Blockchain and Financial Crime: Including use of blockchain analysis tools

Some basic concepts

- Cryptocurrencies are digital currencies supported by blockchain technology.

- All the transactions are visible on the blockchain

- However, blockchains do not contain real-world identities.

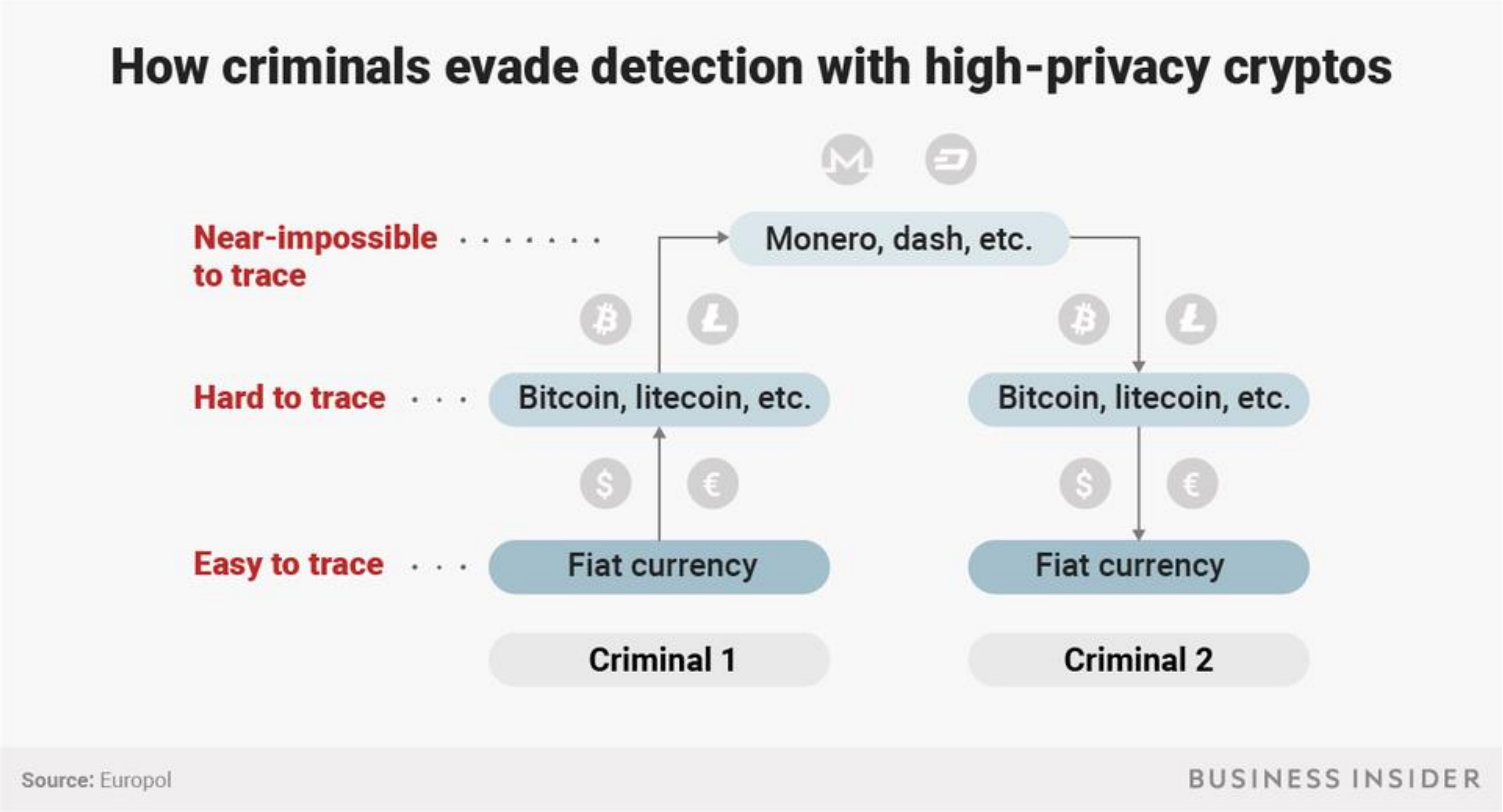
- Therefore, associating these activities with real-world entities and stopping criminals is an ongoing challenge.

Why is it a challenge for law enforcement?

