Blocked and Chained: Blockchain, Radical Transparency, and Democracy

Darra Hofman
University of British Columbia
Vancouver, BC, Canada V6T 1Z1
darra.hofman@alumni.ubc.ca

Alamir Novin
University of British Columbia
Vancouver, BC, Canada V6T 1Z1
Alamir.novin@ubc.ca

Abstract

Blockchain is frequently claimed to be a democratizing technology. However, its relationship to both law and broader democratic institutions remains uncertain. One claim regarding blockchain's democratic potential is that it is radically transparent and can bring such transparency to existing systems of governance. This paper examines that claim against theories of transparency, and against a specific exercise of transparency, freedom of information. This paper finds that blockchain technology, while useful for transparency, will not meet broader transparency goals without addressing political gatekeepers and legal, social, and cultural needs.

Author Keywords

Blockchain; distributed ledger technology; transparency; freedom of information

ACM Classification Keywords

K.4.1 Public Policy

Introduction

"Code is law." [12] Lessig's central provocation is no less relevant now than when he first published *Code* in 1999. It is centrally significant to the blockchain. Wright and De Filippi claim, "[a]s blockchain technology becomes widely adopted, centralized authorities […]

could lose the ability to control and shape of activities of disparate people through existing means" [21] Others are more skeptical. Atzori refers to a blockchain-based "stateless global society" as "the myth of an egalitarian blockchain-based society." [1] Between these two poles, "[t]he central question is not how to regulate blockchains, but how blockchains regulate. They may supplement, complement, or substitute for legal enforcement." [21]

We argue that blockchain, in and of itself, is neither salve nor poison. Rather, the difference between medicine and poison is dose; the ultimate impact of blockchain will be felt, not just due its innate characteristics, but its application. We take as our example the idea of blockchains as a "transparent" technology. The Tapscotts argue that "through smart contracts…[c]ompanies can program relationships with radical transparency." [16] Blockchain transparency is sought for clinical trials [2], corporate governance [22], and real estate [18]. Even the government of Canada is exploring the use of Ethereum to improve transparency [13]. Blockchain clearly holds a great deal of potential as a technology, but its benefits will be fully realized only if we do not underestimate its potential human, societal, and democratic risks. Can blockchain deliver "transparency" and for whom will be it be transparent?

Transparency and "Treacherous Vocabulary"

Angela Walch, asserts that "[blockchain's] unsettled vocabulary is relevant to how regulators understand, discuss, and ultimately regulate (or not) the technology or its uses." [19] Walch points to a number of factors that contribute to the uncertainty around the meaning of such fundamental blockchain terms as "immutable" and "trustless," including:

- Word taint: shifting terminology to escape bad associations, such as Bitcoin with Silk Road;
- Technology variations: there are many different blockchain technologies with their own characteristics and capabilities;
- Cross-field communications: blockchain technologies are very interdisciplinary, with the communication problems attendant thereto;
- Industry "pivots": vocabulary shifts with marketing; and
- Fixing inaccuracies: debates over the accuracy of terminology (such as "miners") has brought language thought to be more accurate (by some) into the fold (such as "validators"). [19]

Thus, validating claims that blockchain technology is fundamentally "transparent" requires examining exactly what is meant by transparent, and in what context. The assertion that blockchain is inherently transparent is based on a few characteristics of the technology:

- The ledger, at least in the permissionless blockchains, is accessible to any and all nodes;
- The ledger is (theoretically) immutable, with full, automatic, timestamped audit trails of every transaction; and
- The disintermediation of the blockchain means that there is (theoretically) no human or institutional intervention in transactions on the chain.

Even if one takes these claims as *prima facie* true, however, that does not necessarily make the case that blockchain is "transparent," at least not in the democratic sense. In part, this is due to the fact that "transparency" itself is "treacherous vocabulary," subject to the same broad invocations and interdisciplinary uncertainty as "trustless." Indeed, "transparency" was unsettled long before Nakamoto's white paper. Transparency works at different levels, with different theoretical assumptions depending upon the role that it is playing. Thus, in the organizational management literature, transparency is understood in relation to organizational theory; in the literatures of administrative law, political science, and archival theory, transparency is understood in relation to democratic theory. Almost all of the models, however, encompass human factors – understanding, trust, benevolence, and learning, for example – that point to transparency being a problem as much social as technological in its dimensions.

