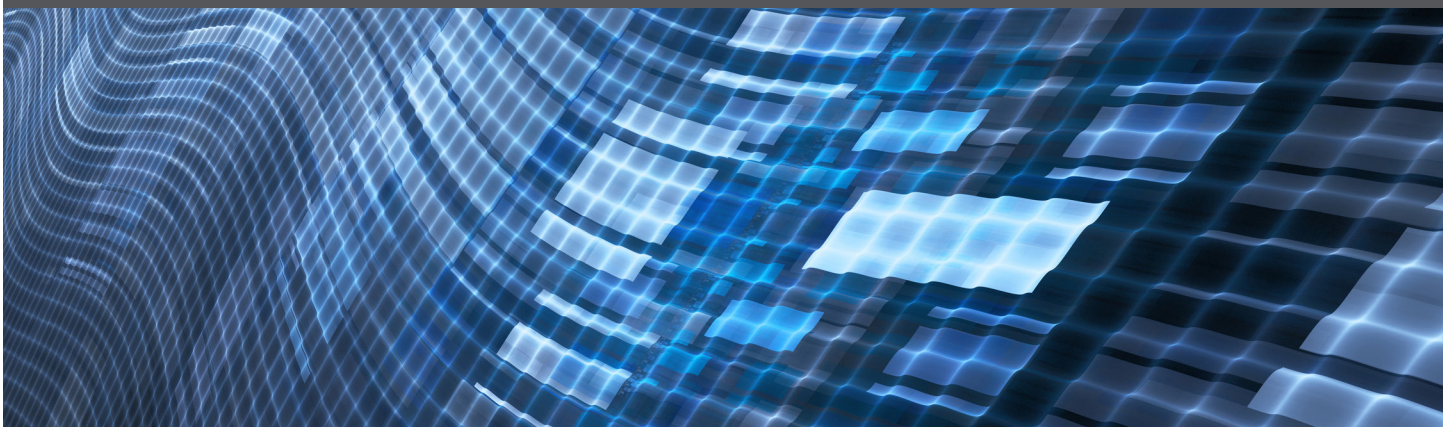
BLANKROME

Blockchain Technology & Digital Currencies



FEBRUARY 2019 • NO. 1

QuadrigaCX's Insolvency: Problems in Tracing and Recovering Cryptocurrency When Keys Stored in Cold Wallets Are Missing

The implementation of compliance protocols for private keys of cryptocurrencies is of the utmost importance for companies that hold custody of cryptocurrencies, as highlighted by the recent, untimely death of QuadrigaCX's CEO leading to the company's insolvency.

Recently, QuadrigaCX ("Quadriga"), one of the largest cryptocurrency exchanges in Canada, filed for creditor protection under the Companies' Creditors Arrangement Act ("CCAA") in Nova Scotia.[1] The filing was precipitated by the sudden death of the exchange's CEO, Gerald Cotton. It has been alleged that Cotton apparently had not disclosed to anyone the password to his hard drive or the keys to more than CAD $190 million (approximately U.S. $ 144 million) in cryptocurrencies held in a cold storage wallet,[2] an offline wallet used to store cryptocurrencies.[3] It has also been reported that there may be irregularities in the flow of funds and cryptocurrencies into and out of Quadriga's accounts and wallets. Regardless of whether issues of fraud become apparent, if no one else has the password and keys, the platform may not be able to unlock the cryptocurrency, and, as asserted, more than 363,000 of Quadriga's clients would not be able access their cryptocurrencies. The death of Quadriga's CEO and the company's insolvency highlights the significant risk that the loss private keys (whether simply lost, destroyed, or forgotten) to wallets can be expected to result in a complete loss of the cryptocurrencies held in those wallets. Quadriga appears primed to become the latest example of this substantial issue.

BACKGROUND

Cotton founded Quadriga in 2013 and was, until his death, the sole officer and director of the company. Quadriga facilitated the purchase and sale of cryptocurrencies, such as Bitcoin, Bitcoin Cash, Bitcoin Cash SV, Litecoin, and Ethereum for Canadian customers.

The alleged facts reflect that Quadriga used a combination of both hot and cold wallets. As the sole officer and director of Quadriga, Cotton apparently ran the business and managed the platform on a personal encrypted laptop and personally maintained numerous cold wallets with users' cryptocurrency. Cotton was the only one with the laptop password and private keys to the wallets. And, although Cotton apparently had medical issues, his death was unexpected. He apparently had not made critical information about the keys available to anyone else. Persons affiliated with Quadriga are now struggling in their attempts to access the cryptocurrency within the company's cold wallets and the encrypted laptop. Reports also indicate that the cold wallets may contain only minimal cryptocurrency units, suggesting that other, more nefarious, activity may ultimately be implicated in this matter. Regardless of whether there is an element of fraud or other criminal

activity, without access to the cryptocurrency, Quadriga appears unable to satisfy its obligations to users with the amounts of deposits currently recorded in Quadriga's database and platform. Since Cotton's death, the company hired an expert to assist in recovering the cryptocurrency from the encrypted wallets, who has had only limited success.

