Probing Bitcoins

January 16 2014

Sarah Meiklejohn is the lead author of "A Handful of Bitcoins."

(Phys.org) —Bitcoin transactions may be anonymous, but they're also completely transparent. This makes stealing easier, but cashing in on the theft without getting caught a lot more difficult. That's one of the findings from "A Fistful of Bitcoins," a computer science paper that takes an in-depth look at how the virtual currency has been used since its introduction back in early 2009. Led by computer science Ph.D. student

Sarah Meiklejohn, researchers documented more than 16 million transactions and more than 12 million public keys-the addresses Bitcoin users use for their transactions-as of April 13, 2013.

"Once you do something with that currency, we can learn more and more about who you are and who you interact with," said Kirill Levchenko, a research scientist in the Department of Computer Science and Engineering at the Jacobs School and one of the paper's co-authors.

Levchenko, who earned his computer science Ph.D. from UC San Diego in 2008, suggested that Meiklejohn look into Bitcoin. "It's a very unique phenomenon-a purely digital currency, not backed by any government," he said.

Contrary to popular belief, Bitcoin is not used mainly for commerce. Most users either play games, such as Satoshi Dice, with the currency, or engage in some form of currency speculation by moving Bitcoin from mining pools where it is created to exchanges where it can be converted to dollars, Levchenko said.

Researchers further refined their analysis and were able to trace back a large number of public keys to specific clusters-for example, 1.6 million public keys were connected to the underground marketplace Silk Road, the public currency exchange and marketplace Mt. Gox and a few other services. Undergraduate student Marjori Pomarole created a visualization of the Bitcoin user network, including vendors, gambling services, mining pools that create the currency, fixed-rate exchanges that process transactions, wallets where the currency is stored and investment schemes (see graphics on this page). The visualization underscores the importance of gambling services in the Bitcoin network. In addition to analyzing the network, researchers conducted 344 transactions of their own, purchasing everything from silver quarters, to coffee, to a calculator and a used CD.

This one-year expedition through the Bitcoin network was quite the experience for Meiklejohn, whose specialty is actually cryptography. "It's a different world," she said. "If someone steals your funds, you can see where they're going."

This, in the end, is what makes the Bitcoin network less than ideal to launder money, the researchers pointed out. Even when criminals use sophisticated methods to conceal their tracks, such as slowly peeling away small amounts of money over a long period of time from an address, they still can be tracked.

While working on the paper, Meiklejohn found herself engaged in a fairly unusual activity for a computer science Ph.D. student. Two of her co-authors are Stefan Savage and Geoffrey Voelker, computer science professors who sometimes work with investigative blogger Brian Krebs, a former Washington Post reporter. Russian hackers planned to mail heroin purchased via the Silk Road to Krebs' house to frame him.

Meiklejohn helped Krebs confirm that the hacker had actually bought the drugs before Krebs alerted the FBI. "The hacker posted, publicly, a Bitcoin address on a forum," she told KPBS. Since then, Meiklejohn has helped reporters from various news organizations understand the Bitcoin network. The media attention took her by surprise, but was welcome. "A lot of the reporters I worked with raised a lot of good questions," she said.

More information: Read the complete paper: cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf

Provided by University of California - San Diego