Nigma

REPORT

Fighting Cryptocurrency Crime: The Emergence of Regulation

Table of Contents

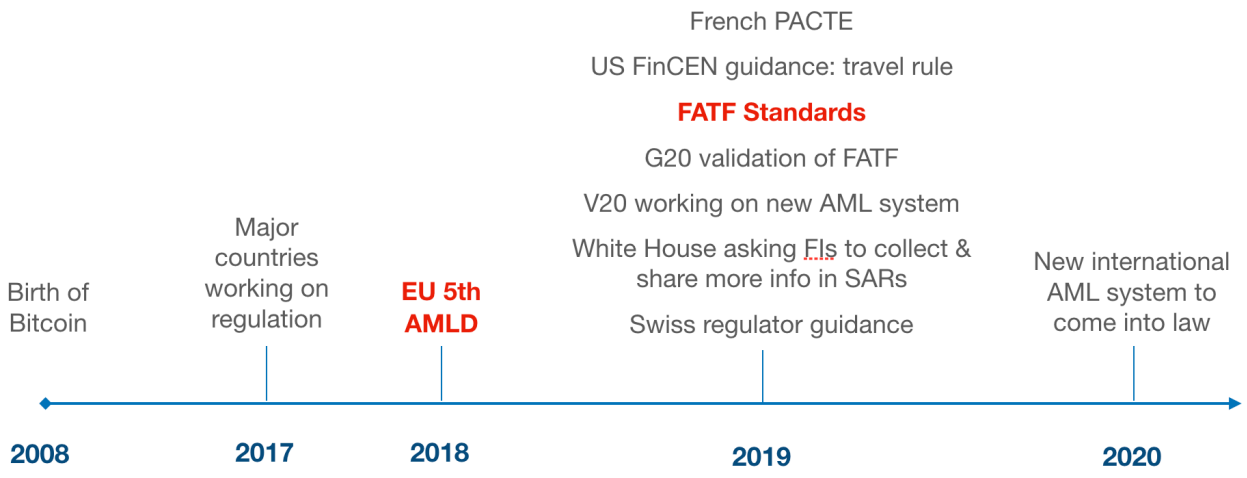
December 2019

SUMMARY

After a decade of technical evolutions and expansion, the 2017 boom, persistent association with crime and scams in the public debate, and above all a long period of legal uncertainty, cryptocurrencies are about to be widely covered by a clear legal framework.

New standards are being set at the initiative of the European Union, the Financial Action Task Force (FATF), national regulators and the cryptocurrency industry itself, with the common goal of fighting money-laundering, terrorism financing, financial crimes, fraud and scams using virtual assets. It is now time for governments and virtual assets service providers (VASP) to implement and enforce these standards

Implementation may still face technical challenges, but the industry has been quick in setting up working groups and sharing their proposals.



Contextual Landscape of Crypto Crime

Various studies have attempted to assess the scope of illicit activities in cryptocurrency. First of all, efforts have been focused on Bitcoin since it is the most widely used cryptocurrency, with a market dominance of 70%, and the most commonly associated with illicit activities. Due to its availability and widespread use in large volumes — around USD 500 billion worth of transactions every month, it is often the one favored for money-laundering, scams or on darknet marketplaces. Payments in Bitcoin on the dark web have doubled in 2018 to reach almost a billion dollars, and are proposed on almost all darknet markets — sometimes it is the only available currency.

Overall, it is estimated that illicit Bitcoin transactions amount to one or two percent of the total volume, or approximately USD 7 billions per year. It could be an underestimation though, since a large part of transactions are made over-the-counter (OTC), between unknown private addresses. Even though cryptocurrency thefts and fraud appear to have fallen in quarter 3 this year, the 2019 total may be above 4.4 billion, that is three times the amount of 2017. Two scams in particular have impacted this evolution: the PlusToken $2.9 billion Ponzi scheme and the $195 million QuadrigaCX fiasco.

One conclusion is concerning though: 97% of Bitcoin payments from illicit sources went to unregulated VASPs, that may be based in environments characterized by lax jurisdictions and that do not conduct know-your-customer (KYC) procedures when onboarding clients. As of today, Coinfirm reports that only 14% of digital currency exchange platforms are regulated and 80% don't have full anti-money-laundering (AML) and KYC policies. More disturbingly, most of the transaction volumes are based on non-regulated platforms that sometimes specifically do not seek to be regulated.

