© *Academy of Management Review*
2024, Vol. 00, No. 00, 1–3.

DIALOGUE

REFRAMING BLOCKCHAIN'S PROMISE: A COMMENTARY ON GREGORY, BECK, HENFRIDSSON, AND YARAGHI'S "COOPERATION AMONG STRANGERS"

Gregory, Beck, Henfridsson, and Yaraghi (2024) present an insightful model that sheds light on how blockchain-based smart contracts can facilitate cooperation among strangers. They conceptualize algorithmic enforcement capability as a continuous construct shaped by distinct technical characteristics, including blockchain infrastructure and smart contract features. This perspective shifts the conversation from asking *whether* blockchains are effective governance mechanisms to investigating *when* they are effective. Specifically, their model helps explain how algorithmic enforcement capability can enhance cooperation among strangers and the associated boundary conditions. Despite the merits of their theorizing, however, this Dialogue highlights four issues that challenge certain aspects of Gregory et al.'s (2024) model, and suggests constructive paths forward in the spirit of cumulative progress.

FROM PROGRAMMED RECIPROCITY TO AUTOMATED RULE ENFORCEMENT

Gregory et al. (2024: 2) argue that what makes blockchain-based smart contracts unique is that they facilitate cooperation through a process they call "programmed reciprocity," defined as "automated instructions for returning good for good (positive reciprocity) and ill for ill (negative reciprocity)." However, it is important to clarify that the principle of programmed reciprocity is not unique to blockchains, as a similar mechanism can also be found in traditional legal contracts. In such contracts, the terms and conditions defining the mutual obligations and expectations between parties are also "programmed"—that is, written according to a set of instructions—albeit in natural language rather than computer code. In our view, however, whether obligations are computer-coded is not the key feature distinguishing smart from traditional contracts. Instead, the real value proposition of blockchain-based smart contracts lies in their superior ability to enforce rules automatically and without reliance on the legal system, thus enabling transparent, automated, and reliable execution of agreed-upon rules without the need for central authority. This novel means of enforcement has previously been discussed elsewhere under the labels "cryptoeconomics" (Werbach, 2018), "blockchain governance" (Lumineau, Wang & Schilke, 2021; Wang, Lumineau & Schilke, 2022), and "lex cryptographica" (de Filippi & Wright, 2018). Understanding the conditions under which blockchain enforcement provides distinct advantages—or creates potential drawbacks—compared to traditional contracts would offer valuable insights for both theory and practice. We encourage future research to develop a comparative framework that systematically contrasts the two mechanisms along relevant dimensions. Specifically, alongside a comparative analysis of transaction costs (see Lumineau et al., 2021), future research could leverage institutional theory (Scott, 2001) to investigate how regulatory, normative, and cognitive pressures may favor or hinder automatic enforcement vis-à-vis traditional contracts. For instance, scholars might study how legal requirements, industry standards, and cultural norms can affect blockchain's implementation.

FROM CONTRACTUAL COMPLEXITY TO CODIFICATION AND VERIFICATION

Gregory et al.'s (2024) focus on "contractual complexity" as a key moderator raises several concerns. Defining this factor as "the number of contingencies and possible outcomes that have to be accounted for in the reciprocal-exchange agreement" (Gregory et al., 2024: 8), the authors argue that complex transactions reduce the positive effect of algorithmic enforcement capability on reciprocity and cooperation. However, this perspective warrants reconsideration, as smart contracts can in fact very effectively accommodate many parameters, such that the sheer number of provisions should not be a major boundary condition. We argue instead that the key consideration is not the *number* of terms but rather the *nature* of those terms—in particular, the extent to which they can be clearly spelled out and transferred into machine-readable language. As such, an analysis of the transaction's codifiability and verifiability (Lumineau et al., 2021) offers a more relevant lens for understanding

Correspondence concerning this article should be directed to Fabrice Lumineau.

Accepted by Dana Minbaeva

the challenges of translating agreements into enforceable smart contracts as key moderators in Gregory et al.'s (2024) model. Future research should develop an operationalization of the codifiability and verifiability of a transaction's terms for empirical testing. Moreover, scholars should also explore how features surrounding the transaction, such as environmental uncertainty, may influence the relationship between automated enforcement and programmed reciprocity, given that blockchain-based smart contracts may be particularly costly to modify.

FROM TECHNOLOGICAL CAPABILITIES TO USER CONFIDENCE

A potential pitfall for future research trying to test Gregory et al.'s (2024) framework lies in the close interrelationship between the model's independent variable (algorithmic enforcement capability) and its second-stage moderator (blockchain confidence). The former focuses on the actual technological capabilities of a blockchain, while the latter concerns users' perceptions of those capabilities. This conceptual proximity calls for a clear justification for treating the two as distinct constructs and theorizing about potential misalignment between them. Unfortunately, Gregory et al. (2024) fail to address what could drive a discrepancy between actual and perceived capabilities, such as a lack of understanding or biased perceptions of the technology. The technology acceptance model (Davis, Bagozzi & Warshaw, 1989) could be particularly useful to investigate the conditions under which even highly sophisticated blockchains may be met with low user confidence. This model's cognitive approach makes it possible to explore how perceived ease of use and perceived usefulness may influence user acceptance. Further, scholars should investigate how developers' reputations impact users' confidence levels (Lumineau, Schilke & Wang, 2023). Moving forward, we suggest that research should aim to identify specific scenarios where high technological capability does not align with user confidence. This could lead to actionable insights for blockchain stakeholders, including developers and regulators, on how to bridge this gap and enhance real-world adoption.

