The Ether Thief

BY MATTHEW LEISING

JUNE 13, 2017

A year ago a hacker stole $55 million of a virtual currency known as ether. This is the story of the bold attempt to rewrite that history.

SUMMER COLDS ARE the worst, and Emin Gün Sirer had caught a wicked bug from his 1-year-old son. So it was with watering eyes and a stuffy nose that the associate professor of computer science at Cornell found himself working from his sickbed on Monday, June 13, 2016. Gün—everyone calls him Gün—couldn't tear himself away from his laptop. He had another type of bug in his sights, a flaw in a line of computer code he feared put $250 million at risk of being stolen.

It wasn't just any code. It was the guts of the newest breakthrough in software design related to blockchain, the novel combination of decentralized computing and cryptography that gave life to the virtual currency bitcoin in 2009. Since then, the promise of blockchain to transform industries from finance to health care has captured imaginations in corporate boardrooms and governments alike. Yet

what the Turkish-born professor was exploring that Monday was the next leap forward from bitcoin, what's known as the ethereum blockchain.

Rather than moving bitcoin from one user to another, the ethereum blockchain hosts fully functioning computer programs called smart contracts—essentially agreements that enforce themselves by means of code rather than courts. That means they can automate the life cycle of bond payments, say, or ensure that pharmaceutical companies can authenticate the sources of their drugs. Yet smart contracts are also new and mostly untested. Like all software, they are only as reliable as their coding—and Gün was pretty sure he'd found a big problem.

In an email sent to one of his graduate students, Philip Daian, at 7:30 p.m., Gün noted that the smart contract he was looking at might have a problem—on line 666. (They say the devil is in the details.) Gün feared the bug could allow a hacker to make unlimited ATM-like withdrawals from the

This staggering amount of money lived inside a program called a decentralized autonomous organization, or DAO. Dreamed up less than a year earlier and governed by a smart contract, the DAO was intended to democratize how ethereum

projects are funded. Thousands of dreamers and schemers and developers who populate the cutting edge of computer science, most of them young, had invested in the DAO. This was real money, a quarter of a billion dollars, their money, meant to build a better version of the world, and every cent was at risk.

Gün, who wears his dark hair short and looks a decade younger than his 45 years, had already been tracking and publicizing flaws in the DAO's design. A few weeks earlier, on May 27, along with two colleagues, he'd urged investors to stop buying into the DAO until security issues could be fixed. It had been too late, however, and the program went live the next day. Smart contracts such as the DAO are built to be entirely reliant on their code once released on the ethereum blockchain. That meant the DAO code couldn't be fixed. Other blockchain experts—including Peter Vessenes, co-founder of the Bitcoin Foundation—had also pointed out security flaws in the smart contract, but Gün

appears to be the first to pinpoint the flaw that put the money in jeopardy. The problem was the code was so new that no one knew what to expect—or even if there was actually a problem in the first place.

Gün had his doubts, too. This wasn't even his job. He does this for fun. Daian didn't think they'd found anything either. Over email, he said, "We might be up the creek ;)." Later, when Gün pointed to the error in line 666, Daian replied, "Don't think so."

Gün says,"We don't sound the alarm bell every time we find a bug that seems suspicious." Instead, he went to bed to try to kill his cold—the one bug he knew to be real. "I was too miserable to sort it out," he says.

Four days later, Christoph Jentzsch lay on the floor of his home office, taking deep breaths, trying not to panic.

It was Friday morning, and software developers all over the Western world were waking up to the

news that the DAO, which Jentzsch had created, was being attacked. Gün had been right.

Jentzsch, who has dark hair and a perpetual five o'clock shadow, lives with his family in the Mittweida region of Germany, a rural spot not far from the Czech border. Mornings in the Jentzsch household are a whirlwind as he and his wife get their five children—age 2 to 9—fed and off to school. Yet today, after his brother Simon woke him with a call that the DAO was being hacked, Jentzsch had to ignore his familial duties. "You've got the kids," he told his wife. "I have an emergency."

