INVESTOR PROTECTION CLINIC
UNIVERSITY OF TORONTO
78 QUEEN'S PARK
TORONTO, ONTARIO
IPC.LAW@UTORONTO.CA
WWW.IPC.LAW.UTORONTO.CA

An IPC Brief - Summer 2021

CRYPTOCURRENCY PRIMER

Although designed to function like traditional currencies—such as Canadian or US dollars—cryptocurrencies have largely been purchased and sold as speculative investments. Cryptocurrency prices have experienced exceptional volatility resulting in both large returns and large losses for investors.
As cryptocurrencies have grown in popularity, there have been a growing number of cryptocurrency frauds. Between 2017 and 2020, cryptocurrency fraud grew by more than 400% in Canada. There have been several high-profile cryptocurrency related frauds that have resulted in significant investor losses. This brief provides a basic overview of cryptocurrencies and highlights some of the more high-profile cryptocurrency frauds that have occurred.

What is a Cryptocurrency?

A cryptocurrency is a digital currency designed as a medium of exchange for the purchase of goods or services. Unlike traditional currencies—like the Canadian dollar—which are issued by governments and managed by central banks, cryptocurrencies are not backed by any organization or government. Cryptocurrencies have no value other than that which is collectively assigned by users of the currency and by those who buy and sell them as an investment.

Cryptocurrencies make use of blockchain technology to track ownership. From the moment a cryptocurrency is created, the blockchain makes a record of all transactions for the individual cryptocurrency. It is referred to as a distributed ledger—or list—because unlike other ledgers, the blockchain is decentralized. This means it is not maintained by any individual or company and instead uses a network of computers—called a peer-to-peer network—to update and maintain the ledger. The record is public and cannot be altered.

Cryptography

Cryptocurrency is secured by cryptography, which ensures that only the intended audience can access the information it is protecting. Cryptography helps secure any transactions involving cryptocurrency by preventing double spending or counterfeiting.

Cryptography also provides a certain degree of anonymity for cryptocurrency users. This helps protect the privacy of the parties involved to a certain extent. However, the anonymous nature of cryptocurrency also makes it suited for illegal activities. It is also worth noting that cryptocurrency is decentralized and does not fall under the control of governments.

The price of cryptocurrency is very volatile due to significant fluctuations in its supply and demand. However, some observers believe that cryptocurrency could provide protection against inflation, much like gold and silver, although others have disputed this idea.

Risk of Fraud

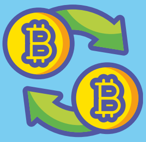
Cryptocurrencies and related investments are not inherently fraudulent and there are many legitimate—albeit risky—ways for retail investors to gain exposure to this new asset class. However, the decentralized, international, and online nature of cryptocurrencies has created a fertile environment for fraudsters.

Before investing in cryptocurrencies, it is important to understand that many of the protections provided by Ontario securities law have proven ineffective at protecting cryptocurrency investors. Most cryptocurrency offerings and exchange providers are based overseas and it can be difficult for Canadian regulators to effectively police their actions. Even though Canadian securities regulators have made clear that cryptocurrency exchanges and crypto offerings are likely subject to registration requirements or prospectus disclosures, providers of crypto services are well-positioned to ignore requirements and evade regulatory discipline.

The Investor Protection Clinic at the University of Toronto is extremely grateful for funding provided by The Law Foundation of Ontario.

QUADRIGACX

QuadrigaCX was a Canadian cryptocurrency exchange that allowed users to buy and sell cryptocurrencies. Quadriga customers would deposit either traditional currencies or their own cryptocurrency assets into Quadriga accounts and then carry out trades on the platform.



When a customer bought, sold, or deposited a cryptocurrency on the platform, it would be stored in Quadriga-operated crypto wallets rather than be deposited into an individual user's wallet. This meant that before investors could access their trading profits or take ownership of their cryptocurrency, they would have to go through Quadriga's withdrawal process. Many investors were happy to leave their holdings in their accounts and trusted Quadriga to safeguard their money and cryptocurrencies.

Contrary to the assumptions of many Quadriga users, the exchange was not registered with any Canadian securities regulator and was not actively subject to any monitoring or insight. In an April 2020 report, the Ontario Securities Commission (OSC) concluded that the founder of the platform used this environment to carry out a Ponzi scheme-like operation that defrauded cryptocurrency investors of millions of dollars.

From the very onset of Quadriga's launch, the exchange's founder used aliases to create fake accounts, crediting himself with fictitious currency balances which he then used to trade with other users. When early customers sought to withdraw their account balances, new client deposits were used to cover deficits generated by the founder's fictitious and fraudulent trading. Eventually, new deposits could not keep up with the increasing withdrawal demand, which caused the scheme to fall apart and left Quadriga clients with a $169 million shortfall.

In the midst of Quadriga's collapse, the founder passed away and the OSC ultimately decided not to pursue any enforcement action against what remained of the exchange. However, in its investigative report, the OSC cautioned investors that Quadriga was able to get away with misleading its clients due to the way in which its founder had complete and sole control over the business and the lack of a proper system of internal or external oversight.

ONECOIN

OneCoin was a cryptocurrency which was created in 2014 and touted as a rival to Bitcoin. There was a rush of investor enthusiasm over this supposedly revolutionary cryptocurrency, as large venues would sell out to hear the founder of OneCoin speak. However, after raising billions of dollars from investors, the founder disappeared and the coin itself was revealed to have no underlying blockchain ledger. This meant that investors in OneCoin did not have the security and authentication backing that blockchain provides, making their cryptocurrency effectively worthless.

HOW DID ONECOIN OPERATE?

OneCoin's main business was selling packages of educational materials. The educational materials also included tokens for mining purposes.

OneCoin also had an internal marketplace, known as the OneCoin Exchange xcoinx. It was accessible by those who had purchased more than a starter package. For those who wished to sell their OneCoin for other currencies, the internal marketplace was the only place to do so.

In 2016, OneCoin was labelled as a pyramid scheme by the Direct Selling Association in Norway and the Hungarian Central Bank. The founder of OneCoin, Ruja Ignatova, disappeared in 2017, while co-founder Sebastian Greenwood was arrested in 2018. Ruja Ignatova's brother, Konstantin Ignatov, was also arrested in 2019.

The Investor Protection Clinic at the University of Toronto is extremely grateful for funding provided by The Law Foundation of Ontario.