Schnackenberg and Tomlinson define transparency as "the perceived quality of intentionally shared information from a sender," and relate it to trust. [15]

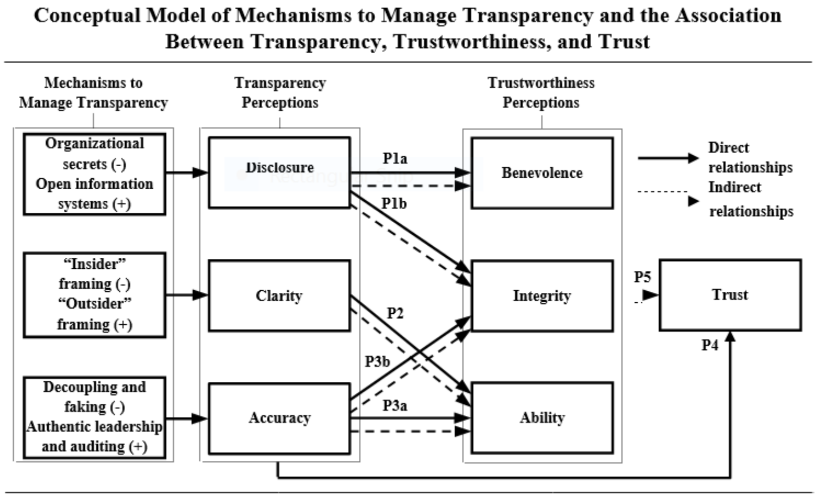
Conceptual Model of Mechanisms to Manage Transparency and the Association Between Transparency, Trustworthiness, and Trust
Mechanisms to Manage Transparency
Transparency Perceptions
Trustworthiness Perceptions
Organizational secrets (-) Open information systems (+)
"Insider" framing (-) "Outsider" framing (+)
Decoupling and faking (-) Authentic leadership and auditing (+)
Disclosure
Clarity
Accuracy
Benevolence
Integrity
Ability
Trust
P1a
P1b
P2
P3b
P3a
P4
P5
Direct relationships
Indirect relationships

Figure 1: "Conceptual Model of Mechanisms to Manage Transparency and the Association Between Transparency, Trustworthiness, and Trust" [15]

Writing in the tradition of organizational management, Schnackenberg and Tomlinson focus on stakeholder trust and organizational trustworthiness – concepts that nonetheless play a significant role in transparency as a construct in democratic theory.

Also writing in organization management, Bernstein claims that "the logic of transparency is fundamentally based on the premise that more – and more accurate – awareness of others improves learning and control and therefore improves performance, as shown by the positive (+) relationships in Figure 2 [3]. However, in considering the effect of transparency on the observed, and not just the observer, Bernstein develops a model of transparency and privacy that captures a desire for privacy triggered by the awareness of others watching. Records professionals believe this fear could trigger "empty archives" due to people refusing to produce records that could be used to hold them accountable [6]:

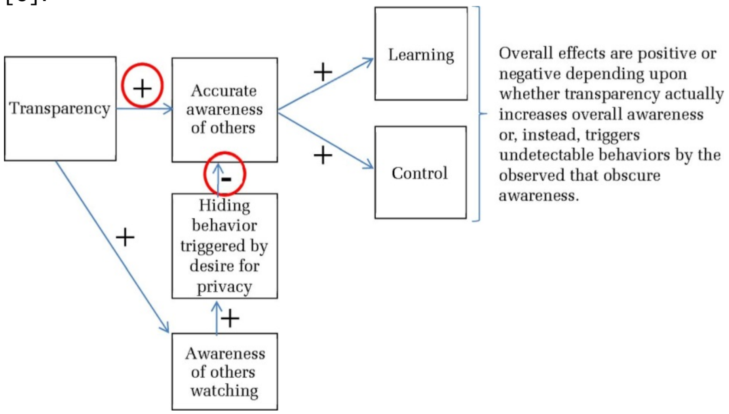
Transparency
+
Accurate awareness of others
+
+
Learning
Control
Overall effects are positive or negative depending upon whether transparency actually increases overall awareness or, instead, triggers undetectable behaviors by the observed that obscure awareness.
-
Hiding behavior triggered by desire for privacy
+
+
Awareness of others watching

Figure 2: "Behavioral Update to Figure 1, Linking Transparency with Privacy" [3]

Vacarro theorizes transparency with regards to the ethical concerns of business organizations' adoption of Information and Communication Technologies (ICTs).