THIS IS THE story of one of the largest digital heists in history. And while you may have heard last

year that hackers breached Swift, the bank-to-bank messaging system, and stole $81 million from Bangladesh's central bank, the DAO attack is in a different category altogether. It played out in front of anyone who cared to watch and couldn't be stopped. Just as the global WannaCry ransomware attack in May laid bare weaknesses in computer operating systems, the DAO hack exposed the early frailties of smart-contract security and left many in the community shaken because they hadn't found the bug in time. The aftermath would eventually pit good hackers against bad ones—the white hats vs. the black hats—in the strange and futuristic-sounding DAO Wars.

The roots of the DAO belong to an idea Jentzsch borrowed from another internet-fueled phenomenon: crowdfunding. The 32-year-old Jentzsch, a theoretical physicist by training, and a few colleagues started Slock.it in 2015. As they considered how to fund the company, Jentzsch approached it as many had—sell a digital currency,

effectively a token, to raise cash. But why should each new startup have to program its own initial coin offering? Jentzsch wondered. What if one huge fund ruled them all?

He introduced his idea to the world at DevCon 1 in London in November 2015. “What is the blockchain way of creating a company?” Jentzsch asked his audience. “Of course, it has to be a DAO.” It would work like this: Ether, a virtual currency like bitcoin, would be used to fund and develop applications on the ethereum blockchain—things such as making a music app similar to iTunes or a ride-sharing service along the lines of Uber. Investors would buy DAO tokens with their ether; the tokens would allow them to vote to fund projects they liked. If the app they backed made money, the token holder shared in the profit.

In the six months he spent creating the DAO, Jentzsch thought it would raise $5 million. From April 30 to May 28, the DAO crowdfunding pulled in $150 million. That’s when ether traded just below

$12. As the price of ether rose in the following weeks to $20.75 the day before the attack, so too did the value of the DAO, putting a $250 million target on this thing Jentzsch had unknowingly brought into the world with a fatal, original sin.

"Our hope was it would be the center of a decentralized sharing economy," says Jentzsch, who now regrets not capping the amount raised. "For such a big experiment, it was way too early." In the weeks after the attack, Jentzsch and the rest of the ethereum community would come to grips with

But why would anyone invest in the DAO in the first place? It has something to do with the strain of digital libertarianism at the heart of the ethereum community, much like the set of beliefs that led to the birth of bitcoin. Think of bitcoin as the first global currency whose use can't be stopped by governments or corporations; on top of that, bitcoin is almost impossible to hack. Ethereum, then, is another level beyond. It's an uncensorable global computer. As amazing and unprecedented as that is, it's also a bit terrifying. Brought to life, the DAO ended up staggering off the table and turning on the community that wanted it so badly.

Accustomed to working into the night to stay in touch with colleagues in North America, Jentzsch blows off steam by jogging or kayaking on the nearby Zschopau River. Yet on that Friday morning, he had the more pressing task of pulling himself up off the floor and dealing with the attack. “I went into emergency mode: Don’t try to save the DAO,” he says. “No, it’s over.”

IT WAS FAR from over.

Several hours later and half a world away from the Jentzsch household in Mittweida, Alex Van de Sande was waking up in his apartment in the Copacabana neighborhood of Rio de Janeiro. The baby-faced ethereum developer had been born in the small fishing village of Santa Cruz Cabrália in

the Bahia region of Brazil and moved with his parents to Rio when he was about 3 years old. These days he's known as "avsa" on Reddit and Twitter. After reaching for his phone to see why it was blowing up with Skype messages, he turned to his wife and said, "Remember when I was telling you about that huge unhackable pile of money?" She nodded. "It's been hacked," he told her.

His first thought was to get his DAO tokens out. He owned about 100,000 of them, valued at about $15,000 at the time. He's the lead designer of the Ethereum Wallet app, a program that allows him and anyone else to interact with the blockchain. Van de Sande scrambled to log in to it, but his password didn't work. It was glitching, and as he worked to fix it, his panic subsided. He realized he shouldn't be bailing on the DAO but trying to save it. And to do that, he needed Griff.

Griff Green, who's worked variously as a massage therapist in Los Angeles and a community organizer in Seattle, is one of only a handful of