FROM AN ECONOMIC TO A SOCIO-TECHNICAL PERSPECTIVE

Finally, the authors make the questionable claim that "strangers, who lack previous interactions, can therefore not rely on human reciprocity mechanisms of cooperation (direct and indirect reciprocity)" (Gregory et al., 2024: 2). This claim seems to overlook important prior research from sociology (e.g., Buskens, 2002; Cook, Hardin & Levi, 2005; Kuwabara, 2015) showing that indirect reciprocity through reputation systems can be very effective at facilitating cooperation among strangers, as seen in platforms like eBay and ride-sharing services like Uber, where users routinely rely on human reviews and ratings to guide their interactions with unknown counterparts. While the authors argue that blockchain-based smart contracts offer a novel reciprocity mechanism, they fail to situate this argument within the broader landscape of approaches fostering cooperation. Blockchain is certainly a promising mechanism, but it is clearly not the only way to enable cooperation among strangers. Future research should take a more holistic view, examining how blockchain-based solutions interact with and complement traditional human-centric reciprocity mechanisms and enforcement logics (Lumineau et al., 2021), from both an economic and a sociological perspective. For example, drawing on social exchange theory (Emerson, 1976), scholars building on Gregory et al.'s (2024) approach could examine how social mechanisms, including reputation systems, can work in concert with blockchain enforcement to reduce behavior uncertainty and promote trust among strangers.

In conclusion, we commend the work of Gregory et al. (2024) for its valuable contributions toward furthering the understanding of blockchain technology and smart contracts and their implications for cooperation. We contribute to this line of work by proposing four adjustments and extensions to their model that aim to achieve enhanced construct clarity and tighter connections with adjacent literatures.

REFERENCES

Buskens, V. 2002. ***Social networks and trust***. New York: Kluwer Academic Publishers.

Cook, K. S., Hardin, R., & Levi, M. 2005. ***Cooperation without trust?*** New York: Russell Sage Foundation.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. 1989. User acceptance of computer-technology—A comparison of two theoretical models. ***Management Science***, 35: 982–1003.

de Filippi, P. & Wright, A. 2018. ***Blockchain and the law: The rule of code***. Cambridge, MA: Harvard University Press.

Emerson, R. M. 1976. Social exchange theory. ***Annual Review of Sociology***, 2: 335–362.

Gregory, R. W., Beck, R., Henfridsson, O., & Yaraghi, N. 2024. Cooperation among strangers: Algorithmic enforcement of reciprocal exchange with blockchain-based smart contracts. ***Academy of Management Review***, Forthcoming.

Kuwabara, K. 2015. Do reputation systems undermine trust? Divergent effects of enforcement type on generalized trust and trustworthiness. ***American Journal of Sociology***, 120: 1390–1428.

Lumineau, F., Schilke, O., & Wang, W. 2023. Organizational trust in the age of the Fourth Industrial Revolution: Shifts in the form, production, and targets of trust. ***Journal of Management Inquiry***, 32: 21–34.

Lumineau, F., Wang, W., & Schilke, O. 2021. Blockchain governance—A new way of organizing collaborations? ***Organization Science***, 32: 500–521.

Scott, W. R. 2001. ***Institutions and organizations***. Thousand Oaks, CA: Sage.

Wang, W., Lumineau, F., & Schilke, O. 2022. ***Blockchains: Strategic implications for contracting, trust, and organizational design***. New York: Cambridge University Press.

Werbach, K. 2018. ***The blockchain and the new architecture of trust***. Cambridge: MIT Press.

Fabrice Lumineau
University of Hong Kong

Wenqian Wang
Hong Kong Baptist University

Oliver Schilke
University of Arizona

https://doi.org/10.5465/amr.2024.0375

Fabrice Lumineau (lumineau@hku.hk) is a professor in strategic management at HKU Business School, University of Hong Kong. He received his PhD from HEC Paris. His research interests include interorganizational partnerships, the interplay between contracts and trust in collaborative strategies, opportunism and ethical issues, and blockchain governance.

Wenqian Wang (wenqianwang@hkbu.edu.hk) is an assistant professor of strategic management at Hong Kong Baptist University. He received his PhD in strategic management from Purdue University, and another PhD in construction management from Tianjin University. His research mainly focuses on the governance of interorganizational relationships, emphasizing both contractual and relational mechanisms, as well as blockchain governance.

Oliver Schilke (oschilke@arizona.edu) is a professor of management and organizations (tenured) and a professor of sociology (by courtesy) at the University of Arizona, where he also serves as the director of the Center for Trust Studies. He received his PhD from the University of California, Los Angeles. His research interests include collaboration, trust, organizational routines and capabilities, and micro-institutional processes.