- The decentralized nature of blockchain protocols introduce several vulnerabilities to traditional law enforcement techniques.

    - Cryptographic techniques
    - Pseudonymous transactions
    - Lack of anti-money laundering software
    - Difficult to identify the original source of funds

Journey of funds example



How criminals evade detection with high-privacy cryptos

Source: Europol

Crypto Assets & Money Laundering

Criminals often:

- utilize the anonymity features of some cryptocurrencies (e.g., ZEC, XMR)
- use multiple new wallet addresses for micro transactions
- use mixing services (e.g., Helix, Coinjoin, Coinmux)
- use multiple cryptocurrency transactions
- engage third-party individuals to act as money mules

Crypto Assets & Criminal Activity

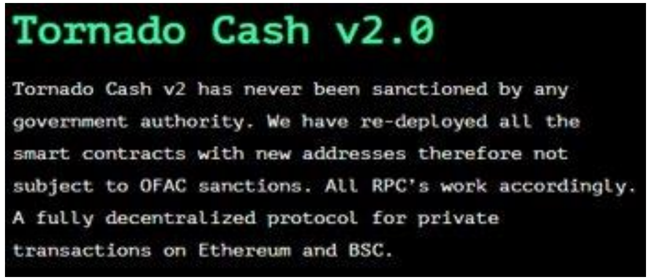
Most VA related offences focused on predicate or ML offences, but criminals do make use of crypto assets to:

- Evade Financial Sanctions
- Money Laundering
- Ransomware
- Darknet markets
- Fraud
- Evade Taxes
- Illicit Activities
- Market Manipulation
- Hacking

Common Web3 Hacks & Scams

- Credential Phishing
- Ad-Hijacking
- Fake Customer Service
- Fake SM Giveaway
- Ponzi Schemes
- Rug Pulls
- Seed Phrase Phishing
- Malicious Wallets & Plugins
- Approval Scam

Criminals' Toolbox



Tornado Cash v2.0

Tornado Cash v2 has never been sanctioned by any government authority. We have re-deployed all the smart contracts with new addresses therefore not subject to OFAC sanctions. All RPC's work accordingly. A fully decentralized protocol for private transactions on Ethereum and BSC.

