OLIVER WYMAN

CRYPTOCURRENCIES: HEAD IN THE SAND IS NOT AN OPTION

UNDERSTANDING IMPLICATIONS ON BANKS' AML, SANCTIONS AND KYC PROGRAMS

APRIL 2018

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Financial institutions cannot avoid cryptocurrency exposures by simply avoiding direct involvement; there are too many ways substantial indirect exposures can be generated and it is not feasible for them to fully unplug from the cryptocurrency ecosystem if their customers or third parties remain involved in it. Institutions need to actively restructure their AML, Sanctions and KYC approaches to track these risks.

This paper reminds readers of the financial crime risks that can be encountered in the cryptocurrency ecosystem and provides suggestions for addressing these systematically. To implement effective risk-management controls, firms must understand the risks involved and be aware of the complexities specific to cryptocurrencies. Those financial institutions that take active measures to adapt their programs to the risks of cryptocurrencies will be well positioned to avoid the pitfalls that are bound to emerge as risks becomes more concrete and regulators become more active in this space.

1. INTRODUCTION

The characteristics of cryptocurrencies, including anonymity and limited participant identification and verification, coupled with their global reach and the lack of a central oversight body, present many new Anti-Money Laundering (AML), Sanctions and Know Your Customer (KYC) risks. For traditional financial institutions, the existing industry most likely to be impacted by the emergence of cryptocurrencies, the associated AML/Sanctions/KYC risks are particularly pertinent.

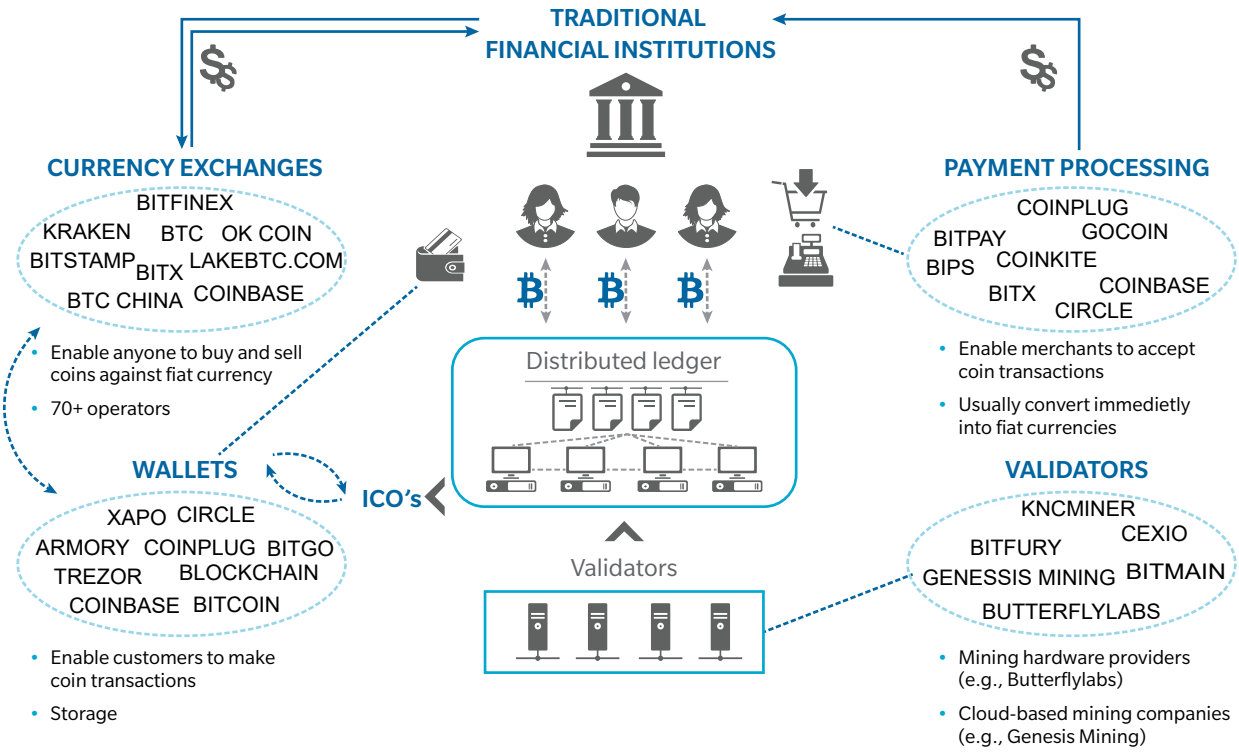
Regulators are rapidly considering the implications of cryptocurrencies on the existing regulatory systems, as demonstrated by the United States Securities and Exchange Commission's request that online trading platforms must register as a national securities exchange and the announcement by the Treasury's Financial Crimes Enforcement Network (FinCEN) that coin developers and exchanges should be considered 'money transmitters' and treated as money services businesses for regulatory purposes. It is, therefore, important that banks immediately begin to consider how they may be exposed directly or indirectly to cryptocurrencies and evolve their AML/Sanctions/KYC programs to address these risks. While there is always much work to do on the Anti-Financial Crime front, banks will also need a well-organized cryptocurrency initiative. The purpose of this publication is to explore the financial crime risks related to cryptocurrencies and provide concrete suggestions on how institutions can approach these from an AML/Sanctions/KYC perspective. For a more general explanation of cryptocurrencies, see Oliver Wyman's recent paper on "Cryptocurrencies and Public Policy – Key Questions and Answers ".

