

## East Midlands Special Operations Unit



# **Bitcoin and Cryptocurrencies** **How they work, why they are the** **flavour of the month and what the** **future may hold**

By Phil Ariss  
Regional Cyber Crime Unit (RCCU)  
East Midlands Special Operations Unit (EMSOU)

In association with



## **Money for Nothing?**

*Speaking at a recent CICM Think Tank, Phil Ariss explains how cryptocurrencies work, why they are the flavour of the month and what the future may hold.*

If you cast your mind back to the 2008 financial crisis, there will be many images that come to the forefront of your mind. It was a genuinely worrying time for millions of people across the world who feared for their savings, businesses and employment. For a small group of people this financial event was the tipping point of their political beliefs, a group that called themselves 'Crypto-Anarchists', a group who believe that maths-based encryption provides users with the ultimate level of security.

In 2008, an online identity by the name of Satoshi Nakamoto released a white paper titled '*Bitcoin: A peer-to-peer Electronic Cash System*' and the idea behind the world's first de-centralised digital currency was born. This was the answer that Crypto-Anarchists needed, a currency that was removed of any control from any corporate or government entity, a currency that was controlled and developed by the users. Bitcoin was a technical and mathematical work of art, and was released as an open source project. It was highly regarded, being incredibly complex behind the scenes and very secure, while allowing ease of use for front-end users.

## **Anti-establishment**

The anti-establishment origins of Bitcoin however cannot be ignored. A hidden message within Bitcoin was revealed on the first ever transaction made. Quoting *The Times* newspaper in January 2009, it used the headline from that day to make a statement of intent: 'Chancellor Alistair Darling on brink of second bailout for banks'.

The undertone from the creators in this message was clear. In essence, their message was 'banks and governments can no longer be trusted with our assets, we must protect our own assets'. The birth of Bitcoin was a quiet and low-key event. The currency had little value and usage was low, however, the headline benefits to the users were clear; a high degree of privacy, a de-centralised network and transparency. Bitcoin just needed platforms to flourish.

Adoption didn't take long. Key events for those that have anti-establishment views played their part. Firstly, WikiLeaks. Overtly supporting and funding WikiLeaks via traditional methods was seen as risky and raising a flag to authorities. Bitcoin allowed those who supported the mission of WikiLeaks to fund their service by sending Bitcoin, using the privacy and de-centralised nature to protect their identity.

Secondly, The Silk Road, the first 'dark-web' marketplace where illicit items could be traded. The Silk Road used Bitcoin as their only choice of currency. Bank transfer, credit cards and Pay-Pal were all too risky as they left a paper/digital trail. Bitcoin was seen as the safest method.

Since that time Bitcoin has gone from strength to strength, and the price has gone through the roof. In May 2010, the price per Bitcoin was less than \$0.01. At the time of writing the price per Bitcoin is now in excess of \$5,200. Those that adopted the currency early and invested just small sums of money are now incredibly wealthy.

The way Bitcoin works is very different from traditional payment methods, from the computer network level, to the public and private key cryptography, and the mechanics of a transaction. Explaining how the currency works is best saved for another time or by watching a video on YouTube – diagrams are helpful!

### **How is it used today?**

It's safe to say that Bitcoin isn't being used as originally intended. It's not yet reached the mass adoption as a payment method the original white paper wanted it to achieve. Yes, it can sometimes be found in shops online and in the high street, however it's a rare sight to see the infamous logo while out shopping or grabbing a coffee. Conversely, Bitcoin seems to have found its current market niche as a tradeable digital asset, an investment opportunity and the way to transfer funds across borders with high security and privacy.

This is where Bitcoin has started to become a favourable tool for those that are involved in criminality. The benefits to the user (privacy, de-centralised and high security) make considerable challenges for law enforcement and for those who work in regulated sectors or risk management. Routine areas of investigation and disruption tactics become extremely difficult or at times, impossible. Bitcoin has been used in all manners of criminality, however the area of most concern is surely money laundering.

Bitcoin is the perfect environment for individuals to launder their criminal gains in an area that's completely unregulated, and largely out of reach of law enforcement. Assets become hidden, easily liquidated or used to purchase other goods or services. Proving this becomes very difficult; with organisations and entities existing in a worldwide network often out of jurisdiction, investigating in this area becomes very challenging and time consuming. That's not to say Law Enforcement do not have success in this area; there have been significant investigations and cases across various law enforcement units that show that while we may be at a disadvantage, opportunities do exist for enforcement and assets can be seized and recovered.

As Bitcoin is still in its infancy, the legitimate use whilst small at present, is certainly on the horizon. Probably the greatest use would be micro-transactions. Paying 5p for a news article on an online platform via conventional online payment methods wouldn't be cost effective, however with Cryptocurrencies it is possible and achievable. Why pay for a "pay-wall" service to have access to articles, stories and content you're not interested in just to read the one article you want, when you can micro-transact for the precise content you want, be that video, music or traditional written media. It makes for a better user experience, not being bombarded with adverts or jumping through hoops to access content.

Reducing payment processing fees is the huge benefit that entices merchants to use Bitcoin, and why companies such as Microsoft, Steam and Expedia accept Bitcoin for their products. Whilst these companies accept Bitcoin they don't make it easy for you to find this payment option, once they start to feel more comfortable and inform their customers of the benefits in using a system, we could see mass adoption of Bitcoin quicker than we anticipated.

To muddy the waters even further, Bitcoin isn't out there alone. Numerous other currencies have been created and a whole industry now exists under the banner of 'Cryptocurrencies', each offering something slightly different, with names such as Ethereum, Litecoin and Dash. It isn't just Bitcoin that has seen significant increases in value, there is a considerable boom in Cryptocurrencies and the latest trend, Initial Coin Offerings (ICO's) give people and organisations an opportunity to invest at the creation of a new Cryptocurrency while being rewarded with a sizeable quantity of the new coin. These can be irresistible to investors and those looking to emulate the early Bitcoin adopter's success, but there can be no guarantee these coins will become widely adopted or gain significant value.

ICOs are the next horizon of law enforcement threat. With countless new Cryptocurrencies being created in this unregulated environment, the danger is that some of these coins are created off fraudulent schemes, doomed to fail from the start, with investors losing their cash or their digital assets with no return in sight.

When I speak to people about my area of work with Cryptocurrencies, I usually get two responses: one of either complete disinterest; or complete profound interest and a desire to know about this fascinating subject, at which point I'm usually asked to point them in the direction of buying some in the hope of making them rich! While I can make no promises, if this brief insight has peaked your interest, I urge you to read more articles and watch some videos of how Bitcoin works, and you may find yourself down a rabbit hole of a fascinating and ever-changing area of business.

*Phil Ariss is part of the Regional Cyber Crime Unit (RCCU) at East Midlands Special Operations Unit (EMSOU).*