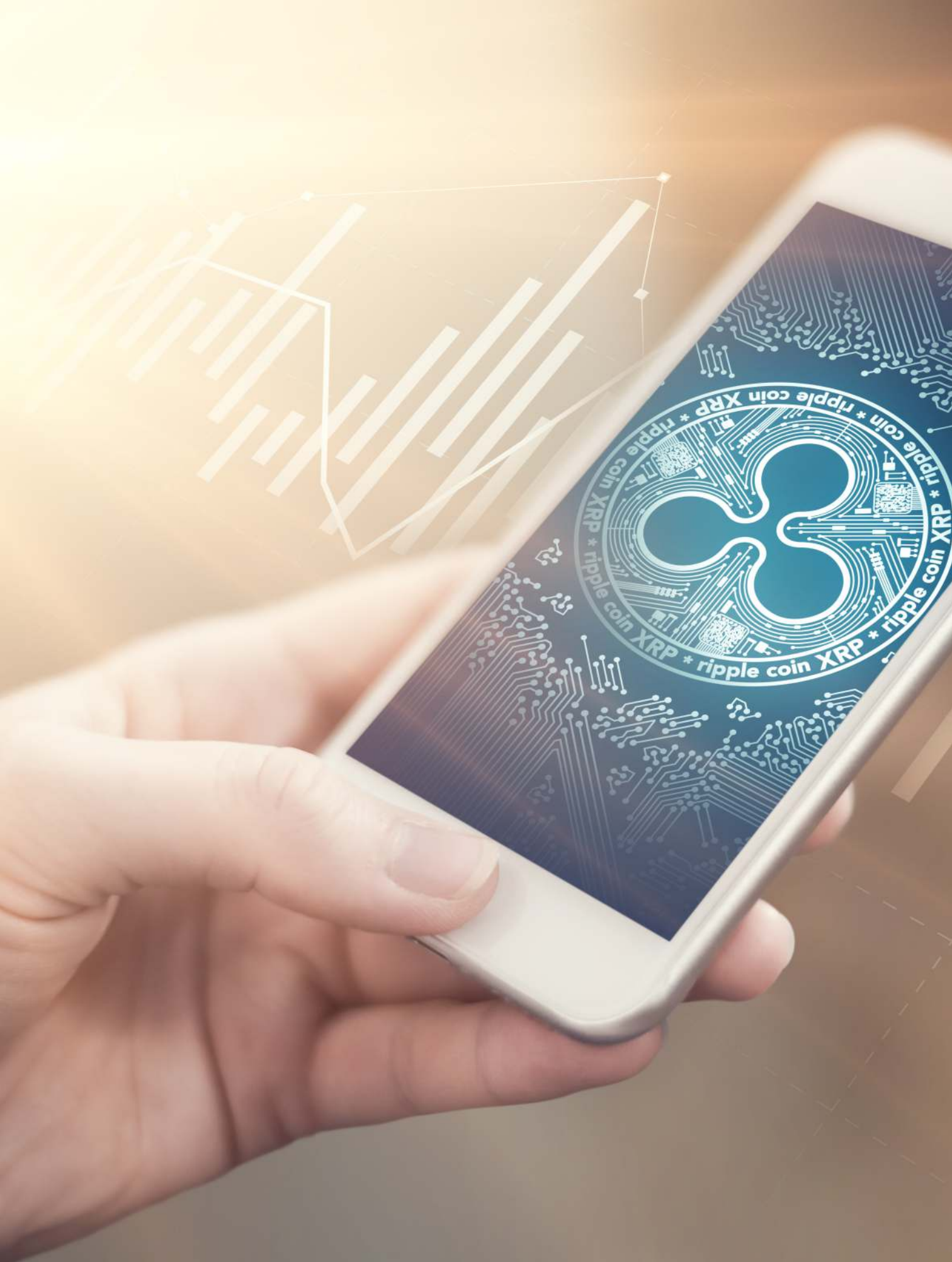
