AML/CFT 101

CFATF Secretariat Research Desk
March 24, 2021

How can Virtual Assets be used for the commission of Financial Crime?

What are Virtual Assets (VAs)?

"A Virtual Asset" refers to a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes.

Virtual assets **do not** include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

Source: *FATF Guidance for a Risk- Based Approach- Virtual Assets and Virtual Asset Providers* ***and the FATF Glossary***

What are Virtual Asset Service Providers (VASPs)?

A Virtual Asset Service Provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

i. exchange between virtual assets and fiat currencies;

ii. exchange between one or more forms of virtual assets;

iii. transfer of virtual assets;

iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and

v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Source: *FATF Guidance for a Risk- Based Approach- Virtual Assets and Virtual Asset Providers* ***and*** ***the FATF Glossary***

What can VAs be used for?

Virtual Assets have many potential benefits. They could make payments easier, faster, and cheaper; and provide alternative methods for those without access to regular financial products. However, without proper regulation, they risk becoming a virtual safe haven for the financial transactions of criminals and terrorists.

The FATF has been closely monitoring the developments in the cryptosphere and in recent years has seen the first countries start to regulate the virtual assets sector, while others have prohibited virtual assets altogether.

However, most countries have not taken any action. These gaps in the global regulatory system have created significant loopholes for criminals and terrorists to abuse.

Source: Easy Guide to FATF Standards and Methodology- Virtual Assets: what, When, How?

Blockchain, bitcoin, crypto assets, virtual currencies

A digital asset which has no intrinsic value, or physical form that is used as a medium of exchange.

Uses cryptography to secure transactions and generate additional units.

Supply not determined by a Central Bank.

Built on the blockchain; a type of distributed ledger data structure.

Cited by many to be “the future of money”.

Valuable only because users believe they are (i.e. there is no underlying asset/intrinsic value).

Bitcoin was the FIRST cryptocurrency to use the blockchain to record and verify transactions.

In circulation since 2009; shortly after global financial crisis.

The largest crypto asset by Market Capitalization.

Each cryptocurrency more or less serves a different purpose; although there are instances of overlap.

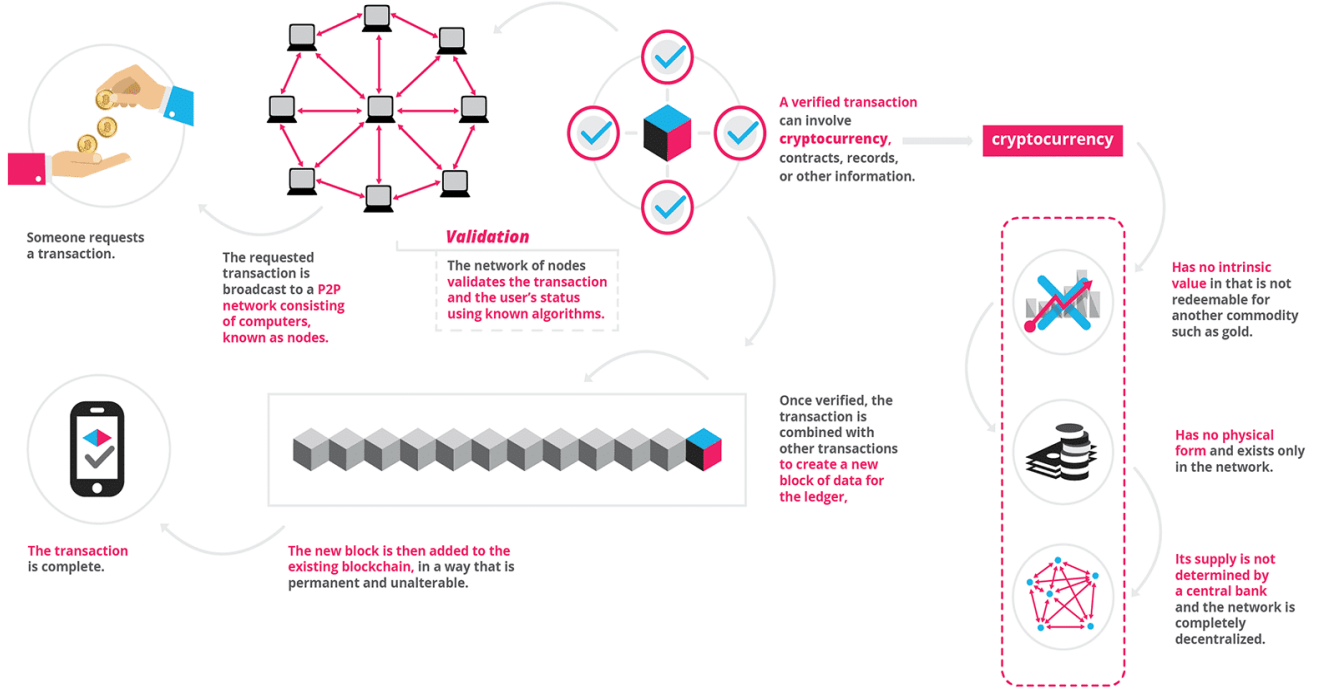
There are 100+ crypto currencies in circulation.