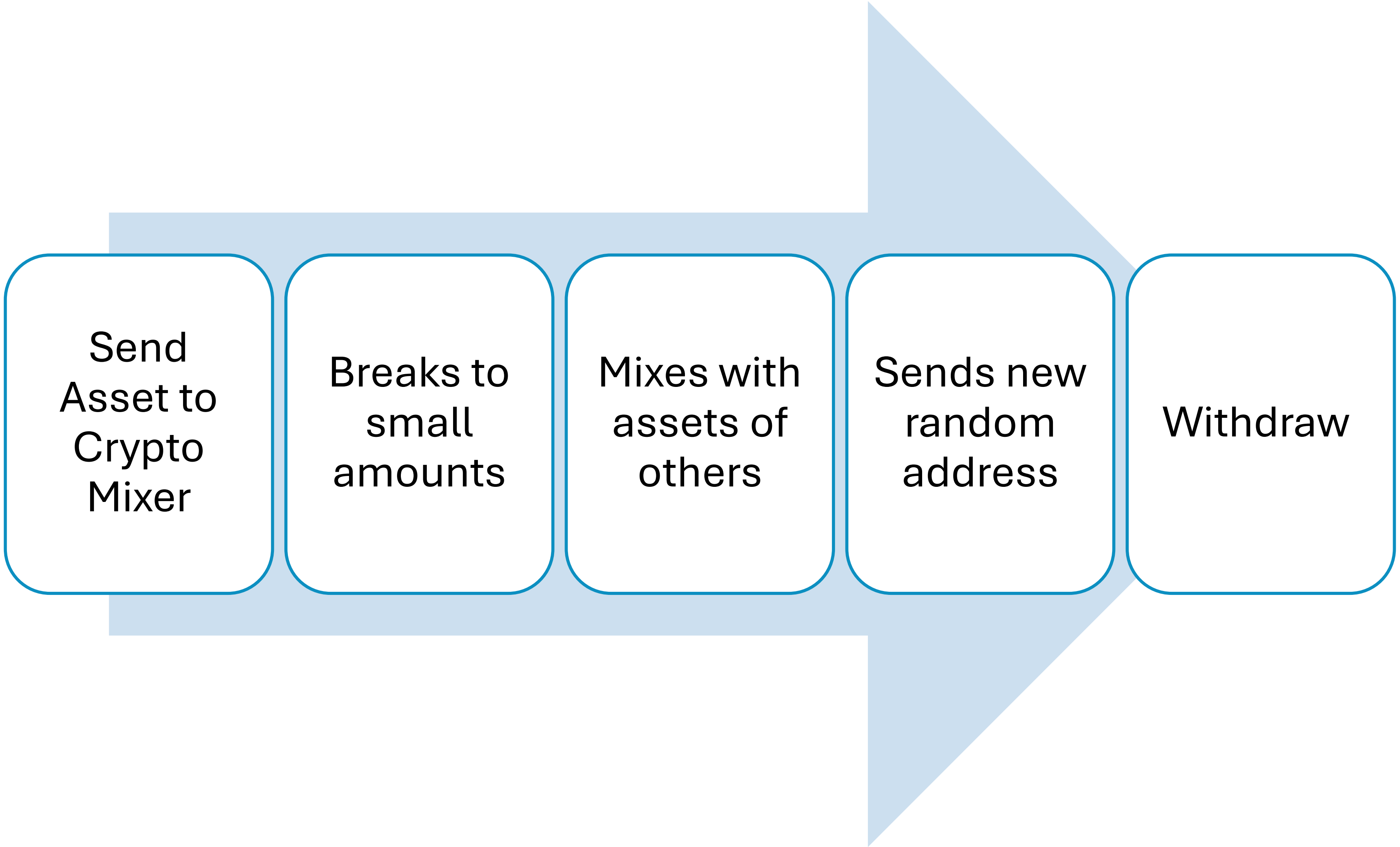
MyCryptoMixer

- Tumbling/Mixing
- Chain hopping/Bridging
- Multiple Wallets and Addresses (Burner Wallets)
- Large number of small transactions
- Privacy enhancing cryptocurrencies (i.e., Monero and Zcash)
- Money mules
- Virtual Private Network (VPN)/The Onion Router (TOR)