As a result of all of these difficulties, on January 28, 2019, the company suspended its platform and ceased accepting cash and cryptocurrency deposits from users. Thereafter, Quadriga commenced a proceeding under the CCAA in the Supreme Court of Nova Scotia. The purpose of the proceeding is to assist Quadriga in its efforts to reorganize its business and, if necessary, sell its operating platform to satisfy its obligations to its users.

REORGANIZATION AND CREDITOR PROTECTION UNDER THE CCAA

In order to provide Quadriga with time to address its liquidity issues and, specifically, time to explore forensic methods of accessing the cold storage wallets, Quadriga sought to obtain a court-ordered stay preventing users, creditors, and other entities from commencing or continuing litigation or collection efforts against Quadriga. Indeed, a stay is necessary as Quadriga customers and others have speculated that Quadriga was a scam or potentially a Ponzi scheme. On February 5, 2019, the Supreme Court of Nova Scotia imposed a stay until March 7, 2019. The stay may be extended further by order of the court.

During the stay period, the proposed monitor will report to the court on investigative options with respect to attempting to access the cold wallets and the encrypted laptop. If forensic experts are unable to access the wallets by finding the private keys, the funds in the cold wallets could be permanently lost, leaving individual users without access to their funds. As is common in the cryptocurrency markets, there is no financial backstop or provider of insurance or other protection for investors. Unlike an insolvent bank, there will be no institutional or governmental bailout to protect individual investors.

Assuming some or all of Quadriga's cryptocurrency is recovered, the volatility in the value of cryptocurrency raises additional complicated questions. For example, how does a court value a creditor's claim and how does it distribute the proceeds to creditors? In Mt. Gox—the hacked and now insolvent Japanese cryptocurrency exchange—the trustee initially converted the value of cryptocurrency into prevailing fiat currency and then planned to pay out claims in accordance with the value as of the petition date. The issue with this approach is that since the commencement of Mt. Gox's bankruptcy case, the value of cryptocurrency skyrocketed (and then largely plummeted). Under this approach, the "increase in value" of the cryptocurrency would result in a surplus after paying creditors and such surplus would belong to the debtor's shareholders, not creditors. A Tokyo court later determined, however, that creditors are entitled to receive their claims in Bitcoin rather than the fiat equivalent at the time the bankruptcy began.[4] The difference is potentially worth hundreds of millions of dollars, depending on the value of Bitcoin, and allows creditors to receive the benefit of the increase in value of cryptocurrency.

CONCLUSION

Creditor recoveries in Quadriga remain uncertain with the risk of complete loss appearing fairly high. The cryptocurrency landscape is constantly evolving and, as cryptocurrencies proliferate, new issues will continue to arise. The loss of private keys is a significant risk that all participants in the cryptocurrency markets should be aware of and consider carefully in their investing and transacting activities within those markets.

For more information, please contact:

Michelle Ann Gitlitz
212.885.5068 | mgitlitz@blankrome.com

Grant E. Buerstetta
212.885.5454 | gbuerstetta@blankrome.com

Evan J. Zucker
212.885.5207 | ezucker@blankrome.com

1. *See Application by Quadriga Fintech Solutions Corp., Whiteside Capital Corporation, and 0984750 B.C. Ltd. d/b/a Quadriga CX and Quadriga Coin Exchange for Relief under the Companies' Creditors Arrangement Act,* available at ey.com/ca/quadriga.
2. *See Pre-Filing Report of the Proposed Monitor,* dated January 31, 2019, available at ey.com/ca/quadriga, and *Affidavit of Jennifer K. M. Robertson,* sworn to on January 30, 2019, available at ey.com/ca/quadriga.
3. A wallet is a software program that stores private and public keys and interacts with various blockchains to enable users to send and receive cryptocurrency and monitor their cryptocurrency balance. A cold storage wallet is stored on a platform that is not connected to the internet, thereby protecting the wallet that holds the keys from unauthorized access, cyber hacks, and other vulnerabilities to which a system connected to the internet is susceptible. A hot storage wallet is similar to a cold storage wallet but it is connected to the internet.
4. *See Announcement of Commencement of Civil Rehabilitation Proceedings,* available at mtgox.com/img/pdf/20180622_announcement_en.pdf; and *Q&As for Filing Proofs of Rehabilitation Claim,* available at mtgox.com/img/pdf/20180823_qa_en.pdf.