2. UNDERSTANDING THE WIDE-RANGING AML/SANCTIONS/KYC RISKS OF CRYPTOCURRENCIES

Regulators, policymakers and law enforcement officials are growing alarmed that cryptocurrencies, with their greater anonymity, could facilitate money laundering and a wide range of other illegal activities, such as tax evasion and terrorist financing.

For traditional financial institutions, avoiding cryptocurrencies entirely is not a viable option. While banks may prohibit certain types of cryptocurrency transactions (e.g., barring customers from purchasing cryptocurrencies or blacklisting certain counterparties), it is not feasible for them to fully unplug from the cryptocurrency ecosystem if their customers or third parties remain involved in it. For instance, as long as customers are able to engage in cryptocurrency transactions – even outside of the perimeter of traditional financial institutions – then the flow of funds through their accounts may represent a risk.

Exhibit 1: Schematic view of the cryptocurrencies ecosystem



Source: Oliver Wyman analysis

Given their access and control of information, and central role in the financial system, traditional financial institutions are the natural first place for regulators to gravitate to for enforcement. Therefore, banks must ensure that they have an appropriate risk management framework in place, which actively considers cryptocurrencies and their implications on AML/Sanctions/KYC compliance and financial crime.

Overall, the rapid adoption of cryptocurrencies by both consumers and businesses has generated new AML/Sanctions/KYC risks. Examples of how these system-wide risks can affect banks in relation to the cryptocurrency ecosystem include:

Traceability challenges: Most cryptocurrencies operate based on book-keeping maintained, shared, and replicated across market participants (i.e., a 'distributed ledger') but several cryptocurrencies have emerged that do not allow the same level of transparency. An increasing number of new cryptocurrencies with names like CloakCoin and StealthCoin are created specifically to limit or eliminate traceability and third-party tools such as BitLaunder and Dark Wallet greatly increase the anonymity of transactions, also affecting banks' and enforcement authorities' ability to monitor this space.

Example: *A criminal organization may take part in transactions using cryptocurrencies that shields users' identities, with the explicit intention to avoid law enforcement scrutiny while carrying out its activities, since authorities may have developed tools to investigate into a public distributed ledger.*

Interaction with anonymous accounts: The decentralized nature of the currencies allows accounts with cryptocurrency services to be created without proper due-diligence (i.e., anonymously or with unchecked information), as well as anonymous funding of accounts and transfers to occur. As a result, financial institutions and their customers or other related parties may inadvertently interact with exchanges lacking proper KYC. Regulators are attempting to crack down on this practice, with countries such as South Korea banning the use of anonymous trading on domestic exchanges, and completely banning foreigners and minors from trading through cryptocurrency accounts, but interaction with anonymous accounts is still possible.

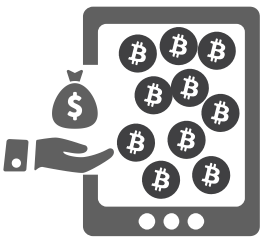
Example: *A drug dealer can "shop" for cryptocurrency exchanges and wallets requiring minimal or no information, or employing weak checks easy to circumvent, in order to create a legitimate account from which to convert and transfer funds to traditional financial institutions, which rely on the crypto services providers' controls for customer due diligence.*

"Laundering" prior to conversion back into fiat currency:

Cryptocurrencies exchanged with other cryptocurrencies prior to conversion to traditional currencies are challenging for detecting the illicit nature of the funds. While most cryptocurrency transactions can potentially be traced on a distributed ledger, innovations in cryptocurrencies have increased AML/Sanctions/KYC risk. Centralized 'currency mixers/tumblers', such has PrivCoin and CryptoMixer, and peer-to-peer tumblers are services that can be used to mix clean and illicit coins to obscure the origination source and complicate tracking. The advent of 'privacy coins' can make transactions virtually untraceable, by removing identifying information (e.g., sender, recipient, amount, etc.) from a blockchain's ledger.

