Benjamin Miller

Professor Laboon

CS1699 Special Topics

12 December 2018

The Impact of Blockchain on Black Markets and Money Laundering

The invention of Bitcoin as an online pseudo-anonymous cryptocurrency has had a tremendous impact upon the world’s economy, as well as fields ranging from philosophy to ecology. The success of the blockchain technology Bitcoin revolutionized has been unparalleled, and has inspired the creation of countless online currencies, social networks, and online marketplaces. However innovation tends to benefit those who capitalize upon it, and criminals and their organizations are no exception. Cryptocurrency properties of decentralization, anonymity, pseudo-anonymity, exchangeability, transportability and availability presents criminal organizations a fantastic solution to the difficulties of money laundering.

Money laundering, as defined by the the U.S. Treasury’s Financial Crimes Enforcement Network as a three step process that turn illegally-gained proceeds (‘dirty money’ or property\_ appear legal (‘clean’). This process includes, “1) placing dirty money in the legitimate financial system, 2) layering it within additional transactions to obfuscate its origins, and 3) integrating it into the financial system with more transactions so the funds appear licit”.1 Traditional money-laundering schemes involving fiat money have many variations, those of which that exist on a large-scale have the most to gain from cryptocurrency. Pertinent examples would be those of casino laundering, bulk cash smuggling, shell companies and real-estate laundering.

In a casino laundering scheme, ‘dirty money’ is cleaned by purchasing casino chips, playing for a while, and cashing out claiming the now clean money as winnings. Step one of laundering yields little risk to money-holder, as there are no steps between the money-holders hand and the casino, who doesn’t have the means to validate the money’s origins. Playing the casino serves layers the dirty money, hiding its initial value. Cashing out returns a sum of clean money that cannot as directly be linked to the sum of dirty money.

A bulk cash smuggling scheme is a money-laundering scheme that can be seen as the most direct beneficiary of cryptocurrency. In this scheme, criminals literally smuggle dirty money into another country. There it is deposited into an offshore bank or similar financial institution that honors client secrecy. Examples of these types of institutions are the infamous banks of Switzerland and the Cayman islands, that are expected to privately hold between $21 and $31 trillion dollars.2

These money laundering schemes tend to be quite successful, but still find issues when it comes to scalability. Large enough sums of dirty money, are generally much easier for law enforcement agencies to trace and prevent from being cleaned. For this reason, large-scale laundering operations involve increasing order of complexity, that begin to involve shell corporations, real estate trading, large-scale embezzlement and banking transactions that increase both barrier-to-entry and risk. In general, all of these schemes end with money in a private offshore bank, slowly and quietly feeding back into the accounts of its owners. To bring things back to the steps defined previously, steps 1 and 3 of entering and exiting are easy and simple, yet step 2 of obfuscating is complex.

During step 2, the dirty money and goods flow through a series of subsidiaries and entities generally owned by the launderers. These entities have a high degree of linkability to their owners, making them targets of law enforcement.

It is here that cryptocurrency can ameliorate such problems of the criminally rich. Bitcoin has been used for exactly this purpose, making it an effective case study. As mentioned earlier, Bitcoin provides its users with pseudo-anonymity. This is accomplished by assigning users with a public/private keypair represented by randomly-generated numbers. Because millions, if not trillions of these addresses are generated every day, can be generated by the same or different people, they can be used as a user’s pseudo identity. In order to spend in Bitcoin, a user chooses which public address they wish to send coin to, and generates a transaction that only shows a pseudo identity as the seller.

When Bitcoin is paired with Tor, a browsing engine that securely hides a client/server’s IP-address, it becomes an international criminal’s dream. A dream realized by Ross Ulbricht when he allegedly created the Silk Road, an online black market that saw the transfer of illegal goods and services from hard drugs to assassination bounties. The Silk Road a rousing success, a reputation as *the* black market. Current analysis of the bitcoin blockchain shows that it accounted for 90% of all illicit laundering activity in 2013, and approximately $23 million in transactions per year, in the final year of its operation.

The Silk Road was closed after a two year investigation, involving numerous law enforcement agencies including the FBI and NSA. It was seen as a major victory, as the most successful online black market had been taken down. This was accomplished almost entirely due to slip-ups by Ross Ulbricht, who was the subject what’s know in bitcoin as “deanonymization via side-channels.” By reusing online identities as well as his personal name and email to conduct Silk Road business, Ulbrecht forfeited his anonymity. However despite the termination of the Silk Road, the numerous black markets that exist today tells us that the proverbial cat was already let out of the bag. A quote from “Heisenberg 2.0,” a supposed creator of Silk Road 2.0 perfectly explains how this was the case.