What is the "Blockchain?" (1)

- A type of Distributed Ledger Technology.
- Picture a spreadsheet that is duplicated millions of times, and distributed across a network of computers.
- This spreadsheet is updated, and those updates are reflected on all copies of the 'spreadsheet' across the computer network.
- Transaction history is stored on 'blocks' of information, validated by network of computer nodes.
- Computer nodes validate transactions by solving complex algorithms (i.e. complex mathematical operations).
- Immutable record of transaction history.

What is the "Blockchain?" (2)

- Blockchain originated just over 15 years ago.
- Blockchain can also be described as innovative technology to swiftly transfer value around the world.
- The fast-evolving blockchain and distributed ledger technologies have the potential to radically change the financial landscape.
- However, because of their speed, global reach and above all - anonymity – they also attract those who want to escape authorities' scrutiny.

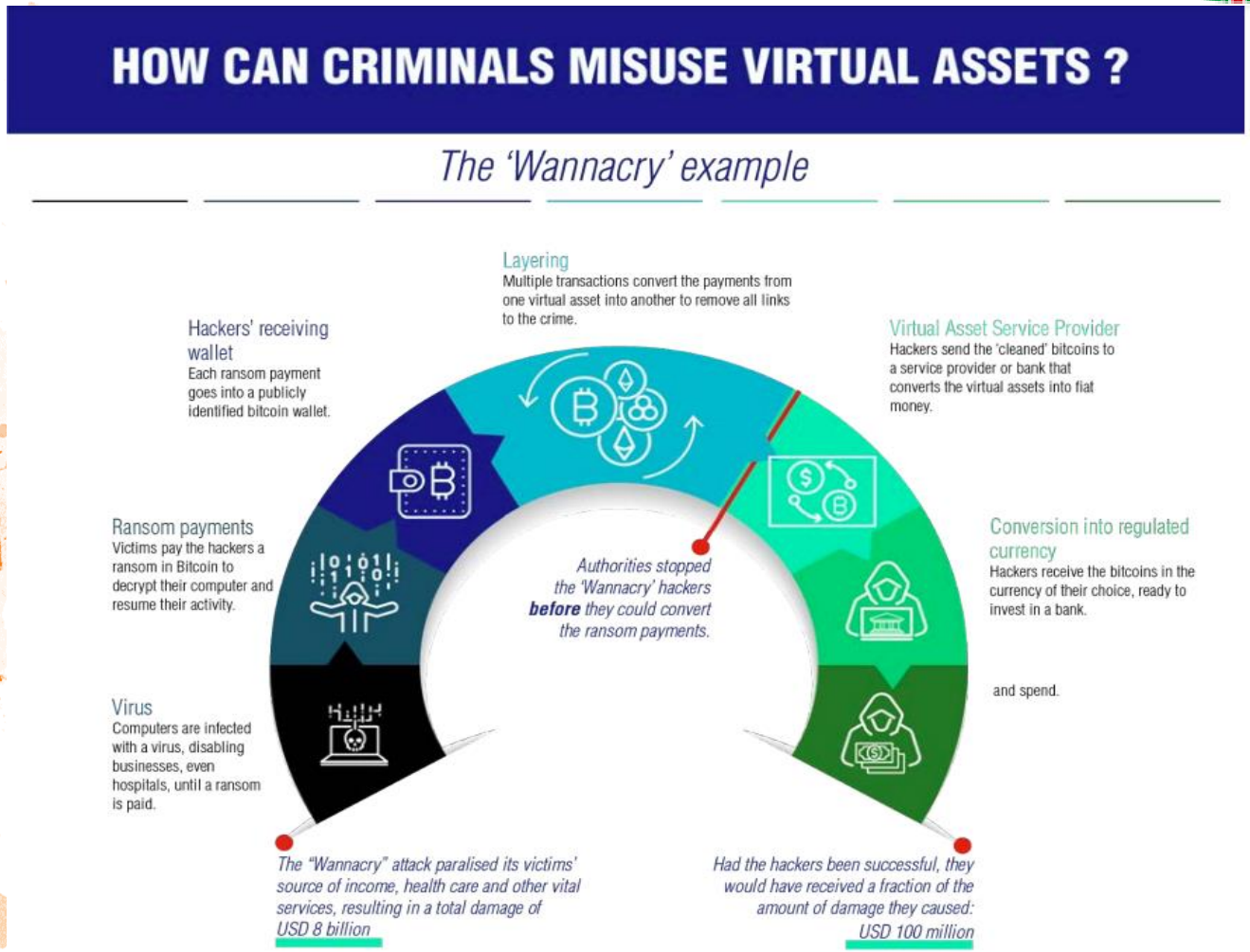


How can VAs be misused for AML/CFT? (1)

The FATF identified potential AML/CFT risks of using VAs as,

- Anonymity.
- Lack of a centralised oversight body.
- Global reach.
- Complex infrastructures as the basis for the cause for concern.
- In 2017 the “Wannacry” ransomware attack held thousands of computer systems hostage until the victims paid hackers a ransom in bitcoin. The cost of the attack went far beyond the ransom payments, it resulted in an estimated USD 8 billion in damages to hospitals, banks and businesses across the world. Other ransomware attacks have happened since and appear to be on the rise. See next slide for more information.

How can VAs be misused for AML/CFT? (2)



Source: Easy Guide to FATF Standards and Methodology- Virtual Assets: what, When, How?

How can VAs be misused for AML/CFT? (3)

Recently, the Caribbean's biggest conglomerate, Ansa McAl, was the victim of ransomware hackers holding some of the company's IT systems hostage.

Tatil, Trinidad and Tobago's biggest insurer, was effectively stalled for about two weeks as the IT department worked to find and expel the ransomware from the company's servers. If not, the company may have to pay the hackers' ransom to free its data.

American cybersecurity specialist and ransomware recovery and prevention expert Eric Taylor (@ITSimplife) first noted the Ansa McAl attack. REvil, a criminal cybergang, has claimed responsibility.

The group says it has "numerous financial documentation, agreements, invoices, reports." A screenshot of the hacked haul reveals a count of 17,000 documents. The group threatened, in the post that confirmed the hack, to release the confidential documents to a public server.

