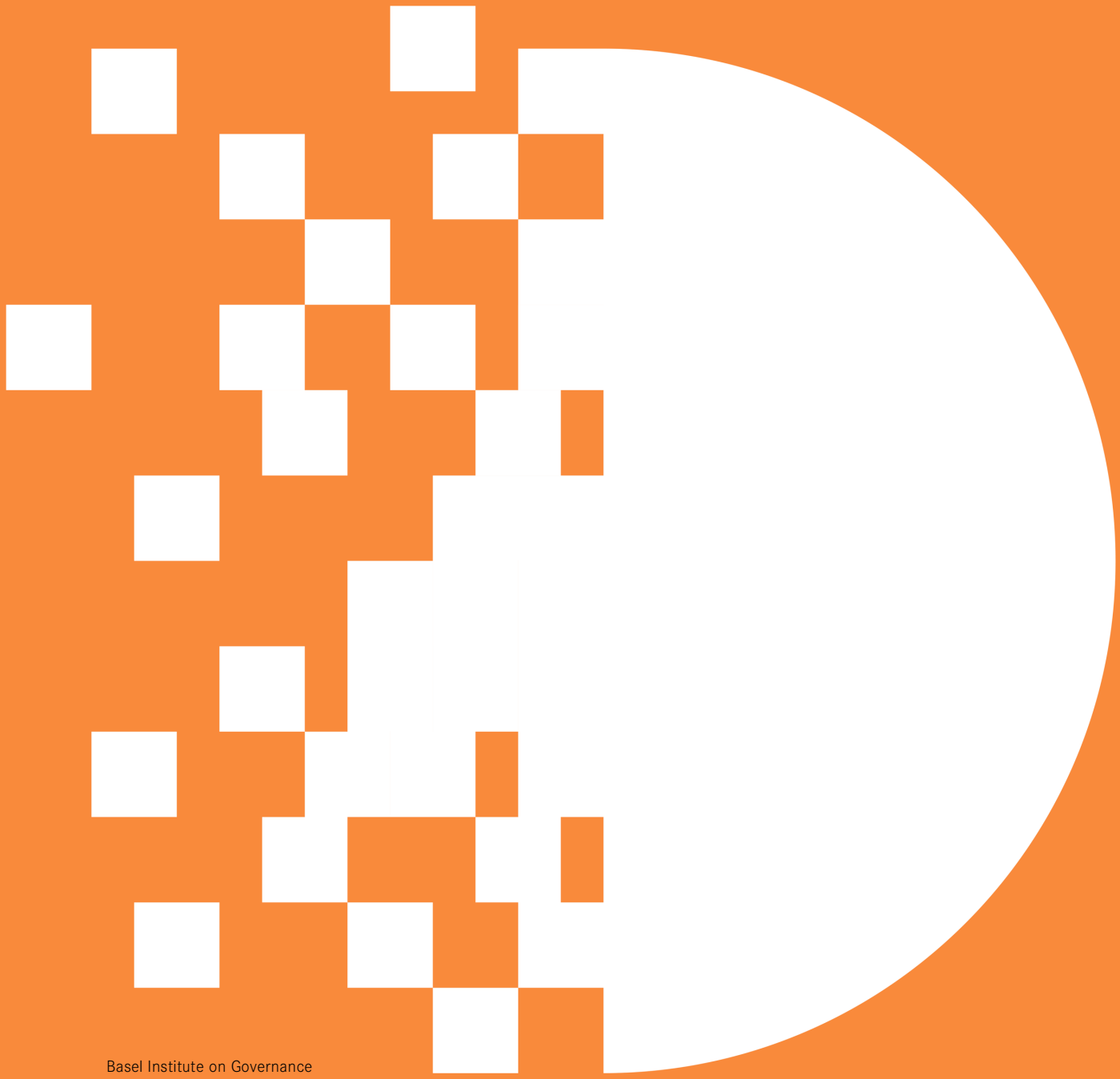
BASEL INSTITUTE ON
GOVERNANCE

Working Paper 28
Regulating cryptocurrencies: challenges & considerations

Federico Paesano | April 2018



Basel Institute on Governance
Steinenring 60 | 4051 Basel, Switzerland | +41 61 205 55 11
info@baselgovernance.org | www.baselgovernance.org