*From a quick scout I’ve counted at least 5 publicly stated projects with said aim of replacing becoming “Silk Road 2.0” … And this is what Law Enforcement is now parading as a victory? Over two youear of investigation, millions of dollars spent and for what so a couple of armchair programmers can build it again in a few days while in the meantime vendors simply move to other sites.*

Heisenberg points out that the blockchain and secure browsing technology had already made the leap to black market applications, and would never go back. This remains true, as black markets like Silk Road 2.0, AlphaBay, and Agora emerged in just the three years since Ulbricht’s arrest. In order to combat online black markets and cryptocurrency money laundering, policy makers have to begin regulating the entities that enable ‘dirty’ crypto coins to become ‘clean.’

Since the days of the first Silk Road, analysis tools like Elliptic have been developed, and allow researchers to better understand the existing blockchain based laundering schemes. A study by the Center on Sanctions & Illicit Finance completed a study in early 2018 that traced Bitcoins with known illicit origins (step 1) to the conversion services that either obscured their origins (step 2) or expelled them as cleaned currency( step 3). The greatest portions of these services were Bitcoin Exchanges, Online Gambling Services, and Mixers.

The study showed that Mixers and Online Gambling services account for about 66-70% of laundering activity. These services obfuscate a Bitcoin’s origins by hiding a transaction’s sender, receiver, and amount while maintaining its validity on the blockchain. This is done with extreme ease, especially in comparison to the elaborate shell company operation and asset smuggling in traditional laundering schemes.

The study also defines coin exchanges as the main source of cashing out bitcoin for fiat money. Here, exchanges operate much like our traditional laundering schemes’ foreign banks as the exit point of the laundering scheme. And thus a clear picture of a modern crypto currency laundering platform is complete. A black market vender accepts payment for their service in bitcoin. Then uses a series of mixers to bounce the coins between a series of fresh pseudo-identities they own, and finally uses an exchange to cash out some of their Bitcoin into fiat money which can be managed just as traditionally laundered money.

The efforts of policy makers to regulate and prevent such successful cryptocurrency money laundering have run into roadblocks that have been previously present in regulating traditional money-laundering. The countries that have sought to regulate, have had success domestically. Large U.S. based coin exchanges have agreed to conform to KYC (know your customer) and AML (anti money-laundering) laws that mostly keep them from criminal use. However there are some countries who prefer the benefits of leaving coin exchanges unregulated for economic growth, leaving regulation coalitions somewhat powerless to stop them.

Until more globalized regulation that prevents blockchain laundering becomes law, it is difficult to see online black markets and cryptocurrency money-laundering ending any time soon. As policy makers fight to keep up with problems nearly half-a-decade old new blockchain technology like Monero, an alternate cryptocurrency using ring-signatures and stealth-addresses for complete anonymity, stack the odds ever more in the e-criminal’s favor.

**Works Cited**

Fanusie, Y., and Tom Robinson. "Bitcoin laundering: an analysis of illicit flows into digital currency services." *Center on Sanctions & Illicit Finance memorandum, January* (2018).

Allen, Frederick E. “Super Rich Hide $21 Trillion Offshore, Study Says.” *Forbes*, Forbes Magazine, 6 Sept. 2012, www.forbes.com/sites/frederickallen/2012/07/23/super-rich-hide-21-trillion-offshore-study-says/#60bd744d6ba6.

Biggs, John. “Deep Web Users Are Ready To Launch Silk Road 2.0.” *TechCrunch*, TechCrunch, 4 Oct. 2013, techcrunch.com/2013/10/04/deep-web-users-are-ready-to-launch-silk-road-2-0/.

“Bitcoin Merchant Services.” *The Digital Currency Challenge*, doi:10.1057/9781137382559.0023.

Dyson, Simon, et al. “The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime.” *The Journal of the British Blockchain Association*, vol. 1, no. 2, Apr. 2018, pp. 1–6., doi:10.31585/jbba-1-2-(8)2018.

“Money Laundering - Definition, Examples, Meaning, and Cases.” *Legal Dictionary*, 29 Oct. 2018, legaldictionary.net/money-laundering/.

Trautman, and Lawrence J. “Virtual Currencies; Bitcoin &amp; What Now after Liberty Reserve, Silk Road, and Mt. Gox?” *By Lawrence J. Trautman :: SSRN*, 11 Feb. 2014, https://tinyurl.com/y759kanh.

Zetter, Kim. “How the Feds Took Down the Silk Road Drug Wonderland.” *Wired*, Conde Nast, 3 June 2017, www.wired.com/2013/11/silk-road/.