Source: Trinidad and Tobago Newsday

FATF's focus on virtual assets

The FATF has been closely monitoring the developments in the cryptosphere and in recent years has seen the first countries start to regulate the virtual asset sector, while others have prohibited virtual assets altogether. However, the majority of countries have not taken any action.

These gaps in the global regulatory system have created significant loopholes for criminals and terrorists to abuse.

With support from the G20, the FATF has issued global, binding standards to prevent the misuse of virtual assets for money laundering and terrorist financing.

The FATF standards ensure that virtual assets are treated fairly, applying the same safeguards as the financial sector. FATF's rules apply when virtual assets are exchanged for fiat currency, but also when they are transferred from one virtual asset to another.

Source: Easy Guide to FATF Standards and Methodology- Virtual Assets: what, When, How?

What to do about it?

Countries need to implement the FATF's measures to ensure transparency of virtual asset transactions and keep funds with links to crime and terrorism out of the cryptosphere. Today, many VASPs are perceived as "risky business" and denied access to bank accounts and other regular financial services.

While implementing the FATF's requirements will be challenging for the sector, it will ultimately increase trust in blockchain technology as the backbone behind a robust and viable means to transfer value. The FATF has revised its assessment methodology, which sets out how it will determine whether countries have successfully implemented the FATF Recommendations regarding the regulation of the VASP sector.

Application of the FATF Standards

The effective global implementation of these Standards by all countries will ensure virtual asset technologies and businesses can continue to grow and innovate in a responsible way, and it will create a level playing field. It will prevent criminals or terrorists seeking out and exploiting jurisdictions with weak or no supervision.

Countries should:

- Understand the money laundering and terrorist financing risks the sector faces.
- License or register VASPs.
- Supervise the sector, in the same way it supervises other financial institutions.

Role of the VASPs

- VASPs need to Implement the same preventive measures as financial institutions, including customer due diligence, record keeping and reporting of suspicious transactions.
- Obtain, hold and securely transmit originator and beneficiary information when making transfers.

Where does a VASP need a license or registration?