Table of contents

About the author 1

1 Introduction 2

2 EU and international legislation 2

2.1 The EU 5th AML Directive 2
2.2 Updates to FATF guidance 3
2.3 Definitions of virtual assets and VASPs 3
2.4 FATF Interpretive Note to Recommendation 15 3
2.5 Potential impacts of new identification requirements 4
2.6 Is it feasible to regulate against anonymity? 5
2.7 Effects on citizens with legitimate privacy concerns 5

3 Blockchain for financial investigations 6

3.1 Benefits for law enforcement and due diligence 6
3.2 Potential longer-term consequences 6
3.3 Lightning: how cryptocurrencies can evolve to avoid scrutiny 7

4 Conclusion 8

Annex 1: About the Working Group on Virtual Currencies 9

About the author

Federico Paesano

Senior Financial Investigation Specialist

Basel Institute on Governance

Federico joined the Basel Institute's International Centre for Asset Recovery as Senior Financial Investigations Specialist in 2010. In this role, he delivers technical training programmes on financial investigations and asset recovery in South America, Africa, Asia and Europe.

Federico graduated from the Military Academy of the Guardia di Finanza in L'Aquila, Italy, and holds a Master of Business Administration degree from the Università degli studi del Molise, Italy. For fourteen years, he worked for the Italian Financial Police, ending his career as Chief Investigator, leading and conducting judicial and financial investigations, focusing in particular on economic crimes such as corruption and money laundering.

In July 2009, he was seconded by the Italian Government to the European Union Police Mission in Afghanistan (EUPOL) as Mentor to the Minister of Interior on Anticorruption.

As part of Federico's work within ICAR, he has developed specific training courses on cryptocurrencies, money laundering and financial investigation involving virtual assets. He was a driving force behind the creation of the Working Group on Virtual Currencies, a collaboration between the Basel Institute, Europol and Interpol. The group co-organises an annual Conference on Cryptocurrency and Money Laundering focused on the emerging threat posed by criminals using new payment methods to conceal the proceeds of their crimes.

1 Introduction

The Third Global Conference on Cryptocurrency and Money Laundering, hosted by Europol in March 2019, came at a time of rapid development in cryptocurrency regulations. Across the world, authorities are reacting to the emerging threat posed by criminals using new payment methods to conceal and launder the proceeds of their crimes.

Some countries are taking a leading role by introducing new crypto-specific legislation. Others have published guidelines for interpreting the existing legal framework in light of the new technologies. Over the next two years, most major financial centres anticipate providing their domestic financial markets and industries with additional guidance on how regulations will apply to distributed ledger technologies (DLT) such as blockchain.

In a sense, the regulations are aiming at a moving target. As the application of anti-money laundering/combating the financing of terrorism (AML/CFT) due diligence requirements becomes stricter and more entities implement preventative measures, criminals are constantly looking elsewhere for potential havens for their illicit activities.

This Working Paper offers an insight into some potential consequences of changes in AML/CFT legislation in relation to cryptocurrency exchange services and virtual assets.

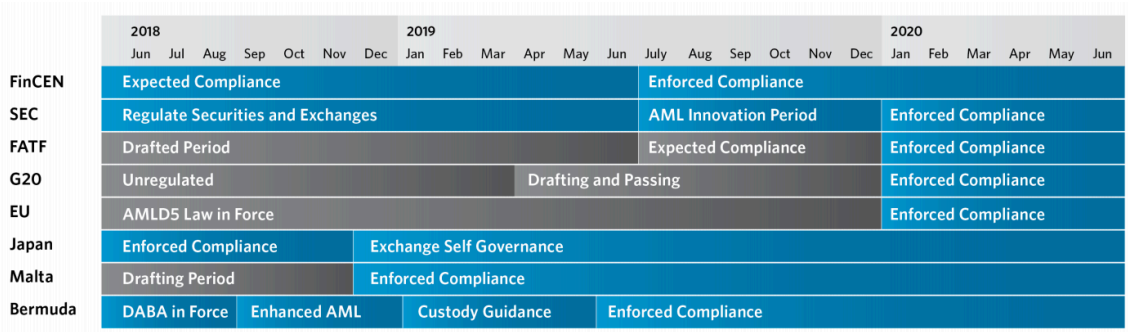


Figure 1 - Global Cryptocurrency AML timeline (Source: CipherTrace Crytpocurrency AML report Q4 2018)

2 EU and international legislation

2.1 The EU 5th AML Directive

New legislation covering cryptocurrencies is being introduced and coming into force at a European level and worldwide. In the EU, Directive 2018/843 (the 5th AML Directive) specifically regulates two types of cryptocurrency business:

- "Providers engaged in exchange services between virtual currencies and fiat currencies" (exchanges).
- "Custodian wallet providers" (wallet services).