[17] Vacarro's model is meant to provide a means to "frame the main ethical problems arising from the adoption and use of ICT for [business organizations'] activities". [17] Less apparent from the above model is that it is meant to be both an internal and external (two-level) model. [17] Despite the seeming simplicity of Vacarro's model, he posits that transparency encompasses "dynamic social processes [imbued with] the complexity, interdependence, and dynamism of the individual, collective, and social variables involved in such processes." [17]

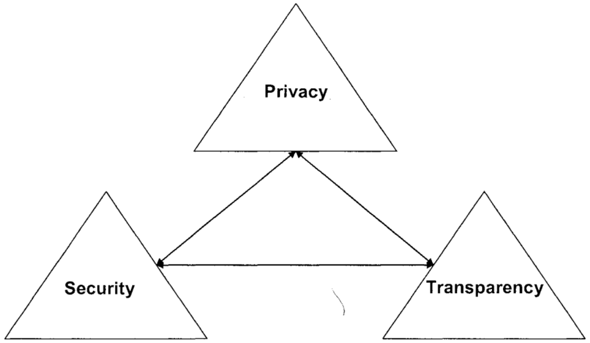

Figure 3: "The Three Dimensions of the Model" [17]

Janssen and van den Hoven's model, below, attempts to capture the complexity and interrelatedness of transparency in the context of Big Open Linked Data (BOLD) for e-government purposes. [8]

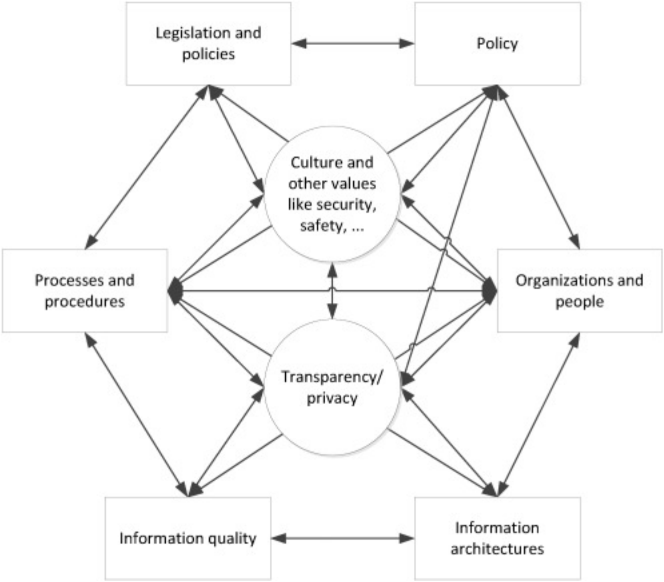

Figure 4: "Elements and dependencies comprising transparency and privacy landscape." [8]

As Fenster notes, a number of assumptions from democratic theory are embedded in models such as Janssen and van den Hoven's, which assume *a priori* that "[t]ransparency and privacy are considered as important societal and democratic values that are needed to inform citizens and let them participate in democratic processes." [5] Their model also highlights the central role of law (both legal instruments, and policy) in our understandings of transparency.

When blockchain technologies are put forth as "transparent" technologies, the focus is upon their technical transparency. As the foregoing shows, however, even the simplest models of "transparency" as a democratic value highlight dynamic, humanoriented processes and concepts. Given the contested, legally-, socially- and culturally-situated nature of "transparency," it seems unlikely that any purely technical solution – blockchain included – could provide democratic transparency without reference to and support from law and other governing institutions. As Werbach argues, "the idea that all online communities will successfully enforce their rules, without regard for governments, will fare as poorly as it did [in the early days of the Internet]." [20] The inability of technology, in and of itself, to deliver democratic values can be seen in the Arab Spring and the 2018 Iranian revolution. Technology is only as democratic as legal, social, and cultural forces allow.

