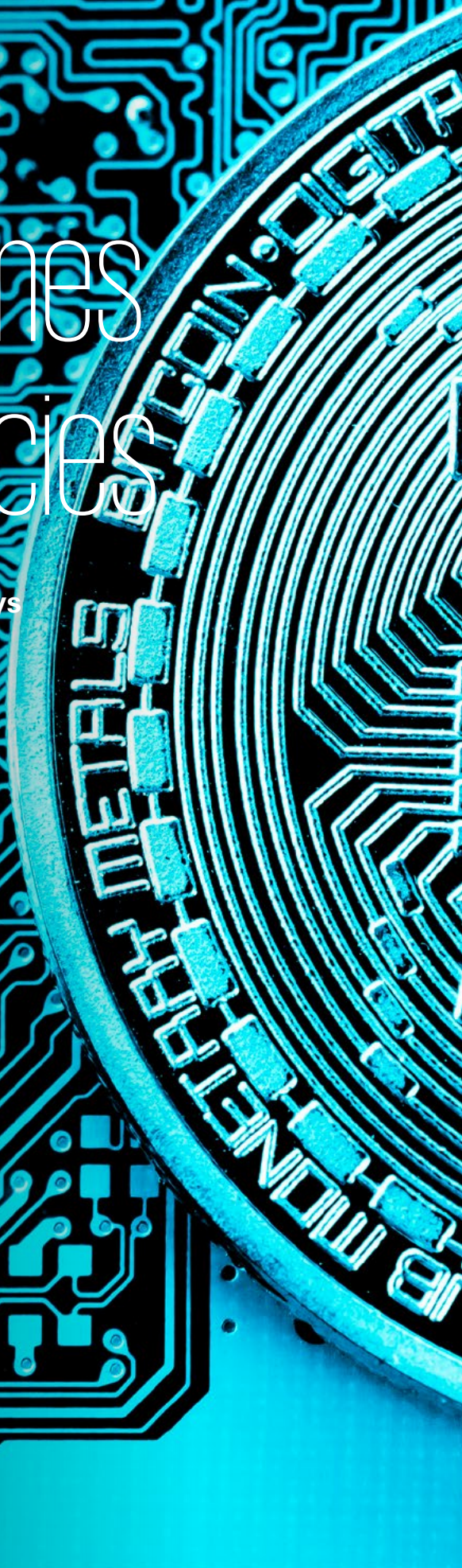
KPMG

Anti-Money Laundering in times of cryptocurrencies

Cryptocurrencies – game changers in many ways

Authors: Pascal Sprenger, Franziska Balsiger



kpmg.ch

Originally, crypto currencies were designed to eliminate the banking system in peer-to-peer transactions and thereby save transaction fees. However, as most people (with the exception of so-called miners) acquire cryptocurrency by exchanging fiat currency, financial intermediaries are nevertheless involved at this point. Once holders of cryptocurrencies decide to exchange these back into fiat currency or use them to buy goods and services, financial institutions have to apply special due diligence when performing AML checks.

While financial institutions have gradually acquired knowledge and techniques to combat money laundering and terrorism financing over the last 40 years for traditional payment services, cryptocurrency has existed only since around 2008. Most financial institutions are hesitant of burning their fingers on a matter that is so intricate and complex to understand and which provides criminals with a whole new way of laundering money or financing terrorism.

The requirement for new approaches poses particular risks financial institutions with regard to sanctions.

The inherent reduction of correspondent banking services to some countries or regions, such as e.g. Caribbean islands, Venezuela or Africa, has caused an increase in crypto activity in these geographies, jeopardizing financial intermediaries' global de-risking efforts. For financial institutions, it is almost impossible to determine whether an anonymous, numbered account correlates to a sanctioned subject as the blockchain underlying the cryptocurrency typically does not store information such as IP addresses or private information that can be used to identify the account holder. Even if a blockchain were to store such information, there are several options to conceal identity and IP addresses, such as by circumventing VPN blocks or using throw-away e-mail addresses and proxy networks such as Thor. At best, financial institutions can only identify one side of the transaction: typically their own client.

