Bitcoin more vulnerable to attack than expected

April 23 2018, by Joost Bruysters

Calculations by University of Twente researchers show that Bitcoin is more vulnerable to attack than people had always assumed. If some Bitcoin users were to form a group that controls 20 percent of the currency's computing power, they could launch an attack and, within a few days, force all other users to accept a new standard for Bitcoin. The researchers presented their results last week, at a scientific conference organized by NASA in the United States.

The Bitcoin network uses blockchain technology. All individual transactions (blocks) are linked to each other, forming a chain that any user can check. Within the Bitcoin network, agreements have been made about how exactly these transactions are linked together.

The Bitcoin world is currently divided into various camps. One camp wants to maintain the current standard. Other camps advocate modifications to enable more transactions to be carried out in a shorter period of time, for example. The current protocol imposes a hard upper limit on the size of individual blocks, which means this global system can process no more than seven transactions per second. Many people feel this limitation makes the network far too slow. It certainly does not bear comparison with the number of transactions that credit card companies can process in a second.

Changes to the Bitcoin protocol can only be implemented if they are accepted by the majority of users. However, calculations by University of Twente researchers show that – provided it holds 20 percent of the

'mining power' – a limited group could use an 'Andresen attack' to implement a new protocol within a few days, and force all other users to adopt it. Ansgar Fehnker, one of the researchers involved, compares it to a situation in which 20 percent of a company's shareholders are able to impose their view on the great majority. As a result of the attack, all transactions carried out in the preceding hours would be annulled, with retroactive effect. This, in turn, would seriously undermine confidence in the current standard.

More information: Fehnker A., Chaudhary K. (2018) Twenty Percent and a Few Days – Optimising a Bitcoin Majority Attack. In: Dutle A., Muñoz C., Narkawicz A. (eds) NASA Formal Methods. NFM 2018. Lecture Notes in Computer Science, vol 10811. Springer, Cham

Provided by University of Twente