Transparency in Action: Blockchain and Freedom of Information (FOI)

So far, this paper has demonstrated that transparency is not just a theoretical concept. It is a grounding cause behind any number of actions on the part of organizations and governments. "[Transparency] operates in the first instance in the humdrum world of administrative laws ('freedom of information' and 'right to know Acts and the like), with its legal and bureaucratic systems that enforce transparency through the mandatory disclosure of government information to citizens." [5] At the heart of this disclosure lies trustworthy records. To be trustworthy, a record must be reliable and authentic. [10] To be reliable, a record must be created by a competent author and have "contents [which] can be trusted as a full and accurate representation of the […] fact to which they attest." [9] Thus, record reliability "is dependent upon the circumstances of [the record's] creation; an unreliable record cannot be made reliable." [7] A record is authentic when "it is the document that it claims to be, [free from] any manipulation, substitution, or falsification." [4]

Blockchain technologies, as ledgers, are fundamentally a recordkeeping technology. However, while their cryptographic immutability is excellent for assuring the authenticity of records, they do nothing to ensure that records are reliable. [10] Blockchain technologies, as currently configured, also fail to preserve the "archival bond," the web of relationships that tie one records to the other records that participate in the same action. [11] Absent the archival bond, it is near impossible to understand the acts and facts of which the records are evidence. Furthermore, without the archival bond, responding to FOI requests – which are often written by lay people, and typically address their request by subject matter, could become more laborious and resource-intensive.

In turn, the increase in labour and resources to fulfill FOI requests, which have both legal and practical deadlines for fulfilment, can create more opacity. Journalists, who often use FOI requests to source needed information, have a professional responsibility to communicate that information in a transparent and timely manner while minimizing harm to vulnerable parties. If a freedom of information officer struggled to locate responsive records in a blockchain-based system – because such systems do not tie records to their context or creators natively – the system would fail to serve the purposes of democratic transparency, because information would not be made available quickly enough for accountability purposes. Blockchain transparency will only be effective as democratic transparency if its role in sociotechnical systems of knowledge and disclosure is understood.

Finally, any blockchain solution for records subject to FOI would have to be both privacy-preserving and accessible. For example, many public records subject to FOI also contain personally identifiable information (PII) that must be protected. Solutions are available, such as the use of off-chain storage or encrypting the data and using zero knowledge proofs. But these solutions come with trade-offs that must be considered against the needs of the system. Off-chain storage systems face the same preservation problems they always have, although the blockchain can provide some authenticity. Zero knowledge proofs are immature. And blockchain can at best improve the human problems of transparency; people can (and will) make errors in data entry, or refuse to make records, thwarting transparency and accountability.

Blockchain and Human Bias

With any new technology, some of the structuralized biases may be difficult to identify immediately. For example, some of the biases of blockchain may lie in the strength of its immutability. As noted *supra,* immutability is one of the features that makes blockchain transparent, however, immutability is valued differently by different communities. For example, the right to erasure ("right to be forgotten"), embedded in both case law and the General Data Protection Regulation (GDPR) in the European Union, is only beginning to be understood vis à vis blockchain technology's immutability, and will undoubtedly evolve as GDPR comes into force. [14] Such a right does not currently exist in Canadian or American law. Managing legally mandated erasure in a solution biased towards immutability requires balancing different concepts of – and purposes for – transparency.

Will a Blockchain Future Be Transparent?

Blockchain technologies have tremendous potential to change how we transact the business of life, including the business of government. However, the capabilities of blockchain alone are not enough to deliver positive social and legal changes. Language such as "transparent" or "democratic," when applied to the blockchain, must be understood in a narrow sense. A true "blockchain revolution" would lie at the confluence of regulatory forces, and must be considered in a careful, interdisciplinary way, with a focus on uncovering the assumptions built into the broad claims about blockchain. "Developing the rules, norms, incentives, and technical architectures [Lessig's four regulatory forces] for a well-functioning community is a very hard problem." [20] Blockchain is but one of those four forces and cannot achieve its potential on its own.

