Bitcoin lets users avoid censorship

December 1 2014

In his graduation research, computer science student Krzysztof Okupski has developed software to encrypt messages with the Bitcoin network. Using his software, it costs around 50 cents to send an A4 page of text. This easily accessible and low-cost method can provide an attractive option for dissidents to avoid censorship, so they can send messages unhindered across national borders. Okupski graduates on 1 December.

Bitcoin is a virtual currency that can be used at increasing numbers of places to make online payments. In fact Bitcoins are unique pieces of code that are calculated by computers. The basic principle is that the system has no central organization or regulators to control the currency. At present the exchange rate of the currently fluctuates around 300 euros

for one Bitcoin.

Okupski has developed two programs: one that posts messages and another to read them. If you want to post a message, the first program converts the text into Bitcoin transactions. The underlying principle is similar to the idea that a succession of payments are transferred to someone, and you have agreed with them that one euro represents an A, two euros represent a B etc. The recipient can then 'see' which word the sender meant to transmit, using the received amounts.

Many options

But in Okupski's case, the way the method works is a lot smarter. "The program that posts the messages creates a million Bitcoin accounts, free of charge, after which money is transferred backwards and forwards between those accounts", explains Boris Skoric, TU/e researcher and supervisor of Okupski. "The number of different accounts, and the fact that you can divide an amount of money into multiple parts, offers a lot of options. The currency itself is extremely small; one Bitcoin consists of 100 million 'Satoshi', and all amounts are expressed in Satoshi. The program that posts the messages converts them into a chain of transactions, and sends them out into the Bitcoin network."

Identifier

Because all Bitcoin transactions are public, the second program is able to convert the chain of transactions back to text. All that's needed is an 'identifier', through which the program knows where it has to start 'reading' the transaction. The principle is similar to tuning an antenna to the right frequency. The only charges involved are the administration costs that have to paid to the Bitcoin network for each transaction. These are around 50 cents for an A4 page of text. There are no real costs to be

paid because senders simply recirculate money within their own accounts.

Anonymous

This method allows uses to avoid censorship, because anyone with an internet connection can use Bitcoin. In other words, no government that allows citizens to use Bitcoin can censor messages that are posted in the transaction chain anywhere else in the world. Only the sender is traceable. "Even if only your account number is known by the Bitcoin network, it's still possible in theory – using the IP address – to trace the owner of an account", says Skoric. "But the readers of messages are always totally anonymous."

Provided by Eindhoven University of Technology