Students aim to enhance crypto-currency transparency

February 3 2015, by Thomas Deane

Students at Trinity College Dublin are "looking under the Bitcoin bonnet" in an attempt to make the crypto-currency more transparent. Increasing the transparency should reduce the risk of fraud while maintaining sufficient anonymity to make it appealing to a wide range of legitimate businesses.

They believe one research avenue that could afford this happy compromise is a Bitcoin 'credit-check' database, in which potential business partners could scope each other out.

The open-source currency, which can be used to pay for goods and services, is attractive because it is not regulated by governments or banks. However, a certain degree of regulation might be a good thing, if only to reduce the risk of fraudulent business practices or money laundering taking place behind Bitcoin's closed doors.

To minimise such risks, a research-led Trinity team of staff and students determined that a 'Bitcoin regulator' would want to know three main things: 1) How much currency is in circulation, 2) how it was distributed and whether anyone was stockpiling it, and 3) whether there were any patterns in the transactions that people should be concerned about.

Professor of Computer Science in the School of Computer Science and Statistics at Trinity, Donal O'Mahony, is overseeing the team's investigations. He said: "We wanted to develop systems that would give a 'regulator' a degree of visibility on the flows of bitcoin in the same way that central banks have this visibility over normal currencies."

It turns out that for all Bitcoin's reputed anonymity, looking under the bonnet is not that difficult - Bitcoin's system is much like that used by Swiss Numbered Bank Accounts. The difference is that every time someone makes a transfer from one numbered Bitcoin account to another, it gets written into a giant ledger that is open for the world to see. Using this giant ledger (called the 'Bitcoin Blockchain'), Professor O'Mahony's students were able to trawl through every bitcoin transaction to date to look for patterns.

While studying at Trinity as a Masters student, Cian Burns initially looked to find out how much each person was holding in currency and to ascertain how much was in each account. There are many millions of accounts but probably far fewer owners, as any one person can hold several bitcoin accounts.

Using a variety of helper websites and by auto-trawling the blockchain on his personal laptop for 24 hours a day, he built a database of all accounts before he set about linking them together to try to understand how some were connected. Once someone goes public with a bitcoin address – say in an email asking for payment – all related addresses can be found to help paint a picture of their activity over time.

Burns said: "The big benefit of such a picture is that if an address is involved in fraudulent activity, tracing related addresses could protect other users from further fraud. Our trawl gave us a unique insight into some very high-profile Bitcoin fraud cases that were being conducted across the world. Regulation is further down the line, but a database of accounts could certainly protect people and raise the appeal of Bitcoin for legitimate businesses."

The projects are continuing this year with many possible new directions.

One might be the creation of an online database that could be used to perform a 'Bitcoin credit-check' on someone you are about to do business with; another might involve linking Bitcoin users to geographical locations, to keep an eye on inter-country bitcoin movements that might indicate nefarious intentions.

Professor Mahony concluded: "You can be sure that like the Skibbereen Eagle of old, Trinity College and its students will be keeping a close eye on Bitcoin from now on."

Provided by Trinity College Dublin

Citation: Students aim to enhance crypto-currency transparency (2015, February 3) retrieved 27 April 2024 from https://phys.org/news/2015-02-students-aim-crypto-currency-transparency.html