Berkeley Center for Law and Business
University of California, Berkeley
School of Law
Boalt Hall #7200
Berkeley, CA 94720-7220

BerkeleyLaw
UNIVERSITY OF CALIFORNIA
Berkeley Center for Law and Business

Millions Trapped in Cryptocurrency Purgatory

By: Liz Bramley, J.D. Candidate 2021 | February 11, 2019

For the cryptocurrency industry, the events of the past week days may seriously upend consumer confidence. Quadriga, a major Canadian cryptocurrency exchange company filed an affidavit with the Novia Scotia Supreme Court seeking creditor protection. The company owes its customers upwards of $190 Million, and technically has the capital, but can't pay them back. Why? Because CEO Gerry Cotton, the only person who knew the cryptographic key to access offline storage, unexpectedly died.

Cryptocurrencies, like bitcoin, are created from and operate within a system of decentralization. That is what made digital-cash so appealing and transformative in the first place. It replaced trust in centralized institutions with trust in a "peer-to-peer" decentralized system of math. In this unregulated system, once hackers take your coin, you can't get it back. Thus, trendy consumers store, sell, and trade cryptocurrency, whatever it may be, on more "secure" exchange platforms. These crypto-custodians use a system of "hot" and "cold" storage to mitigate hacker risk. Funds are allocated to active "hot" wallets for day-to day-transactions or safer offline "cold" storage, with more kept in the latter. While most companies require multiple people with different keys to access this offline storage, unfortunately, Quadriga did not. Now millions of dollars' worth of cryptocurrencies are trapped in cyber purgatory due to consolidated human error.

While Quadriga hired hackers to hack the un-hackable, customers have voiced their outrage, disbelief, and even suspicion that Cotton faked his own death. But as the affidavit states, "there is no governing body that provides oversight to the industry." Legal recourse for economic loss arising from mismanaged cryptocurrency is still uncharted territory.

The turn of events, while ironic, is not surprising. Cryptocurrencies users are quick to distrust regulation and instead rely on reputation. They don't want to bank on the banks, but they will trade where their peers do. Caught up in the hype of cool money, people don't think through the implications of irreversible transactions and unregulated storage. But it is a serious dilemma for companies, governments, and legal systems.

It will be noteworthy to see how this latest industry mishap plays out. Wronged consumers usually struggle for regulatory solutions. But how can cryptocurrency owners expect institutional protection when they facilitate a system that fundamentally values the opposite? Some experts believe that customer values will shift back towards trusting institutions. Recently, Bruce Scheier, cryptographer and fellow at the Berkman Center for Internet & Society at Harvard, wrote, "would you rather trust a human legal system or the details of some computer code you don't have the expertise to audit?"

This latest case goes to show that trust doesn’t even matter. The decentralized system that creates cryptocurrency ultimately relies on centralized systems to trade it. So, whether customers trust institutions or math, at the end of the day, there will be human error. And human error leads to uncertainty. And uncertainty leads to law. It’s just a matter of time before the cryptocurrency industry faces their ultimatum: extinction or regulation?