# Perhaps the QuadragaCX Story Will Have a **Happy Ending**

**Adv. Adrian Daniels**
Corporate Partner

While there are the aficionados who will say that cryptocurrencies will free us of the chains of the global financial institutions, on the occasions when the world of cryptocurrencies intersects with the world in which most of us live, the news is generally bleak. While you may not know one side of a Bitcoin from the other, you probably know that its value has crashed over the last 13 months, you may even have heard about some of some of the larger cryptohacks (that is computer heists through which digital currencies belonging to investors are stolen from crypto trading exchanges). And over the last week or so, you may have read on mainstream news sites about the death of Gerald Cotton the CEO of Canada's largest cryptoexchange QuadragaCX. The death of the CEO of a company that few had previously heard of, was news of course, because in his passing he had taken the passwords to the accounts of his customers with him. The result of this being that about $140 million of their money was stuck somewhere between this world and the celestial ether in which Mr. Cotton now resides. Of course, it wasn't quite told like that. We were fed terms such as "private keys," lack of "multi-signature protection," "cold storage wallets" and more readily understandable – "cryptofraud". Again!

I think that for all its jargon, this story is actually very instructive, but to learn our moral, we need to unpack the concepts a little.

Over recent years, as physical (or fiat) currency has increasingly been traded electronically, governments and financial institutions have been engaged in the development of ever-evolving rules to prevent money laundering and the financing of terrorism, known generally as AML (Anti-Money Laundering) regulations. Because fiat currency originates from the banks, the banking institutions have largely been viewed as the gate-keepers of these AML regimes. On the other hand, cryptocurrencies are digital means of exchange, the motivational ideology of which was to bypass institutional intermediaries (which many felt had been stripped of their credibility after the 2008-9 financial crash) and allow the holders to transact with one another directly. The result of this is that cryptocurrencies were never intended to be held by banks, and banks will not allow you to deposit your cryptocurrency with them.

So, if you can't deposit your cryptocurrency with your local bank, and it does not come in bills or coins, where do you hold it? The answer is, under your digital mattress, except they call it a digital wallet. If you want to purchase cryptocurrency you can go to any one of a number of crypto exchanges (like Quadragax), pay for it in either fiat or another cryptocurrency and then store it in a digital wallet, which may be held by the exchange itself or by you in some other manner. Your wallet will have an address (or public key) which is a sequence of letters and numbers. If you give an exchange or person that address, they will be able to transfer cryptocurrency to your wallet. If you want to withdraw those funds to transfer elsewhere or to convert in to fiat currency, you will need your own private key (or passcode). If you lose it, you will have lost forever whatever you have in your wallet (unless you find a way to retrieve it).

Which brings us to Mr. Gerald Cotton of the Canadian exchange QuadragaCX. There are many exchanges, and they can broadly be divided into 3 groups: trading platforms -which facilitate trades between buyers and sellers; brokers – who will buy from sellers and sell to buyers; and more traditional exchanges – which are platforms which facilitate trades like traditional equities exchanges with quoted prices, and where the exchange assists in the trade and takes a fee. If you want to actively trade on an exchange you will need to open a wallet on the exchange, where your cryptocurrency will be held, bought and sold.

So what happened at QuadragaCX? People opened accounts there and bought cryptocurrency with another cryptocurrency or fiat, or sold their cryptocurrency for another cryptocurrency or fiat. One of the customer pledges marketed by QuadragaCX, was that its accounts were safe from hacks because the funds were held in cold storage wallets, in other words in a wallet that wasn't connected to the internet and therefore could not be hacked. The problems started when some accountholders wanted to cash out but were unable to do so, because the Canadian Imperial Bank of Commerce determined that it could not properly conduct AML checks on the source of those funds (as they emanated from the sale of cryptocurrency) and froze about $28 million, resulting in a court case which is still ongoing. Coincidentally, or not (depending on whom you ask) in late January, the Company announced that its CEO had died unexpectedly on a trip in India and access to all of the funds in cold-storage was lost because Cotton was the only one with the private keys to each of those accounts. Currently the company has sought protection from creditors and has been given time to locate ways to reimburse its customers.

Whether or not what happened was a terrible unanticipated tragedy or a scam by a man who is not really dead and has run off with his clients' money, we may never know, but the fact is this was an episode waiting to happen. Ignoring the potential for market manipulation in the world of crypto (pump and dump schemes, worthless currencies, frauds), and the general fluctuations in value resulting from lack of certainty, holding cryptocurrencies is a risky business, and much of it stems from the lack of regulation of all things crypto. Firstly there is always the risk of hacking if your wallet is connected to the internet, whether or not you hold it directly or through an exchange. Regulation may not necessarily help much here, but a set of minimum security requirements and the threat of sanctions by some sort of authority may go some way to ameliorating the problem. Cotton tried to put his customers at ease by telling them that he held their funds in cold-storage, but this didn't work out so well. As it happens, he promised that the cold-storage wallets were multi-signature protected, which means that he could not access the funds alone but had to do so in conjunction with one or more authorized individuals. Had he done what he promised, it is likely the funds would be accessible today, but he didn't and there was no entity checking up on him, or to which he had to report.

While ideologues might balk at the idea of "institutionalizing" cryptocurrencies, it seems that without a mechanism for holding the ring, there is simply too much risk out there to ever allow cryptocurrencies to achieve their promise. For as long as exchanges are not carrying out sufficient identification and monitoring activities that would allow the banks to bank the proceeds of those trades, there is always the danger that traders will be stuck with currencies that they cannot convert into fiat, and for as long as exchanges are not regulated (whether through some kind of effective self-regulation or through national or international authorities), there is always an increased risk that there are insufficient security measures in place to protect traders from outside hacks or inside frauds.

Whether an elaborate (but painfully clumsy) fraud or sad tragedy, the QuadragaCX story contains a lot of what is wrong with the world of crypto today. Until appropriate measures are in place, the only stories about crypto that will break through to our "real world" newsfeeds, will continue to undermine the "real world's confidence in crypto. However, if some lessons are learned, the QuadragaCX story may also contain the seeds of what is needed to put much of that right.