Equifinality in Blockchain Resilience: The Role of Organizational, Environmental, and Cybersecurity Factors

Brett J. L. Landry[a], Renita Murimi[a], Greg Bell[a]

[a] University of Dallas, Gupta College of Business
blandry@udallas.edu, rmurimi@udallas.edu, gbell@udallas.edu

Abstract

A common misconception of blockchain technologies is that they are inherently resilient. However, recent failures of blockchain-supported applications have demonstrated that other factors play a role despite the strengths of the underlying technology. Existing research has analyzed blockchain resilience within sectors and has not been generalizable across industries. Additionally, much of this research examines the independent effects of individual and organizational factors and their isolated contributions to blockchain resilience. In this paper, we suggest that blockchain resilience is a combined function of organizational capabilities, the business environment, and cybersecurity issues. This approach emphasizes the concept of equifinality, which assumes that a system can reach the same final state from various initial conditions and along a variety of paths. The contributions of this paper are threefold. First, unlike previous sector-based research, we approach blockchain resilience with a broader lens. Our sector-agnostic examination of blockchain resilience will provide applicability across industries. Second, our paper moves beyond exploring factors in isolation to theorizing about the interdependencies of organizational capabilities and environmental and cybersecurity factors, including how they may complement or substitute with one another in contributing to blockchain resilience. Third, we will examine the applicability of equifinality within the blockchain context.

Keywords: Blockchain, Cybersecurity, Equifinality, Organizational Capabilities, Resilience

1. Introduction

The U.S. National Institute for Standards and Technology (NIST) defines information resilience as “the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents” (Joint Task Force Transformation Initiative, 2020). These changing conditions include the adoption of emerging technologies which have the potential to disrupt longstanding socioeconomic structures. One such example of a disruptive technology is blockchain. Blockchain has created opportunities for re-envisioning the role of currency, finance, supply chain management, and record-keeping in general. NIST defines blockchain as “A distributed digital ledger of cryptographically-signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules” (Yaga et al., 2019).

While blockchain technologies can be employed to provide resilience for disaster supply chains (Katina & Gheorghe, 2023), this paper will focus on the factors that provide resilience to the blockchain systems directly. A common misconception of blockchain technologies is that they are inherently resilient. However, recent failures of blockchain-supported applications have demonstrated that other factors play a role despite the strengths of the underlying technology. The factors include organizational capabilities, the business environment, and cybersecurity issues.

2. Equifinality in blockchain resilience

Organizational researchers increasingly acknowledge that numerous factors influence outcomes and that these factors should not be evaluated independently. Instead, they should be viewed as "bundles" or combinations that can enhance each other's ability to achieve crucial organizational outcomes. This research highlights the importance of identifying interdependencies among multiple explanatory factors that contribute to a desired outcome. Studies conducted by Bell et al. (2014) and Furnari et al. (2021) emphasize this aspect of research. This line of research also emphasizes the significance of comprehending how multiple factors operate simultaneously, which is crucial for decision-makers.

The concept of equifinality has been explored in management literature concerning the presence of items or activities. This means that there are numerous ways to achieve the same outcome, and bundles of items should be considered in order to reach that outcome. In the context of blockchain, configurational theory allows scholars to argue that the combination of factors that lead to resilience can result from the presence or absence of various conditions or factors. Conjunctural causation is particularly helpful when there could be multiple reasons for a particular outcome and when causal conditions could combine in unique and various ways to bring about that outcome.

It should be noted that in rapidly changing environments, the bundle components are not fixed and should be regularly reviewed and updated. While having a range of potential solutions to include in a bundle can be advantageous, an excess of options can also cause decision fatigue. This is particularly true because solutions are subject to change, and bundles must be adapted to suit the specific needs of different communities in their respective environments. In addition, bundles are intrinsically dynamic because the technology included changes. For instance, botnets that were once primarily used to disseminate spam are now used extensively for ransomware command and control operations (Jarjoui et al., 2021; Murimi, 2020). As threats continue to evolve, the individual components of a bundle must be revised, replaced, or adjusted. Therefore, organizations must allocate resources to update individual components and determine their impact on other components.

