminal activity analysis required of global law enforcement.

Blockchain and Improving Internet Application Security

End users take the foundational components of the internet for granted. These critical infrastructure applications include the domain name system (DNS), which helps locate destination domain addresses, and the simple mail transfer protocol (SMTP), which ensures the proper sending and receiving of email messages and attachments. While end users rarely recognize the use of DNS or SMTP, the internet is rendered unusable without them. Unfortunately, confidentiality, integrity, or availability were not at the forefront of the developer's minds when these services were created. Thus, DNS and SMTP lack the proper safeguards unless implemented by information technology teams. Blockchain could help enhance trust in these services by including a non-centralized governing body for these online services (ul Hassan et al. 2019).

Aside from core internet functions, blockchain could enhance the security of popular big-data-based products, such as Facebook. This online social network has encountered data and system breaches, partially because of a central management security module. One of the most notable examples was when Cambridge Analytica used the data of over 50 million Facebook users to help predict their presidential choice during the 2016 United States presidential election. (ul Hassan et al. 2019). Using blockchain could have given Facebook greater transparency into the firms or systems accessing Facebook's backend datasets.

A Deeper Dive into Microsoft's Use and Adoption of Bitcoin

Microsoft, one of the largest global technology companies, began allowing customers to pay for Microsoft Store and Xbox content with Bitcoin as early as 2014. Bitcoin was introduced in partnership with a payment processor named BitPay, which allowed customers to convert funds before purchasing anything from Microsoft (Times of India, 2016).

After this, Microsoft began looking into ways to utilize blockchain technology, the foundational component of Bitcoin, to manage and administer user credentials (Hipps, 2019). Since Microsoft includes many different cloud-based services, such as Office 365 and Azure, login and credential management are critical. Because many companies and organizations rely on these Microsoft products, utilizing blockchain for security may warrant further development (Cuen, 2019).

The blockchain product set being developed by Microsoft is an open, decentralized, public, permission-less identity solution named ION. ION incorporates the use of denaturalized identifiers to give the power to control one's username and password to the user, independent of any external group or intermediary (Dingle, 2021). Regardless of whether ION takes off, the effort is likely to have a far-reaching impact since it lays the groundwork for Microsoft to use blockchain in other software (Mierzwa, 2021).

A Brief Discussion of the Corollary Impacts of Blockchain Adoption

Although there are possible benefits to using blockchain technology, it is important to understand that new issues may be introduced with its implementation. Recent news reports have revealed that implementing blockchain solutions, specifically mining systems, consumes vast amounts of power. The Harvard Business Review and the Cambridge Center for Alternative Finance estimate that the Bitcoin system consumes 110 terawatt-hours per year. This energy equates to about .55% of the total global electrical power produced or the yearly energy consumption of Sweden and Malaysia combined. Unfortunately, this energy consumption is partly attributed to the amount of computing power required to encrypt blocks before placing the chunks into the blockchain (Carter, 2021). Initially, a coin could be mined using a simple home computer setup. However, Bitcoin rapidly expanded, and it now takes upwards of nine years' worth of household electricity to mine one Bitcoin (Huang, O'Neill & Tabuchi, 2021). Although specific sectors have benefited, as have cryptocurrency traders, the question remains: does the power being consumed overshadow the benefits of blockchain technology?

For those groups and individuals tasked with securing their organizations, thinking "outside the box", or rather creatively, can bring about positive effects. The cyber threat landscape continues to evolve and morph, and so do the defense mechanisms as well. One such method

is a novel approach from BitTrap, which deliberately plants pre-loaded cryptocurrency wallets on select devices to help determine if a hacker has breached a network environment (Amoroso, 2021). With this approach, an organization can quickly determine if its network has been hacked and learn the details of the breach. While this technique is certainly a niche for now, it is potentially another blockchain integration that aids organizations in cyber defense.

Conclusion

Businesses should consider valuable solutions from different industries to protect information, knowledge, data, and critical organizational systems. This paper discusses how the emergence of blockchain and cryptocurrency solutions can help thwart cyberattacks. The use of blockchain for privacy, confidentiality, integrity, and availability has the potential to positively add to organizations. New models can offer new economic incentives to both the producers of cybersecurity defense solutions and, equally important, the end users and customers (Riesco, Larriva-Novo & Villagra 2019).

Organizational leaders often look for new strategies to add value or solve complex problems. Blockchain technology has seen movement extending beyond's the initial field of finance, into other sectors, such as security. This paper conducted a landscape review of several different areas where blockchain is beginning to add value and contributing towards efforts to further safeguard organizations from cybersecurity threats. The roles that blockchain can play are varied, and in this report an outline of where it can subsidize the work of sharing cybersecurity threat knowledge, to improving IoT communication transactions, and how the functions of identity management and foundational Internet-related applications can benefit were outlined. In future work and efforts, it will be beneficial to outline how the cybersecurity defense field continues to evolve with the use of blockchain, or the next big technological leap innovation.

About the Author

Stanley Mierzwa is the Director of the Center for Cybersecurity at Kean University and an adjunct professor at Kean University on Cybersecurity Risk Management, Foundations in Cybersecurity, Cyber Policy, Firewalls and Secure CPU, and Digital Crime and Terrorism. Stan has over 20 published research publications and is a peer reviewer for the International Journal of Cybersecurity Intelligence and Cybercrime and the Online Journal of Public Health Informatics. He is also on the Editorial Review Board member for the International Association for Computer Information Systems. Previously, he was the Lead Application Security for the State of New York MTA Police. He is a member of the FBI Infragard, IEEE, CSA, ISC (2), and a board member of the global pharmacy education non-profit, Vennue Foundation and President of the Cloud Security Alliance – NJ Chapter.

