Bitcoin-based scams

Jean-Loup Richet

Abstract:
Bitcoin is again drawing scrutiny –media from all over the world titled in February 2015 about "a tremendous fraud with bitcoins". In wake associated with this scandal, Hong Kong's central bank informed customers against acquiring virtual currencies. However, we argue that Mycoin scandal has nothing to do with Bitcoin. It is just a bitcoin-based scam that could have been done with any other crypto, digital or physical currency.

Keywords:
Bitcoin, Mycoin, Ponzi scheme, scam, Hong Kong, currency exchange.

***

Last summer, local Chinese investors took a trip to Hong Kong for a bitcoin event financed by Mycoin, the Hong Kong company that just all of a sudden closed shop, getting an approximated $390 million along with it.

Today, in February 2015, Mycoin's business office is vacant, a managing director has supposedly transferred the firm's financial assets to an Uk Virgin Islands account before leaving, and increasingly more people say that in spite of promoting itself as a hub for currency exchange, Mycoin in fact had no bitcoin at all.

Bitcoin is again drawing scrutiny, and in wake associated with this scandal, Hong Kong's central bank informed customers against acquiring virtual currencies.

However, this has nothing to do with Bitcoin at all: MyCoin was basically running a Ponzi scheme based on Bitcoins.

This generates negative publicity for this cryptocurrency and contributes to its poor notoriety: nearly anonymous (Reid & Harrigan, 2013), risky and insecure (Moore and Christin, 2013; Eyal and Sirer, 2014).

In 2012, the bitcoin trading platform Mt.Gox froze records of users who possessed bitcoins that could be directly related to theft and fraud (Moser, Bohme, & Breuker, 2013). In spite of this, scamming people with bitcoin hasn't ceased at all: it even turn out to be a remarkably lucrative business for cybercriminals (Richet, 2013; Tropina, 2014).

In their empirical study of Bitcoin-based scams, Vasek and Moore (2015) identify 192 scams and classify them into four groups: Ponzi schemes, mining scams, scam wallets and fraudulent exchanges. In 21% of the cases, they found the associated Bitcoin addresses, which enables them to track money into and out of the scams. They find that at least $11 million has been contributed to the scams from 13 000 distinct victims. Indeed, the most successful scams depend on large contributions from a very small number of victims...

References:

Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography and Data Security* (pp. 436-454). Springer Berlin Heidelberg.

Moore, T., & Christin, N. (2013). Beware the middleman: Empirical analysis of bitcoin-exchange risk. In *Financial Cryptography and Data Security* (pp. 25-33). Springer Berlin Heidelberg.

Moser, M., Bohme, R., & Breuker, D. (2013, September). An inquiry into money laundering tools in the Bitcoin ecosystem. In e*Crime Researchers Summit* (eCRS), 2013 (pp. 1-14). IEEE.

Reid, F., & Harrigan, M. (2013). *An analysis of anonymity in the bitcoin system* (pp. 197-223). Springer New York.

Richet, J. L. (2013). Laundering Money Online: a review of cybercriminals methods. *arXiv preprint arXiv:1310.2368*.

Tropina, T. (2014, June). Fighting money laundering in the age of online banking, virtual currencies and internet gambling. In *ERA Forum* (Vol. 15, No. 1, pp. 69-84). Springer Berlin Heidelberg.

Vasek, M., & Moore, T. (2015) There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. *Financial Cryptography and Data Security 2015 Conference*.

***

Blog post from https://blogs.law.harvard.edu/jeanlouprichet/