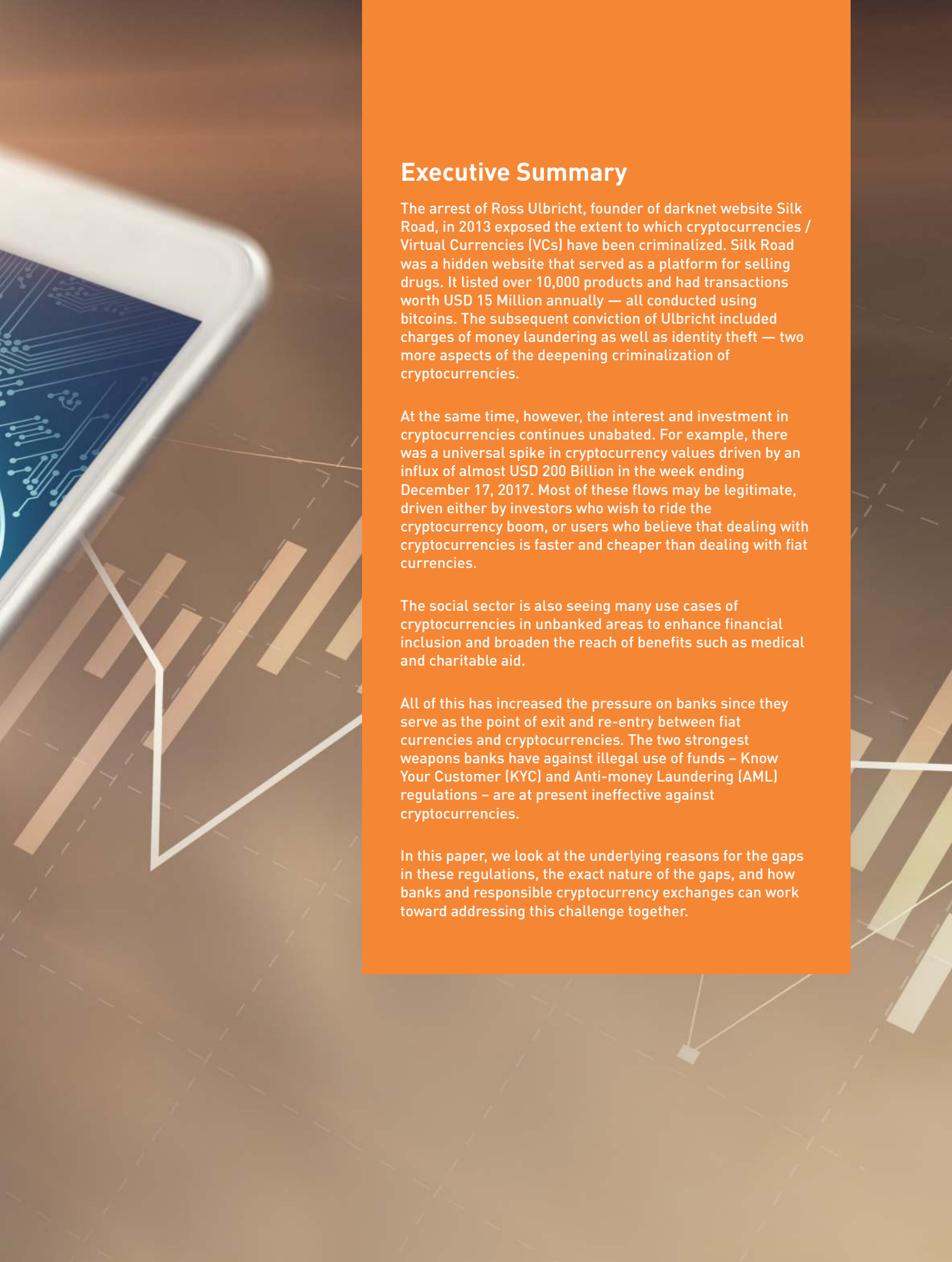
Saurav Banerjee &
Nitin Kashyap,

