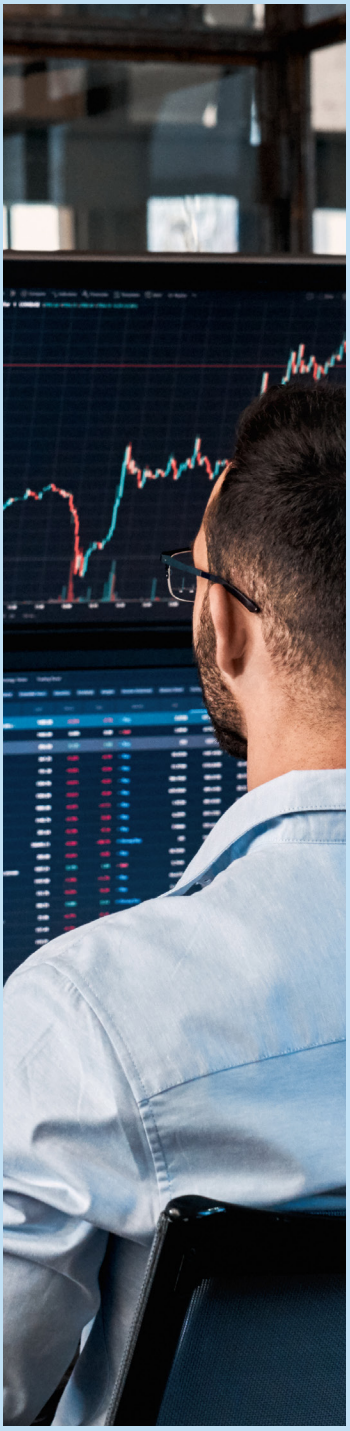
VIEW POINT



THE ANTI-MONEY LAUNDERING RISKS OF CRYPTOCURRENCIES

Abstract

Cryptocurrencies (such as Bitcoin, Ethereum, and Litecoin) have undergone substantial adoption by customers since the launch of Bitcoin in 2009. However, these assets also bring in substantial money laundering risks for the financial services industry. In fact, cryptocurrencies are increasingly turning into one of the most favored means for money launderers.
This viewpoint shares insights on why money launders are attracted to cryptocurrencies, the key methods utilized for laundering money using cryptocurrencies, regulatory responses, and recommendations for firms to minimize their cryptocurrency Anti-Money Laundering (AML) risks.

Infosys®
Navigate your next

Overview

Cryptocurrencies like Bitcoin, Ethereum, Litecoin, etc. have undergone substantial adoption by customers since the launch of Bitcoin in 2009. This is thanks to various factors such as increased efficiency, and low ownership costs, exchange rates and charges for international transactions. As a result, good number of crypto exchanges have sprung up in recent years. Leading banks in several nations have also been welcoming the crypto assets. In fact, the global cryptocurrency market size is expected to surpass US$ 1125.8 million by 2028 (up from ~ US$ 858 million in 2021) at CAGR of 3.5% during the period 2022-2028.[1]

As adoption of cryptocurrencies is increasing with easy passing day, it's bringing in substantial money laundering risks for the financial services industry. Cryptocurrencies are increasingly becoming amongst the most favored means for money launderers and other fraudsters to perpetrate financial crime. As a result, even legitimate organizations are potentially at risk of having their cryptocurrency platforms and services used for cross-border money laundering and terrorist financing.

Cryptocurrency and Financial Crime — Facts and Examples

As per Chainalysis, in 2019, around US$ 2.8 billion money was laundered via crypto exchange. [2]
As per Ciphertrace, in 2020, criminally related bitcoin addresses sent USD 3.5 billion.[3]
It is estimated that 1/3rd of bitcoin sent across the borders goes to exchanges having visibly weak CDD controls. [4]
In June 2021, expert detectives from London Metropolitan Police Economic Crime Command, examining money laundering crimes, confiscated crypto assets of £114 million. [5]
In July 2021, US Department of Justice stated that a Swedish man was punished to 15 years in jail for money laundering, securities fraud, and wire fraud that had cheated 1000s of victims of over US$16 million via investment scam. The man had lured victims to buy shares in investment scheme utilizing cryptocurrency. [6]
In June 2021, China's Ministry of Public Security had arrested over 1,100 persons that were suspected of utilizing cryptocurrencies to launder the illegal proceeds via internet and telephone scams. Also, the police busted over 170 money laundering groups that were charging their criminal clients commission of 1.5-5% to convert their illegal earnings into virtual currencies through crypto exchanges. [7]

Table 1: Facts and Examples of Financial Crime Using Cryptocurrency

Why Are Money Launderers Attracted to Cryptocurrency?

