Mixing and Regulating Crypto Assets

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Outline

- Illegal Trading and Activities on Blockchain Network
- AML in Cryptocurrency

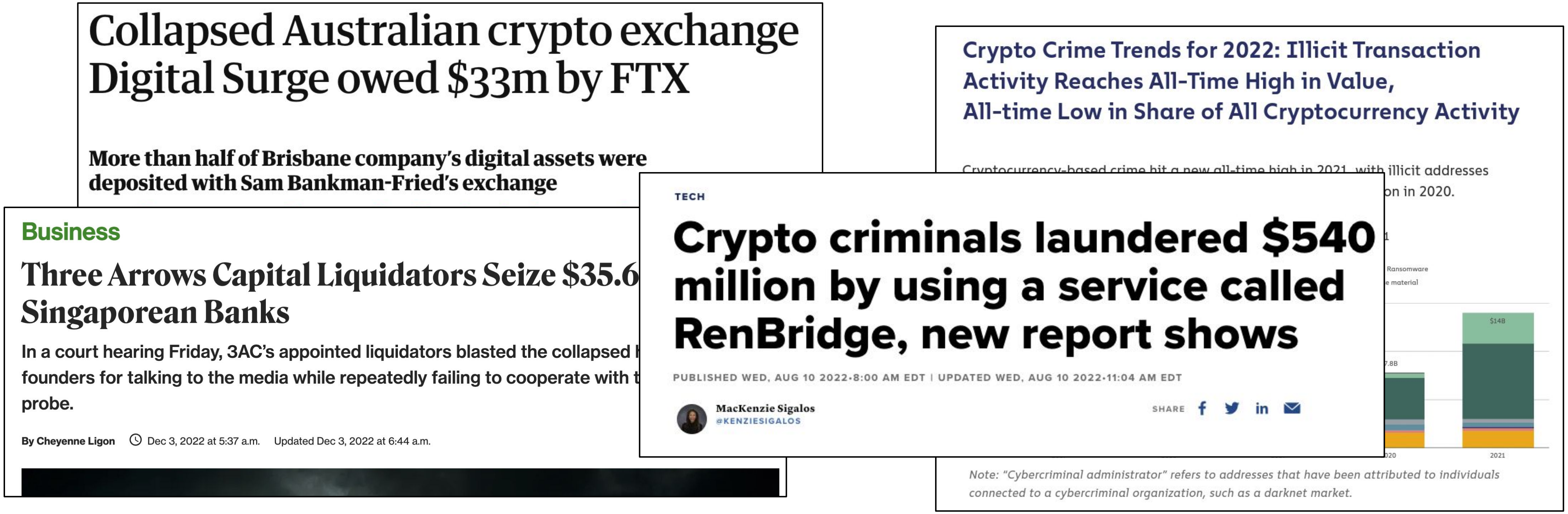
Illegal Trading and Activities on Blockchain Network

SWINBURNE UNIVERSITY OF TECHNOLOGY

Crypto Scandals and Controversial Stories

The crypto market behaves erratically in 2022 and was marred by corruption and fraudulent activity - Chayanika Deka

Cryptocurrency-based crime hit a new all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, up from $7.8 billion in 2020. - CHAINALYSIS TEAM



Collapsed Australian crypto exchange Digital Surge owed $33m by FTX

More than half of Brisbane company's digital assets were deposited with Sam Bankman-Fried's exchange

Business

Three Arrows Capital Liquidators Seize $35.6
Singaporean Banks

In a court hearing Friday, 3AC's appointed liquidators blasted the collapsed h
founders for talking to the media while repeatedly failing to cooperate with t
probe.

By Cheyenne Ligon Dec 3, 2022 at 5:37 a.m. Updated Dec 3, 2022 at 6:44 a.m.

Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-time Low in Share of All Cryptocurrency Activity

Cryptocurrency-based crime hit a new all-time high in 2021, with illicit addresses
on in 2020.

Note: "Cybercriminal administrator" refers to addresses that have been attributed to individuals connected to a cybercriminal organization, such as a darknet market.

TECH

Crypto criminals laundered $540 million by using a service called RenBridge, new report shows

PUBLISHED WED, AUG 10 2022·8:00 AM EDT | UPDATED WED, AUG 10 2022·11:04 AM EDT

MacKenzie Sigalos
@KENZIESIGALOS

SHARE

Introduction of Tornado Cash

Tornado Cash, often referred to simply as Tornado or Tornado Mixer, is a non-custodial privacy solution on the Ethereum blockchain. It allows users to deposit either Ether or certain ERC-20 tokens into its smart contract and then withdraw the same amount from a completely different address after some time, thereby preserving user privacy.

Here's how Tornado works:

Deposit: A user deposits Ether or a specific type of ERC-20 token into Tornado's smart contract. At the time of deposit, the user generates and submits a "commitment," which is a hash of their initial deposit and a secret (or "note").

Introduction of Tornado Cash

Wait: To maximize privacy, the user should wait for some time. This way, other deposit and withdrawal activities mix with the user's, making it harder to trace back.

Withdraw: To withdraw funds, a user needs to submit two proofs:

- That they know the secret associated with a prior deposit.
- That the commitment for that deposit indeed exists in the smart contract.

Once both conditions are met, the user can withdraw funds to a brand-new Ethereum address, breaking the continuity of the fund flow.