Example: *A fraudster who stole cryptocurrency from other individuals' currency wallets can exchange these coins into others through a mixer, which allows to obscure the actual trail of activity and therefore makes possible to limit the ability of authorities to successfully investigate the event.*

Conversion of illicit fiat currency into cryptocurrency:

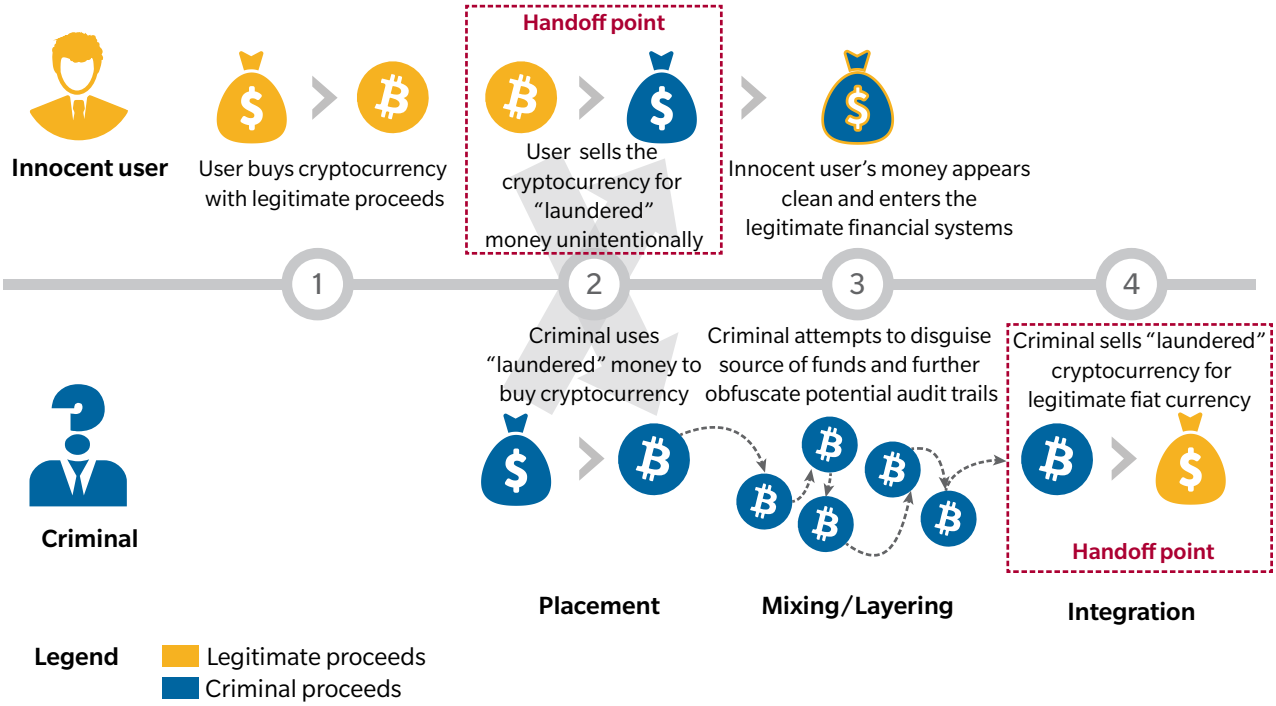


If the source of funds prior to conversion into cryptocurrencies is not monitored, there is potential for illicit proceeds to be used to buy cryptocurrencies before being converted back into traditional currencies and deposited into a clean bank account. The growing popularity of initial coin offerings (ICOs) has seen money originating from unknown sources that are potentially high risk or illegal, and ICOs might represent an entry point for nefarious entities to launder funds or skirt capital controls through conversion into the cryptocurrency.

Example: *Members of a foreign terrorist group aim to move money into a Western country to finance a local cell of the organization. In order to bypass traditional controls, they convert funds into cryptocurrency and transfer these over to wallets from which representatives of the local cell will be able to proceed with withdrawals through a locally-licensed exchange.*

Moreover, the cross-border nature and use of cryptocurrencies, combined with their reliance on complex infrastructures involving several entities in various locations, complicates tracking and monitoring. This means that responsibility for supervision and enforcement may be unclear and shared across institutions and agencies. Additionally, even when components of cryptocurrency systems can be located, they may be situated in jurisdictions without adequate financial crime controls, representing potential privileged entry points for tainted funds.

