DESIGNING A GLASS ORGANIZATION: BOUNDARY DECISIONS FOR COORDINATION AND CONTROL BASED ON GENERALIZED TRUST

YING-YING HSIEH
ANU WADHWA
Imperial College Business School, Imperial College London
South Kensington Campus, London SW7 2AZ, UK
Email: y.hsieh@imperial.ac.uk; a.wadhwa@imperial.ac.uk

INTRODUCTION

Recent management literature makes clear the potential of blockchain to transform organizational coordination and control (Cennamo, Marchesi, & Meyer, 2020; Hsieh, Vergne, Lumineau, Wang, & Schilke, 2021; Vergne, 2020). Specifically, blockchain enables new forms of collaborative organizing, gives rise to new organizational architectures, and substantially reconfigures the scale and scope of transactional activities related to organizing (Lumineau et al., 2021; Snow, Fjeldstad, & Langer, 2017). Blockchain-based organizational systems, which allow autonomous actors to freely move across organizational boundaries and self-organize in decentralized networks without any formal hierarchy, can thus be conceptualized as "meta-organizations," defined as "organization[s] whose agents are themselves legally autonomous and not linked through employment relationships" (Gulati, Puranam, & Tushman, 2012: 573).

To achieve a system-level goal, meta-organizations facilitate coordination and control between autonomous actors, both individual and organizational, by adjusting two key dimensions—*boundary permeability*, which determines the membership criteria for participation, and the *degree of decision hierarchy*, which refers to the extent to which decision rights are concentrated in a small number of key members as orchestrators (Gulati et al., 2012). Meta-organizations typically rely on either dimension, or both, to ensure the confidence of participating actors in the correct and effective functioning of the system (Puranam & Vanneste, 2009). The source of this confidence goes beyond relationships with known partners to instead represent a form of "generalized trust" that is impersonal, "not specific to a counterparty and originates from a broader context" (Vanneste & Gulati, 2021: 1) at the societal or system level (Shapiro, 1987).

According to the organization design literature, achieving a high level of generalized trust is unlikely in open communities such as Wikipedia and the Linux open-source software development (OSSD) due to the absence of membership criteria as well as decision authority (Gulati et al., 2012). Intriguingly, blockchain-based systems, despite being open and non-hierarchical, are intended to solve the very problem of providing generalized trust required in transactions, thereby challenging the prediction of the literature (Nakamoto, 2008; McEvily, Perrone, & Zaheer, 2003). Motivated by this puzzle, we ask:

How does blockchain, as a trust-enabling novel form of organizing, engender varying degrees of generalized trust to facilitate coordination and control?

Note that the "degree of generalized trust" refers to the ability of an organization to ensure actors' confidence in the system to facilitate coordination and control. Blockchain calls for a deeper understanding of boundaries beyond permeability by integrating the notion of *transparency* rooted in the ideas of organizational boundaries as "efficient information envelopes [... for] trust production" (Zucker, Darby, Brewer, & Peng, 1996: 90, 91). Therefore, an informational processing view helps us establish a deeper understanding of transparency boundaries and how they impart generalized trust (Daft & Lewin, 1993; Galbraith, 1973; Tushman & Nadler, 1978). In fact, industry experts have borrowed from architecture the idea of

a "glass bank" to describe how, in a similar way, a blockchain system secures its network with transparent boundaries (Birch, Brown, & Parulava, 2016).

> *New Ideas for Burglar-Proof Banks—Built with glass walls, they would give more safety, as everything inside could be watched outside, and every money transaction at the tellers' open counters would be handled through a pneumatic tube connection to secret vaults…* *The News Leader* (1931: 6)

We argue that the *transparency* of organizational boundaries, which relates to information visibility and accessibility, is a key boundary characteristic that defines the scope of information sharing and information flow to help create an "organizational advantage" within which trust is produced (Schnackenberg & Tomlinson, 2016; Nahapiet & Ghoshal, 1998). We also argue that at the heart of blockchain's transparency-enabling generalized trust is *information processing*, a classic organization design lens that is highly useful for examining our research question (Galbraith, 1974; Tushman & Nadler, 1978). The logic of maximizing information-processing capacity is reflected in boundary decisions with different levels of permeability and transparency.