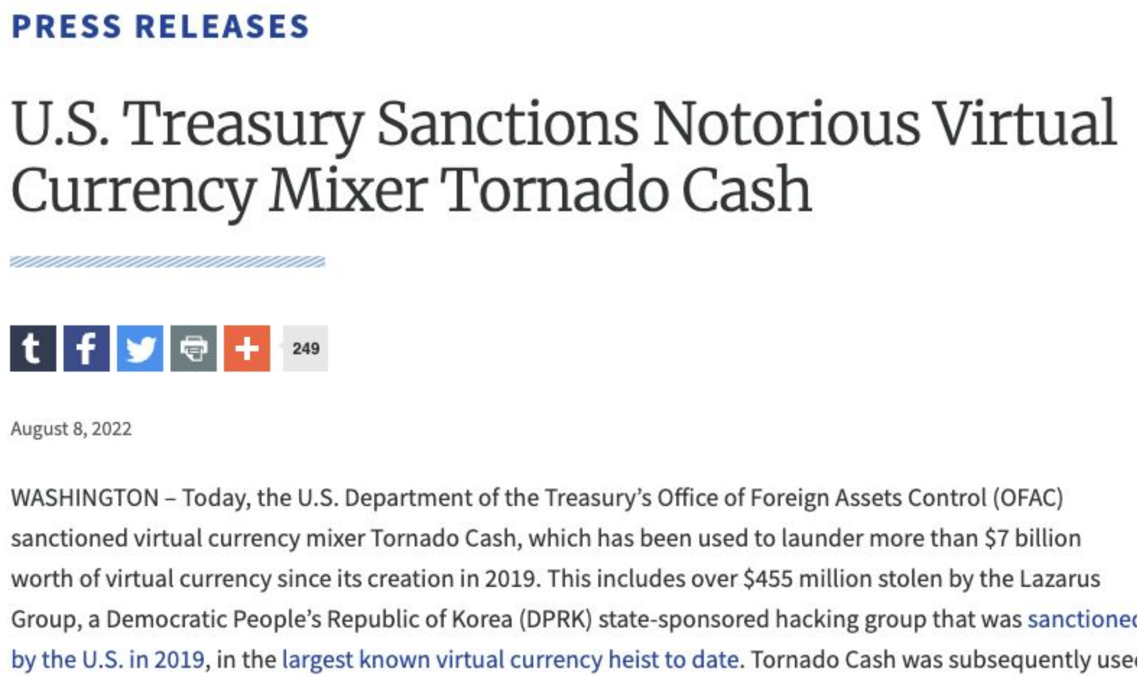
Tornado utilizes zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) to ensure the privacy of withdrawals without revealing any information about the sender, the recipient, or the transaction amount.

In essence, Tornado Mixer is a tool designed for users looking to enhance the privacy of their Ethereum transactions. However, users should always be mindful that the use of mixers might be legally restricted or regulated in some jurisdictions. It's a good idea to familiarize oneself with the relevant laws and regulations before use.

Tornado Cash

"Tornado Cash has repeatedly failed to impose effective controls designed to stop it from laundering funds for malicious cyber actors on a regular basis and without basic measures to address its risks. Treasury will continue to aggressively pursue actions against mixers that launder virtual currency for criminals and those who assist them."

- Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson



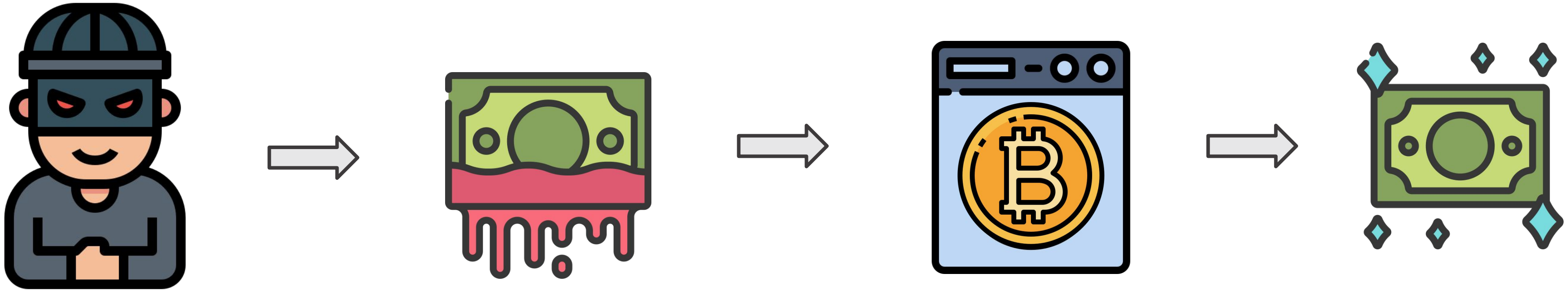
PRESS RELEASES

U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash

August 8, 2022

WASHINGTON – Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned virtual currency mixer Tornado Cash, which has been used to launder more than $7 billion worth of virtual currency since its creation in 2019. This includes over $455 million stolen by the Lazarus Group, a Democratic People's Republic of Korea (DPRK) state-sponsored hacking group that was sanctione by the U.S. in 2019, in the largest known virtual currency heist to date. Tornado Cash was subsequently use

Money Laundering and Mixer (Tumbler service)



Money Laundering and Mixer (Tumbler service)

Money Laundering:

- Definition: Money laundering is the process whereby the proceeds of crime are transformed into ostensibly legitimate money or other assets. It involves making illicit gains appear legal and breaking up the paper trail connecting funds with their source of criminal activity.
- Process: This typically involves three stages: Placement (introducing the illicit funds into the financial system), Layering (complexifying transactions to confuse any paper trail), and Integration (making the funds re-enter the economic system in an apparently legal form).
- Regulation: Many countries have established regulations and laws against money laundering, requiring financial institutions to implement preventative measures and report suspicious activities.

