Mitigating AML & Sanctions Risks Posed by Doing Business with Cryptoasset Firms

Peer-to-Peer Session Leaders

Mónica MacGregor
Principal
Control Risks
monica.macgregor@controlrisks.com
T +1.202.975.3419
M +1.202.423.7590

Charlotte Bhania
Partner
PCB Byrne
cbhania@pcb-byrne.com
T +44 207 842 1657
M +44 7711 404938

Compliance best practices

OFAC – Sanctions Compliance

The growing prevalence of virtual currency as a payment method brings greater exposure to sanctions risk - like the risk that a sanctioned person or a person in a jurisdiction subject to sanctions might be involved in a virtual currency transaction. In this regard, OFAC considers the following to establish the strength of the compliance program:

- Management commitment
- Risk Assessment
- Internal Controls
- Testing & Auditing
- Training

FATF – AML Compliance

This Guidance outlines the need for countries and VASPs (Virtual Asset Services Provider), and other entities involved in VA activities, to understand the money laundering and terrorist financing (ML/TF) risks associated with VA activities and to take appropriate mitigating measures to address those risks. In addition, the following aspects are advised to be strengthened to create a robust compliance program:

- Training
- Information Exchange
- Customer due diligence
- Internal controls and foreign branches and subsidiaries

The UK Regulatory Framework

Regulation So Far – MLR First

The EU's Fifth Money Laundering Directive (5MLD) was transposed into national law in January 2020.

The UK implemented 5MLD via amendment to the The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR)

For the purpose of ensuring that the UK's AML/CTF regime is "*kept up to date, effective and proportionate*''

Since 10 January 2020 the FCA has been the anti-money laundering and counter-terrorist financing supervisor of UK cryptoasset businesses

Of the 300 applications it has received, it has approved and registered 41 (15%), 195 (74%) were either refused or withdrew their application and 29 (11%) were rejected

Work To Be Done

HM Treasury Consultation and call for evidence on the Future financial services regulatory regime for cryptoassets

- Consultation closes on 30 April 2023
- Core Design Principles:
  - Same risk, same regulatory outcome
  - Proportionate and focused
  - Agile and flexible
- Steps are being taken to equip the current UK regulatory framework to harness innovation whilst mitigating the most pressing risks
- A broad range updates and amendments to statute and legislative tools are proposed

The US Regulatory Framework

Regulation So Far – Bank Secrecy Act (BSA) as Amended by PATRIOT Act

- Cryptoasset firms fall under the definition of “Money Service Business.”
- AML – Cryptoasset firms fall under regulatory scope of BSA as amended by PATRIOT Act and are thus required to implement an AML/CFT program, maintain appropriate records, and submit reports to the authorities relating to potentially suspicious activity, among other requirements.
- Sanctions – Cryptoasset firms are subject to OFAC sanctions requirements and procedures, including licensing and enforcement processes.
- Registration with FinCEN is required and is, in and of itself, heavily dependant on existence of a risk-based AML and Sanctions Compliance Program.
- Certain US States require additional registration with State Supervisors as “Money Transmitters” which again calls for existence of risk-based compliance program and reporting on in-state transactions.
- US Regulators have earnest effort to issue guidance customized for cryptoasset firms and their business models.
- AML Act of 2020 placed particular focus on virtual currencies and crypto asset firms.
- Current regulatory scrutiny (April 2023) is being driven by SEC and focused on:
  - Howey Test as to whether crypto token actually a security;
  - Liquidity management; and
  - Trading on volatility inherent to crypto

Primary challenges in designing and implementing effective AML/Sanctions Compliance Program

- **Risk Assessment must be conducted in manner which deviates from traditional banking**
  - Accurate evaluation of business model under which crypto asset firms operate essential
  - Risk assessment must expand to include
    - global client base
    - risk presented by token
    - risk presented by partner in which cryptoasset firm may be embedded
    - speed of transaction
    - mining, minting, staking and other methods for “generating” crypto
    - ability to convert from fiat to crypto, across chains to stable coins for example and back to fiat
    - use of crypto in smart contracts and other defi activities which may limit visibility into transactional activity
    - potential one-stop shop for placement, layering and integration

Primary challenges in designing and implementing effective AML/Sanctions Compliance Program