Subject Matter Experts,
BFSI & Healthcare

Rogue Trade: The AML & KYC Challenge in Monitoring Virtual Currencies

WNS
Extending Your Enterprise


ripple coin XRP * ripple coin XRP * ripple coin XRP



Executive Summary

The arrest of Ross Ulbricht, founder of darknet website Silk Road, in 2013 exposed the extent to which cryptocurrencies / Virtual Currencies (VCs) have been criminalized. Silk Road was a hidden website that served as a platform for selling drugs. It listed over 10,000 products and had transactions worth USD 15 Million annually — all conducted using bitcoins. The subsequent conviction of Ulbricht included charges of money laundering as well as identity theft — two more aspects of the deepening criminalization of cryptocurrencies.

At the same time, however, the interest and investment in cryptocurrencies continues unabated. For example, there was a universal spike in cryptocurrency values driven by an influx of almost USD 200 Billion in the week ending December 17, 2017. Most of these flows may be legitimate, driven either by investors who wish to ride the cryptocurrency boom, or users who believe that dealing with cryptocurrencies is faster and cheaper than dealing with fiat currencies.

The social sector is also seeing many use cases of cryptocurrencies in unbanked areas to enhance financial inclusion and broaden the reach of benefits such as medical and charitable aid.

All of this has increased the pressure on banks since they serve as the point of exit and re-entry between fiat currencies and cryptocurrencies. The two strongest weapons banks have against illegal use of funds – Know Your Customer (KYC) and Anti-money Laundering (AML) regulations – are at present ineffective against cryptocurrencies.

In this paper, we look at the underlying reasons for the gaps in these regulations, the exact nature of the gaps, and how banks and responsible cryptocurrency exchanges can work toward addressing this challenge together.

WNS
Extending Your Enterprise

Rogue Trade: The AML & KYC Challenge in Monitoring Virtual Currencies

Saurav Banerjee &
Nitin Kashyap

Introduction: The Problem of Classification

It's been almost a decade since the first Virtual Currency (VC), bitcoin, was released. But regulatory authorities in most countries are still working toward classifying cryptocurrencies accurately, and in turn, identifying applicable laws to govern them. This lays bare the inherent complexity and ambiguity of cryptocurrencies.

Let's look at the key reasons for this classification challenge:

1. There is no clear definition of the construct. The definitions that do exist (from a regulatory point of view) are more a collation of negative attributes in comparison to fiat currencies. For example, the European Commission's fifth Anti-money Laundering Directive (AMLD5) defines VCs as: "Digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically."

2. The term cryptocurrency broadly includes two categories: coins and tokens. Coins signify bitcoins, the first decentralized VC, or alternatives of the same. Tokens, on the other hand, represent an asset or utility residing on a blockchain. Tokens are essentially tradable, and can be issued to represent units of a cryptocurrency (coin), shares in a fund raising company, loyalty points, votes, or even electricity.

3. Despite the broad spectrum of application and characteristics, coins and tokens are both categorized as cryptocurrencies. This is why regulators are unclear about classifying cryptocurrencies as legal tender, an asset such as property, a commodity like gold, or a security akin to shares.

4. Where regulations do exist, tokens are most often categorized as assets or securities, while regulations on bitcoins are often used as the benchmark for all crypto coins.

5. Japan is the only country that has declared bitcoins as legal tender, while several countries including Canada and India have categorized it as 'not legal tender.' This does not prohibit its use as a means of payment or exchange; it only means there is no regulation over its use or protection for consumers using it.

There are, however, a few countries that have declared bitcoins or cryptocurrencies as illegal. When we consider that the cryptocurrency market today boasts 1640 cryptocurrencies (including coins and tokens) with varying objectives and specifications, and a market capitalization of over USD 330 Billion, we get a sense of the burgeoning size and pace of this construct – and of the challenges facing regulators.

The Jurisdiction Question

One of the fundamental legal issues in regulation is that of jurisdiction. Considering that cryptocurrencies are inherently international, with miners spread across countries, regulatory bodies are at a loss to establish jurisdiction over their production or use. Recently, Mario Draghi, the president of the European Central Bank, in a statement to the European Parliament's Committee on Economic and Monetary Affairs, indicated that his institution does not have the authority to regulate cryptocurrencies.

With control over the base asset proving elusive, a majority of regulators are focusing on addressing the distribution and trade in cryptocurrencies in their countries — which is within their jurisdiction.

They are doing this by either banning such distribution or trade entirely, or classifying the businesses offering these services and regulating them. This is driven primarily by growing instances of fraud, money laundering, tax evasion, and financing of criminal and terrorist activities that have been coming to light.

Regulators fully recognize that bringing cryptocurrency businesses within the ambit of Know Your Customer (KYC) and Anti-money Laundering (AML) rules can go a long way in tracking criminal cryptocurrency flows.