Acknowledgements

Ms. Hofman thanks the Social Sciences and Humanities Research Council (SSHRC), the Izaak Walton Killam Memorial Fund for Advanced Studies, InterPARES Trust, and Blockchain@UBC for their support.

References

1. Marcella Atzori. 2015. Blockchain technology and decentralized governance: Is the state still necessary? Retrieved January 29, 2018, from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713
2. Mehdi Benchoufi, Raphael Porcher, and Philippe Ravaud. 2017. Blockchain protocols in clinical trials: Transparency and traceability of consent. *F1000research* 6:66.
3. Ethan Bernstein. 2017. Making Transparency Transparent: The Evolution of Observation in Management Theory. *Academy of Management Annals* 11(1): 217 – 266.
4. Luciana Duranti. 1995. Reliability and authenticity: the concepts and their implications. *Archivaria* 39: 5 -10.
5. Mark Fenster. 2015. Transparency in search of a theory. *European Journal of Social Theory*18 (2): 150-67.

6. Pekka Henttonen. 2017. Privacy as an archival problem and a solution. *Archival Science* 17(3): 285-303.

7. Darra Hofman, Luciana Duranti, and Elissa How. 2017. Trust in the Balance: Data Protection Laws as Tools for Privacy and Security in the Cloud. *Algorithms* 47(10).

8. Janssen, Marijn, and Jeroen van den Hoven. 2015. Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy? *Government Information Quarterly* 32(4): 363-368.

9. ISO/IEC. 2001. *ISO 15489-1:2001 – Information and Documentation – Records Management – Part I: General.*

10. Victoria Louise Lemieux. 2016. Trusting records: Is blockchain technology the answer? *Records Management Journal* 26 (2): 110-39.

11. Victoria L. Lemieux and Manu Sporny. 2017. Preserving the Archival Bond in Distributed Ledgers: A Data Model and Syntax. In Proceedings of the 26th International Conference on World Wide Web Companion, pp. 1437-1443. International World Wide Web Conferences Steering Committee.

12. Lawrence Lessig. 2006. *Code: Version 2.0*. [2nd]. ed. New York: Basic Books.

13. National Research Council Canada. Exploring blockchain for better business. Blog post. (19 January 2018). Retrieved January 29, 2018, from https://www.nrc-cnrc.gc.ca/eng/stories/2018/blockchains.html.

14. Stan Sater. 2017. Blockchain and the Eureopean Union's General Data Protection Regulation: A Chance to Harmonize International Data Flows. Retrieved March 21, 2018 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080987.

15. Andrew K. Schnackenberg and Edward C. Tomlinson. 2016. Organizational transparency: A new perspective on managing trust in organization-stakeholder relationships. *Journal of Management* 42 (7): 1784-810.

16. Don Tapscott and Alex Tapscott. 2016. *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Portfolio/Penguin, Toronto, Ontario.

17. Antonio Vacarro. 2006. Privacy, security, and transparency: ICT-related ethical perspectives and contrasts in contemporary firms. *Social Inclusion: Societal and Organizational Implications for Information Systems*. Eileen M. Trauth, Debra Howcroft, Tom Butler, Brian Fitzgerald, and Janice I. DeGross (Eds). Springer US, Boston, MA, 245 - 258.

18. Manohar Velpuri. 2017. Joining the blockchain gang. *Land Journal*: 8.

19. Angela Walch. 2016. The Path of the Blockchain Lexicon (and the Law). *Rev. Banking & Fin. L.* 36: 713 – 975.

20. Kevin Werbach. 2017. Trust, But Verify: Why the Blockchain Needs the Law. *Berkeley Technology Law Journal.* Forthcoming. Retrieved January 29, 2018, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2844409.

21. Aaron Wright and Primavera De Filippi. 2015. Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Retrieved January 29, 2018 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

22. David Yermack. 2017. Corporate governance and blockchains. *Review of Finance* 21 (1): 7 - 15.