Blockchain technology is supposed to make the financial world more secure. However, two cases have recently surfaced featuring stars of the fintech sector based in Zug, revealing the insecure side of the technology.

In the virtual and extensively uncontrolled Bitcoin world, hacks and robberies are nothing unusual. But two cases are now causing even hard-nosed defenders of virtual currencies and transactions to feel nervous.

Because they affect two of the sector’s leading lights, whose firms enjoy worldwide status: Shapeshift, led by Erik Voorhees, and Vitalik Buterin’s Ethereum.

Fast, Secure

Voorhees, originally from the U.S., and the Russian Buterin count among the most influential
figures and advocates of bitcoin and blockchain. They have chosen to base their companies and promote their technologies in Switzerland in the bitcoin cluster region of Zug.

Voorhees founded Shapeshift in 2014. The company sells itself as the fastest and most secure exchange platform for cryptocurrencies.

Buterin is the whizkid of the blockchain scene. Through Ethereum he runs a platform on which users can carry out virtual money transactions using blockchain technology.

The 22-year-old programming genius has gained the trust of many in his quest to revolutionize the financial world.

$50 million Vanishes

But at the moment he has other things on his mind: Buterin is trying to get back $50 million that were stolen from him. It is one of the greatest robberies to have occurred in the brief but rapidly evolving history of cryptocurrencies – and it has hit, of all people, the young guru of the sector.

What’s worse, the theft took place in the framework of a project called Dao, a virtual investment vehicle, that puts money – real and converted cash – virtually collected by investors into companies. The whole project operates on the basis of blockchain technology, which is viewed as absolutely secure.

Manipulating Blockchain

The thief found a gap in the programme and over several days in June, managed to channel off $50 million of the collected $160 million. The thief, who goes by the name Attacker, got in contact on Buterin’s blog, claiming he had done nothing wrong, he did not hack any program, just diverted the money. The code programmed by Buterin’s team allowed this to happen.

The theft creates a dilemma for Buterin: It would be easy for him to get the money back; all he would have to do is reset the program. But his hands are tied, because if he were to tamper with the program, he would then provide proof that blockchain can be manipulated, thus negating its main selling point.

Inside Job

A much lower sum of money is involved in the Shapeshift case, $230,000. But the theft, whose
circumstances have been described by Voorhees in exhaustive detail on the Shapeshift blog, is creating just as much concern in the Bitcoin scene because it was an inside job.

An employee first stole some $130,000, then sold the information about the security loophole to a hacker who went on to steal $100,000 in cryptocurrency.

**Insufficient Security**

The significance of this case is not to be underestimated, as it has shown that in contrast to all assumptions up to now, neither the programs nor the technology behind them are secure. The Shapeshift software, over which currencies can be publicly exchanged, was cracked with inside knowledge, which reveals gaps in Shapeshift’s security capacity.

And the Dao case shows that even a blockchain mastermind like Buterin can work mistakes into his own programs without realizing it.

**Vulnerable Financial System**

How Buterin will solve the problem remains to be seen. His team have just under a week to work out a solution, until the program triggers the deblocking of the $50 million and the thief can disappear with the money.

For Voorhees, the solution was clear. He is building a new Shapeshift platform. But the protagonists of the revolutionized financial world cannot afford to make mistakes like this again. They came forward to overtake the old and vulnerable financial system. Now they are examples of how vulnerable a totally digital system can be.