These two categories will soon become "reporting entities" under the new legislation. This means they will be required to conduct customer due diligence much like traditional financial institutions.

2.2 Updates to FATF guidance

At the international level is the Financial Action Task Force (FATF), the standard-setter for money laundering. The body is currently preparing additional guidance on the interpretation and application of its Recommendations – a set of measures that countries should implement to combat money laundering and terrorist financing – to DLT. This will update the initial guidance it published on virtual currencies in June 2014.[1]

The move follows the G20 Leaders' Summit in 2018, which reiterated the position that cryptocurrencies do not pose a risk to financial stability, but requested the FATF to further clarify how its anti-money laundering standards apply to virtual assets. This has in part sparked the recent acceleration in activity we are witnessing right now.

2.3 Definitions of virtual assets and VASPs

One of the first FATF amendments in October 2018 was the addition to the glossary of new definitions for "virtual assets" and "virtual asset service providers" (VASPs).[2]

A "virtual asset" is a "digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes". This broad definition is wide enough to allow the future inclusion of new technologies.

The glossary also defined VASPs as any natural or legal person that 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:

- Exchange between virtual assets and fiat currencies.
- Exchange between one or more forms of virtual assets.
- Transfer of virtual assets.
- Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets.
- Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

2.4 FATF Interpretive Note to Recommendation 15

A new draft section to Recommendation 15 sets out that "*to manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for anti-money laundering and counterterrorist financing purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations*".

[1] http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf
[2] https://www.fatf-gafi.org/glossary

This includes, for example, conducting customer due diligence and reporting of suspicious transactions.

The draft text of the Interpretive Note is online, together with an invitation to experts from the private sector to send their comments.[3] This is the same approach as was taken in the United States when the first attempt to introduce a Bitcoin licence was made in 2015. Once the comments have been reviewed and the noted finalised, it can be formally adopted at the final meeting scheduled for June 2019.

2.5 Potential impacts of new identification requirements

Of particular interest in the Interpretative Note is section 7(b), which reads (in draft form) as follows:

"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 counterparts (if any), and make it available on request to appropriate authorities. It is not necessary for this information to be attached directly to virtual asset transfers.

"Countries should ensure that beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information on virtual asset transfers, and make it available on request to appropriate authorities.

"Other requirements of R.16 (including monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) apply on the same basis as set out in R.16."

As it stands, the Interpretative Note mandates that VASPs verify the identity of both their customers and the recipients of their customers' transfers carried out through their platforms. They must provide that information to the appropriate law enforcement authority if required within the context of a criminal investigation. The same requirements apply to the VASP beneficiary of a transaction.

In addition, just as with any other financial institution, VASPs will also be required to monitor their customers' wire transfers for completeness. They will need to take steps to prohibit transactions with designated persons or entities and report such incidences to the local Financial Intelligence Unit.

Since in all well-regulated jurisdictions, cryptocurrency exchanges already verify the identity of their customers, this new requirement would mean that the exchanges would also need customers to name the person to whom they transfer funds.

This is not easy as it seems. If the recipient is the customer of another cryptocurrency exchange, the information provided by the sender can be easily verified. However, not all cryptocurrency transfers involve the transfer of assets to the custody of an exchange or other VASP; funds may be transferred peer-to-peer to a recipient's wallet. Such transfers do involve any regulated third party or beneficiary.

In order to adhere to the new recommendations, exchanges and other service providers might choose different strategies. One would be to allow VASP-to-VASP transactions only. A customer can initiate a transaction from her account with a VASP *only* if the recipient has an account with another (or the same) VASP. This would mean creating a system where only approved parties can interact.

[3] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html

This is not unlike what happens in the traditional financial system, where a wire transfer from a bank account moves within the financial system to reach the account of another entity whose identity has been vetted in advance by the bank.

2.6 Is it feasible to regulate against anonymity?

Would such a system of "approved parties" work in the crypto world? While on the surface it would appear to keep criminal activities away from cryptocurrency by making it extremely difficult to remain anonymous, this comes with a significant risk.