Therefore, incident bundles require flexible solution bundles that also encompass the idea of equifinality. The attributes of a bundle play an essential role in determining the equifinality of a configuration. This includes the types of resources in the bundle, the challenges that these resources are intended to address, and the interdependence of the resources within the bundle. By considering these attributes, it becomes possible to identify different configurations of resources that can achieve the same outcomes, which is critical. If we establish that equifinality provides different pathways for blockchain resilience, then it is possible that the level of resilience varies based on organizational capabilities, the business environment, and cybersecurity issues. Along these pathways, factors can be positive or negative, and the combination of factors will drive the level of blockchain resilience.

2.1 Organizational capabilities

The first consideration for blockchain resilience is the capabilities of the organization.

Organizational capabilities include a firm's size, resources, capital, and knowledge. Generally, larger firms have more and better resources than small and midsized businesses (SMBs). SMBs typically have "limited resources and do not have the budget, technology, or personnel with the skillsets needed for active cyber defense" (Landry & Koger, 2023, p. 98301) which is paramount for deploying blockchain technologies. Smallwood and Ulrich (2004) suggest that organizational capabilities are based on both an individual's functional competence and the organization's core competencies. They suggest that well-managed organizations have the following eleven capabilities, as listed in Table 1, and these items can be used as part of a capabilities audit. Given that these items can be audited assumes that there are different levels of capabilities with a variable scale. These items can all be considered components in the organizational capability bundle.

Table 1: Organizational Capabilities for Well-Managed Firms
(adopted from Smallwood and Ulrich (2004))

Capability	**Description**
Talent	We are good at attracting, motivating, and retaining competent and committed people
Speed	We are good at making important changes rapidly
Shared Mind-Set and Coherent Brand Identity	We are good at ensuring that employees and customers have positive and consistent images of and experiences with our organization
Accountability	We are good at obtaining high performance from employees
Collaboration	We are good at working across boundaries to ensure both efficiency and leverage
Learning	We are good at generating and generalizing ideas with impact
Leadership	We are good at embedding leaders throughout the organization
Customer Connectivity	We are good at building enduring relationships of trust with targeted customers
Strategic Unity	We are good at articulating and sharing a strategic point of view
Innovation	We are good at doing something new in both content and process
Efficiency	We are good at managing costs

2.2 Business environment

Blockchain technologies can be deployed in a variety of sectors and functions. This is an important distinction because most people think of blockchain and cryptocurrencies as synonymous terms, which is not the case. A better analogy is that all squares are rectangles, but not all rectangles are squares. All cryptocurrencies are blockchains, but not all blockchains are cryptocurrencies. Given that blockchain operates in technology-centric enterprises, the business environment can be examined through the lens of Porter's Five Forces Model (1979)**.** Since blockchain technologies are deployed in technology-centric organizations, the threat of substitute products, the threat of new entrants, and the threat of new entrants are usually high. However, supplier and customer power will vary based on the application. A recent example of low customer power has been the recent cryptocurrency winter, where customers' funds have been locked up in defunct exchanges like Celsius.

However, the competitive landscape is not the only business factor for blockchain resilience. National laws and economic climate are also factors. For example, the demand for cryptocurrencies in Argentina dramatically differs from the need in the European Union due to radically different economies. Additionally, the business climate can radically change when a government decides to ban crypto mining, as China did in 2022 (Tabuchi, 2022).

Another business issue for blockchain is the initial costs and deployment. For example, in November of 2022, the shipping firm Maersk and IBM announced they were discontinuing their development of TradeLens, a blockchain-enabled shipping tracking application (Bousquette, 2022). Development began in 2018, and the application is scheduled to be shut down by the end of the first quarter of 2023. One of the contributing factors to the failure of the program is the technical complexity and investment costs needed by all parties involved. Also, in November of 2022, the Australian Stock Exchange announced that they would be discontinuing a project announced seven years before in which they had already spent $168 million (Muir, 2022). These cases illustrate that blockchain resilience is determined by more than just the technology; it requires that the business case support the investment. There also must be collaboration and commitment from all business stakeholders.

2.3 Cybersecurity factors

While blockchain has incredible integrity protection mechanisms built into the architecture, it does not stop cybersecurity attacks. Cybersecurity is a very complex environment due to high levels of uncertainty (Anant et al., 2019) and a constantly evolving threat landscape. As a result, organizations are constantly under attack. Furthermore, cyber incidents can vary in how their threat vectors manifest. For instance, the effects of a cybersecurity control failure in a healthcare network may differ from that in a supply chain network. Furthermore, the factors that cause a cyber incident in one environment may not be identical to those in another, and the solutions employed to tackle these threat vectors may also differ.

