Towards having your privacy and security and exchanging crypto too

May 23 2022, by Daniel Tkacik

Credit: CyLab

Privacy, security, and control of those things are paramount in the world of cryptocurrencies.

"The whole cryptocurrency decentralized business is about giving control of the digital coins to you," says Aravinda Thyagarajan, a postdoctoral researcher in the Computer Science Department advised by CyLab's Elaine Shi. "You should control your coins, and you don't want to leak any information about them."

This week, Thyagarajan will be presenting a new paper outlining a new protocol towards better privacy and security protections when swapping cryptocurrencies. The paper, "Universal Atomic Swaps: Secure Exchange of Coins Across All Blockchains," is being presented at the 2022 IEEE Symposium on Security and Privacy.

Right now, if two people or entities want to swap one cryptocurrency for another—say, one Bitcoin for one Ethereum—they can swap directly between themselves, but there's always a chance one of the two parties will be dishonest and not hold up their end of the deal. Another option, then, is to have a third-party exchange service mediate the deal. But what if the exchange service is an adversary and steals both parties' coins?

"In the wild west of cryptocurrency, no one should be trusted," says Thyagarajan.

There's also an issue of privacy. If an e-commerce website only accepts one specific cryptocurrency, and you only have coins in a different cryptocurrency, you must perform an exchange into the compatible currency before purchasing from the website. That exchange can reveal sensitive information.

"You lose a bit of your privacy," says Thyagarajan. "Using sophisticated mechanisms, people can learn to some probability information about your assets."

Thyagarajan's paper outlines a protocol that addresses these security and

privacy concerns. First, the protocol is universal—it allows for exchanges across all current and future cryptocurrencies. Second, the swap protocol ensures that the swap will happen honestly or it won't happen at all, meaning no one will maliciously lose coins, without relying on third parties. And lastly, the protocol supports the exchange of multiple types of coins—e.g. Bitcoin, Ethereum, Dogecoin, etc.—in a single swap.

"With this protocol, you can shop on that e-commerce website using a coin that is not the coin that they accept, and keep your privacy," says Thyagarajan. "You're able to do that because you're not relying on third-party services, and also because it doesn't rely on any special features of the underlying currency."

All of this requires an enormous amount of computing power, Thyagarajan says, so one currently can't do this on a laptop or phone, presenting an opportunity for future work. However, for major currencies currently, like Bitcoin, Ethereum, etc., Thyagarajan's paper presents an efficient solution for the exchange that can be run now even on low-end devices.

More information: Sri AravindaKrishnan Thyagarajan et al, Universal Atomic Swaps: Secure Exchange of Coins Across All Blockchains (2022). eprint.iacr.org/2021/1612.pdf

Provided by Carnegie Mellon University