Cryptocurrency was imagined and created for person-to-person transfers. The pseudonymous creator of Bitcoin, the most well-known of the cryptocurrencies, described it as a "peer-to-peer electronic cash system" aimed at keeping middlemen out of the picture. It is not hard to imagine that the proposed approach would likely drive a significant number of actors out of the regulated system to places where regulators and law enforcement have no reach or visibility.

The risk is to create parallel value transmitting systems. One is fully regulated and transparent, with each and every transaction having identified senders and receivers, much like in the traditional financial sector. The second can, thanks to new technologies, easily bypass those regulations. Chief among such new technologies are "privacy coins" like Monero or ZCash, which employ a number of techniques to provide its users with complete anonymity.

Major cryptocurrencies such as Bitcoin and Ethereum use pseudonymous addresses between which value is transferred. These addresses are "pseudonymous", meaning that the individual controlling the assets cannot be identified. However, the address used, the amount transferred, as well as other minimal transaction information are permanently and publicly stored on the blockchain, the immutable ledger containing all the transactions.

Despite the fact that privacy coins offer total anonymity, it seems the best place to hide is often in plain sight: Bitcoin and Ethereum have the biggest market within cryptocurrencies and criminals are still using them to move their ill-gotten funds. Although not completely anonymous, they provide a degree of privacy, as the criminal transaction will be one among millions. Bitcoin also remains the most widely used form of virtual currency for illicit activity for a number of other reasons, including the relative ease with which it can be converted into fiat and its acceptance by an increasing number of merchants.

So, what if a system like the one described above, where only identified and vetted persons could interact economically, were to be implemented? This would likely drive almost all, if not all of the criminal activity towards unregulated cryptocurrencies and foster greater demand for other privacy solutions. And it would take legitimate activity with it as well, for reasons we will now discuss.

2.7 Effects on citizens with legitimate privacy concerns

Increasingly, citizens are becoming conscious of the personal and economic value of their personal data. They are willing to take steps to prevent the use of their data by government agencies conducting surveillance or private industry hoping to sell products.

Financial transactions can reveal a tremendous amount of information, not just about the volume and recipients of transfers, but also about location, social networks, gender, sexual orientation, political views or medical history. There are legitimate reasons why certain people would need to remain anonymous. Just think of activists, investigative journalists, dissidents, to name a few.

An initial shift towards more anonymity could, thanks to the network effect, drive more and more citizens to use privacy-enhancing solutions such as privacy coins.

3 Blockchain for financial investigations

3.1 Benefits for law enforcement and due diligence

Over the last 10 years, we have made significant steps in the analysis of transactions in the blockchain. In many instances, transactions can be deanonymized. Numerous studies have shown that it is possible to identify meaningful patterns and extrapolate important information by looking carefully at transaction data. Private companies crawl the internet with web trackers and techniques that link inbound transactions to an address and to subsequent outbound transactions.

From an investigative point of view, these techniques, combined with the traceability and immutability of transactions on the blockchain, represent an opportunity for law enforcement rather than a threat.

They are also currently an opportunity for financial institutions. As part of enhanced due diligence processes for client onboarding, financial institutions are increasingly making use of blockchain analytic service providers. These services can validate the source of wealth of clients as well as provide a risk rating of the client's historical transactions with a particular virtual asset.

Ongoing transaction monitoring is also being outsourced to such services, which provide "Know Your Transaction" (KYT) risk ratings for destination addresses to which funds are being sent.

3.2 Potential longer-term consequences

Will this opportunity last? Well, while this may seem like a necessary evolution of AML due diligence to the DLT space, the increased transparency of transactions may further push criminals to interact with entities less likely to comply with AML regulations. Legitimate users looking to protect their data or privacy will follow suit – just as they will in the case of identity and anonymity discussed above.

An additional concern is that for individuals who continue to use the more regulated cryptocurrencies, the risk of being identified by such service providers as "high risk" or having transacted in the past with tainted or illicit assets is relatively high.

Figure 2 – Any given Bitcoin – like any used dollar bill – will probably have been involved in illegal activity at some point.

Take the most widely used cryptocurrency, Bitcoin, as an example. The great majority of bitcoins in circulation today have most likely been used in some sort of criminal activity in the past. They may have been used to purchase drugs and illegal goods on the darknet or otherwise involved in hacks, thefts or scams.