Following are some of the key factors that make cryptocurrencies appealing to money launderers:

Lack of comprehensive KYC/AML regulations for entities dealing in virtual and cryptocurrency (virtual asset service providers (VASPs), crypto wallet providers, crypto exchanges, etc.)
Anonymity or pseudonymity of cryptocurrency transactions
Obfuscation of transaction flows and counterparties
Security vulnerabilities present in some of the cryptocurrency system
Cross-border nature of transaction
Capacity to carry out transactions outside the traditional financial system

Table 2: Key Factors That Make Cryptocurrency Attractive to Money Launderers

Key Money Laundering Methods Using Cryptocurrency

Refer below the most popular methods used by fraudsters for money laundering using cryptocurrency.

Tumbling / Mixing Services	Unregulated Exchanges	Online Casinos & Gambling Platforms	Money Mules	Nested Services

Exhibit 1: Key Money Laundering Methods Using Cryptocurrency

Tumbling/Mixing Services: To help conceal their funds' trail before these are transferred to major exchanges or to legitimate businesses, mixing services is provided to criminals where they are permitted to mix dubious cryptocurrency funds with other funds. Mixers mix the digital assets from several addresses before pushing them at random period of time to new destination wallets or addresses. This increases anonymity and makes the illegal coin trail difficult to trace by the auditors. As an example, in Aug 2021, Helix (a custodial mixing service) was charged by US DOJ in a US$300 million conspiracy involving money laundering of the assets produced via drug trafficking and other illegal activities. [8] As another example, Bestmixer custodial mixer was seized and shut down by European police for allegedly facilitating laundering of over US$200 million in cryptocurrency for its customers. [9]

Unregulated Exchanges: To clean their illegal funds, criminals often transact via unregulated cryptocurrency exchanges. Such exchanges have insufficient AML controls in place. For example, these exchanges require no or very little user identity verification for transferring crypto assets. This makes it easy for the money launderers to hide their tracks. For example, this approach was utilized during Coincheck money laundering scandal in 2018. [10]

Online Casinos and Gambling Platforms: In this method, cryptocurrency is laundered through online casino and gambling platforms. Criminals put their bets using stolen coins. After the game is completed, criminals withdraw the winning coins and change these for real money.

Money Mules In this method, money launderers recruit money mules (i.e., individuals with tidy transaction history), to launder the illicitly received cryptocurrencies. In certain cases, criminals utilize Ponzi schemes to gather cryptocurrencies from victims and the money mules move coins between the accounts to conceal the source of illegal coins. As per Europol, 90% of the money-mule transactions in Europe have related to cybercrimes. [11]

Nested services: These are a wide category of services which operate inside one or several exchanges. These services use addresses that are hosted by exchanges to tap into liquidity of exchanges and exploit opportunities to execute trade. On blockchain ledger, nested services transactions show as having been executed by host counterparties (i.e., exchanges) instead of individuals' addresses or hosted nested services. This allows criminals to exploit such anonymity for conducting money laundering. The most common nested service type is an over the counter (OTC) broker, who allows traders to anonymously, securely, and easily trade large values of cryptocurrency.

