## Bitcoin: great financial innovation or great financial risk?

Since it first appeared in 2009 demand for bitcoin has increased exponentially, with its value reaching an all-time high of $2,409 on 24th May 2017 ([Reuters](http://uk.reuters.com/article/us-markets-forex-bitcoin-idUKKBN18K206)). The rise of bitcoin is in fact such that anyone who had invested just $100 in 2010 would now have over $73 million in their online wallet ([briefreport.co.uk](http://www.briefreport.co.uk/news/bitcoin-soars-above-2-400-to-all-time-high-5023657.html)).

The investment potential of bitcoin is clear to see. But what are the other main attractions of this and other cryptocurrencies for the people who use them? And how can governments and financial institutions mitigate the associated risks?

### The appeal of bitcoin

One of the potential attractions of bitcoin and other cryptocurrencies is the relative speed with which transactions can be carried out. Transactions that use cryptocurrencies are generally faster than other transfers, taking ten minutes to complete if the transactions need to be confirmed and even less time than that for ‘zero confirmation’ transactions. Speed can be of the essence in a fast-moving, never-sleeping global economy and, for those who need to move money quickly, bitcoin provides an easy medium to work with.

Another potential attraction is the comparatively low transaction cost. Bitcoin transaction fees are minimal and sometimes there is no fee at all. For cost-conscious businesses and individual investors this is an obvious advantage.

A third attraction is the relative anonymity with which bitcoin transactions can be carried out. To do any kind of financial business you will generally need to provide some form of verifiable identification. But bitcoin transactions do not require this. They simply require a public key (usually a bitcoin address) and a private key (a secret password). The fact that no ‘real world’ ID is required is even touted by promoters of bitcoin as a security strength; if you don’t need to share personal data with a third party processor then that obviously reduces the risks of that data falling into the wrong hands and being used fraudulently.

### Bitcoin, money laundering, terrorism and the dark net

The massive increase in the volume and value of bitcoin shows that the triple promise of increased speed, reduced cost and relative anonymity has clearly attracted a lot of legitimate investors. But those same characteristics *also* have appeal for anyone seeking to move illicit funds around. Money launderers may not be as worried as others about the financial costs they incur but they are *certainly* interested in the speed and anonymity of their transactions. The faster and more discreetly it can be done the better as far as they are concerned.

To make things even *more* anonymous it’s possible for bitcoin users to use ‘mixer’ or ‘tumbler’ services to commingle theirbitcoin with other people’s money. The only way to look at these services is that they are designed deliberately to obfuscate disguise the bitcoin trail. What more could a money launderer ask for?

Governments and regulators have worked hard to protect against such commingling with fiat currencies but cybercurrencies are, as things stand at the moment, largely beyond the reach of regulation and the same rules do not seem to apply. Try Googling ‘bitcoin tumbler service’ and see what you come up with. Here are some examples:

‘Completely erase the origins of your bitcoin and de-couple them from previous transactions. We launder bitcoin to protect your financial privacy online’

‘Using bitcoins is an excellent way to stay anonymous while making your purchases, donations, and p2p payments’.

The language used is the same language used to market any *legitimate* product – it could be a candy bar, a kitchen suite or a car. And the reference to ‘donations’ reminds us that this is not only about the facilitation of money laundering, but about terrorist financing too. Terrorist financiers are just as eager to keep their identities and those of donors as far away as possible from the funds they collect and handle, and it is truly scary just how easy it is to find sites that overtly offer opportunities to hide the identities of those involved.

The TOR anonymity network has supported the proliferation of such sites. TOR software enables people to communicate anonymously on the internet without revealing their location or browsing habits. Whilst ostensibly intended to protect personal freedoms and privacy it is perhaps inevitable that the TOR network has become a ‘dark net’ where criminals can buy and sell whatever they want including drugs and guns.

