New system makes it harder to track Bitcoin transactions

8 February 2017

Researchers from North Carolina State University, Boston University and George Mason University have developed a Bitcoin-compatible system that could make it significantly more difficult for observers to identify or track the parties involved in any given Bitcoin transaction.

Bitcoin was initially conceived as a way for people to exchange money anonymously. But then it was discovered that anyone could track all Bitcoin transactions and often identify the parties involved.

Bitcoin operates by giving each user a unique public key, which is a string of numbers. Users can transmit money in the form of digital bitcoins from one public key to another. This is made possible by a system that ensures a user has enough bitcoins in his or her account to make the transfer. The use of the public keys gave users a sense of anonymity, even though all of the transactions were visible on the public Bitcoin blockchain which lists all transactions. Over time, experts and private companies have developed highly effective methods of de-anonymizing those public keys.

Now researchers have developed a system called TumbleBit, which is a computer protocol that runs on top of Bitcoin.

TumbleBit takes advantage of an existing concept called "mixing service." The idea works like this: instead of Party A paying Party B directly, many different Parties A pay an intermdiary "tumbler," which then pays the Parties B. The more parties are involved, the harder it is to determine which Party A paid which Party B.

"However, this still has a security flaw," says Alessandra Scafuro, an assistant professor of computer science at NC State and co-author of a paper describing TumbleBit. "Namely, if an outside observer can compromise the tumbler, it could figure out who was paying whom."

To address this, TumbleBit takes a three-phased approach.

In the first phase, called escrow, the Parties A notify the tumbler that they would like to make a payment, and the Parties B notify the tumbler that they would like to be paid. This is all done on the public blockchain.

For the second phase, the researchers have put cryptographic tools into place that allow the tumbler to pay the correct parties without actually knowing which parties are involved. Phase two does not appear on the blockchain.

In the third phase, called cashout, all of the transactions are conducted simultaneously, making it more difficult to identify which parties are involved in any specific transaction. Phase three does appear in the public blockchain.

"We tested TumbleBit with 800 Bitcoin users, and found that the second phase only took seconds to complete," Scafuro says.

"One limitation of TumbleBit is that, right now, the system is designed to work with a fixed denomination - so paying amounts larger than that denomination require making multiple payments," Scafuro says. "That's something we're working on."

The paper, "TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub," will be presented at the Network and Distributed System Security Symposium, being held Feb. 26 to March 1 in San Diego, Calif.

More information: "TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub," DOI: 10.14722/ndss.2017.23086

Provided by North Carolina State University