Regulatory Response

In recent years, owing to the increased money laundering via cryptocurrencies, regulators worldwide have been working to enable relevant regulations to counter this menace. Refer below few examples:

Financial-Action-Task Force (FATF): In Oct 2018, FATF had updated its Recommendation 15 which brought virtual assets (including cryptocurrencies) within its AML regulations' scope. Further, in Jun 2019, FATF through its Interpretive Note to Recommendation 15 clarified on how its requirements should be applied vis-à-vis virtual assets (VAs) and VASPs. The updated FATF requirements mandate VASPs and other concerned entities a) to be regulated for AML/CFT, b) be registered or licensed, c) adopt risk-based approach to VA-related activities, d) ensure robust monitoring and supervision, e) implement robust preventive measures (e.g., CDD), record keeping, suspicious transaction reporting, etc.

In June 2019, FATF also adopted Travel Rule which pertains to wire transfers. Under this rule, for payments of USD 3,000 or above, concerned entities such as VASPs must share information (e.g., names, account numbers, and addresses) of both originators and beneficiaries with financial institution or receiving money services business (MSB). Such information must also be made available to the competent authorities, when required.

With the objective to assist regulators, FIs, VASPs and DNFBPs to counter the increasing money laundering menace using cryptocurrency, in 2020, FATF published a report outlining several money laundering/terrorist financing red flag indicators that are associated with virtual assets (VAs). [12]

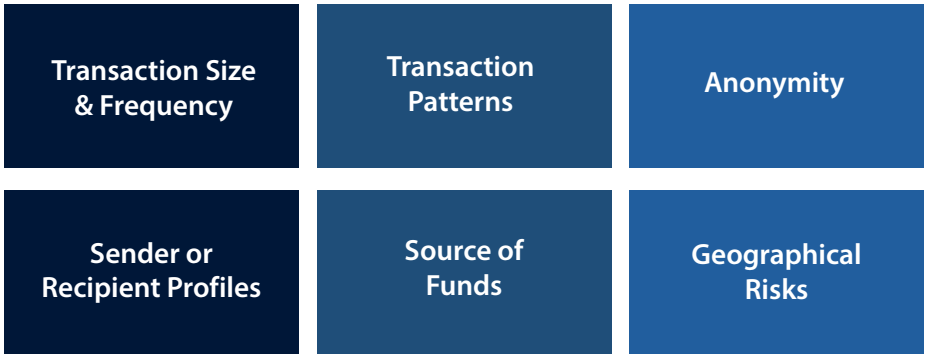


Exhibit 2: FATF Cryptocurrency Money Laundering Red Flag Indicators

United States: In US, cryptocurrencies are regulated by several key agencies such as SEC, CFTC, FTC, Department of Treasury, IRS, OCC and FinCEN. The country places virtual currency exchanges under same regulatory category as the traditional AML/CFT entities such as FIs and money transmitters. Further, US Anti-Money Laundering Act of 2020 (AMLA 2020) expanded the regulation of cryptocurrency and other digital assets. The Act revised the Bank Secrecy Act (BSA) to include cryptocurrency and other digital assets within its regulatory scope. Thereby, it requires businesses dealing in cryptocurrency to register with FinCEN and comply with reporting and recordkeeping requirements for certain virtual currency transactions. Also, cryptocurrency exchange service providers in US need to obtain required license from FinCEN. These entities also need to implement robust AML/CFT and sanctions program. FinCEN also expects cryptocurrency exchanges to comply with FATF Travel Rule.

At state level too, several regulations have been implemented. For example, in 2016, New York State had introduced a licensing framework — named 'BitLicense' — for crypto exchanges and businesses. It requires the concerned firms to attain license from New York State Department of Financial Services (NYSDFS) for holding, buying, selling, or transmitting cryptocurrencies.

Canada: Virtual and cryptocurrency entities in Canada are considered as MSBs and subject to stringent AML regulations. Under Canada's PCMLTFA regulation, reporting entities including MSBs need to comply with several AML/CTF requirements. MSBs in Canada need to comply with the below requirements:

Register with FINTRAC (Canada's FIU). Even foreign MSBs that offer MSB services to people in Canada must register with FINTRAC.
Implement thorough compliance program, including a) written compliance policies and procedures, b) appointment of a compliance officer, c) risk assessment of business relationships and activities, d) ongoing compliance training program, and e) effectiveness review of the compliance program.
Verification of the client's identity (including PEPs and BOs) for certain activities and transactions (e.g., transactions of CAD 10,000 or above in virtual currencies received from an entity/person in single or multiple transaction within 24-hours).
Reporting on certain transactions to FINTRAC (including large cash transactions, electronic funds transfers, suspicious transactions, on terrorist property). Note: Failure to report high value of virtual currency transaction can result in penalty of up to CAD 500,000 for 1st wrongdoing and CAD 1 million for succeeding offences.
Record keeping (including information on names of all entities/persons involved in transaction, nature of their primary occupation or business, and the number of all other accounts that are impacted by the transaction, etc.).

