Brad D. Messner
Indiana University of Pennsylvania

Synopsis of Dissertation Research

Title

A Critical Analysis on the Impact of Blockchain to the Security of Financial Technology Systems

Abstract

Blockchain and its subsequent technologies have grown in popularity, especially in the industries connected to financial systems and financial technology (fintech). Given the sensitive nature of the data in financial systems and the minimal research completed on the security of these systems, many corporations have opted to remain with traditional financial systems. This paper reviews the security of enterprise blockchain financial solutions and compares them against traditional enterprise solutions including acceptance within audits as well as enterprise confidence.

Introduction

While blockchain concepts have been around for decades, the technology to support these concepts is relatively new. Enterprises are struggling to understand the core concepts of blockchain and how it could apply to their operation, but few have sufficiently started the internal conversations related to security and the implications this decentralized and typically public technology might present once implemented.

The introduction and massive acceptance of cryptocurrencies globally over the last decade has brought around large discussions of blockchain technologies and, as a result, increased availability of blockchain solutions for organizations. Fintech globally is amid a broad realignment of tools and systems. By 2030, just short of half of enterprise solutions are believed will be deployed on a decentralized solution.

With all technology, as capabilities increase and availability grows broad, the concern related to security, especially cybersecurity, grows exponentially. As has historically been the situation with new technology solutions, during inception, the focus is on broad deployment and can, sometimes, result in the deployment of less secure solutions. This fear drives many corporations to delay their acceptance of new technology while waiting on more stable, secure solutions to be implemented. Once the acceptance of a new technology has been obtained and then large deployment has been achieved, the threats related to security grow. As blockchain technology is in the midst of this process, a critical and honest review of the potential threats related to blockchain is crucial.

Financial data and systems are some of the most secure platforms within an organization, especially as they contain confidential data and internal processes specific to individual organizations. Fintech was the first technology to deploy blockchain solutions through the use of cryptocurrencies. However, since then, there has only been moderate growth in other aspects of financial technologies while other industries have experienced significant growth through blockchain. One of the reasons for this is the concern of a decentralized, public system based upon trust. This drive fear into many organizations and, especially, within their cybersecurity and quality assurance departments.

Outside of the actual technical analysis, a secondary need arises very specific to blockchain solutions. This has been one of the most discussed and marketed technology platforms compared against other recent technology releases, especially in the fintech space. This increased awareness has placed pressure on many organizations to research the possibility of blockchain solutions in fintech.

Literature Review

Note: As I am still at the beginning of my research, I do not have a fully exhaustive Introduction of Literature Review completed just yet. Enclosed here is a summary of the work I have started so far.

Blockchain is a controversial topic in many large organizations. Technologists are divided on topics on resource utilization and security. Security analysts are divided over public available of data, trust networks and consensus protocols (Alzoubi, 2022). In general, despite what a small minority hold strong to, blockchain is on the verge of changing the financial technology industry and molding a new enterprise ERP and financial ecosystem (de Meijer, 2016).

At its core, blockchain relies upon anonymity and consensus-based algorithms to drive transactions. In a perfect world, this would be sufficient to validate transactions on the blockchain. This introduces a new host of concerns to both auditors and security analysts that have not been necessary prior. The general public is on the verge of acceptance of cryptocurrencies (Pagnotta, 2022), but financial sectors and securities management are significantly lagging behind due to many of these security-based concerns (Workie, 2017).

Many organizations have attempted to seek blockchain solutions, whether it be for research purposes or corporate deployment. Estonia has deployed blockchain concepts and, even, blockchain solutions in many facets of government work. The United States government has already begun research over the feasibility of blockchain solutions (Tshering, 2020).

One of the largest barriers to corporate acceptance is acceptance by internal audits (Hu, 2021). Especially amid large and costly security breaches already happening in the

financial sector, the implementation of new systems, especially systems that many people do not yet understand fully, is slowed down (Digrazia, 2018).

Objectives

There will be two primary objectives of this work. The first objective will be to assess whether the deployment of blockchain within fintech has a negative or positive impact on overall enterprise security. With so much industry-level discussion around blockchain technology, a true assessment needs to happen to address the question.

Secondarily, an alternate objective will be to determine whether the implementation of blockchain impacts the securities and governance associated with said organizations: ideally, are they still able to pass security audits and properly assess their potential risks and threats. Connected to this will be a review of how organizations using traditional fintech view organizations who use blockchain and does that view impact their willingness to potentially partner together.

Hypothesis

H1: Financial Technology Systems that leverage blockchain technology are less likely to have a severe security incident compared to those relying on traditional, enterprise systems.

H2: Financial Technology Systems that leverage blockchain technology have fewer minimal security incidents compared to those relying on traditional, enterprise systems.

H3: Enterprises that use blockchain-based Financial Technology Systems have confidence in the security of their solutions.