This is why governments have been increasingly pushing for a clear definition of global AML standards for the sector, in parallel with concerns over tax evasion.

The European Union Fifth AML Directive

The fifth EU Anti-Money Laundering Directive (AMLD 5) was published in 2016, after terrorist attacks in Paris and Bruxelles and as a reaction to the Panama Papers. It came into force in 2018 and member states have to transpose it in national law by January 10, 2020. Among its key components, the 5th AMLD extends the scope of AML regulation to VASPs:

"For the purposes of AML/CFT, national Financial Intelligence Units (FIU) should be able to monitor the use of virtual currencies" and " to obtain information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency" (Amendments 8 and 9).

Fiat-to-cryptocurrency exchanges and wallet providers need to monitor transactions and conduct due diligence (EDD). KYC and due diligence procedures on clients and beneficial owners are mandatory when starting a business relationship, or for a transaction over €15.000 — be it a one-time transaction or several that appear to be linked, or for a fund transfer over €1.000, or for any suspicious activity.

KYC and due diligence include: client ID verification; beneficial owner ID verification as well as an analysis of the structure for legal entities; purpose and nature of the business relationship; overseeing the business relationship and its transactions. The General Data Protection Regulation applies to the use of personal data collected by VASPs on their customers for AML compliance purposes.

Amendment 29 reads: "Member States shall ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered".

The directive plans a first report by January 2022 and requires that a central database of users' identities and wallet addresses be set up and accessible to European FIUs. Self-declaration forms should also be dispatched for cryptocurrency users.

The European Parliament has however expressed concern in September 2019 over AMLD5 transposition efforts, citing a lack of implementation in many Member States. It called on the European Commission to assess each individual state path to compliance and open infringement procedures for non-compliant jurisdictions. Deadlines for national VASP registries to be operational will not be met and lobbying actions are influencing criteria for the definition of "high risk" jurisdictions lists.

FATF Recommendations and the G20

In June 2019, the Financial Action Task Force (FATF) released its final cryptocurrency guidelines. This international organization gathers 36 member states, the European Union and the Gulf Cooperation Council to develop AML policies. The FATF June 2019 Recommendations include compelling VASPs to collect and transfer customer information to each other during transaction over USD 1.000, a process known as the "travel rule", a longstanding practice for banks.

Recommendation 16, Paragraph 7(b) reads: "*Countries should ensure that originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit the above information to beneficiary VASPs … and make it available on request to appropriate authorities.*"

Such personal information would consist at least of the sender's name, account number (wallet) and physical address or ID or date and place of birth, receiver's name and account number. For instance, sending VASP should screen the name of the beneficiary against sanctions lists.

The FATF is expecting countries and businesses to implement these standards by June 2020. The global AML standard-setter's recommendations allow countries a level of flexibility in their implementation according to their particular circumstances and constitutional frameworks. Although they are not legally binding, countries that don't follow them can be placed on a FATF gray-list, a strongly negative signal for financial institutions and businesses.

Japan has received a green light from the FATF to lead the creation of a SWIFT-like international cryptocurrency payments network.

The new FATF standards regarding cryptocurrency AML and CTF (Counter Terrorism-Financing) have already been validated by the G20, an international forum for the governments from 19 countries and the EU. During the G20 Summit held in June 2019 in Osaka, Japan, the forum made it clear: "We reaffirm our commitment to applying the recently amended FATF Standards to virtual assets and related providers for AML and CFT."

In parallel to the official G20 Summit, a Virtual 20 or v20 was also held with cryptocurrency industry participants as well as public figures to discuss how best to implement the FATF recommendations and overcome the technical issues they raise.

Criticism and challenges

Recommendations made by the FATF have the advantage of setting a global legal standard for actors to comply with, and thus create trust in cryptocurrency to attract institutional actors. But they also bear technical, financial and legal obstacles as well as efficiency concerns.

Technology — Although in use in the banking sector, the travel rule is technically challenging when it comes to cryptocurrencies. The difference is that a bank transfer is wired using an IBAN number that contains details on the country, bank, bank branch and account number of destination, whereas a Bitcoin address consists of randomly generated alphanumeric characters. Moreover, cryptocurrency transactions are not always business-to-business but also sometimes in peer-to-peer or between a business and an individual cold wallet.