Table 3: Regulatory Requirements for MSBs in Canada

European Union: 5AMLD, which came into effect in Jan 2020 — explicitly brings the offerer of exchange services between fiat and virtual currencies, and also the custodian wallet providers into the regulatory scope. 5AMLD also mandates EU countries to ensure registration of such providers. Further, 5AMLD provides FIU the authority to attain addresses and identities of the virtual currency owners. 6AMLD — which came into effect in Dec 2020 — has further tightened the AML/CTF requirements for cryptocurrency exchanges and wallets.

Further, according to its legislative proposal in July 2021, the European Commission plans to extend the AML rules to entire crypto sector. It plans to amend the 2015 EU Regulation on Transfers of Funds to extend its scope to crypto sector. Both senders' and beneficiaries' information will need to be provided by VASPs for crypto transfers — same as what payment service providers do for the wire transfers. Also, EC intends to ban anonymous crypto asset wallets.

United Kingdom: In 2018, the UK Government had created a Cryptoassets Taskforce that comprised representatives from Bank of England, HM Treasury, and FCA. Post the publication of a report by the taskforce, in Jan 2020, FCA was designated as AML/CTF supervisor for the cryptoasset firms. Businesses engaging in cryptoasset activities in UK need to comply with UK MLR 2017 regulatory requirements. These firms need to submit financial crimes related information to FCA as yearly reports. Also, such firms need to register with FCA prior to conducting business — else they face criminal or civil enforcement. FCA's registration requirement helps ensure that these firms have adequate AML controls and systems in place, and their management are capable of effectively executing their AML responsibilities. Application for registration to FCA asks for several information — including key individuals involved in business, organizational structure, beneficial owners, and on AML systems and controls (including on CDD and ongoing transaction monitoring).

Australia: In Australia, AUSTRAC has issued strong cryptocurrency regulations. The rule mandates the regulated entities to gather information for establishing a customer's identity, monitor their transactions, and report the transactions as per the requirements of AML/CTF Act 2006. Unregistered digital currency exchange providers face financial penalties and criminal charges. ASIC too has issued regulatory guidelines that cryptoasset participants need to adhere to.

Singapore: Monetary Authority of Singapore (MAS) has implemented regulations for the cryptocurrency sector under the country's Payment Services Act 2019 (PS Act). In order to sell, buy, transfer or hold cryptocurrencies, an entity needs to seek license and comply with relevant AML/CTF rules. The PS Act covers people who deal in digital payment tokens (DPTs) or facilitate exchange of DPTs to fiat or other DPTs. Also, MAS performs close surveillance of DPT entities. Further, it leverages data analytics techniques — over public, other data sources (e.g., corporate registry info, STRs), etc. — to discover unlicensed DPT activities and take enforcement actions.

Hong Kong: In Hong Kong, SFC treats cryptocurrency assets similar to all other regulated security assets. Crypto exchanges opening a trading venue in the country need to comply with new licensing laws and limit trading to only the institutional clients.

Japan: JFSA had, in 2017, established Fintech Monitoring Office comprising specialists in IT including on blockchain and the experts on AML/CFT regulation. Since then, this team has been monitoring the registered CSPs in the country. They have also been following up with CSPs to address identified shortcomings. To identify the risks and shortcomings and assign risk rating to the individual entities, JFSA has been gathering extensive quantitative and qualitative information from CSPs — including on clients' risk profile, the services provided, varieties of cryptoassets transacted, and the tools utilized by CSPs for transaction monitoring and risk analysis. Further, in 2020, JFSA amended the country's Payment Service Act (PSA) and Financial Instruments and Exchange Act (FIEA) to help safeguard crypto investors, and bring derivatives, STOs and ICOs under JFSA's oversight.