H4: Enterprises that use Financial Technology Systems pass the same industry security audits as those organizations who rely on traditional, enterprise systems.

Methods and Methodology

Given the newness of this topic and lack of large amounts of quantitative data specific to the security within fintech and organizations who are fully utilizing blockchain technology in this domain are limited, a mixed methods approach will be utilized.

Using a secondary data source, a quantitative approach will be taken to assess the risks and vulnerabilities introduced when blockchain is implemented and then compare that to the vulnerabilities that exist in traditional fintech. Afterwards, a collection of panel data will be used to compare multiple points of data over an extended time period to assess

whether the introduction of blockchain shows and noticeable of significant shift in enterprise security.

The second half of this paper will include a case study – an in-depth review of an organization who has already deployed blockchain technology. Using mostly interviews, we will access the security as well as theint4ertal view of how blockchain has impacted their enterprises security.

Limitations

Blockchain technologies have been both conceptualized as well as physically deployed for years; however, the breadth of this usage is still somewhere minimal. Until much more extensive research can be conducted, there will continue to be a gap in the comparable data between traditional financial systems and those based off blockchain technologies. More developers and organizations are beginning to work with blockchain technologies, so the availability of solutions is growing steadily, but not enough in-depth research has conducted to validate those solutions across multiple domains and industries.

This report only conducted a high-level review of policy-compliance, governance, and audit review. In order to properly evaluate full security within blockchain technologies in fintech, a more thorough and invasive review of these topics would need completed.

A final limitation that must be kept in consider is that most enterprises who have been early adopters of blockchain typically are more open to risk than those who have not yet adopted. These organizes are typically more open to risk especially risk that is connected to newer innovations so our results may be a bit skewed given the risk acceptance of these organizations. Additional research would need conducted as blockchain grows in popularity and more organizations begin implementation.

References

Note: Below references are part of the entire dissertation, not just the literature review written above.

Alzoubi, Y. I., Al-Ahmad, A., & Kahtan, H. (2022). Blockchain technology as a Fog computing security and privacy solution: An overview. Computer Communications, 182, 129–152.

Bartoletti, I., Plantié, S., & Sambodaran, A. (2020). Security and privacy risks in the blockchain ecosystem. Cyber Security: A Peer-Reviewed Journal, 3(3), 195–207.

Chih-Ming Chen, Di-Yu Lei, Jui-Hsi Cheng, & Kai-Ping Huang. (2020). Blockchain Technology and Business Transaction: From Security and Privacy Perspectives. International Journal of Organizational Innovation, 13(2), 145–155.

de Meijer, C. R. W. (2016). Blockchain and the securities industry: Towards a new ecosystem. Journal of Securities Operations & Custody, 8(4), 322–329.

Digrazia, K. (2018). Cyber Insurance, Data Security, and Blockchain in the Wake of the Equifax Breach. Journal of Business & Technology Law, 13(2), 255–277.

Gupta, R., Reebadiya, D., Tanwar, S., Kumar, N., & Guizani, M. (2021). When Blockchain Meets Edge Intelligence: Trusted and Security Solutions for Consumers. IEEE Network, 35(5), 272–278.

Hu, Q., Asghar, M. R., & Zeadally, S. (2021). Blockchain-based public ecosystem for auditing security of software applications. Computing, 103(11), 2643–2665.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841–853.

Nathan, J., & Jacobs, B. (2020). Blockchain consortium networks: Adding security and trust in financial services. Journal of Corporate Accounting & Finance (Wiley), 31(2), 29–33.

Pagnotta, E. S. (2022). Decentralizing Money: Bitcoin Prices and Blockchain Security. Review of Financial Studies, 35(2), 866–907.

Rui Zhang, Rui Xue, & Ling Liu. (2019). Security and Privacy on Blockchain. ACM Computing Surveys, 52(3), 1–34.

Ryan, R., & Donohue, M. (2017). Securities on Blockchain. Business Lawyer, 73(1), 85–108.

Siwan Noh, & Kyung-Hyune Rhee. (2019). A Study on the Analysis and Solutions of the Blockchain Security Issues. Journal of Korean Society for Internet Information, 20(4), 1–11.

Tshering, G., & Gao, S. (2020). Understanding security in the government's use of blockchain technology with value focused thinking approach. Journal of Enterprise Information Management, 33(3), 519–540.

White, B. S., King, C. G., & Holladay, J. (2020). Blockchain security risk assessment and the auditor. Journal of Corporate Accounting & Finance (Wiley), 31(2), 47–53.

Workie, H., & Jain, K. (2017). Distributed ledger technology: Implications of blockchain for the securities industry. Journal of Securities Operations & Custody, 9(4), 347–355.

Zamani, E., He, Y., & Phillips, M. (2020). On the Security Risks of the Blockchain. Journal of Computer Information Systems, 60(6), 495–506.