- **AML/Sanctions Compliance program required to mitigate inherent risk must be tailored to risk profile and supported with a variety of technological solutions**
  - Incorporate global, mobile and virtual nature of platforms – facilitates circumvention of regulatory, licensing and other limitations posed on doing business in select markets and requires geolocation, ip verification and other technologies to effectively ensure compliance high AML and Sanctions risk profiles
  - Key Performance Metrics amongst cryptoasset firms is “speed” of transaction which directly at odds with in-depth onboarding/KYC/Screening processes at odds
  - Customer Risk Rating Methodology must be tailored to include specific factors related to:
    - documented nationality vs. physical location
    - form of payment
    - use of higher number of tokens
    - historical patterns including frequency of conversion (fiat to crypto as well as crypto to fiat) and cross chain activity
    - essential to update for clustering patterns detected
  - Managing value and volume of Transaction Monitoring activities is essential to segregate noise
    - traditional definition of “high risk” clients requiring Enhanced Due Diligence is skewed
    - purpose of transaction must be incorporated into rules and parameters *e.g. utility and governance tokens; game/virtual reality specific tokens*

Major areas of risk in Cryptocurrency Industry

Several major areas of risk in the Cryptocurrency industry that is eliciting attention from regulatory bodies and media outlets alike:

- **Failure of internal controls at major institutions and exchanges**
  - Lack of AML & Sanctions policies and procedures in books and records
  - Absence of audit functions
  - Inadequate controls and oversight in financing, lending, crediting and proof of reserves
  - Challenges in volatility & liquidity management
  - Improper valuation of pegged cryptocurrencies
  - Inherent tension between culture of “decentralization”, technology & entrepreneurship vs. culture of compliance

- **Systemic Risks due to the nature of cryptocurrencies**
  - Pseudonymity
  - Concealment and/or opacity of related party transactions
  - Cross chain transactions
  - Specialized blockchain transaction monitoring and investigations skills
  - Mining, Staking and other “asset” generation
  - Relative ease of conversion from crypto to fiat

Threats posed by Cryptocurrency – Illicit Activities and Financial Crimes

- **Using Cryptocurrency Directly to Commit Crimes or to Support Terrorism,** including buying and selling illegal goods and the tools to commit crimes, making ransom, blackmail, and extortion payments, and raising funds for criminal and terrorist activities.
- **Using Cryptocurrency to Hide Financial Activity,** including money laundering, operating unlicensed, unregistered, or non-compliant exchanges, and avoiding taxes and sanctions.
- **Committing Crimes within the Cryptocurrency Marketplace Itself,** including theft and fraud, and so-called "crypto jacking" whereby hackers force compromised computers to generate cryptocurrency. The illiquidity in certain cryptocurrency markets makes it more vulnerable to pump and dump schemes like those seen in the securities fraud context.
- **Darknet Markets** or "darknet websites and marketplaces that allow criminals around the world to connect are also highlighted as a key source of illegal activity. For example, in 2017, the Department of Justice (DOJ) seized and shut down a dark web market known as "AlphaBay," which at the time of its seizure "served over 200,000 users as a conduit for everything from illegal drugs and firearms to malware and toxic chemicals."