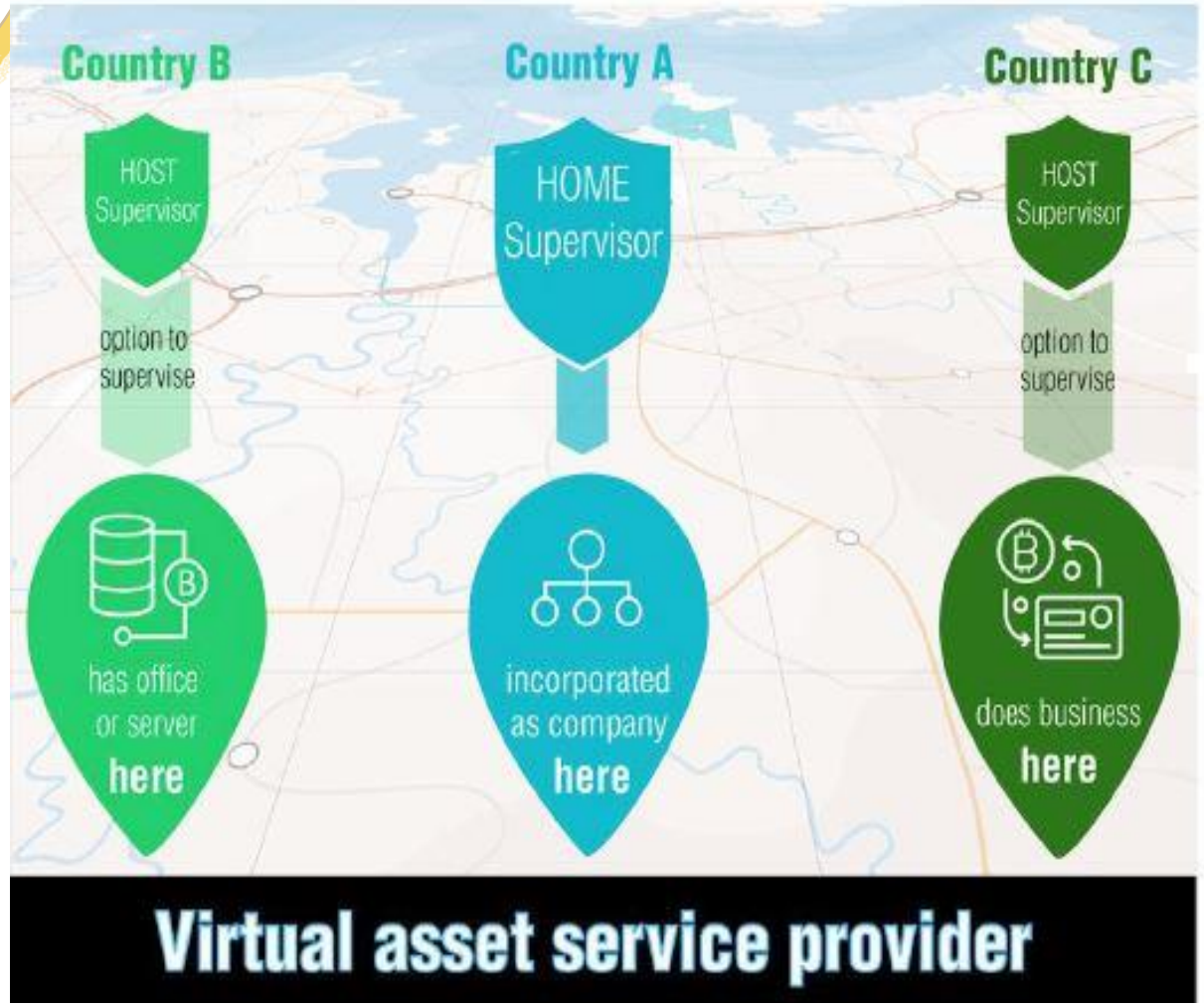
Country where the company is incorporated - always/ mandatory.

Location of management - sometimes/optional for countries.

Location of servers/back-office functions - sometimes/optional for countries.

Countries where you have significant numbers of customers - sometimes/optional for countries.

VASPs may need licenses or registrations from multiple national authorities if they do business in several countries



Source: Easy Guide to FATF Standards and Methodology- Virtual Assets: what, When, How?

FATF Publications and Useful Links

- FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers
- The FATF Standards: FATF Recommendations
- FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems
- Money laundering risks from “stablecoins” and other emerging assets
- FATF dedicated webpage on Virtual Assets