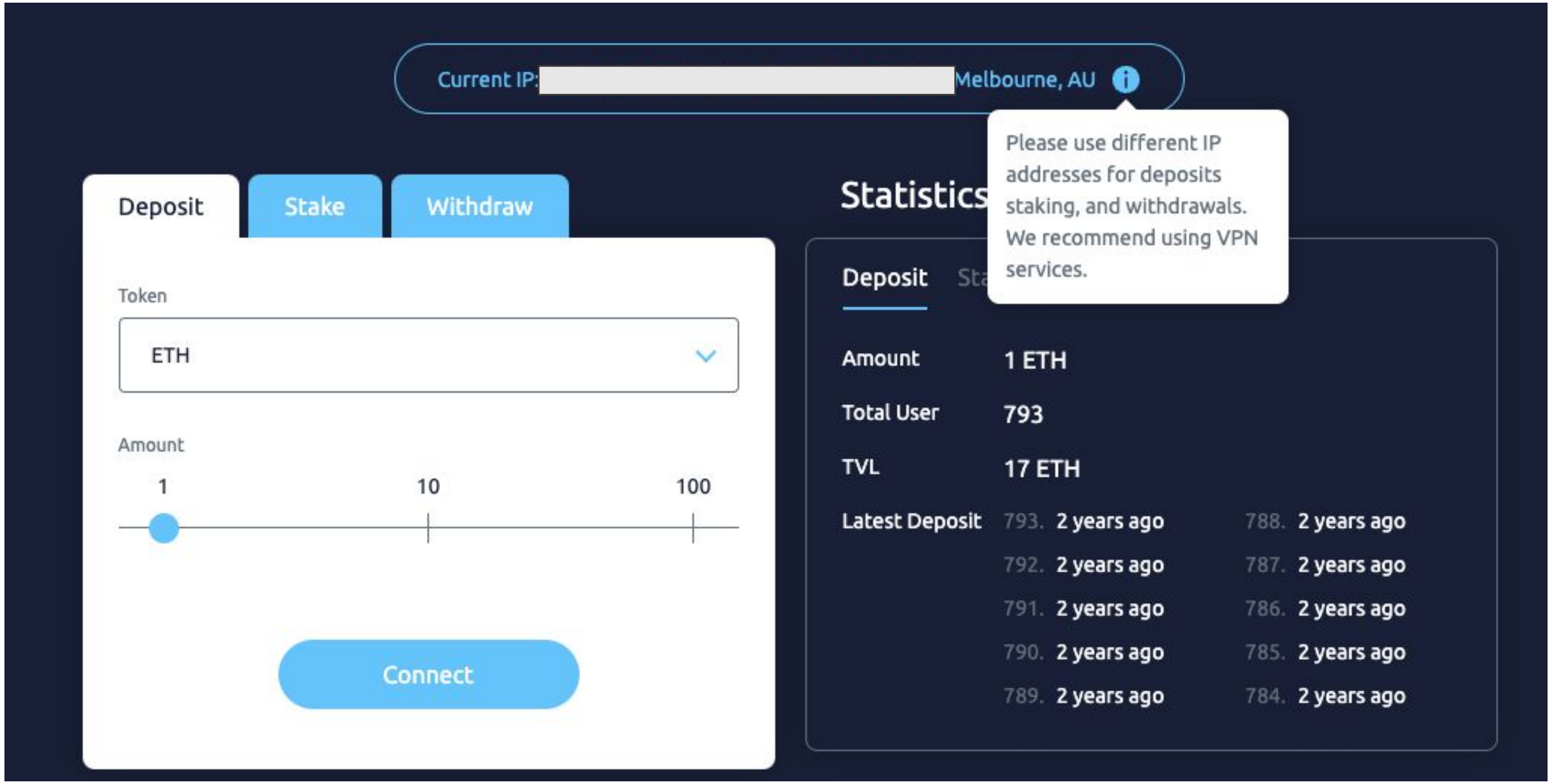
Money Laundering and Mixer (Tumbler service)

Mixer (Tumbler Service):

- Definition: A mixer or tumbler is a service, commonly related to cryptocurrencies, designed to enhance transactional privacy. These services work by receiving cryptocurrencies from users, mixing the sources, and then returning the same amount (minus fees) of cryptocurrency from a different source, thereby breaking the continuity of the fund flow.
- Purpose: While some users utilize mixers to enhance their privacy or security, the service can also be exploited for money laundering or other illicit purposes to obscure the origins of funds.
- Legal Considerations: The use of mixers might be restricted or regulated in certain countries or regions.

It's important to note that while mixers can be used to boost privacy, they can also be misused as a tool for money laundering

Money Laundering and Mixer (Tumbler service)



Current IP: [redacted] Melbourne, AU

Please use different IP addresses for deposits staking, and withdrawals. We recommend using VPN services.

Token: ETH

Amount: 1 (options: 1, 10, 100)

Statistics

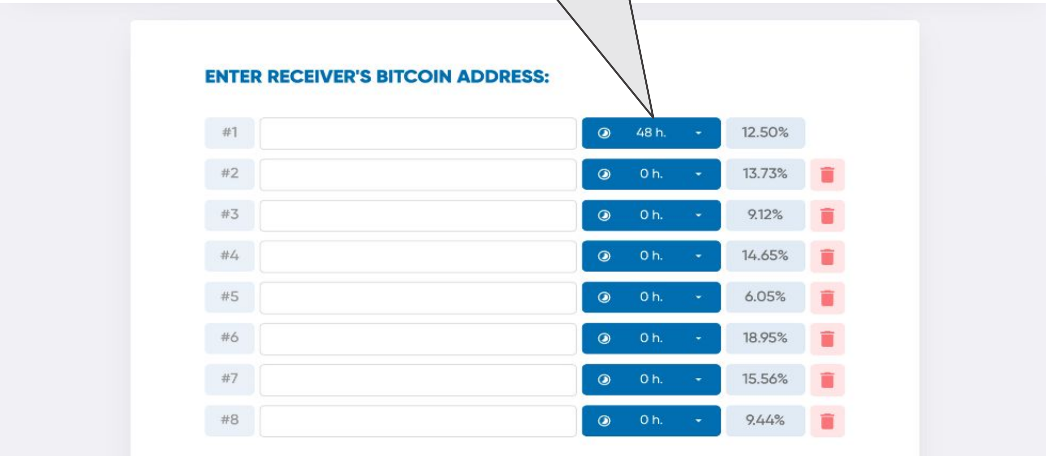
Amount	1 ETH
Total User	793
TVL	17 ETH

Latest Deposit

793. 2 years ago
792. 2 years ago
791. 2 years ago
790. 2 years ago
789. 2 years ago
788. 2 years ago
787. 2 years ago
786. 2 years ago
785. 2 years ago
784. 2 years ago

Money Laundering and Mixer (Tumbler service)