Using crypto cleansing to launder money

In certain countries, crypto cleansing is used to evade international sanctions. This process usually involves organized digital money laundering. Typically, a cleansing process follows the following stages:[1]

1. The criminal purchases a basic cryptocurrency at a digital exchange or by cash or debit card at a digital currency ATM. The first is preferred as most providers of cryptocurrency ATMs are regulated entities with corresponding anti-money-laundering duties. When purchasing cryptocurrency at a digital exchange, criminals often employ strawmen with clean records and corroborated employment. They further strengthen their anonymity by adopting pseudonyms, using anonymous e-wallets and running log-less virtual private networks (VPNs) and blockchain-optimized smartphones.
2. Once the strawmen have been verified by the digital exchange, fiat currency or bank transfers are used to place funds to purchase primary coins (e.g. Bitcoin, Etherum or Litecoin). These primary coins are then used to purchase alt-coins at an advanced exchange. Alt-coins have particular specifications, some of which are privacy coins that offer an elevated level of anonymity.
3. In order to obfuscate the primary coin's audit trail, money launderers use a tactic called mixing or tumbling. This involves using mixing services such as Bitmixer or Helix to swap primary coin addresses for temporary digital wallet addresses to fool the blockchain and break audit traceability.
   Another tactic is it to intentionally use false recipient addresses to re-route transactions to backup addresses, disrupting the audit ledger. In a next step, mixed primary coins are transferred to an advance digital exchange to purchase privacy coins (e.g. Zcash, Verge, Monero, Dash, Desire etc.).
4. The money launderers layer multiple privacy coins, exchanges and digital addresses to sever the audit trail, effectively preparing illicit funds by cleansing them for integration back into the traditional financial system.
5. Having severed the audit trail, the money launderer has several options for withdrawing cleansed funds from the digital currency to obtain fiat currency:
   - Burst-out integration: privacy coin holdings are exchanged for primary coins and later to a basic currency which can be withdrawn to a connected bank account or transferred to real estate, by citing the legal desire to avoid capital gain taxes.
   - Transfer of digital holdings to a hardware crypto wallet or printout of a QR code which can be transported to any desired addressee anywhere in the world.

[1] Crypto-cleansing: strategies to fight digital currency money laundering and sanctions evation, Josua Fruth, https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I, last visited June 27, 2018

How to combat money laundering involving cryptocurrencies

1. Strengthening AML procedures at financial institutions

Due to their position in the money laundering process by way of crypto cleansing, financial institutions should focus on their interface function, i.e. the interchange between financial institutions and basic crypto exchanges. To distinguish normal customer behavior from possible money laundering, specific considerations should be observed.

Higher risks are predominantly found in the following situations:[2]

- Customers whose predominant source of funds is derived from cash or cash-equivalent transactions, digital currency exchanges, and third-party payment providers;
- Recurring international wire transfers to digital currency exchanges;
- Excessive inflows and outflows that do not seem to correspond to the specific customer's known source of funds;
- Legal entities or non-profit organizations transacting by using digital currency exchanges in a way that would be expected of private individuals (could be a sign of a shell company or shelf company);
- Transactions that are structured and micro-structured to evade record keeping and restrictive thresholds;
- Situations where multiple customers send similar values in a similar timeframe to digital currency exchanges;
- Fast outgoing cash and cash-intensive activity at retail banks;
- Rapid flow-through of funds to external financial institutions, where deposit and outflow activity appear similar in aggregate value and timeframe;
- Large purchases of real estate, automobiles and boats;
- Connections, transactions or travel to digital money-laundering hubs (e.g. Russia, Venezuela, Lebanon, Iran, North Korea, Ukraine, Turkey, Paraguay) and those in close proximity to substantial conflicts, corruption, organized crime and terrorist activity.

Banks should further assess their systems and processes in order to not accept:

- Flows from exchanges that do not require identification or KYC information; or
- Proceeds from privacy coins (as far as this is detectable).

2. Transaction monitoring

Whereas the anonymity of cryptocurrency prevents financial institutions from determining the beneficiary of a transaction, IT systems can nonetheless use algorithms that have been developed for fiat currency to identify patterns and behaviors that indicate money-laundering schemes. Once an account is identified as correlating to a criminal activity, due to the cemented history of the public ledger, the flow can be compiled to formulate powerful intelligence for law enforcement.

