GDPO Global Drug Policy Observatory
reportingmonitoringanalysis

Swansea University
Prifysgol Abertawe

GDPO Situation Analysis

March 2015

The Booming Market of Alternative Cryptocurrencies

Alois Afilipoaie and Patrick Shortis

Subject

Since its creation in 2009, Bitcoin[1] has risen to be the first and most popular cryptocurrency in the world and has led to the development of many other alternative cryptocurrencies (or Altcoins) looking to stake their claim in a new and fast-moving financial market. It has also been the most popular currency of choice for users of Dark Net markets due to its semi-anonymous qualities, lack of regulation and effectiveness in laundering the profits made from the sales of contraband online. However, Bitcoin has been criticised by users of the Dark Net as lacking genuine anonymity and providing a trail of evidence for law enforcement to trace payments via its blockchain. This has led to an increase in the development of alternative cryptocurrencies (Altcoins) in which anonymity and security is prioritised in order to make the tracing of payments and laundering of proceeds almost impossible.

Bitcoin

Bitcoin is a decentralised, open source, peer-to-peer virtual currency which is used to purchase goods both online and offline. In essence, Bitcoin is a mathematical equation which appears as a string of data, enabling its users to transfer funds directly from one Bitcoin wallet to another without any third parties involved[2]. To avoid forgeries of the currency, all transactions and deposits are approved by other users in the network and stored in a public record known as the blockchain.

Glossary of terms

Altcoins: Any alternative cryptocurrencies to the popular Bitcoin

Cryptocurrency: An online currency that is decentralised and traded for real currency to purchase goods and services

Blockchain: A decentralised public ledger documenting the transactions of all members of the cryptocurrency

Bitcoin wallet: An online address where transactions can be made from and to. Unlike a bank account, no identification is needed to open one.

Masternodes : A feature of Darkcoin representing a series of computers which automatically launder a user's funds, rendering obsolete the necessity for external laundering services

1 Note: When capitalised the noun refers to the virtual system of cash exchange with all its intricate mechanisms of functioning whereas when the noun is in lower case it refers to the currency itself

2 As explained in the GDPO Situation Analysis "Silk Road and Bitcoin"

- Despite having a market capitalisation of 79.5%, a price of $215.36 per bitcoin and a transfer volume of over $17 million[3], the cryptocurrency is nevertheless extremely volatile. Prices have ranged from $1/bitcoin in April 2011 to over $1200/bitcoin in December 2013[4]. Speculative attacks are also widespread: one of the largest attacks led to a collapse of the price from $950/bitcoin on February 1, 2014 to just $260 on February 16, 2014 (a decrease of 72.6% over a span of just 15 days)[5]

- Due to its semi-anonymous properties Bitcoin has been the currency of choice for illicit transactions over the majority of Dark Net marketplaces, with transaction volumes in the realm of hundreds of thousands of dollars per month in the case of large marketplaces such as Silk Road 1.0[6]. Other large marketplaces with listings of over 20,000 items (the majority of which are illicit narcotics) can be assumed to be producing comparable yields.

- Aside from being decentralised Bitcoins can also be easily laundered via mixers or 'tumblers'. These mechanisms launder a user's Bitcoins at a certain cost and transfer back 'clean' Bitcoins which make it difficult for the funds to be linked to any activity previously undertaken by the user. In fact, this is being done so regularly that Dark Net search engine and advertising company 'Grams' offers a Helix Service that has quickly become a popular tumbler choice for customers and vendors of Dark Net markets.

> 'Bitcoin will likely continue to attract cyber criminals who view it as a means to move or steal funds as well as a means of making donations to illicit groups.'
>
> **FBI Bitcoin Threat Assessment, April 2013**

Criminal uses for Bitcoin have been noted by the FBI in its leaked April 2013 *Bitcoin Threat Assessment* which demonstrates how seriously law enforcement agencies have taken the threat. The FBI also noted that Bitcoin is vulnerable to theft. The hacking of Bitcoin exchange Bitstamp saw roughly $5 million stolen. Another alleged hack on Sheep Marketplace (considered a scam by the owner by many of its users) saw the theft of $100 million in Bitcoin from its users.

Despite being considered as an anonymous currency by many, the fact that the Bitcoin blockchain is publicly available erodes its anonymity. Studies have shown that transactions and deposits can be traced from one wallet to another in order to trace payments, which can sometimes help de-anonymise users. Europol therefore classifies Bitcoin with the term "pseudonymity" meaning that there is security in numbers since it is hard to discriminate between the legitimate users of Bitcoin and those who use the cryptocurrency for illicit purposes. When arresting Ross Ulbricht (the alleged mastermind of the Silk Road Marketplace) the FBI were careful to catch him when he was accessing his computer as this allowed them to pin all his Bitcoin transactions to him via obtaining his Bitcoin wallet addresses and then cross-checking those against the blockchain to use as evidence.

