New cryptocurrency introduces new risks

June 17 2016, by Bill Steele

In the fundraising prospectus for a new business there will always be a disclaimer saying that "any investment carries some risk." That's also true if you're investing digital money.

A recently created venture capital fund that exists only online and deals only in digital currency has a flawed structure that leaves it open to manipulation, according to Emin Gun Sirer, associate professor of computer science.

Sirer and two colleagues have called for the fund, known as "The DAO," to stop doing business until the problems are fixed. Their arguments are presented in a paper circulated to the cryptocurrency community by Sirer, Seattle software developer Dino Mark and DAO curator Vlad Zamfir.

The DAO works with an online currency system called Ethereum, or ether for short, created as a replacement for bitcoins. As with bitcoins, ether currency is created online and given value by computer operators who contribute electricity and computer time to process it. The goal of such "cryptocurrency" has been to have a monetary system that is not controlled by banks or governments. Records are distributed across the internet, owned by the users of the system and protected from interference by redundancy.

The Etherium system allows for the creation of Distributed Autonomous Organizations ("The DAO co-opted the acromym," Sirer explained) whose rules of operation are laid out in a computer program known as a smart contract. The DAO operates with no management; it is purely user-directed, in accordance with its contract.

Like a real-world venture capital fund, The DAO gathers money from investors and invests in startups – mostly, so far, software development projects. It seeks to draw on the "wisdom of crowds" to choose its projects by having the investors vote on each proposal.

At last count The DAO had raised about $150 million, about 15 percent of all the ether in existence.

The glitch, the new paper points out, is in the voting rules. A member who has voted yes or no on a proposal may not withdraw from the fund until voting is finished. So a voter who thinks a proposal is bad and will lose money is still discouraged from voting no, instead waiting for the last minute to see how the voting is going. This could allow an unscrupulous person to throw in a lot of yes votes at the very end to support a self-serving proposal.

Sirer and his colleagues also found ways in which the smart contract program could be hacked, such as tying up funds and demanding a ransom.

So far, Sirer said, the warning has resulted in a "de facto moratorium" on the fund's operations.

"Changes will have to be made, within the provisions of the existing smart contract program, to ensure that the smart contract captures the wisdom of the crowds" Sirer explained. "Or else, whom do you sue if you can't vote because of a bug on line 37?"

Provided by Cornell University

Citation: New cryptocurrency introduces new risks (2016, June 17) retrieved 6 May 2024 from https://phys.org/news/2016-06-cryptocurrency.html