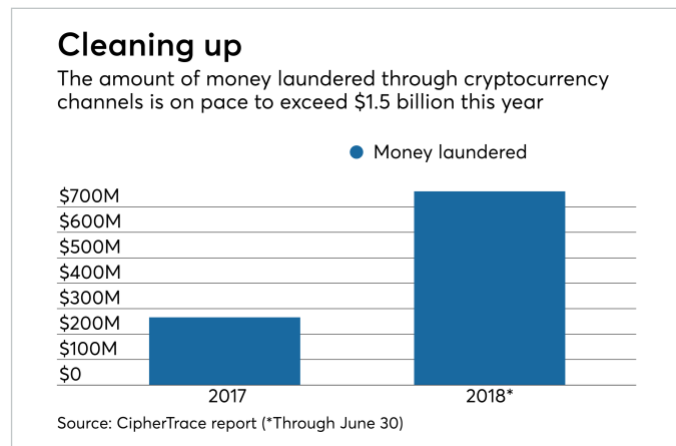# Crypto Money Laundering on the Rise

Since Bitcoin's historic rise in 2017, the number of users participating in the cryptocurrency ecosystem increased from 18 million to nearly 35 million by 2019[1]. This increase in active cryptocurrency users has also led to an increase in cryptocurrencies being used to launder money.

In April 2019, New York State prosecutors secured their first conviction for money laundering involving cryptocurrency.

Cleaning up
The amount of money laundered through cryptocurrency channels is on pace to exceed $1.5 billion this year

● Money laundered

Source: CipherTrace report (*Through June 30)

The two defendants pleaded guilty to laundering more than $2.8 million in cryptocurrency and Western Union payments. The revenue was generated through the sale of controlled substances on the Dark Web; the defendants would take the bitcoin from their sales and launder it through multiple cryptocurrency wallets to hide the source of the money[2].

According to Bloomberg, "FBI Supervisory Special Agent Kyle Armstrong told the Crypto Evolved conference in New York that the agency currently has around 130 different investigations involving cryptocurrencies being used in a variety of crimes, including human trafficking, drug transactions, kidnapping, and ransomware."[3] This isn't just a problem in the United States. In May 2019, eight people in Spain were arrested for operating a money laundering scheme involving cryptocurrencies[4].

Money laundering in the era of cryptocurrency is more convenient but more complicated than traditional laundering schemes[5]. The ability to perform unidentifiable and speedy transactions across multiple jurisdictions augments virtual currency's attraction to money launderers. Add the Dark Web, and you have an anonymous decentralized mixture that creates new challenges for investigators.

Tracking Cryptocurrencies

1 https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/
2 https://www.coindesk.com/new-york-state-sees-first-conviction-for-crypto-money-laundering
3 https://www.bloomberg.com/news/articles/2018-06-27/fbi-has-130-cryptocurrency-related-investigations-agent-says
4 https://cointelegraph.com/news/eight-people-allegedly-arrested-for-money-laundering-scheme-involving-crypto-in-spain
5 https://www.occrp.org/en/daily/8293-report-cryptocurrencies-drive-a-new-money-laundering-era

How can these transactions be tracked? With blockchain technology. Blockchain is an open, decentralized ledger that records transactions between two parties in a permanent way without needing third-party authentication.

Where the tracking comes in is that bitcoin is pseudonymous[6]. A bitcoin pseudonym is the address where users receive bitcoin. Every transaction involving that address is stored forever in the blockchain[7].

If a user's address is ever linked to their identity, every transaction will be linked to that user. Listed below are multiple OSINT tools that allow investigators to search by block number, address, block hash, transaction hash, or public key to
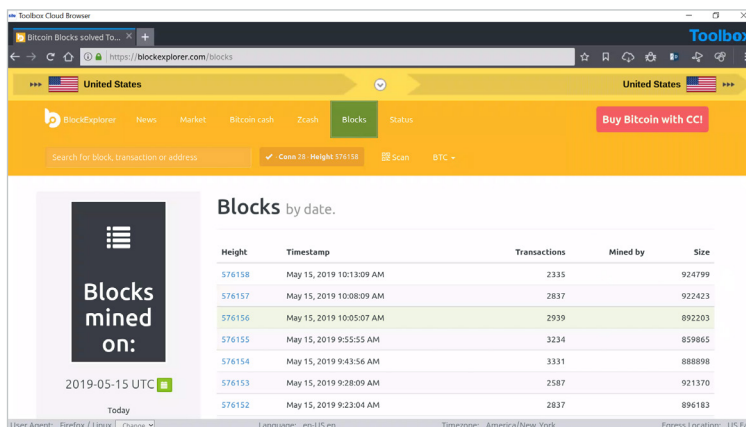
Bitcoin blockchains from blockexplorer.com.

find out more information on bitcoin transactions.

- https://blockexplorer.com/
- https://blockchain.info/
- https://www.chainalysis.com/
- https://bitcoinwhoswho.com/

Due to the pseudonymous nature of bitcoin and transactions being tracked by investigators, money launderers are starting to use a system known as cryptocurrency tumblers. Cryptocurrency tumblers mix potentially identifiable currency with untraceable currency to make it harder to track.

Some addresses can be grouped by their ownership, using behavior patterns and publicly available information from off-chain sources[8]. The challenge for forensic investigators, as usual, is to identify the person behind the keyboard, which may be accomplished through a mixture of traditional investigative and digital forensic techniques[9].

---

6 https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#3d9d125d7bc4
7 https://www.buybitcoinworldwide.com/anonymity/
8 https://bitcoinwhoswho.com/blog/scholarly-works/
9 http://networkcultures.org/moneylab/2018/05/08/flying-money-organized-crime-and-the-new-digital-money-by-geert-lovink/

Bitcoin Address Reports

Once a bitcoin address of interest is identified, it can be run through a blockchain tracking tool. Using bitcoinwhoswho.com, a report has been generated for bitcoin address 1Hz96kJKF2HLPGY15JWLB5m9qGNxvt8tHJ.

BTC Address	1Hz96kJKF2HLPGY15JWLB5m9qGNxvt8tH	# Website Appearances	9
Wallet Name	000a027d20045b7d	Last Transaction IP ❓	47.254.169.156, 52.60.49.56, 148.251.139.241
Current Balance	112.11330270	Total Received	161472.17413649
# Transactions	13121	# Output Transactions	Loading...
First Transaction	13 Jun 16	Last Transaction	16 May 19
Last Known Input	Loading... Loading...	Last Known Output	1BMjmWXy7h... 16 May 19
Repeated Inputs From (50 most recent transactions)	... 37	Repeated Outputs To (50 most recent transactions)	1BMjmWXy7h... 13 1PqU8hFVgy... 9 1NSUvXCtWw... 4

Bitcoin address report from bitcoinwhoswho.com

Example fields of interest

Current Balance/Total Received: Allows analysts to hypothesize the type of address this is. Due to the high volume of transactions, this wallet likely belongs to a bitcoin miner.

Last Transaction IP: Allows analysts to view the last known IP to relay an output transaction involving the selected address. Repeated use of an IP can be used as a unique identifier.

Website Appearances: Allows analysts to view any site where this exact bitcoin address appeared which could be of value for identifying reputation/type of transactions.

Repeated Inputs From/Repeated Outputs To: Allows analysts to view the 50 most recent bitcoin addresses involved with incoming and outbound transactions associated with this address. By looking at the transaction history and frequently interacted-with wallets, investigators can engage in network and link analysis to identify patterns and possible relationships between the disparate bitcoin addresses.

By Authentic8

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.