INTERNAL AUDITOR

Banks and Bitcoin

A financial giant's recent foray into digital coin could mean increased cryptocurrency use — and its accompanying risks — in commercial banking.

Neil Hodge

March 29, 2019

Some 10 years ago Bitcoin became the world's first cryptocurrency, but mass adoption of it and other digital currencies has been hampered by price volatility and a general reluctance by investors, financial institutions, and regulators to get behind the technology. Barriers include lack of understanding about how the cryptocurrency works, as well as a trading process that can be opaque and subject to abuse — namely through hacking, market manipulation, and potential fraud.

That may be changing, however. In February JPMorgan Chase launched "JPM Coin," the first cryptocurrency created by a major U.S. bank. It will be used to settle payments between clients, and the lender will then work to transfer cross-border payments or corporate debt issuance services to the blockchain. The technology will facilitate near-instantaneous settlement of these money transfers and will, according to the bank, mitigate counterparty risk.

The move represents a dramatic change of attitude: Just a few years ago JPMorgan CEO Jamie Dimon called bitcoin a "fraud" and even threatened to fire employees who traded in it. Other banks, including HSBC, State Street, Credit Suisse, and Barclays, have either used blockchain and cryptocurrencies (albeit tentatively) or are planning to do so.

Yet within a month of JPMorgan's announcement, the Basel Committee on Banking Supervision, comprising the governors of 10 key central banks, released a warning about cryptocurrencies. In a statement it said that "while the crypto-asset market remains small relative to that of the global financial system … the continued growth of

crypto-asset trading platforms and new financial products related to crypto-assets has the potential to raise financial stability concerns and increase risks faced by banks."

The committee said that crypto-assets "do not reliably provide the standard functions of money and are unsafe to rely on as a medium of exchange or store of value," adding that crypto-assets are not legal tender and are not backed by any government or public authority. Furthermore, the Basel Committee cited crypto-assets' history of volatility and lack of standardization and pointed to numerous risks it presents to banks, including liquidity risk, credit risk, market risk, operational risk, money laundering and terrorist financing risk, and legal and reputation risks.

Nonetheless, the committee accepts that banks may still want to participate in the crypto-market. As such, if a bank decides to acquire crypto-asset exposures or provide related services, it should adopt certain measures as a minimum — and internal auditors may want to take note.

Crypto-risks

First, adequate due diligence is a must, the committee says. A bank "should ensure that it has the relevant and requisite technical expertise to adequately assess the risks stemming from crypto-assets."

Second, a bank's risk management framework for crypto-assets should be fully integrated into the overall risk management processes, including those related to anti-money laundering, combating the financing of terrorism and the evasion of sanctions, and heightened fraud monitoring. Furthermore, boards and senior management should be provided with timely and relevant information related to the bank's crypto-asset risk profile.

Third, a bank should publicly disclose any material crypto-asset exposures or related services as part of its regular financial disclosures. It should also specify the accounting treatment for such exposures, consistent with domestic laws and regulations.

Finally, the bank should inform its supervisory authority of actual and planned crypto-asset exposure or activity in a timely manner. Moreover, it should provide assurance that it has fully assessed the permissibility of the activity and the risks associated with the intended exposures and services, and explain how it has mitigated these risks.

Daniel Wolfe, managing director at specialized research and investment group Simoleon Long-Term Value in London, says there are four key areas of risk that internal auditors should be aware of. The first is secure storage. "Crypto assets are secured by a private access key, but it is important that this key – essentially, a long

list of letters and numbers — is kept safe, and that it is not just known to one person and held on one laptop."

In February QuadrigaCX gained worldwide media attention due to the unique circumstances surrounding its failure. After the death of its CEO Gerald Cotton, the collapsed exchange no longer had access to his laptop, which contained the keys for over US$100 million worth of customers' funds. And while the company's external auditor has since cracked the code, it found the funds had been transferred out of customers' crypto wallets in April 2018. The company's directors are still in the process of trying to pay off creditors, and many have accused QuadrigaCX of suspicious activity or at least extreme negligence. "It is safer to separate the assets across several private keys so that if a hack does occur or if a laptop goes missing, not all of the cryptocurrencies will be stolen or lost," says Wolfe.

Another key risk that internal auditors need to be aware of, Wolfe says, is the poor governance and lack of adequate controls around cryptocurrency exchanges. "The people behind the technology are more intent on making the trading a possibility rather than focusing on whether the exchange meets the same regulatory standards and levels of assurance as you'd find in a normal exchange," he explains. "Some don't even have basic 'know your customer' controls, for example, raising concerns about money-laundering. As such, the levels of governance, monitoring, and internal control are much poorer in a lot of crypto-currency exchanges."

Wolfe also warns that internal auditors should pay close attention to how crypto-assets are handled on the balance sheet. He points to the lack of standardization on cryptocurrency profit and loss treatment as a potential area of concern when reporting organizational value for tax purposes, particularly in light of current volatility.

Indeed, the volatility around cryptocurrencies is a major risk in itself, Wolfe says. During the space of a year, the total worth of the cryptocurrency market fell to $139.7 billion by December last year — a drop of more than 80 percent compared to a $819 billion market cap in January 2018. "Cryptocurrencies will remain volatile for some years yet, so banks need to question how much of these types of assets they want to hold and for how long," Wolfe says. "Catastrophic losses may seem a remote possibility, but they remain a possibility nonetheless. For example, if Bitcoin was hacked, confidence in the cryptocurrency could collapse overnight."

Lack of Harmony

Jay Gomez, senior associate in the financial services team at Gibraltar-based law firm Triay & Triay, says that internal auditors need to be aware that there is no agreed international standard regarding cryptocurrency regulation, oversight, or risk. "Some

jurisdictions take a very tough line on cryptocurrencies, such as the U.S., while others might be more pragmatic," he says. "Regulatory approaches and views differ from one market to the next, so this may impact how banks might want to provide cryptocurrency services in those jurisdictions."

Gomez also warns that the technology and the development of the cryptocurrency market is outpacing the development of effective regulation. Regulators struggle to keep up with rapid changes, he notes, potentially resulting in cryptocurrency risks that either might not be identified or may be underestimated and not controlled adequately by regulators or industry participants. As a result, Gomez suggests that "banks that want to dip their toes into the cryptocurrency market should keep an open dialogue with regulators about what the banks are doing, and how the regulator may react to developments."

Comment on or "Subscribe" to this article.

Neil Hodge is a freelance journalist based in Nottingham, U.K.