Haileybury MUN
Research report

General Assembly 2

The question of electronic money laundering

By: Ghina Sabeh Aayoun

Definitions of Key Terms:

Money Laundering

Money laundering is the generic term used to describe the process by which criminals disguise the original source of the revenue of criminal activity by making such proceeds appear to have come from a legitimate source in order to stay away from the suspicion of the law and avoid leaving a trail of implicating evidence.

Shell companies

Shell companies are companies that appear to the outside as real and working except they do not have any actual assets and perform no real business.

Cryptocurrency

A cryptocurrency is a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank. It is not attached to a state of government, so it has no central issuing authority or regulatory body.

Private/Public Key

A private key is a secret number that allows Bitcoin to be spent. Every Bitcoin wallet contains one or more private keys, which are saved in the wallet file. The private keys are mathematically related to all Bitcoin addresses generated for the wallet.

A public key is used to ensure you are the owner of an address that can receive funds.

Wallet

A crypto-currency wallet is a software program that stores private and public keys and interacts with various blockchain to enable users to send and receive digital currency and monitor their balance

Block chain

A ledger of past transactions is called the block chain as it is a chain of blocks. The block chain serves to confirm transactions to the rest of the network as having taken place.

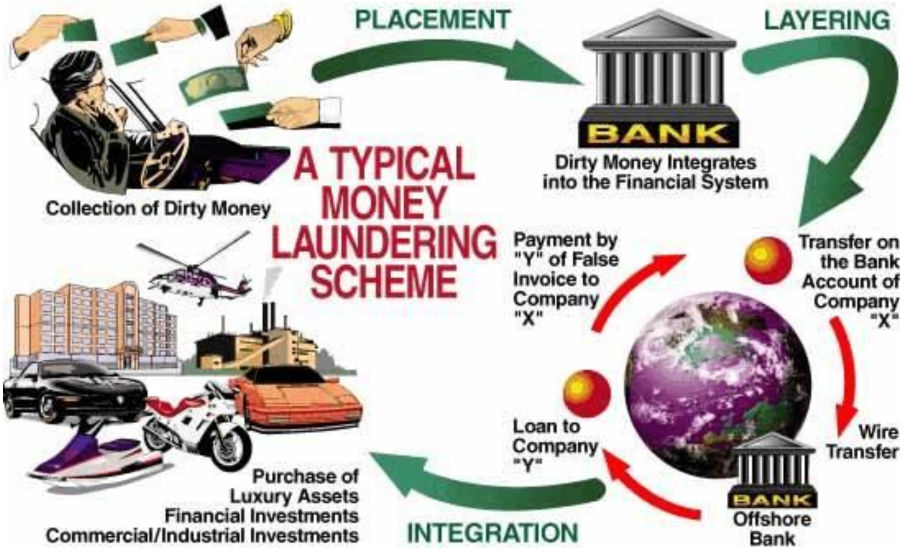
Miners

Bitcoin mining is the process of adding transaction records to Bitcoin's public ledger of past transactions or blockchain

Introduction

Money is the prime reason behind a person's participation in criminal activity. When such money is gained, criminals resort to a process called "money laundering" to "clean" the "dirty" money earned through crime and make it seem like it originated from a legitimate source. The money-laundering cycle can be broken down into three distinct stages; however, it is important to remember that money-laundering is a single process. The stages of money-laundering include:

- The unlawful procedure that gets the cash (known as Placement),
  - i.e.: selling of drugs;
- A complex arrangement of exchanges performed by the launderer (known as Layering),
  - i.e.: the use of shell companies;
- The indirect return of the "laundered" money to the criminal that owns it (known as Integration)


PLACEMENT
LAYERING
A TYPICAL MONEY LAUNDERING SCHEME
Collection of Dirty Money
BANK
Dirty Money Integrates into the Financial System
Payment by "Y" of False Invoice to Company "X"
Transfer on the Bank Account of Company "X"
Wire Transfer
Loan to Company "Y"
BANK
Offshore Bank
Purchase of Luxury Assets
Financial Investments
Commercial/Industrial Investments
INTEGRATION

Picture 1 - UNODC Official Website

Money Laundering makes it easier for corruption to spread and can also destabilize the economies of vulnerable nations. In addition to this, it compromises the legitimacy of financial systems and organizations, giving organized criminal groups the amount it requires to commit further criminal exercises.Money laundering also reduces tax revenue as it becomes difficult for the government to collect revenue from related transactions which frequently take place in the underground economy, making this issue an extremely important one that should be urgently addressed.