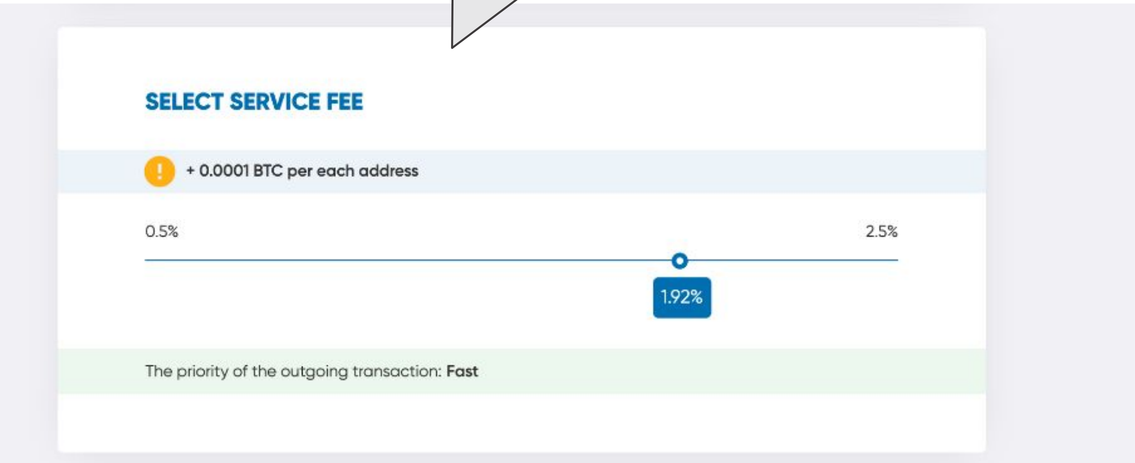
Set delay hour (s)



ENTER RECEIVER'S BITCOIN ADDRESS:

#1		48 h.	12.50%
#2		0 h.	13.73%
#3		0 h.	9.12%
#4		0 h.	14.65%
#5		0 h.	6.05%
#6		0 h.	18.95%
#7		0 h.	15.56%
#8		0 h.	9.44%

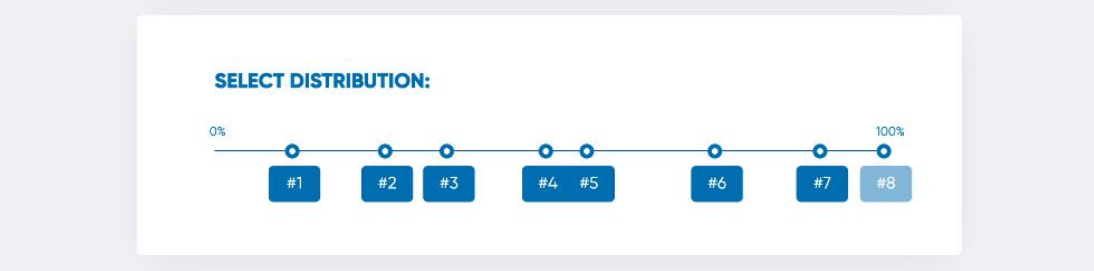
Customise service fee



SELECT SERVICE FEE

+ 0.0001 BTC per each address

The priority of the outgoing transaction: **Fast**

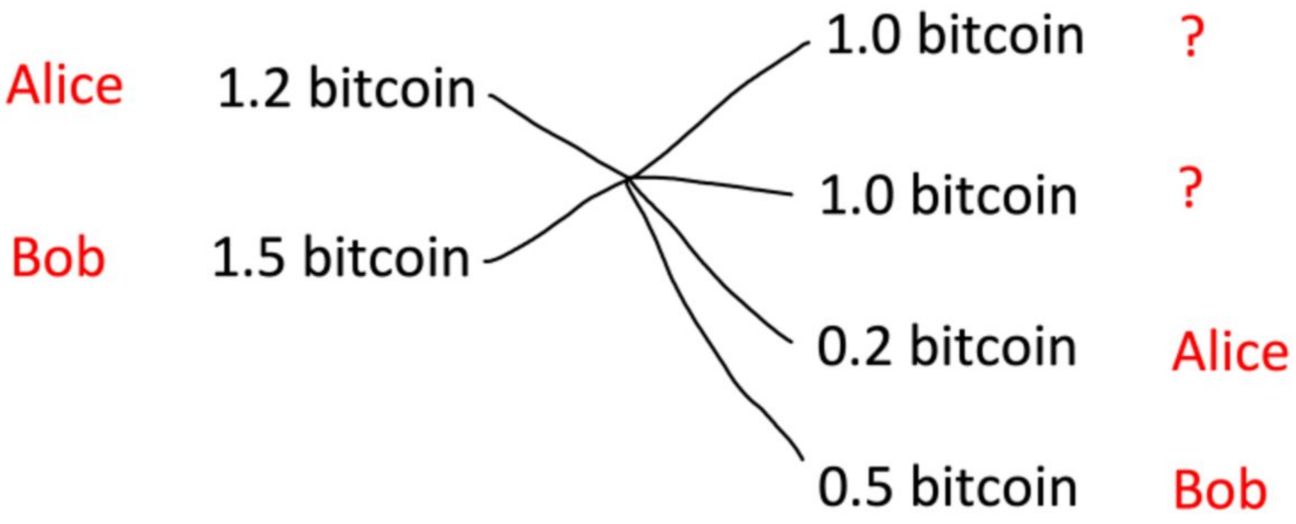


SELECT DISTRIBUTION:

Send cryptos to different addresses (with different distribution)

CoinJoin

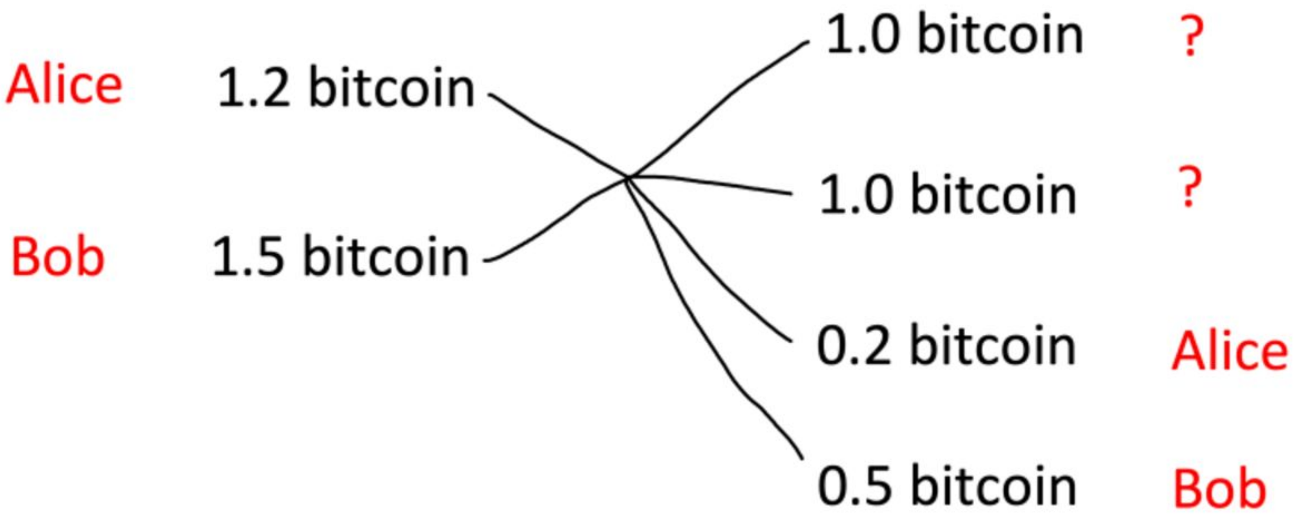
CoinJoin works by pooling together coins from various senders into one transaction. Subsequently, a third party mixes these coins and distributes them to the intended recipients. To enhance privacy, each recipient gets the coins in a new, unused address, minimizing traceability. Essentially, CoinJoin amalgamates transactions to protect the anonymity of the senders.