MONERO

Tor

Tumbling or Mixing



Send Asset to Crypto Mixer

Breaks to small amounts

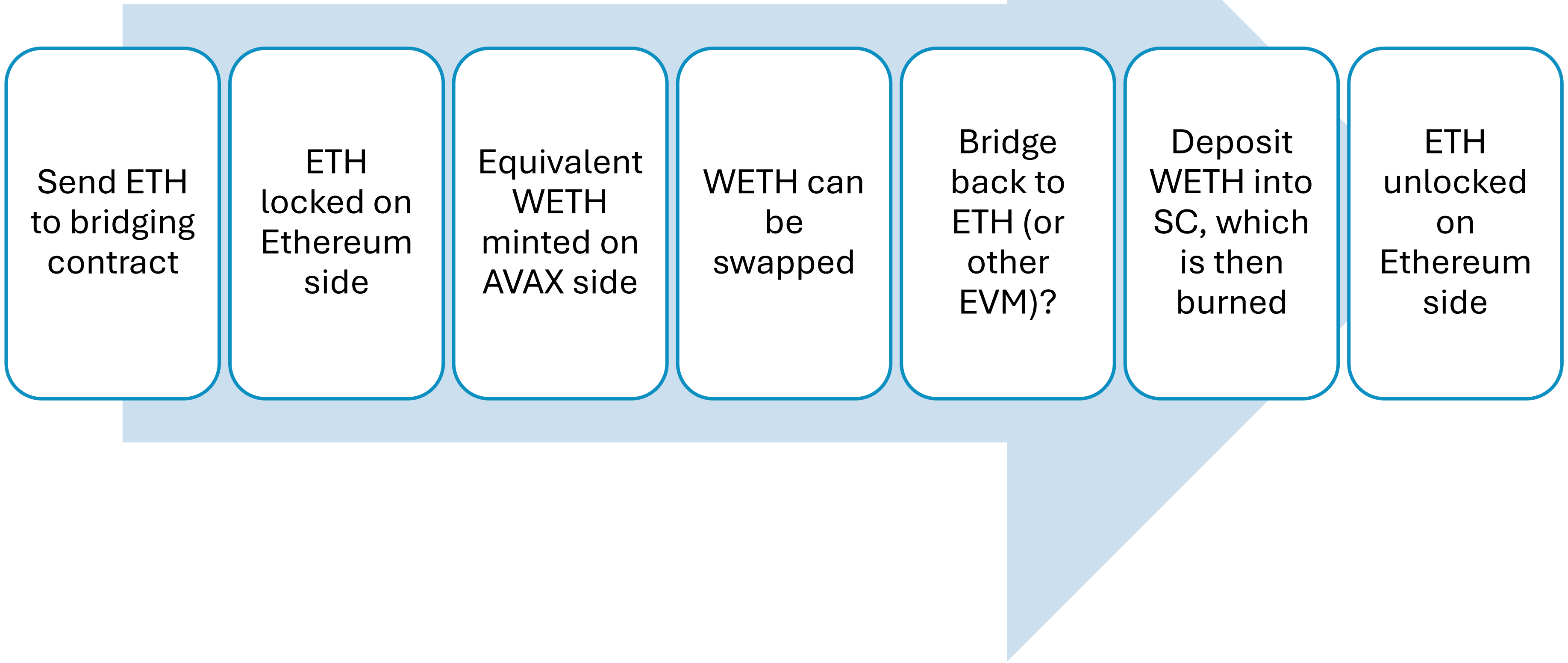
Mixes with assets of others

Sends new random address

Withdraw

Chain Hopping or Bridging

A cross-chain bridge creates a connection between two blockchains facilitating the flow of data, capital, and assets between their respective ecosystems. This works using smart contracts.



Send ETH to bridging contract

ETH locked on Ethereum side

Equivalent WETH minted on AVAX side

WETH can be swapped

Bridge back to ETH (or other EVM)?

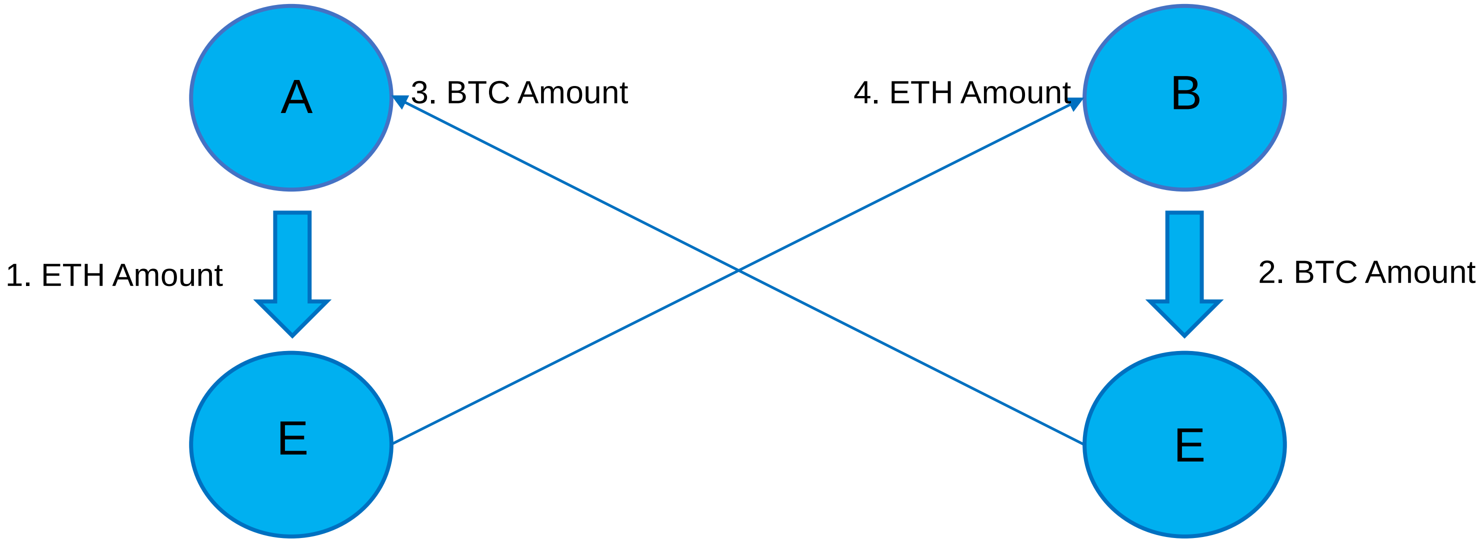
Deposit WETH into SC, which is then burned

