DOI: 10.20472/BMC.2016.004.018

DOMINIK STROUKAL
University of Finance and Administration, Prague, Czech Republic
BARBORA NEDVĚDOVÁ
University of Economics, Prague, Czech Republic

BITCOIN AND OTHER CRYPTOCURRENCY AS AN INSTRUMENT OF CRIME IN CYBERSPACE

Abstract:

Bitcoin and other cryptocurrencies transformed the trade in illegal goods, especially drugs. Thanks to them in conjunction with other anonymization tools could arise dark markets, illegal marketplaces in cyberspace. Despite active intervention by the authorities, their number and quantity of goods on offer is growing significantly. Besides, we observed a tendency to change the structure of the drug market. This article is next to the description of the operation of dark markets based on identified trends and look to the future of how will dark markets look like. . . . . .

Keywords:

Bitcoin, cryptocurrency, cyberspace, cybercrime, dark web, deep web

Introduction

Cryptocurrencies and particularly bitcoin become widely discussed phenomenon in many areas. Frequent are discussions about technological characteristics and economic contexts (Šurda 2014). Last but not least is also opened a debate on the issue of cybercrime, which can use them to make illicit transactions easier than was previously customary.

Bitcoin is a decentralized P2P currency, which automatically verifies the transactions without requiring a trusted third party. Although founded only in 2009, in 2015, already had a market capitalization of around $3.5 billion. Around this new currency naturally emerged an infrastructure that simplify its use, whether for security or to better the user interface, but there were also individuals and groups using this technology to do crime.

For bitcoin is crucial the invention of blockchain, shared and public ledger of transaction records on the network. This unique technology allows to exchange data without requiring third party verification. Thanks to the open code many so called altcoins, or alternative coins, originated next to bitcoin, some of which works on a similar principle as bitcoin (litecoin, dogecoin) and others embark variously a modified distribution and other characteristics (Ripple, Ethereum, NXT, and other). Blockchain due to its transparency allows for the existence of digital currency without a center, on the other hand, it is possible thanks to its characteristics to move information or records such as money anonymously. Anyone can look anytime in any wallet, but it is difficult if not impossible to link a specific wallet to a specific person.

This key feature of bitcoin led in 2011 to opening of the first so called dark market, or illegal internet marketplace, named Silk Road. This market allowed users to purchase a variety of legal and especially illegal goods over the internet and via bitcoin. In addition, currency regulated only by market laws and not by the state lured individuals who started using it to evade their tax liabilities.

This paper aims to describe the functioning of illegal markets that use bitcoin, and determine the direction of possible future developments.

Cryptocurrency and cybercrime

In October 2013 closed the United States (through the FBI, DEA, IRS and other authorities) Silk Road and arrested its founder Robert Ulbricht, who worked at the site under the nickname Dread Pirate Roberts. Although its size was not even close to the size of the largest centers of drug trafficking (two and a half years of existence facilitate the sale of drugs worth 1.2 billion dollars), it was for the development of cybercrime a significant milestone. For this article it is important that Silk Road allowed to purchase drugs and other illicit goods and services only through bitcoin.

Silk Road functioned on the principle known from large international auction sites such as eBay. Users with anonymous nicknames offer and buy products in legal and illegal categories. Vendors use a system of references after the execution of an exchange, which gave them credibility. The exchange itself was implemented using the postal service to send goods mostly because vendors may not state their personal data. The entire process is fully anonymous and sellers' identities remains undisclosed.

To hide the identity Silk Road existed on the Tor network (The Onion Router), which allows anonymous web browsing, especially for sites with the suffix .onion on which are the Silk Road and other dark markets placed. Tor is a network of thousands of volunteer computers connected to each other through which users connect in a combination that makes their movements virtually untraceable. Sites and marketplaces thus operate outside the supervision of standard browsers and search engines, and it therefore became known collectively as the deep web, specifically dark web, which is generally defined as the illegal part of the deep web.