In this study, we propose a typology of boundaries to theorize how variations in boundary decisions shape varying degrees of generalized trust. While prior work on organizational boundaries has primarily, and almost exclusively, emphasized variations based on the permeability of boundaries, our study extends theory in three ways. First, we contribute to the broader management literature by establishing a deep understanding of the role of organizational boundaries in providing generalized trust. Second, we contribute to the organization design literature by proposing transparency as a new boundary, thus extending the traditional focus of boundary studies on permeability (e.g., Gulati et al., 2012; Santos & Eisenhardt, 2005). Finally, we discuss the implication of heterogeneity in boundary decisions for blockchain adoption.

BOUNDARIES IN TRUST-ENABLING ORGANIZATIONS

Blockchain-based systems are *trust-enabling* because they allow autonomous actors to perform tasks, access and verify critical information, and make decisions in a decentralized manner. Such systems are akin to a meta-organization in that both exhibit permeable boundaries (Gawer, 2014; Kretschmer, Leiponen, Schilling, & Vasudeva, 2020). *Transparency* (in addition to permeability) is necessary for decentralized information processing to foster decentralized coordination and control among autonomous actors—similar to how a glass bank makes its full transaction history visible to the public. Drawing from the information processing literature, we conceptualize transparency as disclosure—that is, providing or transacting information in a relevant, timely, and accurate manner (Schnackenberg & Tomlinson, 2016; Joseph & Gaba, 2020).

Information Processing and Boundary Design

Boundary decisions are crucial for coordination and control because they enable trust by shaping the appearance, and consequently, the information-processing properties of the "information envelope" (Zucker et al., 1996: 91). Specifically, we focus on information processing across organizational system boundaries (Altman, Nagle, & Tushman, 2015; Carson et al., 2003; Sutcliffe, 2001) where effective coordination and control are achieved when the system possesses sufficient information-processing capacity (Tushman & Nadler, 1978). In

principle, firms should aim to expand their information-processing capacity while reducing the need for information processing (Galbraith, 1974, 1977; Joseph & Gaba, 2020). As boundary decisions determine which actors are allowed to perform tasks, access and verify information, and modify the rules of the system (Galbraith, 1974), they represent key organization design parameters that directly influence the provision, storage, and flow of information. We thus propose two key metrics that define boundary decisions —the *degree of permeability* and the *degree of transparency*

Permeability. Building on Gulati et al. (2012), we define an organizational system's degree of permeability as the extent to which membership is unrestricted to allow any organization or individual to participate in, and directly influence, the functioning of the organizational system. There are a number of ways in which organizational boundaries can be rendered permeable (Santos & Eisenhardt, 2005). When decentralized actors collectively adopt an organizational structure to achieve common goals, three boundary variations related to permeability may emerge.

Transparency. The degree of transparency refers to the extent to which external actors can access key information generated and stored by the organizational system. Systems high in transparency allow public access to information about the state of the system and the data in the system, whereas systems low in transparency are private and allow few members such uninhibited access. Therefore, organizational transparency is conceptualized as intentional sharing of information (Schnackenberg & Tomlinson, 2016) that is a function of (i) *disclosure*, which refers to the relevance, timeliness, and amount of information made visible and accessible; (ii) *clarity*, which relates to how understandable the information is; and (iii) *accuracy*, which pertains to the reliability and correctness of information. Transparency facilitates information sharing about task structures (Colfer & Baldwin, 2010), by making the task architecture visible to organizational actors (Puranam et al., 2014). We go beyond this theoretical focus on the division of labor and explicate the role of transparency through information processing that integrates effort.

