www.wired.com /2016/06/50-million-hack-just-showed-dao-human/

A $50 Million Hack Just Showed That the DAO Was All Too Human

Klint Finley ⋮ 7-8 minutes ⋮ 6/18/2016

Sometime in the wee hours Friday, a thief made off with $50 million of virtual currency.

The victims are investors in a strange fund called the DAO, or Decentralized Autonomous Organization, who poured more than $150 million of a bitcoin-style currency called Ether into the project.

The people who created the DAO saw it as a decentralized investment fund. Instead of leaving decisions to a few partners, anyone who invested would have a say in which companies to fund. The more you contributed, the more weight your vote carried. And the distributed structure meant no one could run off with the money.

That was the plan, anyway.

The DAO is built on Ethereum, a system designed for building decentralized applications. Its creators hoped to prove you can build a more democratic financial institution, one without centralized control or human fallibility. Instead, the DAO led to a heist that raises philosophical questions about the viability of such systems. Code was supposed to eliminate the need to trust humans. But humans, it turns out, are tough to take out of the equation.

A Never-Ending ATM

DAO developers and Ethereum enthusiasts are trying to figure out how they might reverse the theft. The good news is that time is on their side. The thief transferred the stolen funds into a clone of the DAO that likely includes code that, as in the original system, delays payouts for a few weeks.

Stephan Tual, the COO of Slock.it, the company that built the DAO, says the thief probably never expected to be able to spend the ether. Each unit of ether is unique and traceable. If the hacker tries to sell any of the stolen ether in a cryptocurrency market, the system will flag it.

"It's like stealing the Mona Lisa," he says. "Great, congratulations, but what do you do with it? You can't sell it, it's too big to be sold."

The DAO is a piece of software known as a "smart contract"--essentially an agreement that enforces itself via code rather than courts. But like all software, smart contracts do exactly what their makers program them to do—and sometimes those programs have unintended consequences.

It's not clear yet exactly how the hack worked, says Andrew Miller, a PhD student at the University of Maryland who studies smart contracts and helped audit Ethereum's code last year. But he says the attacker probably exploited a programming mistake that's exceedingly common in smart contracts.

Let's say you have $50 in the bank and you want to withdraw that from an ATM. You insert your card, punch in your PIN number and then request that $50. Before the machine spits out the cash it will check your balance. Once it spits out the cash, it will debit $50 from that balance. Then the machine asks you if you'd like to process another transaction. You tap "yes" and try to take $50 again. But the ATM sees that your balance is now $0 and refuses. It asks you again if you want to process another transaction, so this time you say "no." Your session ends.

Now imagine that the ATM didn't record your new balance until you ended the session. You could keep requesting $50 again and again until you finally told the machine you didn't want to process any more transactions—or the machine ran out of money.

The DAO hacker was probably able to run a transaction that automatically repeated itself over and over again before the system checked the balance, Miller says. That would allow anyone to pull far more money out of the fund than they put in.

The programming language that Ethereum developers use to write smart contracts, Solidity, makes it really easy to make this sort of mistake, says Emin Gun Sirer, a Cornell University computer scientist who co-authored a paper earlier this year pointing out a number of potential pitfalls in the DAO's design. Others have previously spotted places in the DAO code that would have made such a theft possible. Sirer says the DAO developers have tried to be vigilant about preventing such flaws, but because it's such an easy mistake to make, it's not surprising that instances of the bug escaped notice.

All Too Human

As bad as the bug was, Sirer still thinks that both the DAO and Ethereum are worthwhile experiments. The DAO helped raise awareness of the idea of smart contracts, which Sirer thinks will eventually become extremely important to how the world conducts transactions. The project has also called attention to some of the biggest technical challenges.

"This is a rite of passage for the project," he says.

The Ethereum team is now debating how, and whether, to refund the stolen funds. Ethereum works much like Bitcoin does: the system records each transaction in a global ledger that resides on every Ethereum user's computer. The Ethereum team could release a new version of the software that tweaks this ledger to essentially reverse all of the DAO heist transactions. If enough people installed this version, it would be like the hack never happened. That's exactly what many people in the community, including Ethereum creator Vitalik Buterin and the Slock.it team would like to see happen.

"Fourteen percent of all ether is in the DAO," Tual says. "No one wants to see this fail."

But others think that reversing the transactions could have a damaging effect on people's perceptions of ether an cryptocurrencies in general.

Alex Van de Sande, a user experience designer who has contributed to several Ethereum-related projects, and who put money into the DAO, says he believes other ways exist to retrieve the missing funds. Because the thief transferred the pilfered ether into a clone of the DAO, de Sande points out, it may well have the exact same security vulnerability as the original. Developers could just steal the ether back.

The idea behind Ethereum, much like Bitcoin, was to create a computer system that facilitated transactions using the immutable rules of mathematics. The code would eliminate the need to trust anyone. If people can simply reverse transactions they didn't mean to make, it proves that people, not mathematics are really in charge of the system, de Sande says. If the code did something people didn't mean it to do, then people will have to live the consequences.

The fact that a fork is being discussed at all proves that despite the Ethereum team's best efforts, machines will always be subject to the messy politics of the human world. But that also might end up saving the project. The heist has divided people and exposed the inevitability of human weakness. But it's also bringing people together to fix things. Humanity is making that possible, not mathematics.