ETH unlocked on Ethereum side

Crypto Assets & Money Laundering

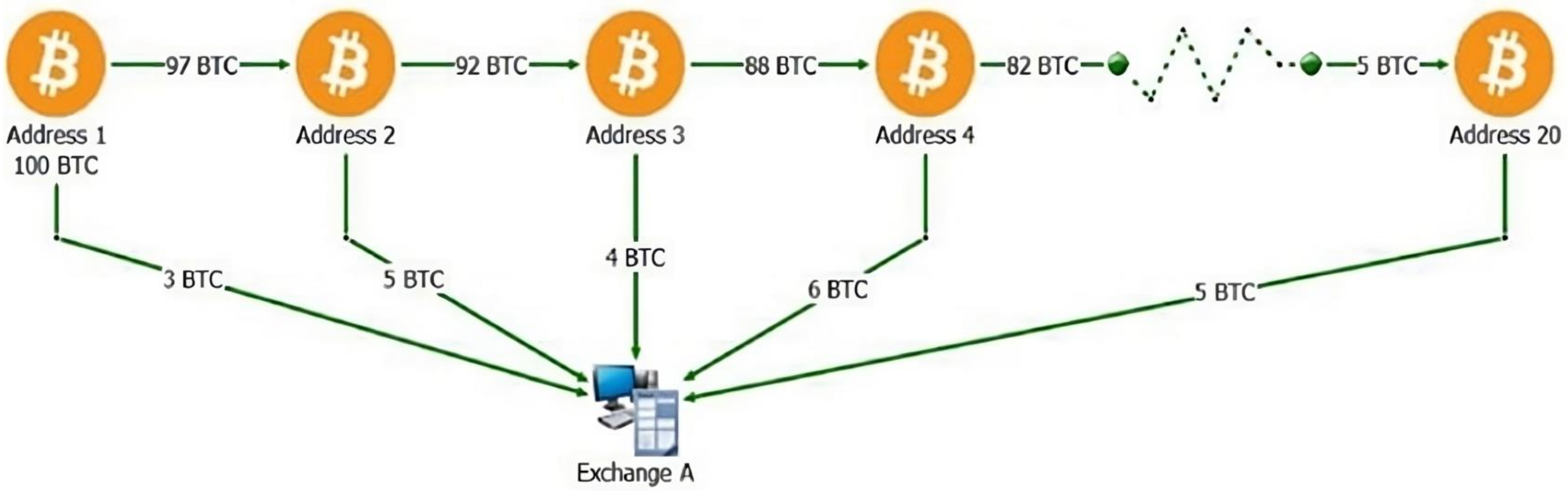
Atomic swaps enable two or more parties to swap crypto P2P without intermediaries, through programmatic escrows.

As such, we can program two escrows to communicate with one another, and depending on their interactions, they can either: Send funds to the intended recipients when specified conditions are met; or refund the original sender of funds within a predetermined amount of time. Cross-chain atomic swaps leverage this dual escrow mechanism.



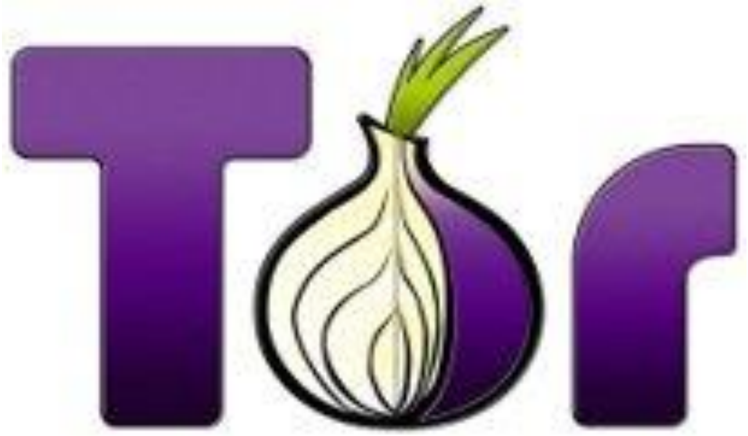
Peel Chain

Peel Chain involves the process of laundering a large amount of cryptocurrency through a series of minor transactions, where a small portion of the funds is gradually "peeled" or moved from one address to another in a sequence of low-value transfers.