Cost — These recommendations also lead to additional costs and therefore constitute obstacles for new actors in the field: such an entry barrier could be considered as anti-

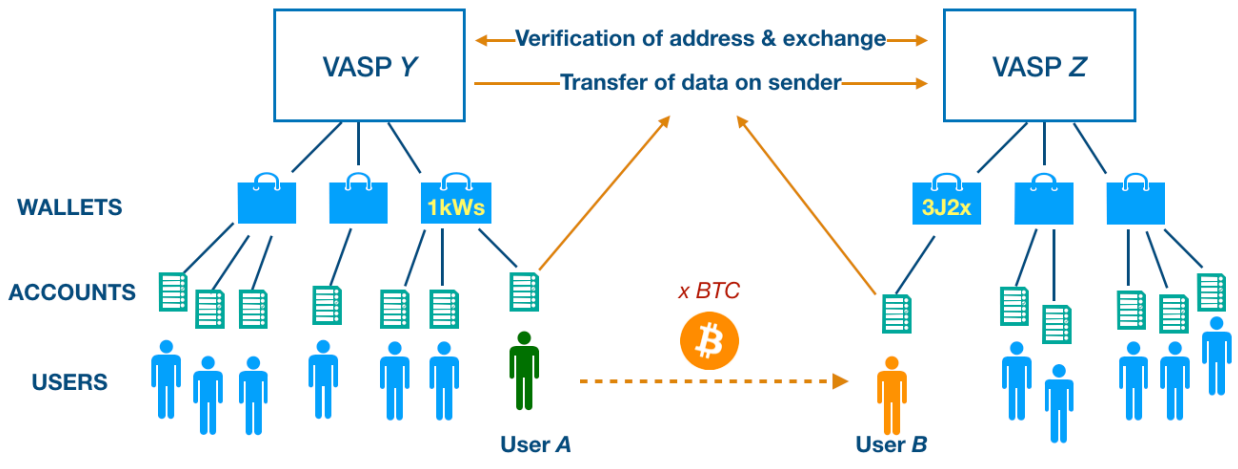
competitive. Implementing compliant KYC-AML-CFT procedures and tools can be costly, added to hiring a compliance officer and training compliance teams on cryptocurrency AML issues and tools.

Efficiency — Aside from technical feasibility, implementing the travel rule for blockchain transactions may also drive users away from regulated platforms, especially for illicit transactions, thus restricting the potential for blockchain investigations tools to track bad actors. To gain efficiency, it would be necessary to relentlessly expand coverage of the travel rule to all jurisdictions and crypto service providers around the world. This is especially challenging.

The Industry's Propositions

During the v20, participants suggested a global nonprofit body to be set up with the mandate of building, delivering and governing the new compliance system. Given the limited timing set by the FATF, a solution should have minimal, or no regulatory impact, especially with regards to data protection in the various jurisdictions. Similarly to its equivalent for banks, the SWIFT, a compliant cryptocurrency transaction system should be global in adoption and include all VASPs. There are also concerns that implementation costs may kill small firms and impede innovation. According to Malcolm Wright, Chief Compliance Officer at Diginex and chairman of the AML Working Group at Global Digital Finance, the ideal would thus be an open-source system.

Technical representation of a new compliant transaction system for cryptocurrencies



Private companies have been prompt to propose their solutions, often guided by their own interest in building and marketing their own system. According to Yana Afanasieva, who led compliance functions at Amazon and PayPal, in most cases their offering would go against the interest of users and allow them to privately control governance of the future cryptocurrency transactions system. Due to the very short FATF compliance deadline, the pitfall to avoid is letting the first proposed solution become the industry standard before the best solution is found. Such a tech-centric approach would lead to fragmentation: several private proposals would compete to address a variety of specific needs depending on VASPs and jurisdictions.

This is why Malcolm Wright and Global Digital Finance have launched the FATF Steering Committee, an industry working group to "collaborate to address an industry solution for FATF Recommendations 16 and effectively define data and operational standards and a governance mechanism to oversee compliance". It aims at designing a technology-agnostic system based on a governance structure and "global standards around data requirements and operational practices".

During the Blockshow Asia Conference in November 2019, representatives of the Swiss Crypto Valley Association (CVA), International Digital Asset Exchange Association (IDAXA), ACCESS Singapore Cryptocurrency and Blockchain Industry Association have launched the OpenVASP project to implement the FATF travel rule. The protocol will allow VASPs to "transmit blockchain transaction information privately, immediately and securely". It is also decentralized across multiple jurisdictions, with no need to register with a central authority.