Based on varying degrees of permeability and transparency, we can conceive three organizational designs: boundaries with (i) LOW transparency and LOW permeability, (ii) HIGH transparency and LOW permeability, and (iii) HIGH transparency and HIGH permeability (see Table 1). Note that we do not consider boundaries with LOW transparency and HIGH permeability because such organizations represent a centrally managed (usually corporate) ecosystem. The first three boundary decisions of an organization can be facilitated by blockchain-based systems. Thus, the adoption of a blockchain system provides an ideal opportunity to study the design and implementation of trust-enabling organizations by relaxing different types of boundaries.

Table 1 About Here

A Typology of Boundaries in Blockchain Systems

Drawing from literature on blockchain-based organizing, we distinguish between three types of blockchain system design (Hsieh, et al., 2018), eachwith different combinations of boundary permeability and transparency. On one extreme, a *permissionless public* blockchain system has unrestricted membership criteria for verification and validation (i.e., very high

boundary permeability), through a public ledger auditable to the general public (i.e., very high boundary transparency) (Quadrant I in Table 1). The goal of such a design is decentralization and autonomy in coordination and control. Bitcoin, the largest cryptocurrency, represents a permissionless public blockchain (Hsieh et al., 2018).

At the other extreme is a *permissioned private* system with very low boundary permeability and very low transparency. Such a blockchain system is built on closed membership, the transaction ledger is visible only to private members and it aims for scalability and security-based autonomy (Quadrant III, Table 1). Finally, the third design, a *permissioned public* system, combines restricted membership (i.e., low permeability) with a transaction ledger auditable to the public (i.e., high transparency) (Quadrant II, Table 1) (Beck et al., 2018). This design is also called a "hybrid" blockchain (Geroni, 2021). Next, we elaborate on these blockchain boundary decisions.

BOUNDARY DECISIONS, GENERALIZED TRUST, AND ADOPTION

Building on the typology of boundaries displayed in Table 1, we formulate propositions by drawing from literature on information processing to conceptualize the incremental effects of increasing transparency and permeability and their effects on generalized trust-based coordination and control. Using permissioned private blockchain systems as the baseline, we argue that a permissionless public blockchain will engender the highest level of generalized trust with a focus on autonomy, as opposed to a focus on scalability (taking decentralization as given for both). In addition, we argue that complementarity between activities influences trust-enabling outcomes. Finally, we discuss implications for heterogeneity in modes of adoption.

Transparency boundaries. The transparency of a blockchain system can vary depending on the frequency and extent of information available to an intended audience. The "radical transparency" (Birch & Parulava, 2018: 375), while improbable for traditional corporations, vastly expands a blockchain system's information-processing capacity, which in turn increases generalized trust (Gulati & Sytch, 2007; Nonaka, 1994; Sutcliffe, 2001). Thus, we propose:

> **Proposition 1:** *Compared with a permissioned private organizational system (i.e., the baseline), a permissioned public boundary decision with additional transparency renders greater information-processing capacity, which in turn lends the blockchain system a higher degree of generalized trust and the ability to achieve a greater level of scalability*.

Permeability boundaries. By design, the scope of a permissionless public system is not defined by legal boundaries, but by permeable boundaries across the efficiency, competence, and power domains (Santos & Eisenhardt, 2005). By extending control to all participants (and minimizing control by regulators or third parties), a highly permeable system allows self-selected actors to influence the system's development and evolution. Compared with a permissioned public (hybrid) system, a permissionless public system expands information-processing capacity by providing resources and competence to secure a highly autonomous system. Therefore, we propose that,

> **Proposition 2**: *Compared with a permissioned private system (i.e., the baseline), a permissionless public boundary decision with added transparency and permeability*

further expands information-processing capacity. Consequently, this system has the highest degree of generalized trust among all boundary designs and is able to achieve the highest level of autonomy.

