

# THE MONEY LAUNDERING RISK OF CRYPTOCURRENCIES



**BY ANDREW  
TARPEY**

Risk Compliance Officer



Bitcoin and other cryptocurrencies, also known as virtual currencies or digital currencies, have generated a lot of talk and taken a prominent place in the financial landscape in the past few years. The rise in value of Bitcoin in 2017 certainly captured the interest of both investors and financial analysts, both of whom are trying to make heads or tails of this relative newcomer to the global financial stage. Famed investor Warren Buffett is dismissive of Bitcoin, calling it “probably rat poison squared” and stating that “the asset itself is creating nothing”. However, some exchanges had the value of Bitcoin increasing exponentially between the beginning and end of 2017. While it can be debated how long digital currencies will remain prominent on the financial landscape, the question facing governments at the

moment is how to deal with it from a regulatory perspective. For starters, is it even really a currency? If it can't be used as a legal tender and isn't issued or backed by governments, do they have the legal authority to treat it as a currency for regulatory purposes? The answer is a hodgepodge of different responses by different countries; some authoritarian regimes predictably have come down hard on the side of regulation, while other countries are taking a more wait-and-see attitude.

Despite Warren Buffett's view, cryptocurrencies have quickly become an important part of many investors' asset protection and investment portfolios. For starters, there is a large potential for returns. An individual who invested \$1,000 in Bitcoin in 2013 would have seen their investment rise to over \$400,000 in late 2017. The ability to liquidate one's assets is also much more favourable with cryptocurrencies than with other forms of investment. Many of the larger cryptocurrencies offer an almost immediate time frame to exchange cryptocurrency for fiat currency. There are also the asset protection benefits that digital currencies offer. Cryptoassets can be easily transferred over to an appropriately selected offshore trustee, thus stymying the ability of a creditor or court to access them. The way cryptocurrency transactions work is that they are executed using a two key system: there is one public key and one private key. The keys are comprised of

a series of numbers and letters. The private key is known only by the owner and allows them to transfer the asset. For asset protection purposes, providing the private key to an offshore trustee in effect means that the funds have moved offshore, and thus out of the hands of a hostile court or creditor. With the growth of Bitcoin and other cryptocurrencies, we can expect that trustees specializing in cryptoassets will only grow larger in the near future.

However, one aspect of cryptocurrencies that is of concern is its ability to be used for money laundering and other nefarious purposes. The anonymity associated with cryptocurrencies allows it to be used as a medium of exchange for criminal organizations and sanctioned governments. The blockchains which underlie cryptocurrencies oftentimes do not store personal data, so they offer no way to identify the individual or organization associated with it. The way someone may launder money through a cryptocurrency is as follows: a person or organization enters the cryptocurrency market by purchasing the virtual currency from a crypto exchange. Criminal organizations may use a "straw man", or someone with a clean background whose name and personal information won't raise any suspicions, to make the initial purchase of the virtual currency. The main cryptocurrencies, of which Bitcoin is the most well known, have an audit trail which can be traced. However, there

are a growing number of exchanges where mainstream cryptocurrencies like Bitcoin can be exchanged for other cryptocurrencies called alt-coins which may offer more privacy and anonymity. Once the initial digital currency is swapped for the alt-coin, the money launderers may use a process called "mixing" or "tumbling" whereby the alt-coin's address, or unique defining specifications, is swapped for a different temporary address which basically removes the audit trail and provides complete anonymity to the holder. Money launderers may use more exchanges and movement methods to ensure the trail is clean before using the laundered funds to purchase primary coins, such as Bitcoin, which can then be withdrawn into a bank account using a currency exchange. This is only a basic example of how funds can be laundered using digital currencies; there are far more advanced, complex ways that criminals can devise to launder illicitly derived funds. Following the trail becomes nearly impossible for investigators trying to navigate it.

So now that we've identified that there are money laundering problems linked to cryptocurrencies, the question remains as to how they should be addressed. This is made more difficult by the fact that virtual currencies are borderless and disconnected from any government issuance, oversight or regulation. It's a safe bet that most governments will at least make an effort to impose a system of regulation to some degree if they haven't already. The question is how to do so, and

and to what degree. China has banned ICOs (initial coin offerings) and exchanges, an expected hard line stance taken by the totalitarian regime that rules the country. Western governments will undoubtedly take a less severe stance, but still see the money laundering problems associated with cryptocurrencies as something to be addressed. Due to its borderless nature, it's likely that any regulation needs to be centered around an international agreement on how to do so, but with the disparate approaches taken by different governments to this point, such an agreement hasn't materialized yet. International anti-money laundering requirements for banks and other financial institutions include verifying the identity of its customers, monitoring customers' banking activity for transactions which appear to be suspicious, and screening the names of its customers against sanction lists. Ideally digital currency exchanges would face the same requirements, but with so many different cryptocurrencies across the globe and new digital currencies popping up regularly, this is easier said than done.

One last thing to note for those who wish to invest in the cryptocurrency market is to keep detailed records of your cryptocurrency transactions. Financial institutions dealing with high-risk clients are required to conduct enhanced due diligence on their clients, and it's likely that those individuals

dealing in virtual currencies will be deemed high-risk by banks. As such, banks will want to know as much as they can about your transactions and where the funds came from. For those banks who are open to the crypto market or will be in the future, expect them to ask for a blockchain history of the cryptocurrency. Although banks have largely shied away from virtual currencies to this point, this may change in the future (JP Morgan recently created the position of Head of Crypto-Assets Strategy). If and when banks dive more deeply into the world of cryptocurrencies, they will almost certainly do so cautiously, so it's important to record the source of any cryptoassets held.

If you would like to discuss this topic further, please contact Southpac at [enquiries@southpacgroup.com](mailto:enquiries@southpacgroup.com)

Southpac Group  
Goddard Centre, Level 1, 16 Grey Street,  
Tauranga, New Zealand.  
T: +64 7 571 8548  
[www.southpacgroup.com](http://www.southpacgroup.com)