FINANCIAL TIMES

September 12, 2016 6:01 am

Cyber attacks raise questions about blockchain security

Hannah Kuchler

A close-up on an abstract design of a display, which is warning about a cyber attack

A series of cyber attacks against digital currencies has left the financial services industry wondering whether new blockchain technology can be made secure enough from criminals.

From established names such as UBS and Santander to new fintech companies Ripple and R3, many in the industry are eager to rip out old systems of moving money and replace them with quicker and cheaper blockchain technology. Developed as a technology to underpinning digital currency bitcoin, blockchain allows transactions to be verified electronically over a network of computers, with no central ledger.

However, cyber criminals have targeted companies using blockchain and digital currencies, attacking DAO and Bitfinex in recent months. The DAO was a kind of crowdsourced venture capital fund that allowed people to make investments using Ether, another digital currency. It had raised over $150m in May, only to have more than 50M drained by cyber criminals in June, cutting the value of the currency by a third. Bitfinex, a Hong Kong-based digital currency exchange, lost about $65m in a cyber attack in August.

Fred Ehrsam, co-founder of Coinbase, a San Francisco-based start-up where merchants and traders can buy and sell digital currency, says blockchain will become more secure with time.

“I think at the beginning you’ll have people who screw up with it. It is true of any new technology, people have to get used to it,” he says.

Even before these attacks, the Financial Stability Oversight Council, a group of US regulators, warned that because these systems, known generically as distributed ledgers, were new, flaws might not become clear until they were “deployed at scale”.

“Like most new technologies, distributed ledger systems also pose certain risks and uncertainties which market participant and financial regulators will need to monitor,” the Council said.

One of the most serious problems is that some cryptocurrency companies rely on new programming code. It is hard to anticipate what the flaws are in new code or a new programming language, as there has not been a history of specialists examining it for flaws.

Stefan Thomas, chief technology officer of San Francisco-based Ripple, which is creating its own blockchain-like network for banks, says. “There’s no history of how to write secure code,” he says. “It is not surprising that it would be easy to miss typical problems.”

Another problem is how to store cryptocurrencies. Some companies keep digital cash like a modern bank — with many accounts’ money mixing in one great pot — and others keep it locked up in individual encrypted packets, much like an old-fashioned security box. The best practice is to avoid using “hot wallets”, connected to the internet, and instead use “cold storage” on servers that are not online and are more difficult to hack without physical access to the server. Following the attack, Bitfinex said it had moved funds to the disconnected servers, as well as taking other security precautions. Coinbase keeps 98 per cent of its bitcoin in “cold storage” and has insurance to cover the value of the rest, Mr Ehrsam says.

Experts are divided over whether the public nature of blockchain helps or hinders security. Mr Thomas argues that a public network, which is constantly tested and examined, is better than the “security by obscurity” that features in the current banking system. Security comes from few people understanding how it works, but if someone does figure it out they can find vulnerabilities, Mr Thomas says, as did the cyber criminals who diverted $81m from the Bangladesh Central Bank in the Swift attack earlier this year.

IBM is creating a blockchain where all participants are verified but — as it can scale to millions of people — this gives the added security of more eyes watching each transaction, argues Arvind Krishna, senior vice-president, IBM Research. “Since everybody has to agree to the transaction it is a lot more secure than what we have today, where all you have to do is get in to one computer,” he says.

Ripple and R3, a London-based fintech start-up, are both looking to take the best of blockchain and build it in a private sphere, catering to large financial institutions. This allows them to adapt the security of the network. For example, Ripple adds the ability to freeze funds — a “sort of backstop that allows us to react to attacks”, Mr Thomas says.

Richard Gendal Brown, chief technology officer at R3, says the start-up was building a blockchain-style distributed ledger but only for regulated financial institutions, where everyone identifies themselves with keys on the network. Authentication — proving you are who you are — is a struggle for every network, from online banking apps to Facebook, but R3 tries to address it by limiting the spread of information about transactions.

“We took a very different design choice and said, ‘we are not a gossip network where we send data to everyone’. We have a more traditional architecture point-to-point messaging, sending information only to those who need to validate the transaction,” Mr Gendal Brown says.

At Coinbase, Mr Ehrsam remains optimistic that, in the long run, blockchain will create a more transparent system in which it is far easier to see if money is being stolen and people can learn from others’ mistakes. At the moment it often takes retailers months to realise that they are all being hit by similar cyber attacks to steal credit card details. A blockchain system would show up such patterns much more quickly. “While it may seem scarier in the earlier days, I think ultimately the blockchain creates a safer world,” he says.

RELATED TOPICS Blockchain, UBS AG, Cyber Security, Fintech

Share Author alerts Print Clip Comments