QuadrigaCX and the dangers of cold storage

MICAH MARCUS, CHRISTOPHER RILEY | BUSINESS INSIGHTS | FEB 19, 2019

A cryptocurrency exchange is an ideal target for cyberattack. Should an attacker gain access to an exchange's reserves, the thief would gain control over a large sum of diversified cryptocurrencies, perfect for conducting anonymized transactions across the internet. As a result, the operators of these exchanges have faced increasingly complex cybersecurity attacks from bad actors against these reserves. In an effort to thwart these attempts, some exchange operators have turned to cold cryptocurrency wallets, isolating the exchange's reserves in off-line data storage centers outside the reach of potential cyberattacks. While this method does prevent any and all online-based attacks against the reserve, it is by no means foolproof and can cause significant issues absent practical business policies and legal protections.

Take, for example, the Canadian exchange QuadrigaCX, or QCX. The founder of QCX, Gerald Cotten, retained the majority of the exchange's assets in a cold storage reserve via an off-line, password-protected laptop. In December, however, Mr. Cotten died unexpectedly, along with the password laptop holding the QCX cold storage reserve. Thus, when Mr. Cotten died, access to the cold storage reserve died with him. At the time of his death, the QCX reserve held approximately 26,000 Bitcoin, 11,000 bitcoin cash, 200,000 Litecoin, over 400,000 Ether, and an assortment of other cryptocurrencies. Without access to these assets, QCX did not have sufficient cryptocurrencies to meet its customers' demands, and the Company shutdown its trading platform. Ultimately, QCX filed for an order of creditor protection under the Canadian law and may yet begin the full bankruptcy process, as continued efforts to access the reserve have failed.

Now, QCX customers, who have a total of approximately $190 million in aggregate stored with the Company, do not know if or when they will ever have access to their assets. The Company continues to attempt to unwind this knot, but given the diversified cryptocurrencies held in the QCX reserve, even the most drastic of attempts to salvage the situation may not work. If, for example, the reserve held only one form of cryptocurrency, it may be possible to initiate a fork on that cryptocurrency's network, which is to rewrite the code and blockchain governing the network to transfer the lost cryptocurrency to its rightful owners. These forks, however, require the support of the majority of the members of the cryptocurrency network at issue and can be quite contentious. Immutability and independent operations are underlying core foundations of most blockchain networks. Changing a network's code via a fork runs counter to that ethos, and networks will generally implement a fork only in the most extreme circumstances. Additionally, the QCX reserve did not store one type of cryptocurrency; it stored dozens. To fully restore its reserve, the Company would have to convince the majority of the members of dozens of cryptocurrencies to initiate forks solely to correct a QCX error, a doubtful proposition.

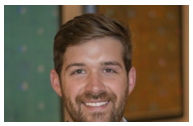
Ultimately, these assets may be lost forever solely as a result of one company's misstep. After all, QCX made the decision to structure the company such that Mr. Cotten "took sole responsibility for the handling of funds" for the Company such that "no one other than him can access the coins in the cold wallets."[1] Had the Company established typical corporate protections, including an emergency succession plan for its key employees and standard cybersecurity password protections policies, QCX could have secured access to the reserve and avoided this issue entirely. Instead, QCX will serve as an unfortunate reminder of the dangers of operating without proper business structure, a small condolence to customers scrambling to recover their assets.

As more exchanges enter the market, users would be wise to conduct diligence on the cybersecurity and redundancy protections offered by their exchange of choice, an effort which may mean the difference between retaining control over your assets and suffering the same fate as the QCX users. If you need any guidance in conducting this type of diligence or to learn how your business can avoid suffering a similar fate, please contact a McDonald Hopkins attorney to see how we can help you and your business best make use of and grow with developing technologies.

[1] Message from QuadrigaCX dated February 5, 2019, available at **https://www.quadrigacx.com/**

MICAH MARCUS

Read More



CHRISTOPHER RILEY

Read More