

Why untraceable cryptocurrencies are here to stay

November 17 2020



Credit: Melvin Silva from Pexels

According to a new study from Copenhagen Business School, on the role of privacy and decentralization in the cryptocurrency community, developers are creating cryptocurrencies in such a way that regulatory

oversight will not be possible, neither will any wait and see attempt to override them in the future. The research is published in the *Journal of Information Technology*.

"If decentralized privacy-preserving cryptocurrencies become popular in the future, to the point they can be routinely exchanged without users having to convert to other currencies and systems, there is no obvious way for regulators to impose post-hoc regulation," says Associate Professor Rob Gleasure from the Department of Digitalization, Copenhagen Business School.

"What the regulators do not realize is those who control the code will control the rules and so far, they have not accepted this and are in denial," he adds.

Monero cryptocurrency

"People tend to focus on less controversial systems like Bitcoin, Ethereum, Hyperledger, etc. We shine a light on those developing the most potentially disruptive currencies," says co-author Dr. Robin Renwick, a [research analyst](#) from the Applied Research and Innovation team at Trilateral Research.

The [case study](#) concentrated on Monero, seen as the posterchild for this privacy-focused cryptocurrency community. They have been described as anti-establishment and cypherpunk and, according to the U.S. Department of Justice using them is indicative of possible criminal conduct.

The research focused on the privacy attitudes of users, developers, cryptographic researchers, business architects and regulators and adopted a boundary object perspective to make sense of disagreements between these collaborating social worlds.

"What makes this research different is we were able to get [good access](#) to users and developers in a community that is not normally researched," adds Dr. Robin Renwick.

Privacy is personal

"Monero strongly believe the privacy trade-off that allows for our digital transactions to leave an explicit data trail behind it has not been worth it. They argue we went into this digital finance system and have given away all of our data, but we did not actually consent to this."

"Basically this whole system of crime detection has been built on tracking our transactions but Monero argue it won't work anymore as it wasn't fair to start with, so regulators will need to find another way to track crime," says Associate Professor Rob Gleasure.

The research points out that even if regulators tried to ban these privacy-preserving cryptocurrencies, it would be extremely hard to enforce across all jurisdictions—given the decentralized nature of these projects.

They recommend regulators and criminal investigators need to begin planning for the future possibility of exchanges which could ultimately mean identity linkable transaction records may not exist.

The Monero protocol, for example allows users and businesses to remain compliant, but keeps the control of this with the entity that owns the information, ultimately being able to be shared when required by investigative agencies or supervisory bodies, instead of transaction surveillance and monitoring.

"If these cryptocurrency communities have their own financial system which exists separately, and they become impossible to regulate, then it's important to understand and understand this early. Once regulators

accept it, they can then begin developing new methods to compensate," concludes Associate Professor Rob Gleasure.

More information: Robin Renwick et al, Those who control the code control the rules: How different perspectives of privacy are being written into the code of blockchain systems, *Journal of Information Technology* (2020). [DOI: 10.1177/0268396220944406](https://doi.org/10.1177/0268396220944406)

Provided by Copenhagen Business School

Citation: Why untraceable cryptocurrencies are here to stay (2020, November 17) retrieved 16 April 2024 from <https://techxplore.com/news/2020-11-untraceable-cryptocurrencies.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.