After closing the Silk Road a number of new dark markets emerged, with famous examples such as the Silk Road 2.0., Sheep Marketplace, Black Market Realoaded, Evolution, Agora, Nucleus or Alphabay. The latter three are currently the largest dark markets. Users learn about the very existence of these dark markets particularly from Reddit, which leads to easy creation of new competition. It is also facilitated through third party services such as darknetsolutions.net (2015).

All modern dark markets, Silk Road and its successors, facilitate the exchange through cryptocurrencies, especially using bitcoin. There are also dark markets using altcoins especially litecoin. The transfer takes place between anonymous wallets and so nobody can track them down unless their owners ascends into the real world and spend money under their real names. Likewise, communication that is not necessary in most stores, is impossible to be tracked, as long as it flows in encrypted form, mostly through PGP.

According to Gwerna (2015) until mid-2015, a total of 85 dark markets were established. Only 6 of them were closed by official authorities (Silk Road, Silk Road 2.0, Blue Sky, TorBazaar, Cloud Nine and Hydra). 10 dark markets were attacked by hackers and closed. The most famous of these was Black Market Reloaded, historically second dark market. Another 22 dark markets were closed voluntarily, and allowed users to withdraw their cryptocurrency. Providers then, according to available information in these markets, did not allow leakage of personal data. One less, 21 dark markets, were closed and robbed the founders and operators themselves. One of them was historically the third dark market Sheep Marketplace and the biggest market of early 2015 - Evolution. The remaining 26 dark markets as of June 2015 has been in operation. Most of dark markets therefore still exists (30%), a large part of them were voluntarily closed (26%), one fewer robbed by their operators (24%), more than a tenth looted by hackers (12%) and least dark markets were closed by the authorities (7%).

After closing the Silk Road and compared to expectations of the authorities the move led to an enormous increase in the number of dark markets. From the six existing until that time (5 of them at the time of closing of the Silk Road including this market operated) their number rose more than fourteen times.

At the same time according to the Digital Citizens Alliance (2015), vendors were increasing the number of products offered. Silk Road closed during the second half of 2013 provided nearly 13,500 offerings and together with other dark markets contained over 18,000 products. A year later were dark markets offering a total of 65,000 products. In the second half of 2015, the figure was about the same. Closing the Silk Road definitely not lead to a decrease in supply.

Problems with robbing their own marketplaces by their own operators were caused mainly due to the need to establish escrow, the custody of funds held by a trusted third party. To ensure the delivery of goods from the seller to the buyer, the buyer's cryptocurrency is sent to the wallet of an operator and the money is released to the seller only after a successful delivery. If the goods are not delivered, cryptocurrency is returned to the buyer. In doubtful cases, the operator acts as a judge. On the other hand, escrow incentivizes the operators to steal the deposited funds, and the likelihood increases with the amount deposited. For this reason, some dark markets decided to implement multisig transactions where the access to the funds is allowed only after a multi-party signature, for example two out of three (buyer, seller and the operator). It is then not possible to steal the money even by the operator, since it difficult to obtain permission to use the stolen bitcons. However, Silk Road and the first dark markets used multisig minimally. But soon marketplaces due to competitive pressures became committed to decentralization and started to implement multisig and other security measures.

Besides dark markets users can find on the dark web also a number of specialized sites that offer just one type of product. Again, this is mostly about drugs, but one can try to buy weapons, fake identity cards and even hire the services of a hacker or an assassin. For a large part of these sites are fraudulent, the last two named are generally considered certain fraud, mainly due to relatively low prices and possibility to prove motivations for the crime itself. Also we lack credible references for these services. As a rule, prices are quoted in US dollars with the conversion to bitcoin according to the current exchange rate.

Discussion

Dark markets include a wide range of products. Although there are no statistics, at first glance, the most common type of goods offered are drugs. Increasing the supply of drugs can be economically considered as an incentive to lower prices and increase the traded quantity. On the other hand, for example Martin (2014) demonstrates that thanks to darknet is the market cleaner and drug trade itself is safer, since it is not

accompanied by a personal encounter with the dealer, which can possibly lead to violence. Martin even shows that some retailers have begun offering drugs that are made in areas unaffected by war or are "fair trade". Aldridge and DeCare-Hetu (2014) confirm these trends and describe how the existence of dark markets works towards reducing violence. They quote many official authorities, such as the European Monitoring Centre for Drugs and Drug Addiction (2015).

Besides cybercrime cryptocurrencies are used and for crime outside the cyberspace. The most straightforward is tax evasion on income in cryptocurrencies. Indeed, there is an incentive not to pay taxes, on the other hand, the entrepreneurs themselves complain about vague and inadequate legislation. In the Czech Republic and in the world there are only a few official statements of monetary or other state authorities to Bitcoin and other cryptocurrencies. The main problem is the ambiguity and determination of the exchange rate between cryptocurrency and a legal tender, since there are significant differences in the tax levied as a result of the volatility and differences between taxes from trade with commodities, money, valuables or other assets. In addition, bitcoin was abused as a ransom required when an anonymous blackmailer demanded payment in bitcoin, otherwise he promised launch of Ebola virus in the Czech Republic (iDnes.cz 2014). Though he has not received the ransom, his threat was not fulfilled.

An important fact for further development of dark markets is their ideological affiliation. Greenberg (2014) says for Wired magazine that in an interview with Silk Road's founder Robert Ulrich he claimed that his motivation was libertarian ideology, which allowed users to buy and sell goods, which, although illegal, does not interfere or destroy ownership of the property of others or their own physical integrity. Silk Road itself actually publicly refused to sell whatever was created to harm other people (Gayathri 2011). So they did not offer stolen credit cards, murders or child porn. They also did not sell guns, but not for ideological but purely practical reasons. The biggest followers of the Silk Road still stick this model. The exception was for example dark market Evolution, which outlawed child pornography, murders, human trafficking and Ponzi schemes, but allowed to offer stolen credit cards or entire identities, which according to references, customers also frequently used. Greenberg (2014) argues that this is a shift towards profit at the expense of ethics, but the following year in March 2015 its own owners robbed Evolution and disappeared with bitcoin worth $12 million.

It is therefore likely that there is a demand for "ethical dark markets" that offer only those services that are unavailable or expensive due to government regulation, but also only with those which do not interfere with the rights of others, namely those who are penalized, despite being victimless crimes. Recently it is even in real politics often to discuss criminalization of drugs. Dark markets possibly reduce the risk of penalties for sale or possession of drugs, effectively bypass anti-drug measures and make them difficult to be enforced. On the other hand, the market does not sell, for example, firearms, since it is difficult to send them securely by mail. It can therefore be assumed

that dark markets will rather focus on those areas where it is easy to send goods by mail and operate where is the difference in price and other costs, including the risks between selling or buying the goods in the real world and dark markets, higher than the cost of buying bitcoin and connect to a dark market. For this reason, today is not profitable for users to buy alcohol on dark markets, but high increase in excise taxes and duties would probably lead to an increase in purchases of alcohol over dark markets. For a similar reason yet insignificant, but growing part of gambling have moved to the world of bitcoin.

Another interesting area for future development is stronger security. While the first Silk Road was secured only minimally, present dark markets use a number of security measures. From decentralized hosting, multisig transactions and double authentication to the option called dead drops. Dead drop is a name for anonymous sending goods not directly to buyers, but rather first to a mediator who for a fee place the goods somewhere in nature or to a location difficult to access without knowledge where shipment is. Then he just sends coordinates to the buyer. In the future we can speculate about mediating role of decentralized automated drones which make the whole system even more secure and possibly even cheaper.

Conclusion

Bitcoin allowed emergence of illegal marketplaces in cyberspace, dark markets. The first of these, the Silk Road, was founded in 2011 and closed in 2013 by US authorities. Since then, their number growed over fourteen times and quantity of offered products has also multiplied. However, significant portion of dark marets was robbed by hackers and their own operators.

Thefts from inside and outside led to several innovations. The first is the introduction of multisig transactions, but we also see effort to transition from Tor to I2P or use altcoins like darkcoin, litecoin or monero. The biggest innovation promises a more decentralized solution combining projects as OpenBazaar (formerly Darkmarket), which plan to use blockchain nott sonly for bitcoin as a means of payment, but also for the marketplace as such, and even for the traditional exchange of money for cryptocurrency and back (Bitsquare). This means that the most vulnerable spot of dark markets, a centralized server that hosts services and manages the money transactions, would be removed. It is difficult to imagine what problems might face this type of service, with the exception of isolated fraud which in turn prevents positive references and further business for the same seller, just as it works in standard auction sites. Additionally, we can expect projects created on a fully anonymous cryptocurrency (Zcash etc.), which in combination with the above innovations can transform the world of dark markets unimaginably.

Moreover, OpenBazaar offers the possibility of decentralized conflict resolution, specifically multisig version of transactions in form 2 out of 3, i.e. the agreement is valid

with at least two of the three actors. Besides the seller and the buyer may someone else have a third key, mostly voluntarily contracted third party, which in the event of a dispute decides to whom to award the money from an unfinished deal. On the other hand, the seller and the buyer must agree to pay her a fee. To find the third party they can use a help of a market, in which these judges offer their services, along with the accompanying references.

At the same time, we confirm the demand for ethical behavior of dark markets. For it is regarded merely to be a place offering such goods and services that do not harm third parties. Dark market as a matter of principle do not offer child pornography, murder and weapons of mass destruction. Offering such services can be a signal to users that operators do not hinder to rob their own dark markets, as it was in the marketplace Evolution. Contrary to expectations, dark markets may not pose an insurmountable problem, moreover, in a world where we are publicly talking about decriminalization of drug use.

Economically it can be shown that drugs are the most common commodity mainly because of the high risk of punishment when caught, the risk of conflict in personal exchange and relatively low transaction costs of buying and selling drugs on dark markets. By contrast, high transaction costs for the sale of firearms, although in terms of the above-described point of view of similar goods, and therefore are offered exceptionally. It can be expected that in the future other major items will be those for which will the difference between the price at dark markets and price when selling in the real world significantly increase. It may be gambling, counterfeited money, alcohol, counterfeited branded goods, with the exception of electronics, or counterfeits of personal documents. It will still be difficult to send electronics by mail. The existence of dark markets must be taken into account when designing economic policy and legislation, as it can reduce or even trump the intended effect of the measure.

References

Aldridge, Judith, a David Décary-Hétu. 2014. *Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation.* SSRN Working Paper.

darknetsolutions.net. 2015. *Darknet Solutions.* 8. 8. www.darknetsolutions.net.

Digital Citizens Alliance. 2015. *Monitoring the Darknet.* 29. 5. www.digitalcitizensalliance.com.

European Monitoring Centre for Drugs and Drug Addiction. 2015. *Drugs supply and the markets.* 1. 6. http://www.emcdda.europa.eu/publications/edr/trends-developments/2015/online/chapter1.

Gayathri, Amrutha. 2011. *From marijuana to LSD, now illegal drugs delivered on your doorstep.* 11. 6. http://www.ibtimes.com/marijuana-lsd-now-illegal-drugs-delivered-your-doorstep-290021.

Greenberg, Andy. 2014. *Dark Web Evolution.* 18. 9. http://www.wired.com/2014/09/dark-web-evolution/.

Gwern. 2015. *Gwern.net.* 7. 6. http://www.gwern.net/Black-market%20survival#analysis.

iDnes.cz. 2014. *Neznámí lidé vydírají Česko, hrozí rozšířením eboly, oznámila policie.* 27. 10. http://zpravy.idnes.cz/neznami-lide-vydiraji-cesko-hrozi-rozsirenim-eboly-fhi-/krimi.aspx?c=A141027_130655_krimi_jav.

Martin, James. 2014. *Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs.* Palgrave Pivot.

Šurda, Peter. 2014. *The Origin, Classification and Utility of Bitcoin.* SSRN Working Paper.