Exhibit 2: Money laundering using cryptocurrencies



Source: Europol, Why is cash still a King, 2015, Oliver Wyman analysis

Currently, cashing in and out is required to launder money, but as the cryptocurrency ecosystem grows laundering could increasingly take place within a closed system. A larger and more established cryptocurrency ecosystem would likely result in greater integration with the traditional financial system, but also a redefinition of responsibilities for identification and prevention of suspicious activity. Until then, traditional financial institutions remain the systemic first line of defense against financial crime in this space and need to ensure that an adequate AML/Sanctions/KYC compliance regime is in place to deal with these new instruments.

3. GETTING STARTED AND SHAPING AML/SANCTIONS/KYC PROGRAMS TO ACCOUNT FOR IDENTIFIED RISKS

In a short span of time, some banks and regulators have started reacting to address some of the risks posed by cryptocurrencies. However, this is only the beginning and many significant risks still need to be addressed.

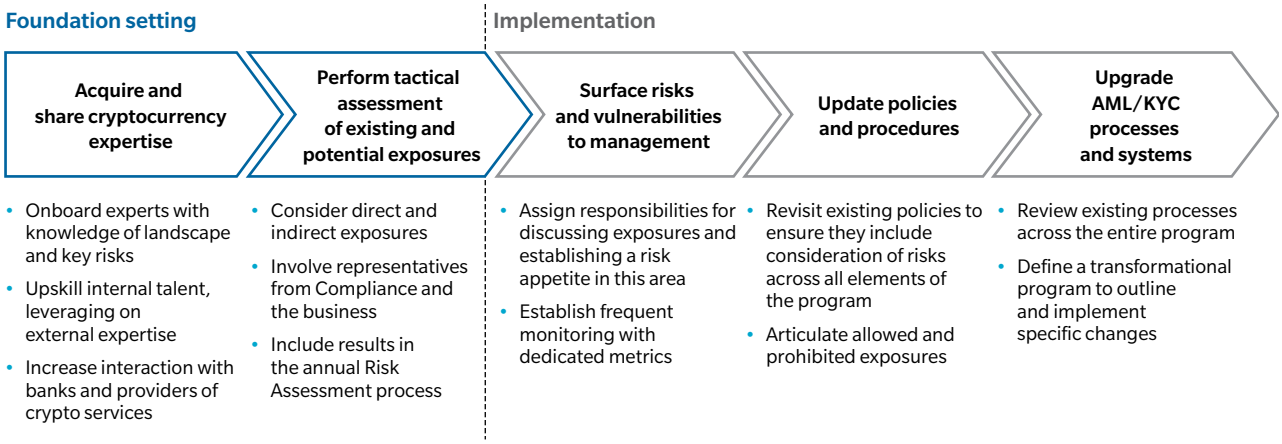
Regulatory and government bodies worldwide are increasing oversight on the use of cryptocurrencies for money laundering. In the US, the New York State Department of Financial Services (NYDFS) allows exchanges to trade virtual currencies only when issued a license dubbed 'BitLicense', which requires complying with a minimum set of anti-financial crime compliance standards. Elsewhere, a variety of regulatory efforts are ongoing, with the EU Parliament and the European Council agreeing to amend the 4th Anti-Money Laundering Directive, making virtual currency platforms and wallets subject to beneficial ownership-reporting requirements, and major Asian cryptocurrency markets taking action. The People's Bank of China announced that it would block access to all domestic and foreign cryptocurrency exchanges and ICO websites, South Korea is considering a system based on the NYDFS's 'BitLicense' model, and Japan has subjected cryptocurrency services to regulatory supervision of the Japan Financial Services Agency and demanded compliance with AML/Sanctions/KYC regulations.

Some banks have taken initial action to combat potential money laundering using cryptocurrencies. Most large US and UK banks – including JPMorgan Chase, Bank of America and Lloyds – have barred customers from using credit cards or other payment methods to purchase cryptocurrencies.

In general, institutions have mostly been taking a reactive stance on the issue of cryptocurrency risks. Banks can begin to more effectively manage the risk of cryptocurrencies by systematically thinking through the impact of cryptocurrencies on the AML/Sanctions/KYC risk framework and taking concrete steps to ensure their program accounts for these risks. Institutions should not only build frameworks that enable them to address risks within the current environment, but

also operate under the assumption that there is a chance this space will continue to grow and more participants will join the cryptocurrency ecosystem. This should be done expeditiously and kicked off as a cross-business initiative.