And the predominant currency in this dark net? Bitcoin of course. The [Silk Road case](http://www.bbc.co.uk/news/technology-24371894) provides a classic example of how the TOR anonymity network, the trade in bitcoin and the use of bitcoin ‘tumblers' enabled Ross Ulbricht between 2011 and 2013 to run Silk Road, an e-bay style site for trading in illegal goods. Other high-profile cases involving the use of bitcoin or other cryptocurrencies to facilitate money laundering include:

* The case of [Liberty Reserve](http://www.insightcrime.org/news-analysis/liberty-reserve-case-exposes-new-frontiers-in-laundering-digital-cash), where a Costa Rica-based money transmitter set up and used its own cryptocurrency to assist the laundering of $US 6 billion of criminal funds
* The case of [Western Express International](http://www.fraud-magazine.com/article.aspx?id=4294993652), where a New York-based virtual money-changer and unregistered money transmitter played a key role in laundering the proceeds of identity theft cyber-fraud schemes.

### Bitcoin and ransomware

Bitcoin has also been linked to a sharp rise in ransomware attacks, the largest and most recent of which was the May 2017 ‘Wannacry’ attack. This affected more than 200,000 systems across more than 150 countries, with the hackers instructing victims to pay a ransom to one of three bitcoin addresses in order to restore access to their files.

The Wannacry hackers drew a huge amount of attention to themselves with the sheer scale of the attack and those three little bitcoin addresses must surely be three of the most intensively scrutinised digital spaces on the planet. No-one has so far attempted to withdraw funds from these accounts as to do so would almost certainly blow their cover. However the anonymity afforded the hackers by using bitcoin has made them difficult to identify and to date there have been no arrests either.

It may seem that the Wannacry hackers have rather shot themselves in the foot and maybe they will never see the loot. But they are by no means the first to use ransomware, nor the first to select bitcoin as the preferred method of ransom collection. A recent study found that ransomware attacks increased by 3,500% from 2015 to 2016 and in the same period the ransoms paid increased tenfold ([Information-age.com](http://www.information-age.com/ransomware-exploded-bitcoin-123464668/)). Bitcoin provides a convenient, anonymous and accessible network for the easy collection of ransom payments and some authorities see a definition correlation between this and the rise in ransom attacks.

### Regulation and risk mitigation

So far we have focused strongly on the downsides of bitcoin but there must surely be an upside too. The speed and ease of bitcoin transactions will save time and money and that is surely an attraction for global business. But there are risks that need to be managed and, as yet, no clear consensus about how this will be done.

There is, for example, no international consensus regarding the legal status of bitcoin. The majority of countries – for example Hong Kong - explicitly allow the use and trading of bitcoin. Some jurisdictions – for example the US – have ruled confirming bitcoin’s status as a legal currency and, therefore, as taxable property. Only relatively few countries such as Ecuador and Bangladesh have banned it entirely, whilst others such as China have imposed restrictions on its use. Russia previously prohibited the use of bitcoin but in November 2016 declared bitcoin legal.

Many jurisdictions take the view that existing regulations already cover unlawful activities such as fraud or money laundering and that these same provisions should extend to such activities where they involve bitcoin. In 2016 the European Parliament presented proposals to set up a task force to monitor virtual currencies and to consider new measures to protect against their use in money laundering and terrorist financing. Many other jurisdictions have however indicated that they have no specific plans to regulate bitcoin. Lack of international consensus means that, for the moment at least, bitcoin operations will remain unregulated and outside of central bank control across much of the world.

There are significant risks here, not least because of the attractiveness which bitcoins holds for money launderers, fraudsters and other criminals. Questions to test the level of risk include the following:

* Can the parties be identified and their identities verified?
* Are the transactions taking place in an environment that is subject to ongoing transaction monitoring?
* Are electronic transaction records routinely retained, and are these reliable and obtainable?
* Are there limits on the frequency and size of the transactions?
* Do the funds originate from a regulated financial institution subject to anti-money laundering controls?
* Are P2P transactions (i.e., without the involvement of a third party processor) prohibited?

Without further immersion in transparency technology, with bitcoin the answer to these questions is negative, putting it fairly and squarely at the upper end of the risk scale. The most obvious way to mitigate this risk, as with other financial risks, is not just through technological innovation but also through regulation and enforcement good practice. Whether there is an international will to make this happen remains to be seen.