Threat actors have a variety of tools in their toolboxes. Old VPNs accounts can be used to install ransomware, as in the 2021 Colonial Pipeline attack (U. S. Department of Energy, 2021). Poor cybersecurity practices allow threat actors direct access to critical systems, as in the Oldsmar water treatment plant, where a compromised PC was used to release dangerous levels of lye into the water supply (Bergal, 2021). However, threat actors do not only have technical tools in their toolbox. Social engineering is a human attack, as in the case of Robinhood, where a threat actor convinced an employee over the telephone to install remote access software on his PC (Abrams, 2021; Barry, 2021). However, human and technical attacks are not mutually exclusive. For example, the 2013 Target breach was a mix of human attacks and technical vulnerabilities by combining a phishing attack with poor network design. In 2013, a Fazio Mechanical employee responded to a phishing email that compromised their device (Dube, 2016), and then that device was able to access point of sales devices due to poor network design.

Modern networks' complexity and attack surfaces pose significant challenges for effective cybersecurity. Although cybersecurity tools are continually evolving to scan for potential cyber incidents, it is challenging to secure digital environments completely. After a cyber incident, root cause analysis typically identifies a set of factors that contributed to the incident. However, these factors are just a few of the many possible attack vectors that threat actors could have exploited. The multiplicity of causes, environments, threat vectors, motives, and attack outcomes further compounds the ongoing battle between attackers and defenders in cyberspace.

The type of blockchain can determine resilience. For example, permissionless blockchain networks allow anyone to read and write without authorization. On the other hand, permissioned blockchain networks limit participation using authentication controls to limit access to individuals or organizations. Thus, the type of blockchain employed is another factor contributing to resilience.

2.4 Research Proposition

To extend this research, we propose the following proposition.

Proposition 1. Multiple *combinations of organizational capabilities, business environments, and cybersecurity issues lead to high levels of blockchain resilience.*

3. Discussion

We believe that blockchain resilience is a combination of factors; organizational capabilities, the business environment, and cybersecurity issues. Each of these factors represents supersets of items, such as the eleven capabilities of successful firms, as Smallwood and Ulrich (2004) described. The same is true for the other two factors, and equifinality can be used to explain how multiple pathways can achieve blockchain resilience.

Qualitative Comparative Analysis (QCA) is a valuable methodology for cybersecurity scholars and practitioners to understand configurations that lead to incidents and those associated with recoveries. QCA uses a set-theoretic approach to develop causal claims by analyzing supersets and subsets. This methodology allows for multiple conditions to produce an outcome which in this case is blockchain resilience and helps to identify how various factors (organizational capabilities, business environment, and cybersecurity issues) combine to lead to the outcome. Moreover, QCA permits outcomes to occur due to the presence or absence of variables, as discussed earlier. Thus, achieving blockchain resilience with low organizational capabilities could be possible if the business environment and cybersecurity issues were supportive.

In recent years, the use of set-theoretic methods has increased among scholars investigating economic and organizational phenomena (Fiss, 2007; Fiss, 2011; Grandori & Furnari, 2008; Pajunen, 2008). QCA offers several advantages over traditional quantitative techniques in evaluating the configurations that lead to cyber incidents and recoveries. Unlike quantitative techniques, QCA does not assume permanent causality, additivity, or causal symmetry (Ragin, 2008). Additionally, QCA can handle multiple conditions leading to an outcome and identify how multiple factors combine to produce the outcome. Furthermore, QCA allows outcomes to occur due to the presence or absence of variables. The technique can be used with crisp or fuzzy sets to analyze multiple cases simultaneously and explore which factors contributed, was absent, or did not contribute to the incident bundles. However, using crisp or fuzzy sets is not an either-or case. Crisp and fuzzy sets can be used together to maintain fidelity to the data.

Future research should consider what elements of organizational capabilities, the business environment, and cybersecurity issues are binary and examined as crisp data sets, and which are membership based and examined as fuzzy sets. This examination would help academics and practitioners identify the pathways that best contribute to blockchain resilience.