Implementation around the world

Several jurisdictions have already expressed a clear stance regarding cryptocurrency compliance standards with a similar spirit. But governments that have already fully implemented these standards are scarce.

United States of America

In the USA, the Treasury's Financial Crimes Enforcement Network (FinCEN) had already released guidance on cryptocurrency in May 2019, mentioning the travel rule as mandatory for VASPs. Businesses must be able to "track and monitor the transaction history of a [cryptocurrency] through publicly visible ledgers". Any cryptocurrency service provider that interacts with US customers must comply (and this is retroactive).

Hong Kong

In a Conceptual Framework published in 2018 by the Securities and Futures Commission, the Hong Kong regulator requires that cryptoasset trading platforms "employ technology solutions which enable the tracking of virtual assets through multiple transactions to more accurately identify the source and destination of these virtual assets." It also requires that platforms apply Enhanced Due Diligence for "transactions involving virtual assets with a higher risk or greater anonymity" (privacy coins).

When high standards defined by the regulator are met, VASPs can integrate the SFC Regulatory Sandbox before applying for a license.

United Arab Emirates

In May 2019, Abu Dhabi's regulator (ADGM) has created a licensing regime called 'Operating a Crypto Business' (OCAB) with clear AML rules. Cryptocurrency businesses must have policies and procedures in place to identify the source or destination of funds. License holders have a duty to "maintain lists of tainted wallet addresses and, […] utilize third-party services to help identify such addresses". "An OCAB Holder should have a process for the management of when such 'indicators' (for example, certain Client, or the use of "mixer" and "tumbler" services) are triggered."

OCAB holders have to perform due diligence on their clients while onboarding them so to make it possible to link a wallet addresses to a specific user: "If a transaction is detected that originates from or is sent to a 'tainted' wallet address belonging to a known user, that user should be reported."

France

The Autorité des Marchés Financiers (AMF), the French regulator, is the single point of contact for cryptocurrency businesses when it comes to compliance and regulation. The AMF has created an opt-in framework that came into force with the PACTE law in April 2019. The framework allows for VASPs to voluntarily apply for AMF visa and supervision.

However, providers that offer cryptocurrency custody or cryptocurrency-to-fiat trading services must register with the AMF, regardless of whether or not they choose to obtain optional approval. Obliged entities must register and demonstrate AML/CFT measures. Businesses who comply with this regime will have guaranteed access to traditional financial services.

Switzerland

Switzerland has gone further in June 2019 by allowing cryptocurrency transactions only between clients of Swiss regulated cryptocurrency businesses, with an exchange of customer data between sender and receiver before validating or rejecting a transaction. This framework could ideally be expanded to all virtual assets service providers of all jurisdictions, but the reality will be a number of varying local frameworks in various jurisdiction.

Germany

In July, 2019, Germany approved the draft bill for the transposition of the 5th EU AMLD. Crypto assets are now financial instruments and subject to the German Banking Act (KWG). As a consequence, cryptocurrency custodians and exchanges will require a licence from the German regulator, the BaFin, and to implement strong KYC-AML onboarding, monitoring and reporting procedures. Businesses must notify BaFin of the intention to apply for permission until February 1, 2020, and submit a complete application before June 30. The bill also separates the handling of crypto assets from traditional financial services.

However, the Federal Council has passed a new law implementing the fourth EU money laundering directive on November 29, 2019. Per this law, German banks are now entitled to propose digital assets storage and trading directly to their customers, without having to rely on third party providers. The new regulation, which will enter into force on 1 January 2020, indeed deletes the separation bid that forbade banks to offer traditional investment products and digital assets within the same legal entity.

Cryptocurrencies remain defined as "digital representations of a value that has not been issued by any central bank or public agency," but is "accepted as a means of exchange and payment or for investment purposes".

Netherlands

In the Netherlands, implementation of the Fifth AMLD into national law is subject to emotional tensions due to the painful $900 millions fine inflicted to Dutch bank ING in 2018 for money-laundering compliance breach. After the 2008 economic collapse and 2018 fine against ING, the ministry of finance and Dutch national bank face pressure from the cryptocurrency sector that accuses the government of pushing for stringent additions to the EU's AMLD5. Under the new legislation, cryptocurrency businesses are expected to pay for their own supervision costs and undergo a strong and costly

registration process. The Finance Ministry being under FATF pressure with a fraud evaluation next year, "they want to be seen as the best kid in class (and) implement each FATF rule to the letter and beyond," according to Banking compliance consultant Simon Lelieveldt.