Exhibit 3: High-level steps to establishing an AML/Sanctions/KYC program that considers risks of cryptocurrencies



Source: Oliver Wyman analysis

FOUNDATION SETTING

1. ACQUIRE AND SHARE CRYPTOCURRENCY EXPERTISE

- For an AML/Sanctions/KYC program to be effective in this space, it is essential for the institution to be able to leverage someone with adequate knowledge of the cryptocurrency landscape and understanding of related risks.
- Seniority is less important than practical knowledge of the cryptocurrency landscape, as this will be particularly helpful in identifying areas where risk could be present and appropriately managing touchpoints with the cryptocurrency ecosystem. In fact, banks may very well have existing team members that are knowledgeable in this space but have a role that is not related to cryptocurrencies.
- Recognizing there are multiple actors in this space, banks should look to interact more proactively with each other and with the main cryptocurrency service providers, in order to enable a better alignment of objectives and initiatives in the anti-financial crime space.

2. PERFORM A TACTICAL ASSESSMENT OF EXISTING AND POTENTIAL EXPOSURES

- A targeted assessment of direct and indirect exposures to cryptocurrencies, and related AML/Sanctions/KYC risks, should be performed; the assessment should extend to sanctions programs and PEP/negative news screening.
- Such an assessment will require extensive review of media sources and available intelligence in the space, and involvement of not only Compliance teams but representatives from the business that can think through the direct and indirect exposures.
- Exposures and potential exposures detected through the tactical exercise should be frequently assessed and ultimately be considered as part of the BAU annual risk assessment process, as well as continuously enhanced as additional expertise is gathered.

IMPLEMENTATION

3. SURFACE RISKS AND VULNERABILITIES TO MANAGEMENT

- An appropriate management group (most likely an existing BSA/AML governance committee) should be accountable for discussing exposures to establish an appetite for risk in this area.
- In order to keep track of the risks identified, AML/Sanctions/KYC risks related to cryptocurrencies should be reported on relatively frequently (e.g., quarterly) given continued rapid evolution in this space, which will require definition of dedicated metrics to measure exposure and potential risks (e.g., trade volume, medium of exchange). Risk appetite should continue to be a key topic of conversation as exposures are being monitored by the institutions.

4. UPDATE POLICIES AND PROCEDURES:

- Banks should revisit their AML/Sanctions/KYC policies to make sure these include adequate consideration of risks associated with cryptocurrencies across all the elements of the program. In particular, policies should clearly articulate what exposures are allowed or prohibited, and what risks the institutions will accept or should avoid.

5. UPGRADE AML/SANCTIONS/KYC PROCESSES AND SYSTEMS

- Having clarified what risks are acceptable or not acceptable, and incorporated these into the risk taxonomy and assessment process, institutions should review the full suite of processes associated with their AML/Sanctions/KYC program, encompassing customer onboarding and due diligence, AML transaction monitoring, sanctions screening, PEP/negative media screening.
- Process enhancement will require a program to outline and implement specific changes to existing processes across the institution's full surveillance program. For instance, watch lists screening should be revised to account for lists that include potential sources of tainted cryptocurrency funds. Transaction monitoring should be enhanced with appropriate consideration of hacked accounts and detection models should be updated to consider scenarios where transactions originate from cryptocurrency services. Investigation processes can be enhanced by enabling agents to research cryptocurrency ledgers to review associated transactions and parties involved.

Institutions should ensure that the steps outlined above become part of the BAU operations of the organization, with new expertise acquired when available, ability to recognize changes in exposures, continuous communication and escalation, and appropriate translation of emerging risks into policies and processes.

AUTHORS

Allen Meyer

Partner - Oliver Wyman
allen.meyer@oliverwyman.com

Stefano Boezio

Principal - Oliver Wyman
stefano.boezio@oliverwyman.com

CONTRIBUTORS

Chris Allchin

Partner - Oliver Wyman
chris.allchin@oliverwyman.com

Chris DeBrusk

Partner - Oliver Wyman
chris.debrusk@oliverwyman.com

Tammi Ling

Partner - Oliver Wyman
tammi.ling@oliverwyman.com

About Oliver Wyman

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS
+1 212 541 8100

EMEA
+44 20 7333 8333

ASIA PACIFIC
+65 6510 9700

www.oliverwyman.com

OLIVER WYMAN