It is therefore quite likely that an individual's transaction history is falsely rated as high risk, even though that individual may not have been the beneficial owner of the assets at the time they were employed in illicit activities. It is crucial in these cases to carefully consider the extent to which the customer had control over the asset at the moment it was being involved in criminal activity.

3.3 Lightning: how cryptocurrencies can evolve to avoid scrutiny

The recent development of "lightning network" technology for Bitcoin offers an example of how new ways for cryptocurrency users to avoid regulatory interference can evolve. Traditionally, if we can use that word, each and every crypto transaction is published on the blockchain. With lightning, things work differently: if Alice and Bob want to send money to each other, they can open a "payment channel". This information is stored in the blockchain. Once they have finished transacting, they can close the channel and this information is again published on the blockchain.

However – and here is the important part – as long as the channel is open, none of the transactions that take place within the channel are published.

Similar to the hawala system, funds are not really moving as long as the channel is open. Alice and Bob will keep updating the status of their channel, noting down credits and debits to each other, and the channel can stay open as long as they want. If and when they decide to close it, the information about the final balance is published on the blockchain. But only the initial and final asset balance are published.

Furthermore, if Bob has another channel opened with Charlie, and Alice needs to send a payment to Charlie, she can route her payment to Charlie via Bob without it being published on the blockchain.

We therefore see how it will be very difficult for blockchain analysis firms to monitor transactions that are not reflected on the blockchain. The system is still in its infancy but it throws yet another shadow of uncertainty onto the future. If lightning technology or another like it is widely adopted, it could seriously hamper the ability of law enforcement to trace transactions.

VASPs could in theory open lightning channels with their customers (and *for* their customers), as well as with other VASPs, allowing all parties to transfer assets independently. Meeting the FATF recommendation to obtain, record and disclose details about the originator and destination names and addresses of such transactions may prove difficult.

Similar to the approach taken by the FATF in regulating fiat and crypto gateways, the recommendation may be applied to the initial onboarding of customers by providers of payment services using the lightning network. This would help prevent the use of such services by sanctioned or high-risk individuals or entities.

4 Conclusion

It is inevitable that virtual assets will increasingly be regulated. Moreover, VASPs are the ideal candidate to play a major role in the fight against money laundering and terrorism financing.

What must be considered, however, is that for the first time in history, value can be transferred from peer to peer without the support of regulated entities. Any national or regional regulation or recommendation made by the FATF should consider this new dynamic. We must aim for effective preventative measures that will truly reduce criminal activity where it's likely to take place.

The alternative is to impose additional administrative burdens on innovating VASPs that result in high operational costs with little impact and, in many cases, will push criminals and their dirty money even deeper into the blackness of the darknet.

Annex 1: About the Working Group on Virtual Currencies

The Third Global Conference on Cryptocurrency and Money Laundering was held at the Europol headquarters in the Hague in March 2019. The conference is organised by the Working Group on Virtual Currencies, a group of practitioners that meets annually to discuss the emerging threat posed by criminals using new payment methods to conceal and launder the proceeds of their crimes.

The Working Group was conceived by the Basel Institute on Governance in 2014 with the purpose of bringing together practitioners active in the new field of cryptocurrency investigations. The initial meeting gathered around 30 people in a room at the University of Basel to discuss the details of the single case known at that time. There were investigators, prosecutors, banks, as well as representatives of Europol and Interpol. Further discussions were held between the Basel Institute, Europol and Interpol, after which the collaboration was formalised and the Working Group established in 2016.

Since then, the Basel Institute, Europol and Interpol have taken turns organising conferences focusing on sharing investigative technics and trends in cryptocurrency-related criminal activities.

The second gathering was held in Doha, Qatar in 2017, where almost 400 law enforcement personnel met and discussed dozens of cases and investigations. For the first time, regulation was included as a topic, as many jurisdictions had begun regulating the field.

At the 2018 meeting in Basel, the Working Group used the opportunity to train the participants on the peculiarities of investigating cryptocurrencies. Almost 50 practitioners carried out a simulated investigation designed to take them through a complex money laundering scheme and allow them to unravel the maze of transactions.

The next conference will be held in 2020.

To find out more about the Working Group and Global Conference on Cryptocurrency and Money Laundering, contact Federico Paesano at federico.paesano@baselgovernance.org.