# Crypto Assets, Financial Crime & Forensic Accounting

*In this article I explain how cryptocurrencies are used to launder illicit funds and how this affects the asset tracing work of forensic accountants.*

**Forensic accountants** use their expertise in finance, accounting and transaction processing systems to investigate fraud and other financial wrongdoing. Their work includes assisting clients on financial crime risks and controls, detection, investigation and litigation support, as well as asset recovery. Two aspects of this work are money laundering and asset tracing.

**Money laundering** is the transformation of the proceeds of crime from their original form (such as cash) into new assets and locations to disguise their origin and make them appear legitimate. Typically, the assets may have been moved through a complex chain of entities, such as bank accounts, companies, trusts and special purpose vehicles. Often these will span multiple jurisdictions. All this is done to ensure the trail is as hard to follow as possible. What began as cash received through a UK Ponzi scheme might end up in mega yachts in Monaco, property in Spain and blue-chip investments in the London Stock Exchange. The money could be laundered via companies in Switzerland, bank accounts in Guernsey, trusts in the Cayman Islands and law firm client accounts in Gibraltar.

**Asset tracing** is the process of carefully uncovering the trail of an asset from origin to ultimate destination, documenting each step along the way, in a forensically sound manner that can stand up to court scrutiny.

**Cryptocurrencies** such as bitcoin provide new opportunities for money launderers, through the partial anonymity they can provide and the lack of centralised supervision. Both these attributes are seen as key attractions by genuine and dishonest users alike. Two examples are the notorious case of Ross Ulbricht, the founder of Silk Road, which was the first dedicated black market on the dark web; and the more recent alleged activities of Russian intelligence operatives accused of seeking to interfere with the US presidential election in 2016.

**Silk Road** was created by Ross Ulbricht in 2011 as an online marketplace free from government oversight and interference. It provided anonymity through the Tor system, which helps internet users conceal their location and communications. Silk Road used bitcoin as the currency for all transactions. Bitcoins are held in online "wallets" whose ownership can be kept anonymous. Silk Road quickly became the main electronic bazaar for the buying and selling of black market goods, mainly drugs but also other illegal items such as stolen identity documents. According to the US authorities,[1] the Silk Road site generated approximately $1.2 billion in sales revenue and $80 million in commissions – all of which was in bitcoin. Ulbricht was eventually caught and convicted, but only through old fashioned forensic investigation and not by breaking bitcoin's security technology. However, his conviction was assured by another key feature of bitcoin, its tamper-resistant method of record-keeping – more on that later.

**Russian interference in the 2016 US presidential election** was alleged by the US authorities in July 2018. The investigation by Special Counsel Robert Mueller led to the indictment of 12 Russian intelligence officers for "hacking into the computers of US persons and entities involved in the 2016 US presidential election" and conspiring "to launder the equivalent of more than $95,000 through a web of transactions structured to capitalize on the perceived anonymity of cryptocurrencies such as bitcoin."[2] It is alleged that bitcoins were used by the defendants to evade scrutiny when purchasing servers, registering domain names and making other payments as part of their hacking activity.

**So what are cryptocurrencies, exactly?**
Cryptocurrencies, such as bitcoin, are "any publicly available electronic medium of exchange that features a distributed ledger and a decentralised system for exchanging value."[3] They are an exciting innovation that seem to offer certainty, security and transparency without government regulation or any central authority being involved. They are lauded by many as a true free-market innovation.

Cryptocurrencies are actually a combination of four technologies:
1. Distributed ledgers: each participant can have a copy of the whole ledger (transaction record), which for bitcoin and many other cryptocurrency systems is structured in a "blockchain".

2. Decentralised control: participants can deal directly with each other, not through a central authority or controlling entity like a bank.

3. Use of cryptography: to protect and authenticate transactions, balances and participants.

4. Automation: the ability to automate transactions programmatically, such as in smart contracts or by triggering the payment of interest on a bond once a specified event occurs.

