Researchers investigate how conflicting interests threaten to negatively impact the Bitcoin ecosystem

April 9 2015, by Stephanie Koons

Bitcoin, a peer-to peer online payment system that was conceived in 2008, has experienced considerable growth in popularity and increasingly has been adopted as a viable payment scheme in mainstream electronic commerce. Now researchers — including Jens Grossklags, an assistant professor at Penn State's College of Information Sciences and Technology — are working to provide guidelines for ensuring that the currency remains long-term viable and trustworthy. Credit: Penn State

Bitcoin, a peer-to peer online payment system that was conceived in 2008, has experienced considerable growth in popularity and has increasingly been adopted as a viable payment scheme in mainstream electronic commerce. However, according to researchers, the decentralized and quasi-anonymous nature of Bitcoin renders it vulnerable to self-interested parties that seek to exploit the system.

"There's still a lot of uncertainty about the stability of the currency," said Jens Grossklags, an assistant professor at Penn State's College of Information Sciences and Technology (IST).

Grossklags, along with Benjamin Johnson, a researcher at the University of California, Berkeley, and Aron Laszka, a research scholar at Vanderbilt University, are investigating how conflicting interests threaten to negatively impact the Bitcoin ecosystem. The overall goal of their research is to provide guidelines for ensuring that the currency remains long-term viable and trustworthy. They presented the results of their study in their paper, "When Bitcoin Mining Pools Run Dry: A Game-Theoretic Analysis of the Long-Term Impact of Attacks Between Mining Pools."

"Healthy competition is normal," Grossklags said. "However, we want to avoid down the road that distributed denial of service (DDoS) attacks or other adversarial events are disrupting the overall Bitcoin economy."

Published in 2008 and released as open-source software in 2009 by Satoshi Nakamoto, Bitcoin is a cryptocurrency system that is controlled through an online communication protocol and facilitated in a decentralized fashion. Transactions are verified by network nodes and recorded in a public distributed ledger called the block chain. The ledger uses its own unit of account, also called bitcoin. The system works

without a central repository or single administrator, which has led the U.S. Department of the Treasury to categorize it as a decentralized virtual currency. While most stakeholders have jointly benefited from the growing importance of Bitcoin, according to Grossklags, Johnson and Laszka, misaligned incentives may undermine the stability of the system.

"In particular, incentives to derive short-term profits from attacks on mining pools threaten the long-term viability of Bitcoin," they wrote in their paper.

Bitcoins are created as a reward for payment processing work in which users offer their computing power to verify and record payments into the public ledger. This activity is called mining and is rewarded by transaction fees and newly created bitcoins.

The process of mining new bitcoins is organized in the form of a race in which the miner that solves a proof-of-work task first will be rewarded; all other miners will leave empty-handed. Individual miners have found it beneficial to join forces in the form of mining pools, as averaging mining proceeds across many participants makes earnings more predictable. In fact, a miner working alone may not win any race in a reasonable amount of time.

The specific setup of each mining pool, according to Grossklags, Johnson and Laszka, typically differs across several dimensions which can be tangible (e.g., related to the computing and communication infrastructure) or intangible (such as reputation or details of the payout schemes). The researchers term the sum of these factors the "attractiveness" of a mining pool.

However, the rules governing how Bitcoin operates as a currency leave room for cheats to destabilize the system.

First, attackers may abuse the resources of unsuspecting computer users for mining purposes through security compromises.

Second, attackers may attempt to redirect or siphon off mining capabilities from a competing pool.

Third, attackers may diminish the mining power of competing pools through DDoS attacks or by exploiting weaknesses in the implementation of the procedure/software used by a particular pool.

"Botnets, which are networks of infected machines, can be put in play and could give one or another mining pool some advantage over the other," Grossklags said. "Such malicious attacks may be conducted to increase the earnings of one pool."

In their paper, the researchers developed a game-theoretic model that allowed them to capture short-term as well as long-term impacts of attacks against mining pools. Game theory is a way to mathematically calculate how individuals might choose to cooperate, compete or cheat given the options available to them and the strategies of others. Using this model, they studied the conditions under which the mining pools have no incentives to launch attacks against each other (i.e., peaceful equilibria), and the conditions under which one mining pool is marginalized by attacks (i.e,, one-sided attack equilibria).

"It is better for everyone involved that the equilibrium is peaceful," Johnson said. "If one of the pools doesn't get too big or attractive, then it is more likely that all the miners productively work for the system."

According to the researchers, evidence from the Bitcoin mining community has shown that the size of mining pools appears to be related to the probability of being targeted by an attack. The observations indicated that larger mining pools were more frequent victims of attacks.

Building on those findings, Grossklags and his colleagues investigated the adversarial interaction between two representative mining pools that can choose between productive and destructive investments (i.e. computing power vs. DDoS attack on its competitor).

They found that in particular the relative size of the mining pools is a critical factor for the incentives to engage in attacks. This insight complements what is a well-known threat to the viability of Bitcoin. A mining pool controlling 51 percent of all bitcoin mining power could tamper with the block chain to do things like spend bitcoins twice.

"People are most worried about the economic side of the currency," Johnson said. "If you have one entity that controls more than 50 percent of the currency, this can prevent others from mining for it.

"As a pool gets larger and larger, then the economic incentives actually point towards the other pools attacking it," he added. "The upside is that if the pools are attacking each other, it mitigates the possibility of one pool growing too big."

The research helps to understand how complex incentives impact the stability of Bitcoin mining, Grossklags said. The results imply that, in order to achieve a peaceful equilibrium, Bitcoin needs a proactive and informed user population to balance the objectives of short-term and long-term success. Aiming for mining dominance threatens to destabilize the economy well before any pool reaches the critical threshold of 51 percent.

While Bitcoin has achieved undeniable success in the past several years, Grossklags and Johnson said, it remains to be seen whether the virtual currency will ever achieve the same legitimacy as credit cards or paper money. The international aspect of Bitcoin adds further complications, Grossklags said, since "malicious actors may be outside the

jurisprudence of the U.S." and could be difficult to prosecute.

"Our study provides findings that are chipping away at the space of uncertainty surrounding Bitcoin mining," Grossklags said. "Hopefully, our work will contribute to making this currency system more viable in the future."

Grossklags and Johnson presented their research on Bitcoin at the 2015 International Conference on Financial Cryptography and Data Security that was held in late January in San Juan, Puerto Rico.

More information: fc15.ifca.ai/

Provided by Pennsylvania State University