Blockchain and Privacy

Catherine Tucker
MIT Sloan, MIT, Cambridge, MA, USA

Abstract

The unique value proposition of 'smart contracts' based on blockchain technology is the creation of a permanent public record of agreed-upon transactions that cannot be changed retroactively. Though this is attractive in terms of reducing the potential for fraud, a person entering into a smart contract pre-commits both their current self and their future selves, no matter what changes occur to them or to their circumstances. The advantages of such pre-commitments can be substantial, but even in an age of increasing adoption of distributed ledger technologies, self-reinvention remains important. From a surveillance perspective, it is important to prevent governments from reliably associating a particular cryptoasset transaction with a particular person. For individuals, it is important to preserve the ability to assume new identities both formally and informally. This presentation will present an expanded and refined understanding of what it means for a blockchain use case to "protect privacy," and in particular, how such use cases can encourage a notion of personal identity that is inflexible and matches poorly with individuals' notions regarding their identities. In addition I discuss how privacy regulation may itself shape the development of blockchain.

2012 ACM Subject Classification Security and privacy → Block and stream ciphers

Keywords and phrases Blockchain, Privacy

Digital Object Identifier 10.4230/OASIcs.Tokenomics.2021.12

Category Invited Talk

Acknowledgements I want to thank Alex Marthews for coauthoring the paper with me that inspired this talk.

3rd International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2021).
Editors: Vincent Gramoli, Hanna Halaburda, and Rafael Pass; Article No. 12; pp. 12:1–12:1
OpenAccess Series in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany