The Use of Cryptocurrency in Money Laundering and Cyber Crime

Erin L. Dickerson

Northeastern University

360 Huntington Avenue

Boston, MA 02115

College of Professional Studies - Master of Arts in Strategic Intelligence and Analysis

ProSeminar 2018

dickerson.e@husky.neu.edu

Executive Summary

Since the inception of Bitcoin in 2009, Bitcoin has been linked to criminal activity in the public mind. The newspaper articles highlighting its use on The Silk Road, an underground marketplace for criminals, were some of the first exposure citizens had to the concept of Bitcoin. But Bitcoin is not inherently evil, it is a neutral digital currency that has the potential for criminal use.

Bitcoin and other cryptocurrencies are an alternative to fiat currency (a currency whose value is backed by government). They are new and constantly evolving, as is the case with most technologies. As a result, they create complicated issues for law enforcement on their own, let alone when combined with other aspects of cyber crime. Thus it is important to understand what Bitcoin is, how it functions, how it can be used, and the fact that it is **not anonymous**. It is absolutely possible to catch and prosecute those who use cryptocurrencies for illicit and illegal purposes, and do it in a way that the return on the investment in enforcement remains high.

This paper proposes the creation of a team or a unit that combines both a direct use of Bitcoins and other cryptocurrencies, with information gathering attacks on Tor and other dark Web systems. The team will have a Bitcoin miner to create a bank of Bitcoins for use in dark Web marketplaces. They will also have the ability to launch Bad Apple, man-in-the-middle, and eavesdropping attacks on Tor browsers. The combination of these two approaches will provide identifying information on criminals looking to launder money and purchase illegal goods and services on dark Web and Tor hidden marketplaces.

This method preys on the fact that most people believe that a) Bitcoin and other cryptocurrencies are anonymous, which they most certainly are not, and b) Tor and other dark Web browsers augment that anonymity. This may be true, but neither of these things are infallible.

It is absolutely possible with an investment in a team and a miner to start actively and effectively investigating and arresting criminals on the dark Web who are looking to use the "anonymity" of Bitcoin and other cryptocurrencies to profit.

Keywords: cryptocurrency, Bitcoin, money-laundering, enforcement, Tor

The Use of Cryptocurrency in Money Laundering and Cyber Crime

Abstract

This paper intends to present a solution to the problem of the use of cryptocurrency in criminal activity and money-laundering. If a reasonable solution is not arrived at in a timely manner, cryptocurrencies will continue to grow in an aggressive way for people to launder money, transfer funds untraced across borders, conduct illegal business, and other undesirable activities. This paper will discuss the basics of cryptocurrency, money laundering, Bitcoin uses in cyber crimes, deanonymizing Bitcoin users, using Bitcoin to catch cyber criminals, and the combined solution. This paper will present a viable solution to catching and preventing those misusing cryptocurrencies.

Cryptocurrency: The Basics

When people think of cryptocurrency they usually think of Bitcoin, the "original" cryptocurrency[1]. Bitcoin was founded in 2008 by a programmer using the pseudonym "Satoshi Nakamoto". Bitcoin and other cryptocurrencies are peer-to-peer ("P2P") digital currencies, meaning that they have no third-party intermediary (such as PayPal or a sovereign bank). This means that in some ways these cryptocurrencies are "decentralized"; they have no sovereign or fiat currency to back them, nor are they backed by a sovereign bank. While Bitcoin and a variety of other cryptocurrencies currently use encryption software called blockchain, there are other encryption processes such as Directed Acyclic Graph ("DAG") which is notably being used by a cryptocurrency called Byteball, and IOTA which is using a variation of DAG. **For the purposes of clarity for this white paper, we will be calling all cryptocurrency "Bitcoin" from this point on**. At this point and for the foreseeable future, DAG and IOTA do not vary from the Bitcoin model enough to provide any further complicating roadblocks.

How it Works

Jan Lansky of the University of Finance and Administration in Prague provides the following definition of cryptocurrencies, including Bitcoin:

1. The system does not require a central authority, [it is] distributed to achieve consensus on its state.
2. The system keeps an overview of cryptocurrency units and their ownership.
3. The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
4. Ownership of cryptocurrency units can be proved exclusively cryptographically.

[1] Cryptocurrencies such as B-Money and BitGold did exist prior to Bitcoin, however they did not last long. The concept of cryptocurrencies as theory has been around since the internet has existed. The concept of decentralized currency has been around for even longer than that.

5. The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
6. If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them. (Lansky, 2018)

The users of Bitcoin are provided with both a public key and a private key. Their public key is similar to a username or identification. Their private key is similar to a password or signature. A transaction must include a peers public key and one's own private key. The transaction then enacts the transference of ownership of Bitcoins.

The blockchain operates as a "public, distributed ledger". The blockchain is transparent; anyone can see it. It is on the blockchain that transactions are verified and double-spending is prevented. In order to verify transactions, a complex mathematical problem must be solved by a peer (usually by providing large amounts of computing power) who is then rewarded with a Bitcoin or a fraction thereof. This process is called "mining".

Wallets

In order to convert fiat money into Bitcoin and conversely convert Bitcoin into fiat money, one needs to utilize something known as a "wallet" or intermediary. The wallet is also needed in order to conduct transactions, as it stores the users public and private encryption keys. There are several different kinds of wallets, including "hot" wallets (those located on some kind of network), and "cold" wallets (stored offline). Many wallet applications exist in many forms to assist users in performing transactions.

Anonymity

It is a common misconception that Bitcoin provides its users with anonymity. Because of the concepts listed above (public- and private-key encryption and blockchain), the most Bitcoin can do is provide pseudonymity. Because public-keys are linked to users and their public-keys are then published to the blockchain each time a transaction occurs, and the blockchain is a transparent record of each transaction, for most users there is a complete record of their Bitcoin history. "It is very difficult to stay anonymous in the Bitcoin network.. Once[2] Bitcoin intermediaries are fully compliant with the bank-secrecy regulations required of traditional financial intermediaries, anonymity will be even less guaranteed, because Bitcoin intermediaries will be required to collect personal data on their customers." (Brito, 2013). However, there are obviously ways around this for those users who would choose to subvert this, which is where issues arise.

Subverting Pseudonymity - Preserving Anonymity

[2] Brito's use of the word "once" here seems optimistic. At the time of writing, there is little to ensure intermediaries comply with bank-secrecy regulations, and nothing promising on the horizon.

As with most internet usage, it is seemingly possible to become anonymous or nearly so while utilizing Bitcoin. The use of a TOR browser as well as an IP spoof or Virtual Private Network ("VPN") all provide layers between a users purported location and identity and their real identity, on top of Bitcoin's original provided pseudonymous public-key.

However, none of these methods of becoming anonymous are foolproof. TOR browsers are subject to man-in-the-middle attacks, Bad Apple attacks, and eavesdropping at entrance and exit nodes. Researchers have shown that P2P networks (including BitTorrent and Bitcoin) used by TOR browsers are especially susceptible to exploiting distributed hash tables ("DHT"). This means that an attacker is "able to reveal a target's IP address by looking it up in the DHT even if the target uses TOR to connect to other peers" (Manils, 2010). These weaknesses (especially Bad Apple attacks) provide ample opportunity for law enforcement to determine if not the identity then at least the Bitcoin pseudonym of a user.

Money Laundering

It is generally agreed that money laundering has three basic stages: "placement, layering, and integration" (Brown, 2016). In the world of cryptocurrency, this involves putting "dirty" money into wallets, purchasing Bitcoin, and then using the purchased Bitcoin to buy goods or services, or withdrawing it again in exchange for fiat money that has now been "washed" and legitimized.

Logistics

For anyone who is not particularly technologically savvy, laundering money through Bitcoin anonymously (or near anonymously) is quite a bit more difficult than laundering fiat money.

Firstly, the launderer (as we will call them) must "smurf" or distribute the dirty cash. This can be done as normal, by depositing the fiat money into various financial institutions in quantities low enough so as to not trigger the Cash Transaction Reporting Systems ("CTRS").

Thereafter the money will have to be transferred from the various bank accounts into either an intermediary (a company or application that connects a user and their bank account with a wallet or Bitcoin) or directly into a wallet for conversion into Bitcoin.

Once the fiat currency has been converted into Bitcoin, it can be transacted, spent and otherwise "laundered" and then placed into a new wallet, then sent to an intermediary or wallet for withdrawal into an international bank account, and then transferred back into a U.S. account.

Alternatively, "smurfing" can be done by dispersing the fiat currency to associates in countries such as Romania, where Bitcoin can literally be bought at a "free-standing electronic

payment console" using a single use phone and a single use email address with minimal personal information provided.

Problems with Laundering Money this Way

At the time of writing there are several inherent issues and risks with laundering money using Bitcoin. These include but are not limited to:

1. Market volatility;
2. Arduousness of withdrawing Bitcoin and converting to fiat currency;
3. Perceived anonymity but actual pseudonymity;
4. Tediousness of attempting to preserve anonymity; and,
5. Risk of total loss by fraud or loss of private-key or other means.

These liabilities reduce the draw of Bitcoin to criminals who would potentially use Bitcoin as a method of laundering money, however there are additional approaches to making Bitcoin unattractive to criminals and finding those who are determined enough to use it anyway.

Bitcoin Uses in Cyber Crimes

Bitcoin, like cash, can be used for many different purposes. It is inherently a neutral object until someone acts on it. Unfortunately for it, it has been inextricably tied to criminal marketplaces such as The Silk Road. "The Silk Road Online Anonymous Marketplace (Silk Road) was an anonymous online marketplace that emerged in the deep web in 2011." (Phelps, 2014). The Silk Road was known as "an eBay for drugs" (Phelps, 2014), but that is hardly the extent of their market. It was also a place to buy class-A narcotics, art and antiquities (illegally obtained, naturally), hitmen-for-hire, and a plethora of other goods and services. Their payment of choice was Bitcoin due to the perceived anonymity of it. Certainly, Bitcoin affords a client and seller greater privacy than bank transfers, but it is important to note that as with anything, it is not infallible.

Deanonymizing Bitcoin Users

An April 11, 2018 study has shown that "using Bitcoin as a payment method is a serious threat to the anonymity of Tor hidden services and their users. Yet, Bitcoin is the most popular choice for these services for accepting donations or selling merchandise." (Jawaheri, 2018). It shows that "using Bitcoin as payment method for Tor hidden services leaks information that can be used to deanonymize their users. This represents a serious threat to these users, because they actively seek to maintain their anonymity by using Tor. The deanonymization is mainly due to the lack of retroactive operational security present in Bitcoin's pseudonymity model. In particular, by inspecting historical transactions in the blockchain, an adversary can link users, who publicly share their Bitcoin addresses on online social networks, within hidden services, which publicly share their Bitcoin addresses on their onion landing pages." (Jawaheri, 2018).

The most important takeaway from this study is that "Bitcoin addresses should always be assumed compromised as they can be used to deanonymize users" (Jawaheri, 2018).

A 2010 study explains how to exploit P2P information leakage on Tor, which is extremely useful as Bitcoin is a P2P system. This particular study is on BitTorrent, which is a different P2P system, but the concepts are applicable to Bitcoin. Anyone can "host a Tor exit node, [so] performing the attacks described" is absolutely possible. (Manils, 2010). By hosting a Tor exit node, it is possible to view users utilizing Bitcoin, harvest their IP addresses, and then authenticate their IP addresses thereafter.

Another potential method for gaining useable information from users is "exploiting the DHT" (Distributed Hash Table). Tor browsers do not allow DHT connections, thus DHT attacks push the user to connect to the DHT "using the public network interface and publishes its public IP and listening port into the DHT".

Using Bitcoin to Catch Cyber Criminals

In 2017, a Benton County, Arkansas Sheriff's Office implemented a program to enhance their capability of catching cyber criminals. Detective Olin Rankin lent the sheriff's office his personal Bitcoin mining equipment, and the sheriff's office kept their mined Bitcoin in an offline hardware wallet. The department managed to earn a number of Bitcoins. In order to keep the source of Bitcoin "clean", it is important to mine the coin rather than purchase it.

Until the implementation of this program, the vice division was brutally behind the times in the cyber crimes department. They were familiar with the dark Web and many Tor hidden services, but were unable to use Bitcoin to interact with these services. For example, "when the sheriff's office previously posted ads [on Tor hidden sites] prior to using Bitcoin, they had problems getting the ads at the top of the page, drastically affecting the efficiency of their operations." (Zimmer, 2018). By having a Bitcoin reserve for the operation team at the sheriff's office, the team was able to "buy their way into other dark web illicit activities, such as child exploitation rings".

Vice crimes at this particular agency claims to be frustrated with the fact that "the agency may never trace the illicit activities to an individual" based on the false assumption that Bitcoin is anonymous unless the user makes a mistake and "turns the Bitcoin into cash… at an exchange that's in the U.S." (Zimmer, 2018). Based on the previous section we know this is not true. It is entirely possible to deanonymize the user.

The Combined Solution

The most potent way to approach the issue of illegal use of Bitcoin is a two pronged attack. It is easy to see that the path of the Benton County sheriff's office, while admirable and forward thinking, is only a part of the sum total. Conversely, while it is possible to operate solely on the deanonymized user information provided by Bad Apple and man-in-the-middle

attacks (etc.) on Tor browser interactions with Bitcoin, doing so will not provide the complete picture either. Thus, the two pronged approach.

The first step is to create a dedicated unit within the cyber crimes division which will focus on Bitcoin. This unit should have a Bitcoin miner to mine coins for use in criminal transactions and sting operations. These Bitcoins will prove useful for a multitude of investigations into criminals operating on the dark Web and Tor hidden services. As shown in the Benton County, Arkansas example, they will prove an effective tool for both those in the field and analysts. However, unlike those in the sheriff's office in Benton, a further step must be taken.

The cyber crimes units' use of Bitcoins must also be combined with data gathering and analysis done by this same unit. Employees must be hired who have knowledge of and talent for running deanonymizing attacks on Tor clients and Bitcoin users who are suspected of laundering money or using Bitcoin for other illicit and illegal means. It is imperative for the government to stay current with the technology being used by criminal enterprises.

For example, Alice works for Homeland Security in this new Cryptocurrency Crimes Unit ("CCU"). Her supervisor has been running a Bitcoin miner for the last three weeks and has made enough money for Alice to conduct an operation on The Silk Road (no longer in existence, thanks to a lot of great effort from law enforcement, but there are a lot of Tor hidden marketplaces that are similar, so we will use it for illustrative purposes). Alice places an ad on The Silk Road advertising fake passports for sale, which costs her a fraction of a Bitcoin. Bob answers the ad, and Alice uses the unit's secondary wallet for Bob to send his Bitcoins to. After the transaction, Alice has Bob's public-encryption key (and Bob has Alice's secondary wallet's public-encryption key). If this was Benton County, Arkansas, that would be all Alice had to go on, which would make it a lot harder to find Bob's true identity.* Since we've set up a two-pronged attack though, we already had Cynthia set up a Distributed Hash Table ("DHT") attack. We know Bob is using a Tor browser (since he had to, in order to access The Silk Road). By sending him a DHT attack, we push him (without his knowledge) into a public domain browser, thereby revealing his IP address while he is interacting with Alice. With Bob's IP address, we can gain all kinds of information about Bob, including who he is and where he lives.

*Alternatively, even with just Bob's public-encryption key it is not impossible to discover Bob's true identity and the identity of co-conspirators. Bob is likely to have posted his public-encryption key on his social profiles, especially those he thinks are safe or anonymous such as those on the dark Web. With Bob's public key, we can look on blockchains for patterns of transactions for the public keys of those he regularly does business with as well.

Conclusion

Bitcoin and other cryptocurrencies seem relatively new as compared to fiat currencies. They pose complex problems to law enforcement, especially when looked at behind the obscured glass of the dark Web and Tor browsers that most criminals use. To lift the fog and begin

catching lawbreakers in earnest, it is crucial to first understand what one is dealing with. Once one has a firm grasp on the "what" of Bitcoins and cryptocurrency (as well as their accoutrements like wallets, intermediaries, blockchains, etc.), it is then possible to begin tackling the "how" of catching and prosecuting those who misuse them.

It is important to note that only a team that combines both the direct use of Bitcoins and other cryptocurrencies with information gathering attacks on Tor (and other dark web systems) will be successful on this front. A team like that in Benton County, Arkansas which only has use of Bitcoins will have little success identifying the criminal with only the information gained in the transaction. A team that only launches information gathering attacks will be overbroad and time wasting, a sure waste of resources that will inevitably and inadvertently target those who are utilizing cryptocurrencies in a legal way.

Although policymakers are and will be looking at regulating both cryptocurrencies and intermediaries (like wallets), it is important to act now rather than wait for those regulations to come into effect. There is currently no consensus on whether Bitcoin is a currency or a security, a commodity or money. The International Monetary Fund is still in talks with the World Trade Organization over who has jurisdiction over it. It may be a long time (or never) before the United States and the world sees a cohesive viewpoint on how to treat Bitcoin.

It is best to take a proactive, anti-criminal stand on Bitcoin now rather than later.

References

Akhoondi, M., Yu, C., & Madhyastha, H. V. (2014). LASTor: A Low-Latency AS-Aware Tor Client. *Networking, IEEE/ACM Transactions on,22*(6), 1742-1755. doi:10.1109/TNET.2013.2291242

BoE push for cryptocurrency regulation will boost crypto market, says deVere. (2018). *Banking Newslink*.

Bradbury, D. (2014). Unveiling the dark web. *Network Security, 2014*(4), 14-17. doi:10.1016/s1353-4858(14)70042-x

Brito, J., & Castillo, A. M. (2016). *Bitcoin: A primer for policymakers*. Arlington, VA: Mercatus Center at George Mason University.

Brown, S. D. (2016). Cryptocurrency and criminality. *The Police Journal: Theory, Practice and Principles, 89*(4), 327-339. doi:10.1177/0032258X16658927

Financial Action Task Force. (2016). *International standards on combating money laundering and the financing of terrorism & proliferation: The FATF recommendations*. Financial Action Task Force. Retrieved May 03, 2018, from http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

Greenberg, A. (2017, June 03). 'Dark Wallet' is about to make Bitcoin money laundering easier than ever. Retrieved from https://www.wired.com/2014/04/dark-wallet/

Guadamuz, A., & Marsden, C. (2015). Blockchains and Bitcoin: Regulatory responses to cryptocurrencies. *First Monday, 20*(12). doi:10.5210/fm.v20i12.6198

Hughes, S. J., & Middlebrook, S. T. (2015). Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries. *Yale Journal on Regulation, 32*, 495-591.

Jawaheri, H. A., Sabah, M. A., Boshmaf, Y., & Erbad, A. (2018). When A Small Leak Sinks A Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis.

Lansky, J. (2018). Possible State Approaches to Cryptocurrencies. *Journal of Systems Integration, 9*(1), 19-32. doi:10.20470/jsi.v9i1.335

Manils, P., Abdelberri, C., Blond, S. L., Kaafar, M. A., Castelluccia, C., Legout, A., & Dabbous, W. (2010). Compromising Tor Anonymity Exploiting P2P Information Leakage.

Meltzer, P. (1991). Keeping Drug Money from Reaching the Wash Cycle: A Guide to the Bank Secrecy Act. *The Banking Law Journal, 108*(3), 230.

Paul, K. A. (2018). Ancient Artifacts vs. Digital Artifacts: New Tools for Unmasking the Sale of Illicit Antiquities on the Dark Web. *Arts, 7*(2), 12. doi:10.3390/arts7020012

Phelps, A., & Watt, A. (2014). I shop online recreationally! Internet anonymity and Silk Road enabling drug use in Australia. *Digital Investigation, 11*(4), 261-272. doi:10.1016/j.diin.2014.08.001

Rozen, M. (2017). Cryptocurrency: A Regulatory Frontier. *Corporate Counsel, 24*(12), 19-20.

Sovbetov, Y. (2018). Factors Influencing Cryptocurrency Prices: Evidence from Bitcoin, Ethereum, Dash, Litcoin, and Monero. *Journal of Economics and Financial Analysis, 2*(2), 1-27. doi:10.1991/jefa.v2i2.a16

Suirelav. (2017, December 27). Introduction to Byteball - Part 2: The DAG. Retrieved from https://medium.com/@Suirelav/introduction-to-byteball-part-2-the-dag-ce84ca4c4e01

Zimmer, A. (2018, April). Arkansas Agency Catches Criminals with Cryptocurrency. *Law Enforcement Technology*. Retrieved from https://www.officer.com/investigations/article/20996785/alabama-agency-catches-criminals-with-cryptocurrency