As criminals seek new methods of money laundering, the online space has proved to be a very resourceful outlet. With the unbelievable technology development that the world has seen, many banks around the globe have switched to binary, creating a single global information space where people can manage their assets, enter into agreements and make fast transactions without any personal contact. That information space becomes a platform and an instrument of a crime, opening up the world to electronic money laundering. Electronic money laundering, also known as Transaction Laundering, is the most common, but least enforced, method of money laundering. The principle is simple: an unknown online business uses an approved merchant's payment credentials to process credit card transactions for unknown products and services. For example, a cyber-criminal can set up a website in a matter of minutes, accepting payment via card, and disguise their income from illegal activities by rerouting payments through a legitimate merchant account, like an online book shop.

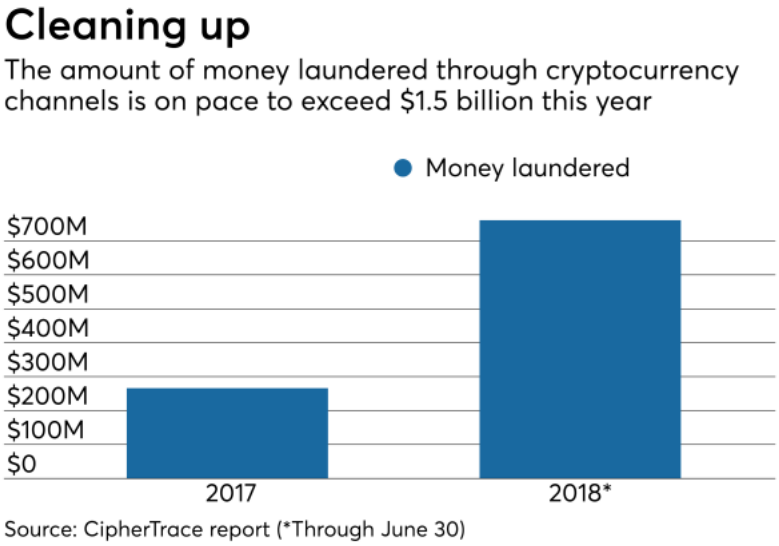
Transaction laundering is especially attractive to criminals due to the following factors:

- the transfer of monetary values in electronic form both between users (peer-to-peer) and between a user and a system merchant, do not necessarily have to go through the intervention of either a centralised structure or the traditional financial intermediaries
- the transfer of monetary values is indifferent to geographical distances and barriers.
- it offers an opportunity to “spread” a financial crime across different jurisdictions: thus, a crime can be committed in one country and then be judged in another country
- it is simple, fast, and has low cost
- electronic services are easy to hack and are therefore easier to launder money from.

Money Laundering makes it easier for corruption to spread and can also destabilize the economies of vulnerable nations. In addition to this, it compromises the legitimacy of financial systems and organizations, giving organized criminal groups the amount it requires to commit further criminal exercises.
Money laundering also reduces tax revenue as it becomes difficult for the government to collect revenue from related transactions which frequently take place in the underground economy.

Key Statistics:

In the last decade, the world has seen a rise in cryptocurrency. The cryptocurrency market is still considered very new and not many people are familiar with the industry. The semi-anonymous and decentralized nature of many cryptocurrencies has meant that authorities fear that certain platforms could be used for money laundering. In 2017 the value of Bitcoin increased massively, reaching $16,000 on Dec. 27th, 2017 and $17,500 on January 7th, 2018.
According to the 2018Cipher Trace Q4 Cryptocurrency Anti-Money Laundering (AML) Report reveals that $1.7 billion in cryptocurrency was stolen and scammed in 2018, a dramatic rise in criminal activity despite a slump in the market. Theft from cryptocurrency exchanges accounted for the majority of the criminal activity: more than $950 million was stolen by hackers in 2018, representing 3.6 times more than in 2017.



The report also identifies the Top 10 Trending Crypto Threats, providing actionable threat intelligence for anyone dealing with cryptocurrency:

1. SIM swapping: An identity theft technique that hacks a victim's mobile device to pilfer credentials and hijack wallets or exchange accounts to steal cryptocurrency.
2. Crypto dusting: A new form of blockchain spam that slowly destroys the recipient's reputation by sending cryptocurrency from known money mixers.
3. Sanction evasion: Iranian and Venezuelan governments are examples of nation states that use cryptocurrencies to avoid sanctions imposed onto them by other countries.