CoinJoin

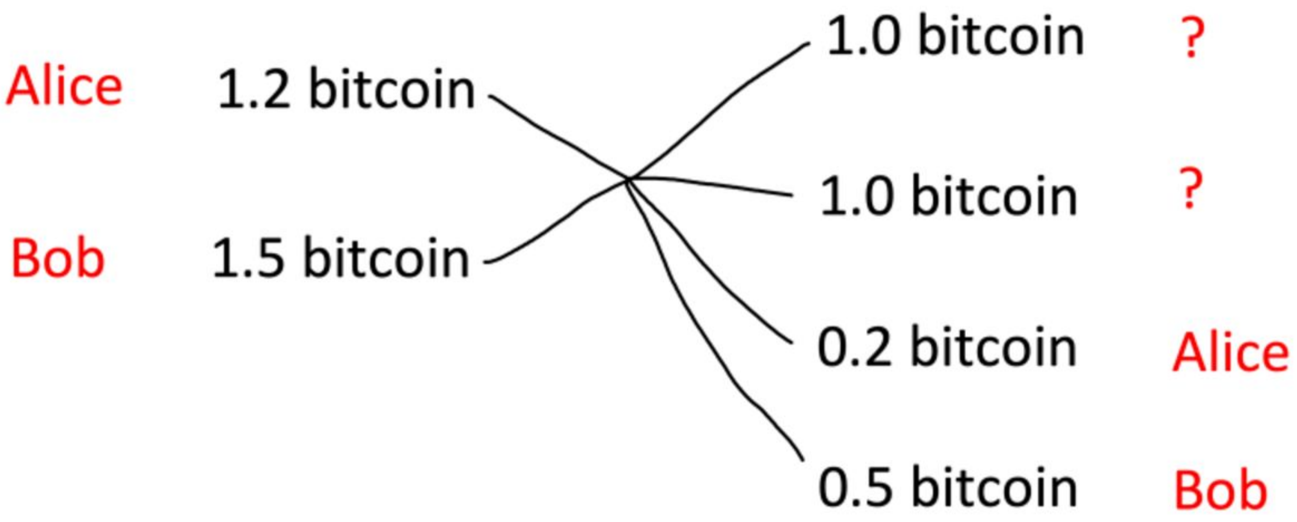
Gathering: Multiple participants (e.g., Alice, Bob) decide to create a transaction together. They each provide their own transaction inputs and outputs.

Merging Transactions: These inputs and outputs are combined into a single transaction. This means that there will be multiple inputs and multiple outputs in the final merged transaction.



CoinJoin

Privacy: Since all the inputs and outputs are mixed together, it's challenging to determine which input corresponds to which output. For instance, an external observer might not be able to determine if the funds from participan A are being sent to participant B, C, or an external address.



Signing and Broadcasting: Once all participant have provided their inputs and outputs and agreed on the merged transaction, they each sign the transaction. Once all necessary signatures are collected, the transaction can be broadcast to the network and confirmed by miners.

ZK-SNARKs

"ZK-SNARKs" stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge." It's a concept in cryptography that allows for the creation of a proof that can be verified for its correctness without any interaction and without revealing any information contained in the proof. Here's a simplified breakdown:

Zero-Knowledge:
This means that one party (the prover) can prove to another party (the verifier) that they know a piece of information without revealing the information itself.

Succinct:
This means that the proof is very small in size and can be verified in a very short amount of time, regardless of the size of the original data.

ZK-SNARKs

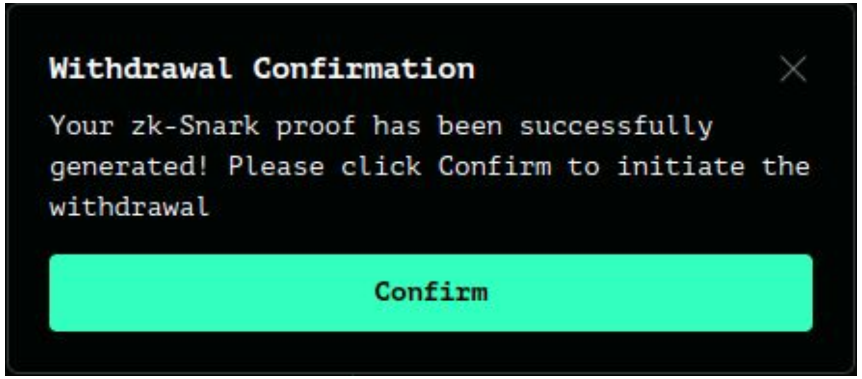
Non-Interactive:
This means that there's no interaction required between the prover and the verifier. The prover can generate a proof, and the verifier can validate it independently, without any further interactions.

Argument of Knowledge:
This implies that the prover is not just demonstrating that a statement is correct, but also proving that they know why it's correct without revealing any additional details.

ZK-SNARKs are often used to enhance privacy and efficiency. For example, they're employed in certain cryptocurrencies like Zcash to facilitate private transactions, where a user can prove the validity of a transaction without revealing the amount, sender, or recipient.

