Blockchain Links to Cybercrime have been Overplayed

Jeremy Barnett

Summary

Jeremy Barnett is one of a number of contributors to a recent article where a number of Legal experts have dismissed claims that crypto-currencies and blockchains coupled with reliance on "creaking technology systems" are enabling cybercrime within the banking industry.

In a recent article written by **Jimmy Nichols in PaymentsCompliance,** a number of contributors have commented on a paper from consultancy firm PricewaterhouseCoopers (PwC) and the Centre for the Study of Financial Innovation (CSFI), a research body which flagged anxiety around crime as the second greatest threat to the sector, above regulation and just behind the state of the macro-economic recovery.

Click here to download the full article which is reproduced below.

David Lascelles, senior fellow at the CSFI and co-author of the report, told **PaymentsCompliance** that rising fears around crime were overwhelmingly linked to online crime, with banks having more experience of combating older threats such as tax evasion and money laundering.

"This is the first year that anybody has actually reported crypto-currencies as a particular threat," he noted.

"The whole cyber area is not well understood, that is what makes people frightened."

North America was also ahead of the Far East Pacific and Europe in emphasising the criminal risk to banking, perhaps because of the strength of the US recovery and the wave of large breaches against American firms in the past few years.

However, regulatory expert Jeremy Barnett, a barrister at [Gough Square Chambers], told PaymentsCompliance that the risks of blockchains were significantly less than those presented by automated trading platforms, particularly "blind pools" managed by financial institutions.

He said that the automated tools give "an advantage to institutions over individuals and creating the risk of severe pricing swings which creates uncertainty".

Blockchain uncertainty

According to Lascelles, the survey reflected "uncertainty" around crypto-currencies and blockchains "because nobody really understands how they will work".

Ashley Dowson, chairman of the Sepa Consultancy in the UK, told the survey he foresaw "potential for even greater threats as financial institutions experiment with new technologies [such as] crypto-currencies, distributed ledgers, and real-time payments and settlement".

Much of the concern around corporate blockchain use has focused on the development of in-house crypto-currencies such as Citigroup's Citicoin or Goldman Sachs' SETLcoin, or other internal blockchain technologies.

"The advantage of blockchain is that the community accredits the integrity of the transaction," Barnett said. "Most banks or institutions however are looking at running their own private blockchains which do not have the benefit of transparency.

"The risk in my view is that these blockchains will appear to be 'safer than existing cloud based or legacy systems' but will in fact be more likely to have inherent weaknesses, as each owner seeks to design his or her own requirements or specifications."

Although some banks are developing their own blockchains in-house, others such as JPMorgan, Barclays and UBS are supporting the start-up R3, an invitation-only, industry-wide effort to create a private blockchain run between financial groups.

UBS is also working with Ethereum, a blockchain start-up which specialises in open source technology, the inner workings of which can be viewed by anybody.

The wide array of attempts to harness blockchains led fintech expert Adrian Shedden, a senior associate at the law firm Burges Salmon, to claim it was "too soon" to say what danger cyber-crime posed to banks experimenting with these new blockchain-based technologies.

"There are so many iterations of these technologies, without there being one industry standard operating within a clearly defined regulatory framework, that it is not possible to generalise the threat of criminality or quantify its severity as each iteration will have its strengths and weaknesses," he told PaymentsCompliance.

However, he was hopeful that with the large number of financial institutions backing R3, as well as interest from the Bank of England and the UK's Financial Conduct Authority, industry standards would soon be properly defined.

Human risk factor

Many of the risks around the blockchain involve technical matters; however, fears around crypto-currency use can have a greater human element.

For instance, if a given crypto-currency is not taken up, early adopters can be left holding tokens that have little or no value, or might even be incapable of being redeemed or used to purchase something.

Like physical currency, crypto-currencies can also be vulnerable to theft, as has been proven with the jailing of a US Secret Service agent this week for the theft of $820,000 (£546,000) worth of bitcoin while investigating the Silk Road online marketplace.

"While there is a full and accurate record available for investigators to later piece together what has happened, there is nothing to stop a fraudulent wallet provider or exchange stealing the tokens," Barnett said.

Put another way, although a pound coin is unlikely to be counterfeited, that does not prevent a genuine article being stolen.

Although there are concerns around new technologies, the lawyers PaymentsCompliance spoke to emphasised that these risks may be overblown, particularly when compared with the use of legacy IT to run banks.

"The nature of the criminal threat has shifted away from the era in which the legacy systems were designed and which could not anticipate the evolution of the criminal threat, meaning that the legacy systems are struggling to keep up," Shedden said.

"And it is the new technologies that are being designed with the new nature of the criminal threat in mind that will be able to deal with the threat more efficiently."