3 As of 21 January 2015: Coin Market Cap (2015) Crypto-Currency Market Capitalizations. [Available: http://coin-marketcap.com/. Last accessed 21/01/2015]

4 XE Currency Charts. (2015). XE Currency Charts: Bitcoin to USD. [Available: http://www.xe.com/currency-charts/?from=XBT&to=USD&view=2Y. Last accessed Jan 2015]

5 Ibid

6 See Christin, N. (2012) Traveling the SilkRoad: A Measurement Analysis of a Large Anonymous Online Marketplace. *Carnegie Mellon INI/CyLab* [Available: http://arxiv.org/pdf/1207.7139v1.pdf/. Last accessed 21/01/2015]

Enter Altcoins

There are hundreds of alternatives to Bitcoin and these Altcoins are not all geared towards anonymity. However, due to the attention from law enforcement as well as studies that have shown weaknesses in Bitcoin's anonymising properties, plus the attempts to regulate its use, there is an increasing interest in creating an Altcoin that provides much more security to users who might employ them for illicit purposes.

When it comes to creating an anonymous Altcoin, key factors in development include the removal of the public record such as blockchain as well as the insertion of other anonymising mechanisms into the currency's processes. As such, many Altcoins are already technologically superior to Bitcoin's centralised mixing system:

- **Zerocoin/Zerocash** - Originally proposed by a team at John Hopkins University, Zerocoin worked more or less as an add-on to the Bitcoin protocol allowing a far greater level of anonymity to users. The system allowed Bitcoins to be pooled, swapped for a Zerocoin token and then back into Bitcoin in a way that made backtracing coins to specific wallets almost impossible. Whilst the authors hoped that it would be mass-adopted by the Bitcoin community, the reality proved otherwise. Nevertheless, their method could theoretically be applied to any other Altcoin. They have since reinvented the project into a potential Altcoin named Zerocash which has yet to be released.

- **Monero** – This Altcoin was based on Cryptonote technology and groups transactions into rings before establishing a specific signature for each ring, which makes it impossible for the investigation team to see who sent what and to whom. With a market capitalisation of a mere 0.03%, a price of just $0.2 per Monero, the developers of the currency show no concern with its growth in contrast to its anonymising capacity, and some have considered it a strong contender to the leading anonymous Altcoin: Darkcoin.

Top 10 Crypto-currencies according to their market capitalisation*

1. Bitcoin: 79.50%
2. Ripple: 13.00%
3. Litecoin: 1.20%
4. BitShares: 0.75%
5. PayCoin: 0.69%
6. Stellar: 0.44%
7. Dogecoin: 0.38%
8. Nxt: 0.34%
9. MaidSafeCoin: 0.33%
10. Darkcoin: 0.20%

* Data provided by: http://coinmarketcap.com/

Moving Further Up the Scale: 'Darkcoin'

In terms of anonymity, Darkcoin represents an evolution in technology, employing a mechanism by which various mixing nodes established throughout the system automatically helix (launder) the coins sent from one wallet to the other. It offers an in-built process of obfuscation through its Darksend+ feature, which means that third party outlets such as Bitcoin Fog or Grams are no longer required in order to tumble the coins. Thus, Darkcoin automatically mixes the user's coins through a series of masternodes. In case of a transfer the coins, which are already anonymised through the masternodes, are divided (for example 20 DRK = 8 DRK + 8 DRK + 4 DRK) and sent in a random order to the receiving wallet. Any user can host a masternode for the sum of 1000 DRK, and, once a masternode is established, they will receive 10% of all Darkcoin blocks that are mined. The sole weakness is that someone could buy all the masternodes and corrupt the system, but as long as this is avoided the masternodes remain independent and the system decentralised.

A cryptocurrency needs to have a competitive advantage over Bitcoin in order for it to be adopted by a Dark Net marketplace. It also needs to be relatively stable and have a higher value than the vast bulk of other Altcoins. There are a few, albeit very small Dark Net marketplaces which have accepted Darkcoin, making it the first Altcoin to be accepted on a Dark Net marketplace. In the event that a major marketplace like Agora or Evolution starts accepting an Altcoin then it is very likely that many others will follow.