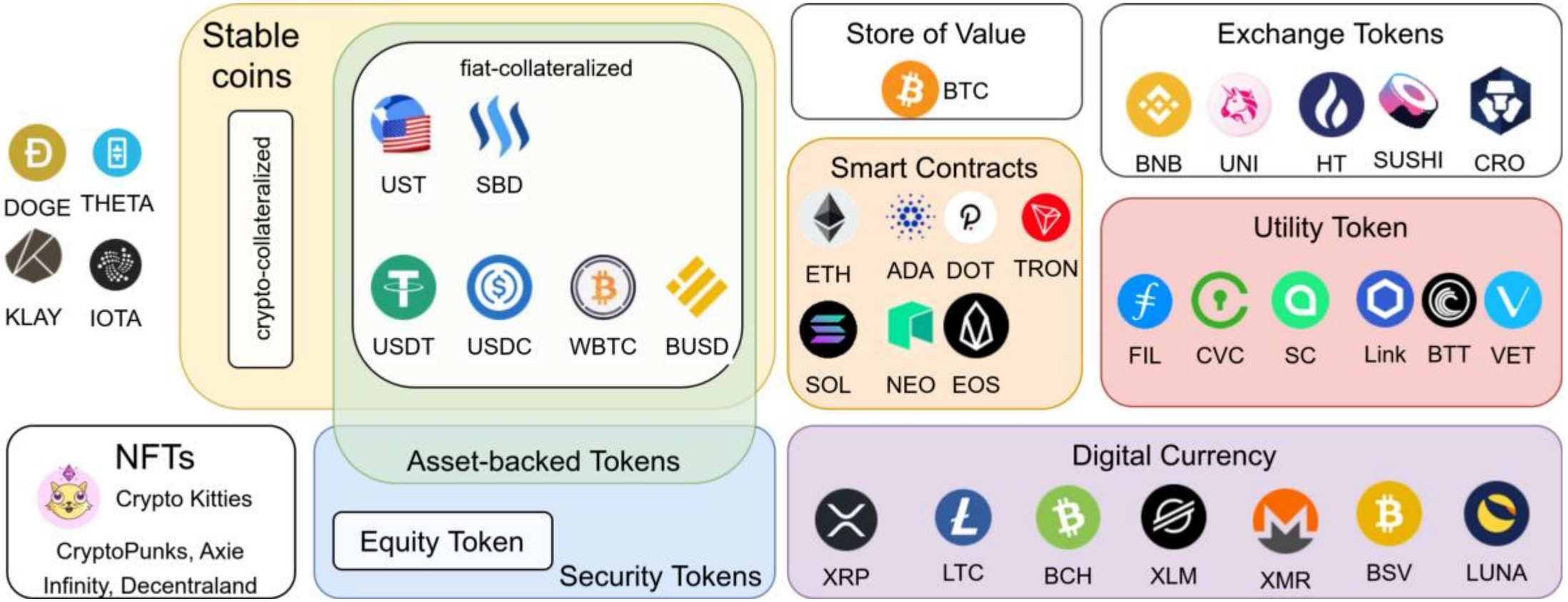
What is a Cryptocurrency

Cryptocurrencies build off the blockchain technology to allow a system of financial transactions to be conducted in a purely electronic format. As with the blockchain technology, cryptocurrencies are digital stores of units that are anonymized, traceable, and decentralized.

Over the past decade, an expansive ecosystem has been built around the technology. Some key concepts and features in this ecosystem include:

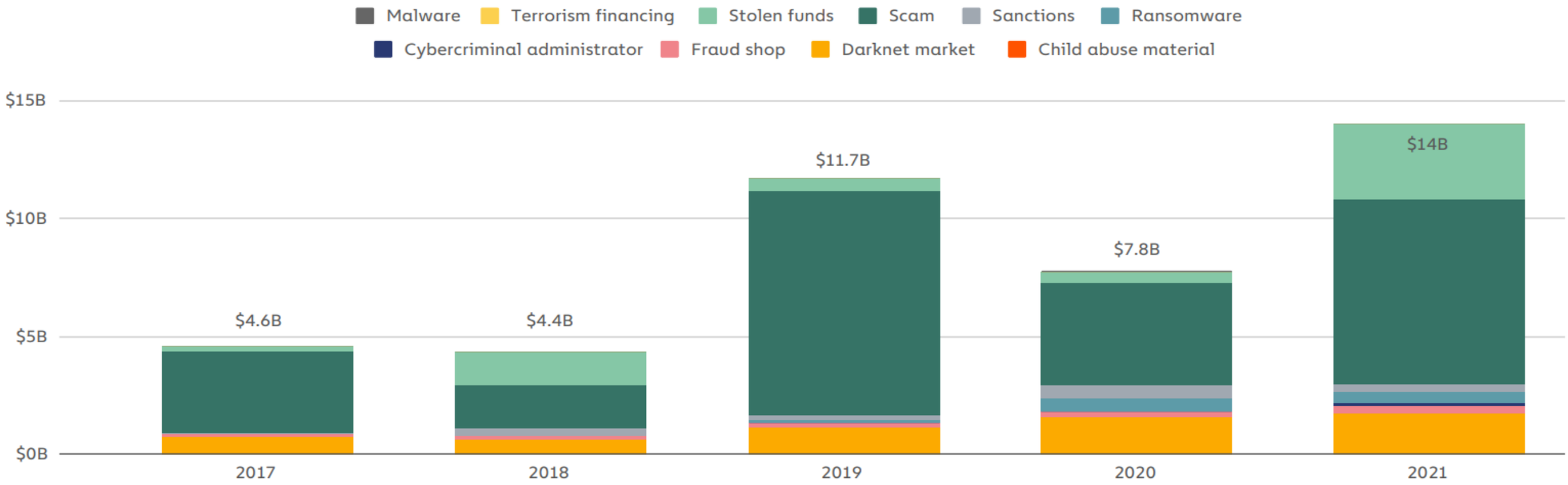
- **Exchanges** – Exchanges such as Coinbase, Binance, and Gemini are marketplaces where you can buy and sell cryptocurrencies. These are often the main sources of on- and off-ramps for exchanging fiat currencies (e.g., USD and GBP) for cryptocurrencies.
- **Wallets** – Crypto wallets (both hardware and mobile apps) allow you to store cryptocurrency in a private and secure, localized environment, as opposed to holding an account with an exchange; akin to holding money in a physical wallet as opposed to depositing it in a bank.
- **Decentralized Applications (dApps)** – digital applications or programs that exist and run on a blockchain/cryptocurrency. Ethereum is an example of a dApp that provides flexibility of applications and programs (e.g., Smart Contracts, Games, and NFTs) to be built on top of its blockchain.
- **Decentralized Finance (DeFi)** – An array of services that have arisen in contrast to financial institutions and centralized exchanges. DeFi is a set of peer-to-peer (P2P) services mirroring the services that financial institutions typically provide, such as lending, loan issuance, trading, and buying and selling derivatives.
- **Non-fungible Tokens (NFT)** – A store of code, [typically] built on top of the Ethereum framework, that can be associated with any form of digitally stored data (pictures, videos, audio, documents, etc.). Each store of code is unique and cannot be replicated, sold, or traded.