The Onion Router

- Free and open-source software for enabling anonymous communication.
- Encrypted internet traffic through a series of randomly selected nodes.
- Each node decrypts only a "layer" of the encryption.
- Widely used to access the "deep web".



Browse Privately.
Explore Freely.

Defend yourself against tracking and surveillance. Circumvent censorship.

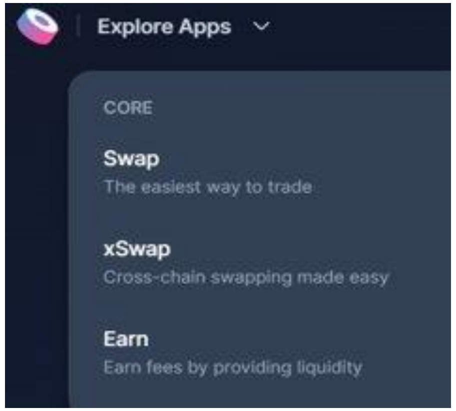
Privacy Wallets

- Open-Source
- Non-Custodial
- Focused on Privacy & Security
- Use CoinJoin Techniques

Decentralized Exchanges - Dexes

- Decentralized exchanges, often referred to as DEXs, are platforms that facilitate peer-to-peer cryptocurrency trading without the need for intermediaries or centralized control. These exchanges operate on blockchain technology, enabling users to directly trade cryptocurrencies with each other using smart contracts and decentralized protocols.

- Key Features:
- Decentralized control: DEXs are not controlled by a single entity, which means that users have full control over their assets and are not subject to the policies or regulations of a central authority.
- More privacy: DEXs often offer more anonymity than centralized exchanges because they do not require users to provide personal information to create an account.


Explore Apps
CORE
Swap
The easiest way to trade
xSwap
Cross-chain swapping made easy
Earn
Earn fees by providing liquidity

UNISWAP

FATF New Technologies & Travel Rule

Interpretive Note clarifies the application of AML/CFT standards to crypto assets

•VASPs (Virtual Asset Service Providers) must comply with AML/CTF requirements as traditional financial institutions

•Travel Rule: transactions above a designated threshold (USD/EUR 1000) require VASPs to conduct CDD (Customer Due Diligence)

•Countries must ensure that beneficiary VASPs obtain, hold and make available originator and beneficiary information for virtual asset transfers

•Information must be available on request to appropriate authorities.

FATF New Technologies & Travel Rule

Providers of crypto services must ensure the identities of the individuals or legal entities with whom they are transacting (business relationship) in their records, in compliance with the sanctions' regulations.