Here are a few instances of existing regulatory norms across regions:

- Canada has designated VC businesses as Money Service Businesses (MSBs), requiring them to comply with AML and KYC requirements

- The European Parliament has adopted the European Commission's proposal for AMLD5, the scope for which includes, "addressing the risks of virtual currencies and prepaid cards being used for terrorist financing and money laundering"

- The U.S., because of its fragmented jurisdiction between federal and state authorities, has several disjointed views on cryptocurrencies:

  – The Commodities Futures Trading Commission (CFTC) has categorized cryptocurrencies as commodities and is focused on regulating the nascent cryptocurrency futures market

  – The Securities and Exchange Commission (SEC) views cryptocurrencies and tokens issued via Initial Coin Offers (ICOs) as securities and is targeting the regulation of crypto exchanges, primarily with a view to protect investors from fraudulent issues

  – A few states such as New York and Washington have defined licensing requirements for bitcoin sellers

However, at present, all these attempts are at fairly early stages. Differences in regulations and treatment of cryptocurrency businesses across geographies provide enough loopholes for criminal activities to thrive.

Additionally, as we see in the following section, the technology and innovations underpinning cryptocurrencies offer continued opportunities for anonymity and subversion, leaving regulators to play catch up.

The Conduits for Moving Cryptocurrencies

Cryptocurrencies enable peer-to-peer digital transactions between two consenting parties without the need of a central validating authority or intermediary. This makes cryptocurrency transfers *faster, cheaper* and *more private* than transfers involving fiat currencies. Its underlying technology, blockchain, functions as a distributed ledger enabling *trust* in the system, while its

cryptographic programming makes the transactions *secure* and *anonymous*. These attributes have made VCs the favored currency for illegal transactions despite the rise in use cases for legitimate and positive disruptions through cryptocurrencies.

Let's look at four critical steps in money laundering using cryptocurrencies to understand how criminals use them and the points at which banks intersect with these cryptocurrency businesses.

Step 1: Ingress

VCs can be purchased from any cryptocurrency exchange. Most exchanges accept fiat currencies from banks and have some form of identity verification procedures. However, often, to buy cryptocurrencies, only some basic identity information is required.

Most money launderers first open an account with these exchanges using strawmen with clean records, pseudonyms, encrypted e-mail services, logless Virtual Private Networks (VPNs) and encrypted, blockchain-optimized smartphones to provide layers of protection and separation. Fully verified cryptocurrency accounts are also available for purchase on certain social media platforms.

Once verified, money launderers purchase 'primary coins' such as bitcoins or litecoins, which can be easily bought with fiat currencies. A record of these transactions as well as the cryptographic security for the buyer's identity – in the form of private and public keys – are stored in digital wallets, which are then used to transact further with the coins.

Step 2: Mixing

In the next step, money launderers use 'mixing services' such as Bitmixer or Helix that remove any link between them and their bitcoin transactions. These services essentially help exchange 'dirty' coins or coins that have a transaction record on the blockchain for 'clean' ones that have never been used before.

This obfuscates any attempt to track the fiat currencies converted into bitcoins beyond this point. While some of these mixing services reside on the darknet, they are fairly well known and easily accessible. Interestingly, 'mixing services' are not illegal.

Money launderers then trade these clean coins for 'alt-coins,' which are nothing but alternatives of bitcoins. Alt-coins are bought from advanced crypto exchanges that do not accept fiat currencies, and, therefore, often do not have mandatory identity verification procedures. This gives money launderers another step of separation from regulated institutions like banks.

Additionally, as some alt-coin blockchains do not maintain transaction audit trails, money launderers can easily avoid any bread crumbs. These are called 'privacy coins,' which protect all details regarding the number of coins owned, bought or sold on those specific blockchains.

Step 3: Layering

After buying privacy coins, money launderers can move the funds easily across different crypto exchanges, layering different privacy coins and using different digital wallets that are held anonymously.

Other options used by money launderers in this stage include cryptocurrency peer-to-peer lending platforms, crowd funding platforms and even Massively Multiplayer Online Role-Playing Games (MMORPG), all of which offer various options to place and layer their money.

Step 4: Egress

After several such layers, money launderers effectively have clean funds that are ready for integration back into the traditional financial system. They purchase primary coins with the clean privacy coins and then trade those for fiat currencies, effectively moving funds back into designated bank accounts. These primary coins are also used to directly buy real estate as a legitimate means of saving on capital gains taxes.

Banks: Gatekeepers on the Dark Side

With governments and regulators still far from mapping the cryptocurrency ecosystem and its players, the onus to identify and thwart illegal flow of funds into and from VCs falls squarely on banks. Regardless of the regulatory support, if banks find themselves linked to money laundering or terrorist financing flows, the reputational and compliance-related losses can be significant.