Cryptocurrencies are not regarded as true currency – they are not official money, which is called "fiat currency". They are not legal tender and currently are not widely accepted across society. However, they can offer the following benefits:

- Security
- Speed
- Low transaction costs, avoiding banks and intermediaries
- Convenience
- Relative anonymity
- Decentralised dealings without any central oversight or monitoring

One key aspect of a classic cryptocurrency such as bitcoin is the distributed blockchain ledger technology. What this means is that is every single transaction, since day one, by every party in the cryptocurrency system, is recorded in a ledger, which is a chain or sequence of transaction "blocks" called a "blockchain". The net result of the history of all the transactions affecting a user's wallet determines the closing balance on that wallet. Every user can have a copy of the whole ledger, and can therefore see all the transactions, though the identity of wallet holders may be unknown. This sharing of information about transactions across the whole system makes it very hard to falsify the records. Because everyone else has a full copy of the ledger, altering one's own copy will have no effect: each new block of transactions is only finalised and accepted – and then shared with all the users – once it has been properly validated by a special class of users called "miners" using complex cryptographic techniques. The transparency of the ledger record helps make it very hard to tamper with.

**What are the financial crime risks?** As already mentioned, cryptocurrencies can offer a degree of anonymity and the ability to move financial assets across jurisdictions without government oversight or regulation. A person can open a cryptocurrency wallet, which appears simply as a computer address on the system, without disclosing anything about his or her identity. As we saw with Silk Road, many illicit items can be bought and sold using cryptocurrency. It is often the preferred means of exchange for items such as stolen personal data, ransomware payments, drug dealing and other black market goods and services. It is also increasingly used to evade state sanctions that prohibit the use of official currencies, such as the US dollar. Several sanctioned countries have reportedly indicated that they are developing their own cryptocurrencies, including Iran, Russia, Myanmar and North Korea.

However, while cryptocurrencies may provide a safe space for criminals to transact with each other, the range of legitimate assets that can be purchased with cryptocurrencies is still fairly limited. Ultimately, if they want to spend their ill-gotten gains on useful items, criminals will eventually need to get their assets out of cryptocurrencies and into the "real" economy. They also need to convert the proceeds of their crimes into the cryptocurrency in the first place. This highlights two key areas of vulnerability from the criminals' perspective: the points of entry and exit.

Criminals who make their money in the real economy, for example through investment fraud, will need to convert their proceeds into cryptocurrencies, which means finding a party willing to accept fiat currency in exchange. In practice - for transactions of any size - the payment of the real currency will need to pass through a financial institution such as a bank. If the financial institution has strong anti-money laundering controls then it will consider whether the source of the funds and the nature of the transaction seems suspicious and, if so, report it to the authorities. Similar considerations apply when cryptocurrency is converted back into fiat currency. This is one area on which forensic accountants can focus when trying to trace assets: regulated financial institutions are required to follow stringent "know your customer" rules, and their records can therefore be a useful source of information about the identity of the parties.

One weakness from the regulators' point of view has been poor regulation of cryptocurrency exchanges – companies that buy and sell cryptocurrencies, providing the entry and exit points to customers. These have typically been exempt from anti-money laundering regulation. However, with the rise cryptocurrencies and the associated money laundering risk this is changing. The EU's 5th Anti-Money Laundering Directive, which came into force in July 2018, requires member states to introduce tighter rules, bringing regulation of cryptocurrencies and cryptocurrency exchanges in line with existing rules for fiat currency and banks. In December the UK government announced it will address the risks by going significantly beyond the requirements of the new directive, and will be consulting on this during 2019. Other governments around the world are taking similar action: for example, in 2018 the US Treasury Department's Office of Foreign Assets Control issued guidance expressing how it believes transactions in digital currencies should be treated similarly to those in fiat currencies.

So how big a problem is cryptocurrency money laundering? The UK government's 2015 and 2017 National Risk Assessment of Money Laundering and Terrorist Financing initially assessed the risks associated with cryptoassets to be relatively low.[4] However, since then, money laundering with cryptoassets has been identified as a growing problem. Europol has estimated that £3-4 billion is laundered through cryptoassets each year in Europe, which is a relatively small proportion of total laundered funds, estimated at £100 billion.[5] However, this seems set to rise.