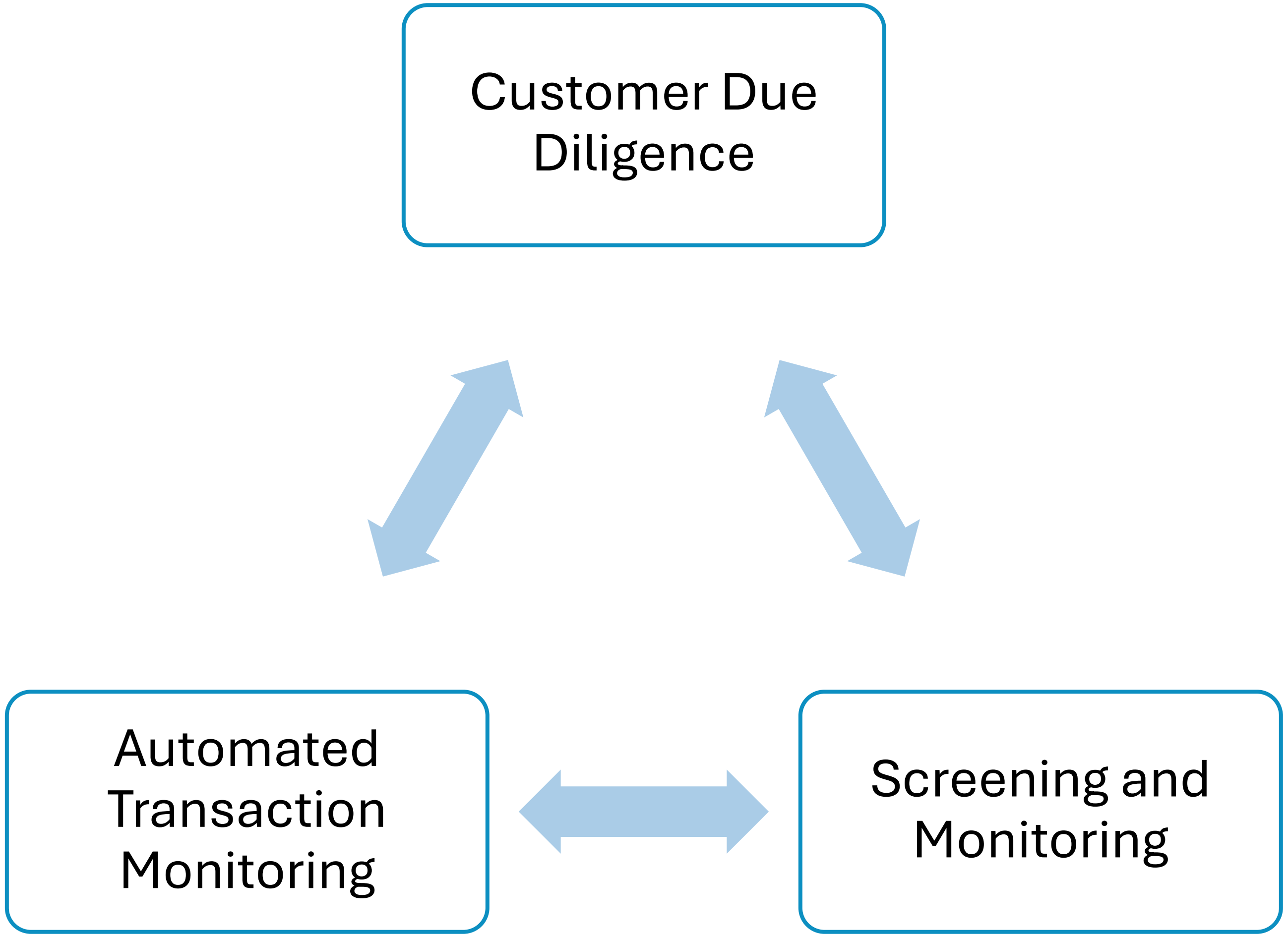
In transactions to and from non-custodian wallets, crypto service providers must be able to effectively verify the identity of a party in a relationship with a person or legal entity referred to in the sanctions' regulations.

Enhanced Due Diligence

Additional information should be collected for high-risk customers, such as:

- purpose of the transaction or payment
- source of funds / proof of funds ownership
- identities of the transacting parties
- the identity and the beneficial ownership of the counterparty

AML Compliance for Crypto Assets



Customer Due Diligence

Automated Transaction Monitoring

Screening and Monitoring

How to comply with AML Regulations for Virtual Assets

✓ **Customer due diligence:** Crypto service providers should build their risk profiles and transaction monitoring measures on accurate CDD.

✓ **Screening and monitoring:** Cryptocurrency service providers should inform their transaction monitoring process by screening and monitoring for a variety of crucial risk data including their customers’ PEP status, involvement in adverse media stories, and presence on relevant international sanctions or watch lists.

✓ **Automated Transaction Monitoring:** The employment of automated blockchain transaction monitoring and forensic tools to ensure that suspicious activity is detected and reported to the authorities.

Tracing Measures – What is Blockchain Analysis?

“Blockchain analysis is a process of investigating, classifying, and monitoring blockchain addresses and transactions to understand the activities of various actors on the blockchain.”
Dr. Klitos Christodoulou – University of Nicosia

How Blockchain Investigations Work

Step-1: Isolate parties and transactions of interest

Step-2: Export transaction details into a Blockchain Forensic tool for investigative analysis

Step-3: Analyze movement of cryptocurrency assets

Step-4: Identify suspicious addresses that are associated with known hacks, third-party watchlists and fraud library

Step-5: Document findings by each case

Step-6: Identify relationships between transactions by linking cases

Step-7: Generate case reports that show transactions’ movements

Challenges for Monitoring Tools

Big Data Volume

Many blockchains with large volume of transactions

Multiple wallet addresses owned by the same user

Incorporation of enhanced anonymity techniques with the use of cryptography

Ring signatures

Blockchain protocol updates and hard forks

Updates to the core protocols (e.g., Bitcoin Taproot)

New Decentralized products and services

How to determine the valuation of Non-fungible tokens (NFTs)?