3. Improving regulation

While critics of cryptocurrencies often say that the lack of identification information throughout the digital transaction is a major obstacle to monitoring and combating money laundering, cryptocurrencies have - at least in theory - certain elements such as identifying the parties and information or recording transactions, which could serve to detect or prevent money laundering. In order to effectively contain cryptocurrency risks, worldwide KYC has to become more rigorous when issuing e-wallets. In other words, global standards need to be developed. Such standards would require consensus between key industry players and complementary regulation.

As one of the international standard setters for the prevention of money laundering, the FATF in February 2018 decided to implement an additional initiative to address the risks of cryptocurrency in money laundering[3]. It invited Korea's FSC to brief the other 36 member-states on its work to incorporate anti-money laundering compliance rules for domestic cryptocurrency exchanges, which was initiated after detecting an unregistered movement of USD 600 million that was moved through trading services for investment by anonymous accounts. The FSC introduced a rule banning anonymous trading accounts and requiring exchange platforms to perform real-name verifications. New regulation mandates that all e-wallets must be registered to an existing person, so that anonymous or pseudo-named wallets are no longer possible.

4. Placing third-party ID providers under state supervision

Third-party ID providers may become key to guaranteeing a degree of anonymity for law-abiding citizens while allowing authorities to pursue criminal elements They could avoid burdensome identification and KYC data collection by entities active in the crypto-world, which, by their nature, are not as strong in safekeeping personal identification

[2] Crypto-cleansing: strategies to fight digital currency money laundering and sanctions evation, Josua Fruth, (fn 1)

[3] Global AML Watchdog to Step up Crypto Money Laundering Scrutiny, Wolfie Zhao, https://www.coindesk.com/global-aml-watchdog-to-step-up-crypto-money-laundering-scrutiny/, last visited June 27, 2018

details of customers. Various incidents, such as those in Korea, demonstrate that personal information stored with crypto entities is vulnerable to data and identity theft. It would therefore make sense to place third-party ID providers who take over the storage of data for crypto companies under state supervision to enhance their accountability.

5. Regulating cryptocurrency exchanges, especially advanced digital exchanges and exchanges offering to purchase primary cryptocurrencies

Regulating exchanges that offer primary currencies is an easy start due to the fact that they often accept fiat currency in exchange for primary cryptocurrencies. However, the focus should also be on the regulation of so-called advanced digital exchanges that only offer to exchange primary coins to alt-coins. These are harder to regulate due to the fact that they do not accept fiat currency and only accept primary coins in exchange for alt-coins. The latter are often decentralized and therefore difficult to capture in local, non-coordinated regulation. Regulating advanced digital exchanges should be of a particular interest, however, due to the fact that privacy coins' audit trails might be anonymous but digital exchanges are able to view they own trades and digital wallet balances. The collaboration of international standard setting bodies such as the FATF are unavoidable to effectively combat money laundering by crypto cleansing with a set of international standards.

6. Using blockchain as a solution

Blockchain technology inherently possesses the potential to reduce anti-money laundering risks compared to fiat currencies. A blockchain is maintained on an online public ledger, which enables the supervision, validation and recording of the complete history of each transaction. Readers of the public ledger and crypto miners are immediately notified of transactions as they occur. Furthermore, as opposed to counterfeit hard currency, cryptocurrency is almost impossible to forge as each type carries its own unique characteristics, which are verified through end-to-end miners. Without verification of all transaction phases, including the departure wallet, the destination wallet, the currency type and amount, the transaction would be immediately blocked without any human interference. In this sense, the digital trail could serve anti-money laundering regulation better than existing fiat paper trails. It would also be technically feasible to revise the blockchain protocol to limit transactions to KYC–verified wallets so that all transactions could be traced back to an identified wallet. By using blockchain technology, further anti-money laundering risk analysis as well as alert and reporting mechanisms could be integrated into the cryptocurrency system, allowing much more than the supervision of only entry and exit points. Making use of the blockchain technology's inherent characteristics would eventually help to overcome anti-money laundering challenges but come at the price of higher transaction cost and less anonymity.

Contact

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

kpmg.ch

Pascal Sprenger
Partner,
Financial Services,
Regulatory & Compliance
+41 58 249 42 23
psprenger@kpmg.com

Franziska Balsiger
Director,
Financial Services,
Regulatory & Compliance
+41 58 249 68 77
fbalsiger@kpmg.com