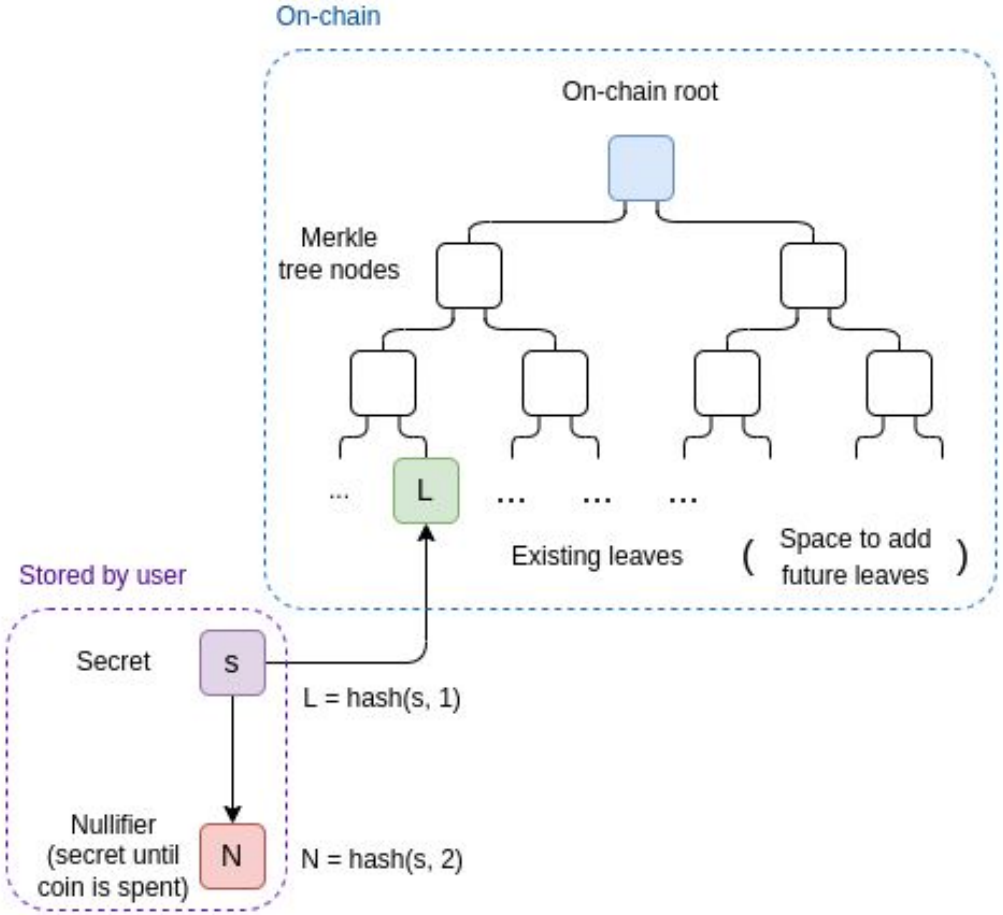
ZK-SNARKs

A crypto mixer, or a mixing service, aims to obfuscate the transaction history of coins, making it challenging to trace their origin. zk-SNARKs contribute to this by allowing the prover (the mixer) to convince the verifier (anyone auditing the transaction) that they possess certain information (the valid transaction) without revealing what that information is.



Withdrawal Confirmation

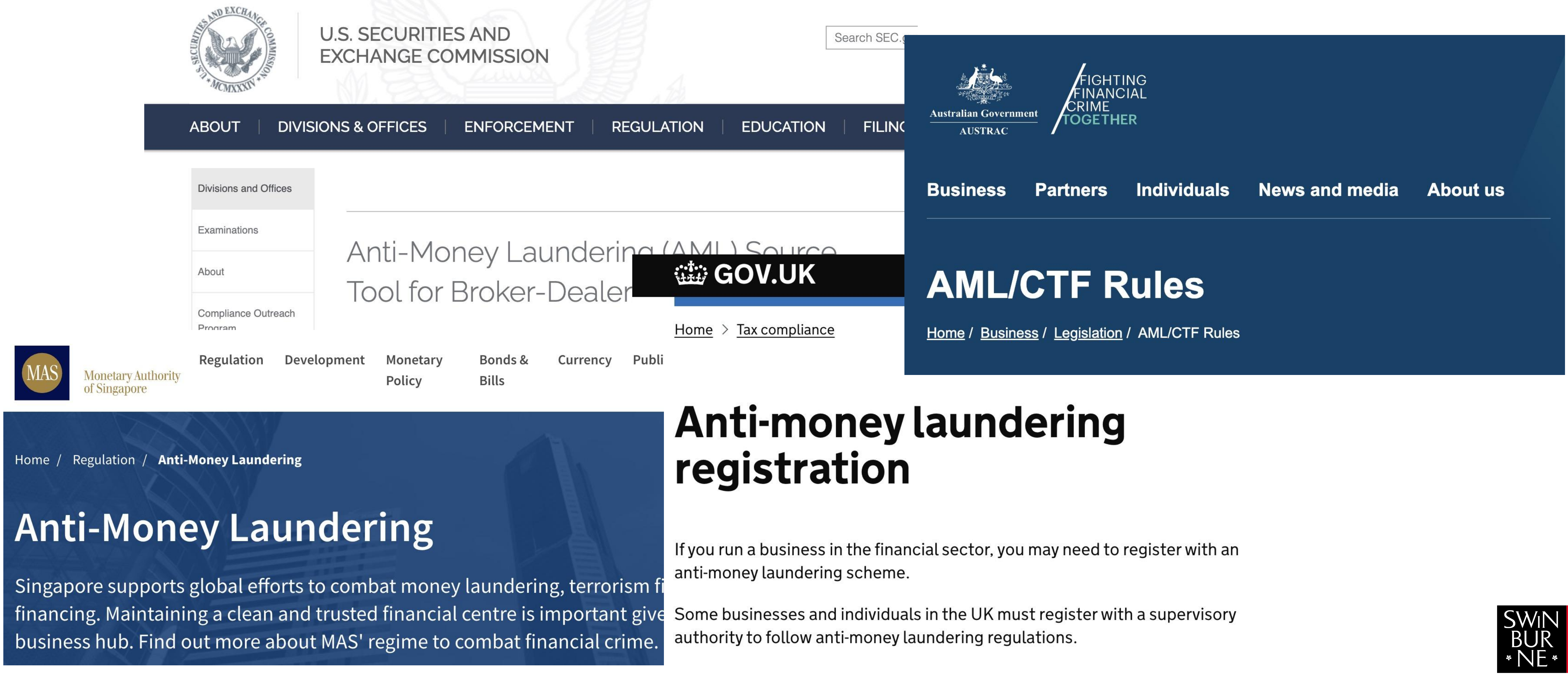
Your zk-Snark proof has been successfully generated! Please click Confirm to initiate the withdrawal



AML in Cryptocurrency

AML

Anti-Money Laundering (AML) processes are designed to prevent and detect activities related to money laundering and other financial crimes.