References

Abrams, L. (2021). *7 million Robinhood user email addresses for sale on hacker forum.* BleepingComputer. https://www.bleepingcomputer.com/news/security/7-million-robinhood-user-email-addresses-for-sale-on-hacker-forum/

Anant, V., Bailey, T., Cracknell, R., Kaplan, J. & Schwartz, A. (2019). *Understanding the uncertainties of cybersecurity: Questions for chief information-security officers | McKinsey & Company.* https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-blog/understanding-the-uncertainties-of-cybersecurity-questions-for-chief-information-security-officers

Barry, C. (2021). *Robinhood breach illustrates the impact of social engineering attacks.* https://blog.barracuda.com/2021/11/19/robinhood-breach-illustrates-the-impact-of-social-engineering-attacks/

Bell, R. G., Filatotchev, I., & Aguilera, R. V. (2014). Corporate governance and investors' perceptions of foreign IPO value: An institutional perspective. *Academy of Management Journal*, *57*(1), 301-320. https://doi.org/10.5465/amj.2011.0146

Bergal, J. (2021). *Florida hack exposes danger to water systems.* https://pew.org/3btxWBc

Bousquette, I. (2022, Dec 15). Blockchain fails to gain traction in the enterprise. *The Wall Street Journal* https://www.wsj.com/articles/blockchain-fails-to-gain-traction-in-the-enterprise-11671057528

Dube, L. (2016). Autopsy of a data breach: The Target case. *International Journal of Case Studies in Management*, *14*(1)

Fiss, P. C. (2007). A set-theoretic approach to organizational configurations. *The Academy of Management Review*, *32*(4), 1180-1198. https://doi.org/10.5465/AMR.2007.26586092

Fiss, P. C. (2011). Building better causal theories: A fuzzy set approach to typologies in organization research. *Academy of Management Journal*, *54*(2), 393-420. https://doi.org/10.5465/AMJ.2011.60263120

Furnari, S., Crilly, D., Misangyi, V. F., Greckhamer, T., Fiss, P. C., & Aguilera, R. (2021). Capturing causal complexity: Heuristics for configurational theorizing. *Academy of Management Review*, *46*(4), 778-799. https://doi.org/10.5465/amr.2019.0298

Grandori, A., & Furnari, S. (2008). A chemistry of organization: Combinatory analysis and design. *Organization Studies*, *29*(3), 459-485. https://doi.org/10.1177/0170840607088023

Jarjoui, S., Murimi, R., & Murimi, R. (2021). Hold my beer: A case study of how ransomware affected an Australian beverage company. In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-6). https://doi.org/10.1109/CyberSA52016.2021.9478239

Joint Task Force Transformation Initiative. (2020). *SP 800-53r5: Security and privacy controls for information systems and organizations.* National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-53r5

Katina, P. F., & Gheorghe, A. V. (2023). *Blockchain-enabled resilience: An integrated approach for disaster supply chain and logistics management*. CRC Press.

Landry, B. J. L., & Koger, M. S. (2023). Leveraging unified threat management based honeypots in small and midsized businesses and educational environments. In *Proceedings of the Decision Sciences Institute Southwest Region* (pp. 98301-98306).

Muir, M. (2022). *Case for blockchain in financial services dented by failures.* https://www.ft.com/content/cb606604-a89c-4746-9524-e1833cd4973e

Murimi, R. (2020). Use of botnets for mining cryptocurrencies. In *Botnets* (1st ed., pp. 359-386). Routledge. https://doi.org/10.1201/9780429329913-11

Pajunen, K. (2008). Institutions and inflows of foreign direct investment: A fuzzy-set analysis. *Journal of International Business Studies*, *39*(4), 652-669. https://doi.org/10.1057/palgrave.jibs.8400371

Porter, M. E. (1979). How competitive forces shape strategy. *Harvard Business Review*, *57*(2), 137-145.

Ragin, C. (2008). *Redesigning social inquiry: Fuzzy sets and beyond*. University of Chicago.

Smallwood, N., & Ulrich, D. (2004). Capitalizing on capabilities. *Harvard Business Review*, https://hbr.org/2004/06/capitalizing-on-capabilities

Tabuchi, H. (2022, Feb. 25,). After Chinese ban, Cryptocurrency mining got worse for climate. *New York Times* https://www.nytimes.com/2022/02/25/climate/bitcoin-china-energy-pollution.html

U. S. Department of Energy. (2021). *Colonial Pipeline cyber incident.* Energy.gov. https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). *NISTIR 8202: Blockchain technology overview*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202