Complementarity. When the disclosed task-related information is highly complementary, visibility of the information will allow actors performing complementary tasks to more effectively combine information to generate insights for monitoring, validation, and verification. Similarly, through role clarity around complementary activities, contributors with complementary skill sets can more readily access information to create open innovation that engenders generalized trust (Altman et al., 2015). Therefore, we propose:

Proposition 3: *A high level of complementarity among activities performed within the blockchain system strengthens the positive relationship between transparency and the ability of the system to enable generalized trust.*

Boundary permeability enables actors to perform complementary tasks such as validating transactions, upgrading the source code, and building applications—through increased information-processing capacity. Complementary activities thus lead to greater generalized trust.

Proposition 4: *A high level of complementarity among activities performed within the blockchain system amplifies the positive relationship between the degree of permeability and the ability of the system to enable generalized trust.*

Modes of Adoption: Actor-centric vs. Technology-centric adoption. Given the mutual embeddedness of technology and organizational design inherent in a blockchain system, its adoption requires an architecture in which actors as well as technology can assume prominent roles in facilitating coordination and control (Fjelstadt et al., 2012; Snow et al., 2017). The organization design literature suggests that "boundaries and goals jointly identify organizations uniquely" (Puranam et al., 2014: 164), and an effective organization design relies on aligning the organization with its environment (Thompson, 1967; Tushman & Nadler, 1978). We proposed two modes of adoption—actor-centric vs. technology-centric, each of which align the goal of the organization with is participants through trust production, trust distribution, and trust convergence.

Proposition 5: *A permissioned private blockchain system will be adopted following an actor-centric mode of adoption, whereby trust production, trust distribution, and trust convergence take place primarily though human actors.*

Proposition 6: *A permissionless public blockchain system will be adopted following a technology-centric mode of adoption, whereby trust production, trust distribution, and trust convergence take place primarily though technology.*

Hybrid Mode of Adoption. A hybrid mode of adoption involves "using a public blockchain where a private network is hosted," and consequently, "[s]ome aspects of the network can be made public depending on which data to share" (Geroni, 2021). A hybrid mode of adoption is used when actors aim to build an enterprise-grade, scalable system based upon some

form of restricted membership, yet deployed with information auditable beyond individual organizational boundaries.

> **Proposition 7:** *A permissioned public blockchain system reflects a hybrid mode of adoption, which is optimal when a system varies the level of its transparency boundaries in terms of which information to make public or keep private. This flexibility enables a hybrid blockchain system to host a more diverse range of actors and a broader range of use cases compared with the other two modes of adoption.*

CONCLUSION

We make several key contributions. First, we contribute to the organizational design literature by examining the nature of organizational boundaries, which have been conceptualized as permeable membranes that may allow the movement of people, resources, and influence (Gulati et al., 2012; Santos & Eisenhardt, 2005). Second, we expand the role of organizational boundaries to include transparency and permeability to contribute to the broader management literature, which has largely focused on the restriction of membership as the key mechanism for producing trust within an organizational system (Zucker et al., 1996). Finally, we contribute to the literature on innovation adoption by taking an organization design lens to explain the drivers of heterogeneity in the adoption of trust-enabling organizational innovations. By paying careful attention to pre-adoption boundary choices related to permeability and transparency as well as to the technology structure and the material features of the technology, adopters may be able to achieve an architectural alignment, and thereby achieve their goals. This architectural alignment determines the trust model and whether the mode of adoption should follow an actor-centric or a technology-centric logic for trust production, trust distribution, and trust convergence.

REFERENCES AVAILABLE FROM THE AUTHORS

TABLE 1

Typology of Organizational Boundaries

		Boundary Permeability	
		Low	High
Boundary Transparency	High	*(Quadrant II) Permissioned public (hybrid)* Eg. industry-specific blockchains Main goals: Decentralization & scalability	*(Quadrant I) Permissionless public* Eg. Bitcoin, most pre-2015 cryptocurrencies Main goals: Decentralization & autonomy
	Low	*(Quadrant III) Permissioned private* Eg. consortium blockchains Main goals: Scalability & autonomy (with a focus on security)	*(Quadrant IV) Not relevant to blockchain* Eg. Managed ecosystems (Uber, Airbnb) Centralized platforms; not applicable for a glass organization