U.S. SECURITIES AND EXCHANGE COMMISSION

Search SEC.g

ABOUT | DIVISIONS & OFFICES | ENFORCEMENT | REGULATION | EDUCATION | FILINC
Divisions and Offices
Examinations
About
Compliance Outreach Program

Anti-Money Laundering (AML) Source Tool for Broker-Dealer

Australian Government AUSTRAC

FIGHTING FINANCIAL CRIME TOGETHER

Business
Partners
Individuals
News and media
About us

AML/CTF Rules

Home / Business / Legislation / AML/CTF Rules

GOV.UK

Home > Tax compliance

Anti-money laundering registration

If you run a business in the financial sector, you may need to register with an anti-money laundering scheme.

Some businesses and individuals in the UK must register with a supervisory authority to follow anti-money laundering regulations.

MAS Monetary Authority of Singapore

Home / Regulation / Anti-Money Laundering

Anti-Money Laundering

Singapore supports global efforts to combat money laundering, terrorism fi financing. Maintaining a clean and trusted financial centre is important give business hub. Find out more about MAS' regime to combat financial crime.

Icons have been designed using resources from Flaticon.com

AML Red Flags

Financial Action Task Force (FATF) has conducted research into the characteristics of cryptocurrency money laundering. The research drew from previous FATF investigations into crimes involving virtual assets and from over 100 case studies contributed by jurisdictions across the FATF Global Network since 2017.

Transaction Type

- Making a series of high-value cryptocurrency transactions in a short period of time
- Structuring cryptocurrency transactions in small amounts to avoid reporting thresholds.
- …

Transaction Pattern

- Transactions involving multiple cryptocurrencies or multiple accounts with no logical business explanation.
- Frequent transfers of large amounts of crypto within a set period of time (day, week, month) to the same account from more than one person.
- …

Anonymity

- Transactions involving more than one type of cryptocurrency, or cryptocurrencies offering high levels of anonymity.
- Move funds from a transparent public blockchain to a centralized cryptocurrency exchange, and then immediately trading those funds for an AEC or privacy coin.
- …

AML Red Flags

Senders and Recipients

- Users that create multiple accounts under different names to circumvent the exchange’s trading and withdrawal limits, or that attempt to open accounts frequently using the same IP address.
- Transactions that originate from untrustworthy or suspicious IP addresses or high-risk jurisdictions.
- …

Source of Funds

- Transactions involving cryptocurrency accounts with known links to illegal activities, such as fraud, extortion, ransomware or darknet marketplaces, or transactions to or from online gambling sites.
- A single cryptocurrency wallet linked to multiple credit or debit cards that are used to withdraw large amounts of fiat currency.
- …

Geographical Risks

- Cryptocurrency funds that originate in or are being sent to an exchange that is registered in a different country than the customer or the exchange.
- Customers using cryptocurrency exchanges or service providers located in high-risk jurisdictions or that are known to have inadequate AML/CFT measures.
- …

Crypto Companies and Their AML Procedures

AML procedures are crucial for crypto companies to ensure they comply with regulations and prevent illicit activities. Here's a general overview of how they typically follow AML procedures:

Customer Due Diligence (CDD)
verify the identity of their users through Know Your Customer (KYC) procedures.

Transaction Monitoring
Companies employ sophisticated tools to monitor transactions in real-time.

Risk Assessment
Crypto companies assess the risk associated with each customer.

Crypto Companies and Their AML Procedures

Automated Systems
Automated AML systems that can quickly analyze large amounts of data.

Reporting and Compliance
If a transaction raises suspicions, the company must report it to relevant authorities.

Ongoing Monitoring
Continuously monitor customer transactions and update their risk assessments as needed.

Training and Awareness
Employees are trained to recognize potential money laundering activities.

Blockchain Analysis
Use blockchain analysis tools (KYT) to trace the source and destination of funds on the blockchain.

AML Compliance Officer
Appoint an AML compliance officer or team responsible for overseeing and enforcing AML policies.

KYC (Know-Your-Customer)

KYC is designed to protect financial institutions against fraud, corruption, money laundering and terrorist financing.

Establish customer identity

Understand the nature of customers' activities

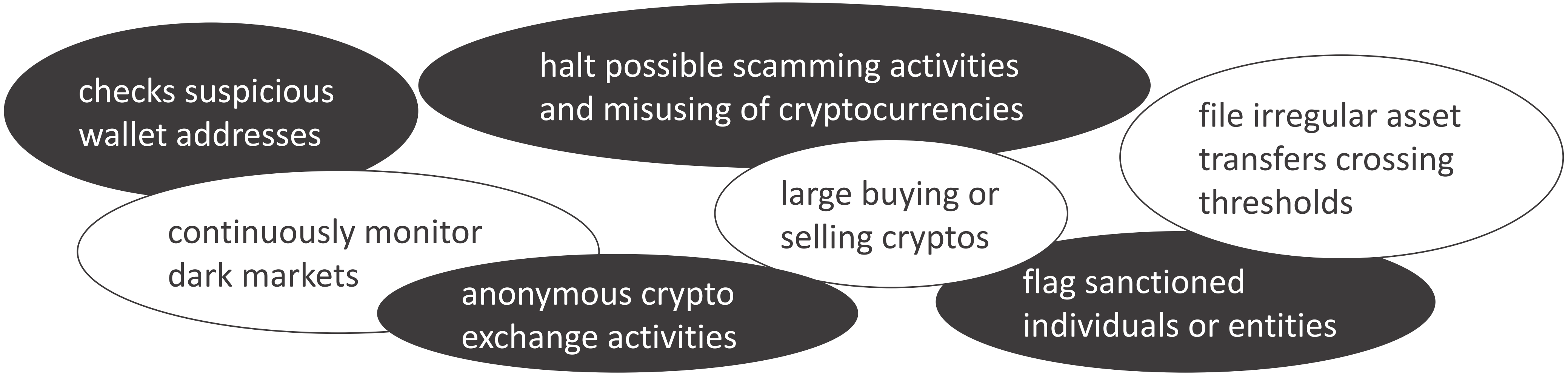
Qualify that the source of funds is legitimate