4. Next-generation crypto mixers: Money laundering services that promise to exchange dirty tokens for freshly mined crypto, but, in reality, launder cryptocurrency through exchanges.
5. Shadow money service businesses (MSBs): Unlicensed MSBs that bank cryptocurrency without the knowledge of host financial institutions, thus exposing banks to unknown risk.
6. Datacenter-scale crypto-jacking: Takeover attacks that mine for cryptocurrency at a massive scale and that have been discovered in datacenters, including AWS.
7. Lightning Network transactions: Enabling anonymous bitcoin transactions by going "off-chain" and now scaling to $2,150,000.
8. Decentralized stable coins: Stabilized tokens that can be designed for use as hard-to-trace private coins.
9. Email extortion and bomb threats: Mass-customized phishing email campaigns by cyber-extortionists using old passwords and spouse names and that demand bitcoin. Bomb threat extortion scams spiked in December.
10. Crypto robbing ransomware: New malware distributed by cyber-extortionists that empties cryptocurrency wallets and steals private keys while holding user data hostage.

In our current times, transaction laundering has proven to be the source of financing for numerous terror attacks, namely the violent attack on the offices of French satire magazine Charlie Hebdo. More so, the FBI recently announced that ISIS was using Transaction Laundering to finance a US domestic terror agenda through eBay and PayPal. According to The Wall Street Journal, the FBI revealed that an American-born ISIS militant and US citizen was arrested after he received nearly $10,000 via PayPal for fraudulent sales of counterfeit computer printers through eBay. The Daily Beast also recently reported that Russian criminals are using Airbnb to cleanse illicit money from stolen credit cards. Unlike other Transaction Laundering cases, the Airbnb instance also involves fraudulent, complicit hosts instead of merchants, who all participate in the exploitation of Airbnb's online marketplace to conduct illegal activity. The scam is simple: criminals use stolen credits cards to launder the illicit money through complicit Airbnb hosts they meet in underground, online forums. Once the Airbnb booking transaction is completed, no one actually stays at the advertised accommodation; instead the two parties split the payment and create fake end-of-stay reviews to close the transactional loop.

The international effort to develop and implement effective anti-money laundering controls is persistent. The United Nations Office for Drug Control and Crime Prevention (UNODCCP), the Financial Action Task Force (FATF), the Caribbean Financial Action Task Force (CFATF), the Organization of American States Inter-American Drug Control Commission (OAS-CICAD), the Inter-American Development Bank (IDB), the European Commission, the Council of Europe, the Asia Pacific Group on Money Laundering (APG), the Offshore Group of Banking Supervisors (OGBS), the Basle Committee on Banking Supervision, Interpol, the World Customs Organization (WCO), and the Egmont Group of Financial Intelligence Units – are all international organizations that aim to develop anti-money laundering laws and regulations. However, regulators are finally catching up with electronic money. Anti-Money Laundering regulations are starting to sync with the digital world. There are an estimated 40 million e-commerce websites worldwide, making manual monitoring processes inefficient and overall impossible. But as new technologies such as "Regulatory Technology", or "RegTech" advanced, the detection and prevention of Transaction Laundering becomes easier, as it integrates a shared responsibility among law enforcement agencies, e-commerce players, and individual users. With the right digital tools in place, electronic money laundering can be detected, and ultimately intercepted. After a decade of hiding their illicit practices behind the computer screen, e-money launderers have good reason to be worried.

Possible solutions:

- Tackling the issue of monitoring cryptocurrencies
    - Installing a regulatory body that uses artificial intelligence to detect and intercept transaction laundering (i.e. RegTech)

  - Sharing responsibility of such monitoring processes with individuals considering the large e-commerce-based websites spread across the web

- Tackling the issue of public ignorance towards money laundering and electronic money laundering through raising awareness about
  - How cryptocurrencies work
  - How transaction laundering happens
  - How to protect yourself from e-launderers,
  - How to detect transaction laundering
  - How to properly report or intercept transaction laundering

Recommended Cites:

1. https://www.unodc.org/
2. http://www.unodc.org/unodc/en/money-laundering/laundrycycle.html
3. http://www.fatf-gafi.org/
4. https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm
5. https://www.state.gov/j/inl/rls/nrcrpt/2015/vol2/239471.htm
6. https://ciphertrace.com/crypto-aml-report-2018q4/ - contains useful statistics for the year 2018
7. https://knepublishing.com/index.php/Kne-Social/article/view/1581/3731- a lot of useful information around the topic

References:

1. Giorgio Merlonghi, (2010),"Fighting financial crime in the age of electronic money: opportunities and limitations", Journal of Money Laundering Control, Vol. 13 Issue 3 pp. 202 – 214 http://dx.doi.org/10.1108/13685201011057118
2. “United Nations Global Programme against Money Laundering Proceeds of Crime, and the Financing of Terrorism.” U.S. Department of State, U.S. Department of State, www.state.gov/j/inl/rls/nrcrpt/2015/vol2/239471.htm.
3. IMF, www.imf.org/external/np/leg/amlcft/eng/aml1.htm.
4. “Latest News.” FATF-GAFI.ORG - Financial Action Task Force (FATF), www.fatf-gafi.org/.
5. Локшина, Юлия. На Схемы Наложили Взыскание. 2 Feb. 2017, www.kommersant.ru/doc/3208167.
6. “ЦБ Указал Банкам Способы Борьбы с Новой Схемой Отмывания Денег.” РБК, www.rbc.ru/finances/07/02/2017/5898c55b9a7947265d4eb0c3.
7. “Прачечная Со Скидкой: Как Telegram Используют Для Отмывания Денег.” РБК, www.rbc.ru/money/10/03/2017/58c2d2a89a7947ef7749d2d2.
8. Karlov R. G., (2018), “The Impact of New Methods of Money Laundering on the Economy of the State” in III Network AML/CFT Institute International Scientific and Research Conference “FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies”, KnE Social Sciences, pages 491–500. DOI 10.18502/kss.v3i2.1581 https://knepublishing.com/index.php/Kne-Social/article/view/1581/3731
9. “Отток Капитала Из России в Январе-Апреле 2017 Года Вырос Более Чем Вдвое.” РБК, www.rbc.ru/rbcfreenews/5915bc8a9a79474771420a4b.
10. “Black Money: The Business of Money Laundering.” Shipping Industry, Shipping Sector | Economy Watch, www.economywatch.com/economy-business-and-finance-news/black-money-the-business-of-money-laundering.08-06.html.
11. “Cryptocurrency Market Capitalizations.” CoinMarketCap, www.coinmarketcap.com/.
12. Bell, Alexon. “Is Money Laundering Easier in a Digital World?” IT Pro Portal, ITProPortal, 10 May 2018, www.itproportal.com/features/is-money-laundering-easier-in-a-digital-world/.
13. Teicher, Ron. “Transaction Laundering - Money Laundering Goes Electronic in the 21st Century.” Finextra Research, Finextra, 4 June 2018, www.finextra.com/blogposting/15423/transaction-laundering---money-laundering-goes-electronic-in-the-21st-century.
14. Crosman, Penny. “Crypto Money Laundering Up Threefold in 2018: Report.” American Banker, 3 July 2018, www.americanbanker.com/news/crypto-money-laundering-rose-3x-in-first-half-2018-report.
15. Schlabach, Adam. “Cryptocurrency Anti-Money Laundering Report – Q4 2018.” CipherTrace, 29 Jan. 2019, https://ciphertrace.com/crypto-aml-report-2018q4/.
16. “CipherTrace Research Shows $1.7 Billion in Cryptocurrency from 2018 Thefts and Exit Scams Needs Laundering.” Halo Top Creamery Is Now the Best-Selling Pint of Ice Cream in the United States | Business Wire, 29 Jan. 2019, www.businesswire.com/news/home/20190129005618/en/CipherTrace-Research-Shows-1.7-Billion-Cryptocurrency-2018.

17. “Bitcoin and Money Laundering: Complete Guide to Worldwide Regulations.” Blockonomi, 2 July 2018, https://blockonomi.com/bitcoin-money-laundering/.
18. Saeed, Teya, et al. “United Nations Office on Drugs and Crime Model UN Background Guide - HHHSMUN'18.” Houssam Eddine Hariri High School, Oct. 2018. http://www.mak-hhhs.edu.lb/English/HHHSMUN/new/assets/files/UNODC%20guide.pdf