South Korea: South Korea implemented AML requirements for cryptocurrency businesses in 2021. Crypto exchanges need to implement several KYC and AML measures. Registered VASPs in the country need to file suspicious transaction reports (STRs) with Financial Services Commission (FSC). Also, they need to verify their customer identities and can be subjected to compliance inspections. Crypto firms engaging in trading, custody, exchange, sales, and digital wallet services need to register with FSC. These requirements are in addition to those stipulated under the Special Payments Act — a comprehensive regulatory act on cryptocurrency. In South Korea, privacy coins (e.g., ZCash, Monero, and Dash) — which add an additional layer of anonymity to cryptocurrency transactions — are banned.

India: In 2018, owing to AML, consumer protection, and market integrity concerns, RBI had banned cryptocurrency trading and forbade Indian banks from dealing with cryptocurrency exchanges. However, in 2020, the Indian Supreme Court revoked the ban. India has also started work on state-backed CBDC, the digital rupee. Also, in 2021, a proposed crypto regulatory framework was published on the website of Lok Sabha.

Recommendations for Firms to Minimize Their Cryptocurrency AML Risks

Risk assessment: When evaluating their cryptocurrency risks, firms should thoroughly evaluate and understand the type of cryptocurrency they are dealing with, and the risks related with each type. This is because, each type of cryptocurrency presents a different form of risk. For example, privacy coins pose the biggest AML risk.

Also, firms should take a holistic approach to risk assessment. For example, if a client is bringing cryptocurrency in from exchange, firms should have a mechanism in place to work with the particular exchange and understand all the cryptocurrencies and transaction types that the said client has been dealing in. In case an FI engages VASPs to offer cryptocurrency services, they must upfront conduct thorough due diligence and risk assessment of the concerned VASPs — on all aspects (including regulatory compliance, business process, and AML technology capabilities).

AML Process: Firms should effectively implement all AML processes — including KYC verification, CDD/EDD, PEP screening, sanctions screening, adverse media screening, transaction filtering, ongoing transaction monitoring, record keeping, suspicious transaction reporting, etc. — that have been traditionally implemented by FIs to counter money laundering using fiat currency. Also, to prevent money laundering, wallet addresses and transaction hashes should be diligently verified. For KYC, focus should be on combining the on- and off-chain data, along with transaction history to develop comprehensive profile. Also, firms can leverage existing registries to get the KYC scores of crypto exchanges.

Technology: Firms should leverage advanced analytics, artificial intelligence and machine learning enabled solutions to help analyze and trace the cryptocurrency transactions and identify the potential money laundering incidents. Such a solution would offer firms an end-to-end trail of the transactional data. It would enable real-time tracking of 100s of risk indicators, automated screening, and real-time transaction monitoring and alerting across all cryptocurrency types. It would also help proactively identify high frequency transactions to specific crypto exchanges or crypto entities.

Collaboration: All concerned stakeholders across the globe — including governments, international bodies, regulators, SROs, FIs, VASPs, crypto wallet providers, crypto exchanges, crypto custodians, etc. — should actively cooperate and implement consistent cryptocurrency-related KYC and AML/CFT mandates and standards. This is crucial to effectively counter the money laundering vulnerabilities associated with cross-border nature of cryptoassets and prevent regulatory arbitrage. Also, stakeholders should enhance their information sharing vis-a-vis emerging money laundering typologies and AML/CFT trends and practices in the cryptocurrency domain.

Conclusion

With new types of cryptocurrencies continuing to emerge — for e.g., using coins-split (hard-fork), etc. — the associated AML risks for firms would continue to rise. All concerned stakeholders must therefore work proactively and concertedly to bolster the relevant AML regulations and capabilities.