Naturally, criminals gravitate to exchanges in jurisdictions with the weakest anti-money laundering defences. While this means it is difficult to stamp out money laundering, it does result in illicit activity being

pushed towards "rogue" jurisdictions. As a forensic accountant, seeing transactions pass through such jurisdictions raises red flags, which is useful since it can help narrow the focus of an investigation onto the areas where criminal activity is most likely.

**What specific techniques can forensic accountants use to investigate cryptocurrency transactions?**
It is a common misconception that digital currency is untraceable and completely anonymous. While it may be true that wallets are stored as anonymous computer addresses within the technical cryptocurrency system, there are multiple ways it may be possible to link wallets to the parties that control them. These can include traditional forensic investigation techniques, such as transaction pattern analysis (for example matching property transfer records with transactions in the cryptocurrency ledger), or simply obtaining information from co-operating parties. More advanced techniques include analysis of internet traffic through particular servers and IP addresses.

In fact, cryptocurrencies can be the forensic accountant's best friend, because literally every transaction is indelibly recorded in the blockchain. And for traditional cryptocurrencies like bitcoin, this is a freely-available public ledger. Every transaction is literally there for all to see and analyse.

This allows forensic accountants to use graph technology and network theory to analyse the recorded transactions, aided by sophisticated graph database systems (in mathematics, a graph is a network of nodes, such as wallets, and links, such as transactions between wallets). These systems can be used to analyse hundreds of thousands of transactions between different wallets to identify patterns of activity, such as heavy traffic routes and clusters of activity, or the ultimate destination of apparently disparate individual transactions. Since all transactions are fully recorded, it can be possible to trace flows across numerous intermediate nodes in the network to their entry and exit points. From there the focus can move to the relevant cryptocurrency exchange, where the assets are converted between crypto and traditional assets, and then into regular bank accounts. As mentioned above, more traditional techniques can be employed to identify who controls each of the nodes.

Therefore, once the technology of cryptocurrencies is understood, the forensic accountant can use a range of traditional and new tools to crack open transaction secrets. And once anonymity has been breached the cryptocurrency ledger can become a treasure trove of complete and accurate information, all neatly tied in: something rarely possible in traditional forensic asset tracing.

**Postscript – how Ross Ulbricht was caught** and convicted. Ulbricht's anonymity was breached through an error he made that was spotted by Gary Alford, an Inland Revenue Service investigator working in his spare time. Alford had been working with the US Drug Enforcement Agency to find a way to bring down Silk Road. He noticed that Ulbricht had recently openly used the online nickname "altoid". He recalled that this same pseudonym had previously been linked to the early days of Silk Road. Ulbricht's use of the same name much later provided the lead that connected him to Silk Road. Thus, it was old fashioned forensic investigation techniques, and a mistake by Ulbricht, that blew his anonymity, not a flaw in bitcoin.

The Federal Bureau of Investigation seized Ulbricht's computer and discovered it contained hundreds of thousands of bitcoins, many of which had been received recently. During his trial Ulbricht claimed that the bitcoins were his, but he said they had nothing to do with Silk Road. Although he admitted he had originally set up the site, he claimed to have stopped running it long ago. However, since the anonymity of Ulbricht's wallet had been breached, it was easy for the FBI to analyse the transactions through his wallet and demonstrate the provenance of his bitcoins. Since the bitcoin ledger – which is publicly available – is a full record of every transaction ever conducted, it was a simple exercise for the FBI to track Ulbricht's bitcoins back to their source: Silk Road. He was convicted of money laundering, computer hacking and conspiracy to traffic narcotics. He was handed a double life sentence plus forty years without the possibility of parole.

**References**


1, Ulbricht indictment, 27 September 2013.
2, Indictment, US vs. Viktor Borisovich Netyksho, et al., 13 July 2018.
3, "Dear CEO letter" from the UK Financial Conduct Authority to chief executives of regulated institutions, 11 June 2018.
4, Cryptoassets Taskforce Final Report, October 2018. This is a report by a UK government-sponsored taskforce including HM Treasury, the Financial Conduct Authority and the Bank of England.
5, Ibid.



Article by **Paul Doxey**
Paul is a Senior Consultant to the Forensic Services Practice of Charles River Associates
+44-20-7959-1424.
pdoxey@crai.com
www.crai.com