Types of Cryptocurrencies



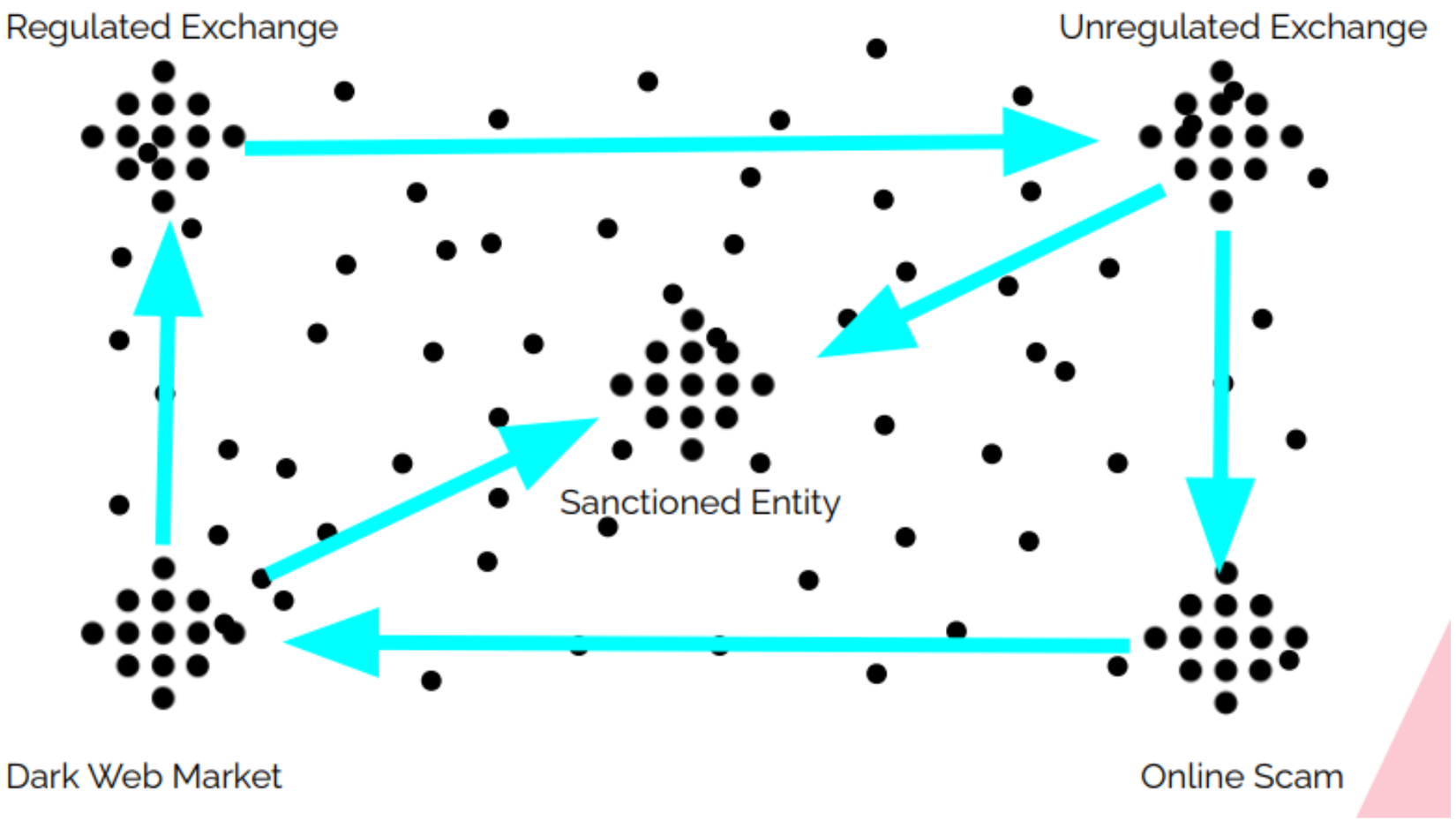
Crypto and Financial Crimes

Total cryptocurrency value received by illicit addresses



Chainalysis - The 2022 Crypto Crime Report – Feb 2022

Identifying Illicit Actors on the Blockchain



Cryptocurrencies in an investigative context

Cryptocurrency is an ever-evolving landscape of new tokens and coins. In an investigative context, this makes it difficult to develop the skillset to trace and track every crypto asset available.

However, it is useful to think about the landscape of cryptocurrencies through the lens of what is more likely to be used for illicit purposes:

- **Obfuscation vs. Simplicity** – Cryptocurrencies where asset tracing can be more easily obfuscated are more likely to be used for illicit purposes. Obfuscation can take many forms, such as complexity, highly secure encryption, and asset blending, among others.
- **Liquidity vs. Illiquidity** – As with fiat currencies, liquid markets are more attractive to carry out transactions for illicit purposes (i.e., money laundering). Conversely, like securities assets, illiquid markets can be conducive to carrying out schemes with the asset itself – e.g., pump and dumps, and other market manipulation tactics.

Obfuscation in cryptocurrencies

Despite the intent that cryptocurrencies be an open and transparent system, the complexities of the ecosystem that has been built on top of it has served only to obfuscate the traceability of transactions. Obfuscation can take several forms:

Complexity

dApps and DeFi continue to evolve and expand into much more sophisticated offerings. This has led to increased complexity in transactions, particularly within Ethereum and its ERC-20 Tokens. This complexity now makes it much more difficult to untangle transactions and understand their provenance and destination.

e.g. A transaction that swaps 235.7 FARM coins for 23,907.54 USDC

Security and Encryption

As Bitcoin and other cryptocurrencies have become more legitimized, transactions for illicit trades have moved to cryptos with higher levels of anonymity and stronger encryptions. Cryptos such as Beam, Zcash, and Monero have taken over as the preferred choice of currency for illicit trades, due to its private blockchain and ability to anonymize or outright hide addresses from the ledger.

Asset Blending and Washing

In recent years, asset-backed tokens and NFTs have emerged to provide another avenue to blend and wash illegitimate funds. As there is such a rampant speculative market, this makes it harder to discern between speculative (but legitimate) bids versus bids to blend and wash illegitimate funds – especially given the anonymity of wallets and transactions.

e.g. Cryptopunk #5822 recently sold for 10K ETH, approximating $32M.