Assess money laundering risks associated with customers

KYT (Know-Your-Transaction)

KYT (Know-Your-Transaction) refers to **examining both fiat and crypto transactions**. It gives institutions the aptitude to break down and structure crypto transactions

KYT is essential to determine money laundering, fraudulent activities, or suspicious behaviours, sometimes as serious as a mass proliferation of weapons or drug trafficking.



checks suspicious wallet addresses

halt possible scamming activities and misusing of cryptocurrencies

file irregular asset transfers crossing thresholds

large buying or selling cryptos

continuously monitor dark markets

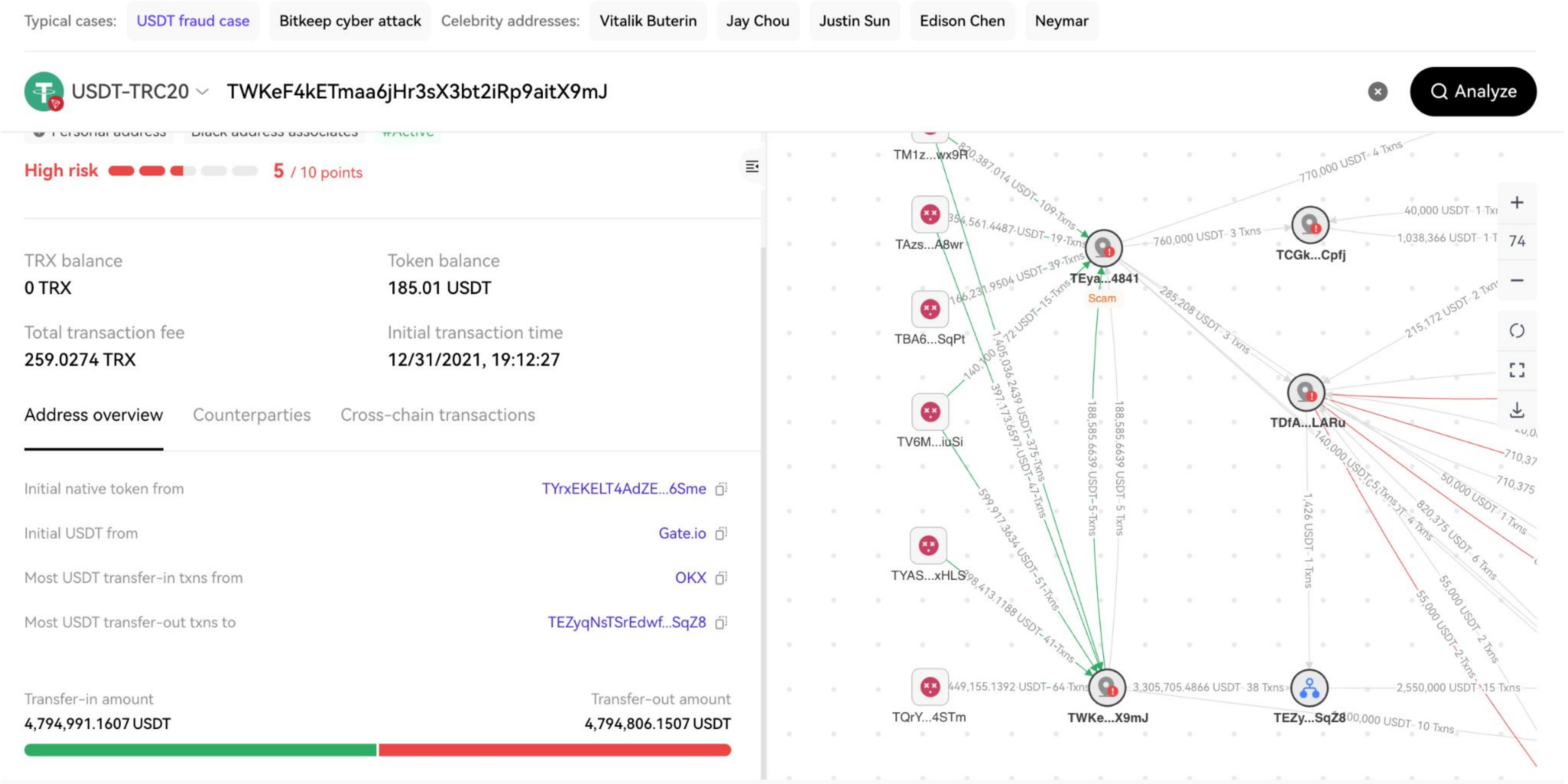
anonymous crypto exchange activities

flag sanctioned individuals or entities

Icons have been designed using resources from Flaticon.com

KYT Tracing Platform

KYT tracing platforms offer KYT services or transaction tracing for compliance purposes. These platforms often use advanced algorithms and data analysis techniques to trace the flow of cryptocurrencies and detect suspicious or high-risk transactions.



Typical cases: USDT fraud case | Bitkeep cyber attack | Celebrity addresses: Vitalik Buterin | Jay Chou | Justin Sun | Edison Chen | Neymar

USDT-TRC20 TWKeF4kETmaa6jHr3sX3bt2iRp9aitX9mJ

High risk 5 / 10 points

TRX balance
0 TRX

Token balance
185.01 USDT

Total transaction fee
259.0274 TRX

Initial transaction time
12/31/2021, 19:12:27

Address overview | Counterparties | Cross-chain transactions

Initial native token from	TYrxEKELT4AdZE...6Sme
Initial USDT from	Gate.io
Most USDT transfer-in txns from	OKX
Most USDT transfer-out txns to	TEZyqNsTSrEdwf...SqZ8

Transfer-in amount
4,794,991.1607 USDT

Transfer-out amount
4,794,806.1507 USDT

KYC vs KYT

KYC	KYT
A **static assessment of the client**, require information provided by the client	Client activities are **monitored in real-time** without creating extra hassle for the clients. Clients are only approached when a transaction hits a red flag
Rely on publicly available data of the client, and information provided by the client	Brings **data-driven conclusions** by examining transactions in real time