Bitcoin Vs Altcoins

With enhanced security features, an Altcoin can see its price increasing dramatically due to demand, but it does not mean that it will necessarily become the currency of choice for the wider majority. Darkcoin was one of the cases. Due to the anonymising capacity of its Darksend+ feature, its price rose from $0.75 to $7 in one month since it was launched. One Bitcoin developer, Kristov Atlas, has said that the jump in price was not a speculative bubble, but instead that it was based on the value of the coin. However, the Darksend+ technology's masternodes, which are responsible with automatically mixing the coins, failed repeatedly and despite initial optimist beginnings Darkcoin crashed. This led to a loss of trust in the technology, severely driving its price downwards, with 1DRK now at $1.63

Several Altcoins are technologically superior to Bitcoin, more secure against theft as well as offering the user more anonymity than Bitcoin does with faster transaction rates. They also offer safety in numbers as there are over 500 crypto-currencies being traded online, accounting for a market volume of over $750 million and many have different set-ups and anonymising features. This makes it almost impossible to trace a trail of money that was transferred across several different Altcoins. However solely using a poorly-adopted anonymity-focused cryptocurrency may present a security issue for users, as law enforcement may consider merely adopting it suspicious when there are few legal and popular uses for it and its value is low.

Bitcoin provides pseudonymity, which is not offered by any Altcoin. With Bitcoin people can buy anything from a laptop to groceries and drugs, therefore the pool of users is simply so large that LE has a difficult time narrowing down all the suspects. Moreover, Bitcoin is also regulated in an increasing number of countries, making its users indirectly more anonymous. With regulation, the suspicion that all people using Bitcoin engaged in illicit activity will significantly decrease and consequently the adoption of the cryptocurrency will increase. As people start using Bitcoin on a wider scale, the need to exchange Bitcoin into a fiat currency will also decrease.

No other cryptocurrency has more price stability and widespread adoption than Bitcoin, and that is the reason why most Dark Net Markets are dealing exclusively in Bitcoin and will continue to for the time being.

What next?

Whilst Bitcoin will continue to be the key currency of choice for Dark Net Market users for the foreseeable future, the growth in anonymous Altcoins and anonymising Bitcoin-applicable technology does pose some serious threats to long-term law enforcement strategies to halt illicit trade on Dark Net Markets.

- The birth of cryptocurrencies has allowed even small time drug dealers access to simple, fast and effective money laundering technology, and if used effectively it removes the need for complex shell companies or corrupt bank officials to make it work.
- Law enforcement strategies and capabilities will have to keep up with the fast placed flow of these cryptocurrency markets and technologies if they want any chance of being able to follow a money trail for evidence in cases. If anonymous Altcoins do end up becoming the currency of choice for Dark Net transactions then the likelihood of cryptocurrency money trails being a viable form of evidence in court becomes greatly reduced.

> 'There is a substantial threat to [a] country's finances if more and more transactions for goods and services in the national economy disappear from the tax net'
>
> '…it is well-documented that virtual currencies could provide an alternative channel whereby the proceeds of crime could be used to purchase goods and services'*
>
> **Gareth Murphy, senior official at the Central Bank of Ireland**
>
> * Retreived from: https://coinreport.net/central-bank-of-ireland-official-warns-cryptocurrency-threat/

- If law enforcement increase their capabilities and begin to regularly analyse the Bitcoin blockchain, the famous cryptocurrency can benefit from the developments made by Darkcoin, as Darkcoin's main feature Darksend+ is applicable to Bitcoin clients. Therefore Bitcoin could continue to be the key currency for the Dark Net for the foreseeable future.

- Due to its notoriety and mass adoption Bitcoin will continue to become the primary target of regulation, for example the state of New York recently placed stricter regulations on the use of Bitcoin. Whether or not this will see a rise in the number of people switching to an Altcoin depends on the enforcement of regulation, which is claimed by many in the industry[7] to be very problematic.

- If more legitimate vendors begin to accept Darkcoin and its pseudonymity improves than we could see a shift towards the currency from both users of the Dark Net markets and cryptocurrency enthusiasts or even regular customers. However this depends on whether or not legitimate businesses, many of which have been cautious about accepting bitcoin, will then accept payment from a cryptocurrency that is designed to be impossible to trace.

7 Brito, J. (2013). *US regulations are hampering Bitcoin's growth.* [Available: http://www.theguardian.com/commentis-free/2013/nov/18/bitcoin-senate-hearings-regulation. Last accessed 21/01/2015]

supported by

OPEN SOCIETY FOUNDATIONS

About the Global Drug Policy Observatory

The Global Drug Policy Observatory aims to promote evidence and human rights based drug policy through the comprehensive and rigorous reporting, monitoring and analysis of policy developments at national and international levels. Acting as a platform from which to reach out to and engage with broad and diverse audiences, the initiative aims to help improve the sophistication and horizons of the current policy debate among the media and elite opinion formers as well as within law enforcement and policy making communities. The Observatory engages in a range of research activities that explore not only the dynamics and implications of existing and emerging policy issues, but also the processes behind policy shifts at various levels of governance.

Global Drug Policy Observatory

Research Institute for Arts and Humanities

Room 201 James Callaghan Building

Swansea University

Singleton Park, Swansea SA2 8PP

Tel: +44 (0)1792 604293

www.swansea.ac.uk/gdpo

@gdpo_swan

GdPO Global Drug Policy Observatory

reportingmonitoringanalysis