Estonia

As per the 2017 Anti Money Laundering and Terrorism Finance Act, VASPs can legally operate in Estonia if they are licensed by the national Financial Intelligence Unit (FIU), hire a Money-Laundering Reporting Officer and respect strict KYC procedures and reporting. However, 2,335 authorizations have already been granted and the Parliament is about to pass legislation to strengthen the conditions for approval, especially with regards to monitoring of transactions and due diligence investigations.

Ukraine

On December 6, the Ukrainian Parliament, the Verkhovna Rada, has voted in second hearing an amended draft law to implement EU and FATF recommandations. The bill defines cryptocurrencies as a legal means of payment and investment. The country's Ministry of Digital Transformation will be in charge of overseeing the compliant use of cryptocurrencies in Ukraine, which requires a monitoring of transactions and sharing of user identifying information to the government. Sender's public key has to be submitted for transfers under $1300, while both the sender and receiver's keys have to be reported for bigger transactions. Their business relationship also has to be identified in the latter scenario. The law still needs to be signed by the President before entering into force.

Conclusion

Both the EU and FATF tend towards a harmonized framework which could be a first step in the construction of a global cryptocurrency compliance system. However, the EU has already pointed out a lack of transposition of its 5th AML Directive by Member States, and the timeframe set by the FATF is also a short one.

What most jurisdictions tackling cryptocurrency compliance require is for cryptocurrency businesses to implement exhaustive KYC-AML-EDD procedures and tools. These include the new transaction validation system, client profiling, having a compliance officer, frequent training of compliance teams, but also blockchain analytics tools.

These tools like the e-NIGMA crypto AML platform allow for risk-scoring cryptocurrency wallets and monitoring their activity to detect suspicious behaviors. They are also instrumental in identifying real-life entities owning a wallet and helping law enforcement agencies track stolen funds, scammers, fraudsters or money-launderers. When a wallet has been identified as being used for such illegal activities, law enforcement can then issue a subpoena to a given virtual asset service provider for the uncovering of client data before legal action.

REFERENCES

Official

https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843

https://finma.ch/en/news/2019/08/20190826-mm-kryptogwg/

https://europarl.europa.eu/doceo/document/TA-9-2019-0022_EN.pdf

https://www.amf-france.org/Reglementation/Dossiers-thematiques/Fintech/Vers-un-nouveau-regime-pour-les-crypto-actifs-en-France

https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

adgm.complinet.com/net_file_store/new_rulebooks/g/u/Guidance_Regulation_of_Crypto_Asset_Activities_in_ADGM_140519.pdf

https://www.sfc.hk/web/EN/files/ER/PDF/App%202_%20Conceptual%20framework%20for%20VA%20trading%20platform_eng.pdf

https://www.mof.go.jp/english/international_policy/convention/g20/communique.htm

https://www.riigiteataja.ee/en/eli/517112017003/consolide

http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66949

Media

https://www.financemagnates.com/cryptocurrency/news/the-companies-competing-to-create-cryptos-fatf-solution/

https://www.bloomberg.com/news/articles/2019-07-01/bitcoin-criminals-set-to-spend-1-billion-on-dark-web-this-year

https://paymentscompliance.com/premium-content/insights_analysis/estonia-put-brakes-crypto-licences-approvals-soar

https://news.tunf.com/dutch-cryptocurrency-startups-in-fight-with-regulators-over-scope-of-eu-money-laundering-rule/335817

Academic and private sector

https://www.gdf.io/2019/09/12/global-digital-finance-initiates-a-fatf-steering-committee-to-foster-collaboration-to-establish-global-standards-and-a-governance-model-for-vasp-compliance-with-financial-action-task-force-fatf-reco/

https://v20.io/

https://coinmarketcap.com/fr/charts/#dominance-percentage

https://blog.chainalysis.com/reports/decoding-darknet-markets

https://www.kaggle.com/ellipticco/elliptic-data-set

https://coinfirm-prod.objects.frb.io/assets/Coinfirm_Exchange_Report_March_2019_Public.pdf

https://medium.com/@philippsandner/germany-harshly-regulates-crypto-assets-as-of-january-1-2020-what-are-the-best-strategies-for-186e471421ec