Stan holds an M.S. from the New Jersey Institute of Technology and a B.S. in Electrical Engineering Technology from Fairleigh Dickinson University. He is currently working on his Ph.D. in Information Technology with a cybersecurity specialization. He is also a Certified Information Systems Security Professional (CISSP).

About the Kean University Center for Cybersecurity

The Kean University Center for Cybersecurity provides industry professionals, government agencies, non-profits, academics, and students necessary skills to develop proper awareness, preparedness, and resiliency when they encounter cybersecurity-related issues. The Center provides educational curriculum and implementation guidance to a diverse client base that includes emergency responders, academia, NGOs, and local and state government departments.

Through the four-step process—**Analyze, Educate, Train, and Communicate**— the Center creates semi-customized, focused training exercises that raise behavioral awareness and address organizational cybersecurity risks in reflection of internal policies, standards, and procedures.

About ICIT

The Institute for Critical Infrastructure Technology ([ICIT](#)) is a 501c(3) cybersecurity Think Tank with a mission to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders.

References

- Alotaibi, B. (2019). Utilizing Blockchain to Overcome Cyber Security Concerns in the Internet of Things: A Review. *IEEE Sensors Journal*. 19(23).
- Ajwani-Ramchandani, R., Figueira, S., Torres de Oliveira, R. & Jha, S. (2021). Enhancing the circular and modified linear economy: The important of blockchain for developing countries. *ScienceDirect*. 168.
- Amoroso, E. (2021). Cryptocurrency Grab-n-Go for Cyber Defense. LinkedIn Commentary. As retrieved from: <https://www.linkedin.com/pulse/cryptocurrency-grab-n-go-cyber-defense-edward-amoroso>
- Bajpai, P. (2021). Countries Where Bitcoin Is Legal and Illegal. Investopedia. As retrieved from: <https://www.investopedia.com/articles/forex/041515/countries-where-bitcoin-legal-illegal.asp>
- Baur, A., Buhler, J., Bick, M. & Bonorden, C.S. (2015). Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co. Conference on eBusiness, e-Services and e-Society. 63-80
- Biel, J. (2020). 9 Industries That Blockchain Has Infiltrated, and the Companies Leading the Charge. *Oracle Netsuite – Business Strategy*. As retrieved from: <https://www.netsuite.com/portal/resource/articles/business-strategy/blockchain-companies.shtml>
- Carter, N. (2021). How Much Energy Does Bitcoin Actually Consume? Harvard Business Review. As retrieved from: <https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume>
- Cuen, L. (2019). Microsoft Launches Decentralized Identity Tool on Bitcoin Blockchain. COINDESK. As retrieved from: <https://www.coindesk.com/markets/2019/05/13/microsoft-launches-decentralized-identity-tool-on-bitcoin-blockchain/>
- Dingle, P. (2021). ION – We Have Liftoff! Microsoft Tech Community. As retrieved from: <https://techcommunity.microsoft.com/t5/identity-standards-blog/ion-we-have-liftoff/ba-p/1441555>

- Hipps, T. (2019). Microsoft Wants to Protect Your Identity With Bitcoin. Wired Business. As retrieved from: <https://www.wired.com/story/microsoft-wants-protect-identity-bitcoin/>
- Huang, J., O'Neill, C. & Tabuchi, H. (2021). Bitcoin Uses More Electricity Than Many Countries. How Is that Possible? New York Times. As retrieved from: <https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html>
- INTERPOL. (2019). Real Time Network, Text, and Speaker Analytics for Combating Organized Crime (ROXANNE) project. As retrieved from: <https://www.interpol.int/en/News-and-Events/News/2019/Real-Time-Network-Text-and-Speaker-Analytics-for-Combating-Organized-Crime-ROXANNE-project>
- Mierzwa, S. (2021). Blockchain Technologies Will Be Integrated with Information Security and Cybersecurity Products. As retrieved from: <https://cisomag.eccouncil.org/blockchain-technologies/>
- Moore, J. (2020). 11 Industries Blockchain Will Change Forever. BlairesDev. As retrieved from: <https://www.bairesdev.com/blog/industries-blockchain-will-change-forever/>
- Moradi, J., Shahinzadeh, H. Nafisi, H. Gharehpetian, G.B. & Shaneh, M. (2019). Blockchain, a Sustainable Solution for Cybersecurity Using Cryptocurrency Financial Transactions in Smart Grids. IEEE Explore.
- Nasdaq. (2021). PayPal Accepts Bitcoin for Merchant Payment. As retrieved from: <https://www.nasdaq.com/articles/paypal-accepts-bitcoin-for-merchant-payment-2021-04-05>
- Riesco, R., Larriva-Novo, X. & Villagra, V.A. (2019). Cybersecurity threat intelligence knowledge exchange based on blockchain. *Telecommunication Systems*. 73. 259-288.
- Sraders, A. (2021). Corporate crypto 101: How companies are using Bitcoin and other digital currency. Fortune. As retrieved from: <https://fortune.com/2021/07/29/companies-using-bitcoin-btc-crypto-101/>
- Times of India. (2016). Microsoft continues Bitcoin support; apologize for wrong info [Computing].

Vance, T.R. & Vance, A. (2019). Cybersecurity in the Blockchain Era. A Survey on Examining Critical Infrastructure Protection with Blockchain-Based Technology. *IEEE. Explore*.

Vidyapeeth, B. (2014). Computer Virus and Antivirus Software – A Brief Review. *International Journal of Advances in Management and Economics*. 4(2). 01-014.

Ul Hassan, F., Ali, A., Latif, S., Qadir, J., Kanhere, S., Singh, J. & Crowcroft, J. (2019). Blockchain And The Future of the Internet: A Comprehensive Review. *arXiv: 1904.00733v1*.