Glossary

Acronym	Expansion	Acronym	Expansion
AML	Anti-Money Laundering	FSA	Japan's Financial Services Agency
AMLA 2020	U.S. Anti-Money Laundering Act of 2020	FSC	South Korea's Financial Services Commission
AMLD	EU's Anti-Money Laundering Directive	FTC	Federal Trading Commission
ASIC	Australian Securities and Investments Commission	FIEA	Japan's Financial Instruments and Exchange Act
AUSTRAC	Australian Transaction Reports and Analysis Centre	ICO	Initial Coin Offering
BO	Beneficial Owner	IRS	U.S. Internal Revenue Services
BSA	Bank Secrecy Act	JFSA	Financial Services Agency of Japan
CAGR	Compound Annual Growth Rate	KYC	Know Your Customer
CBDC	Central Bank Digital Currency	MAS	Monetary Authority of Singapore
CDD	Customer Due Diligence	MLR 2017	UK Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
CFT	Combating the Financing of Terrorism	MSB	Money Services Businesses
CFTC	Commodities and Futures Trading Commission	NYSDFS	New York State Department of Financial Services
CSP	Cryptoasset Service Provider	OCC	Office of the Comptroller of the Currency
CTF	Counter Terrorist Financing	OTC	Over the Counter
DNFBPs	Designated Non-Financial Businesses and Professions	PCMLTFA	Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act
DOJ	U.S. Department of Justice	PEP	Politically Exposed Person
DPT	Digital Payment Token	PSA	Japan's Payment Service Act
EC	European Commission	PS Act	Singapore's Payment Services Act 2019
EDD	Enhanced Due Diligence	RBI	Reserve Bank of India
EU	European Union	SEC	U.S. Securities Exchange Commission
FATF	Financial Action Task Force	SFC	Hong Kong's Securities and Futures Commission
FCA	UK's Financial Conduct Authority	SRO	Self-Regulatory Organization
FI	Financial Institution	STO	Security Token Offering
FinCEN	U.S. Financial Crimes Enforcement Network	VA	Virtual Asset
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada	VASP	Virtual Asset Service Providers
FIU	Financial Intelligence Unit		

About the Authors

Anjani Kumar

Anjani is Principal Consultant in the Global Risk & Regulatory Technology Practices of Infosys Financial Services Domain Consulting Group. He has over 20 years of comprehensive experience in IT, domain, and process consultancy.

He manages several strategic initiatives including thought leadership showcasing, solution enablement support, research and competency development program, and marketing efforts from a domain perspective. He has authored large number of whitepapers and articles; including many that have been published on reputed external forums.

References

1. Global Cryptocurrency Market Is Booming Worldwide to Hit US$ 1125.8 million By 2028, At a CAGR of 3.5%, Feb 19, 2022, globenewswire.com.
2. Criminals laundered $2.8 billion in 2019 using crypto exchanges, finds a new analysis, Mike Orcutt, Jan 16, 2020, technologyreview.com.
3. Cryptocurrency Crime and Anti-Money Laundering Report, February 2021, ciphertrace.com.
4. FSI Insights on policy implementation No 31— Supervising cryptoassets for anti-money laundering, Rodrigo Coelho, Jonathan Fishman and Denise Garcia Ocampo, Apr 2021, bis.org.
5. The Rise in Cryptocurrency Money Laundering Cases in 2021, tookitaki.ai.
6. Cryptocurrency Fraudster Sentenced for Money Laundering and Securities Fraud in Multi-Million Dollar Investment Scheme, Jul 8, 2021, justice.gov.
7. China arrests over 1,100 suspects in crackdown on crypto-related money laundering, Jun 10, 2021, cnbc.com.
8. Helix Operator Pleads Guilty for Laundering $300 Million in Bitcoin, Arnab Shome, Aug 19, 2021, financemagnates.com.
9. Bestmixer seized by police for washing $200 million in tainted cryptocurrency clean, Charlie Osborne, May 23, 2019, zdnet.com.
10. Yet Another Theft From A Cryptocurrency Exchange - But Who Is Really To Blame?, Frances Coppola, Feb 11, 2018, forbes.com.
11. Money Muling, Dec 01, 2021, europol.europa.eu.
12. Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, Sep 14, 2020, fatf-gafi.org.

For more information, contact askus@infosys.com

Infosys®
Navigate your next