With rapid advances in regulatory technology backed by advanced analytics and machine learning capabilities, banks can now enhance existing KYC and AML tools to cover evolving cryptocurrency transactions. They can trace connections between customers across international networks, broaden transaction monitoring capabilities to cover affiliated brokers and MSBs, and quickly model new suspicious transaction scenarios by using self-learning algorithms.

The challenge, however, remains keeping abreast with the ever-growing ways in which cryptocurrency flows are being criminalized.

Most of the existing scrutiny for KYC and AML fraud can be extended to cover instances where funds are funneled into cryptocurrency exchanges (ingress). For example, banks should include the following in their watchlist for cryptocurrency transactions:

- Accounts investing in cryptocurrencies where several people are signatories, but have no apparent connection with each other
- Business or non-profit organizational accounts with a large number of cash or international wire transactions, which are then used to purchase cryptocurrencies
- A dormant or minimally active account that suddenly receives larger than usual deposits that are then funneled into cryptocurrency exchanges
- Multiple accounts in the name of one person, with numerous small deposits that do not match their income level, and scattered instances of cryptocurrency purchases
- Use of multiple personal and business accounts to collect and then funnel funds into cryptocurrencies
- Foreign exchange transactions that are performed on behalf of a customer by a third-party followed by transfers of the funds to cryptocurrency exchanges
- Frequent deposits in small amounts, followed by multiple small amount purchases of cryptocurrencies to avoid triggering of thresholds

Another strong monitoring scenario is identifying instances where multiple bank customers are sending funds to crypto exchanges in identical values and similar timeframes. Identical value transactions provide a means for additional anonymity later in the mixing and privacy coin layering stages.

Banks also need to be equally vigilant about funds flowing back into customer accounts from cryptocurrency exchanges. At the point of egress, banks should monitor:

- Cryptocurrencies being converted to fiat currencies in cash at retail banks or digital currency ATMs
- Flow of funds in similar value and timeframe from crypto exchanges to external financial institutions
- Purchases such as real estate, boats and other expensive, luxury goods using proceeds from cryptocurrency exchanges
- Connections, transactions or international travel to digital money laundering hubs such as Russia, Venezuela, Lebanon,

Iran, North Korea, Ukraine, Paraguay, former Soviet-bloc nations, and countries with substantial conflict, corruption, organized crime and terrorist activities

Crypto Exchanges: Bidding for Legitimacy

Several cryptocurrency businesses, especially crypto exchanges, are worried that the rising criminal use of cryptocurrencies will impede their legitimate growth and adoption. With countries such as India banning banks and financial institutions from entering into any service relationship with crypto exchanges, these businesses are finding it difficult to drive volumes in many markets.

As a result, there are growing instances of cryptocurrency exchanges adopting self-regulations and pushing authorities for greater regulatory clarity. CryptoUK, a trade group dedicated to the cryptocurrency industry in the U.K., has written to British MPs with a detailed proposal for a regulated cryptocurrency market. The proposal includes the suggestion that a 'crypto-license' be issued to KYC and AML compliant cryptocurrency exchanges.

Similarly, Canadian cryptocurrency exchanges are offering the Financial Transactions and Reports Analysis Centre of Canada (Fintrac) voluntary registrations and reporting to earn credibility and trust with their customers.

From a KYC and AML perspective, following are some of the monitoring scenarios that a compliance program for crypto exchanges would include:

- Utilizing the blockchain to validate customer behavior in conjunction with information gained through customer due diligence processes

- Identifying customers (and their transacting partners) who are using mixers to conceal sources of funds and to maintain anonymity
- Investigating instances when customers may be using a licensed, reputable exchange to move funds from less-compliant crypto platforms back into banks
- Following regulatory guidance with regard to more traditional AML programs, including how MSBs have been addressed by regulators

There is also a growing number of blockchain-based forensic software startups that are working with law enforcement agencies to track the use of cryptocurrencies for criminal activities. By developing software that is able to use the blockchain's ledger to track usage patterns and associations between digital wallets, these startups are helping law agencies track cryptocurrency transactions for drugs, money laundering or ransoms.

Such startups are now being hired by banks, financial institutions and cryptocurrency exchanges to help them stay compliant with KYC and AML regulations, and avoid accepting cryptocurrency that has been unlawfully obtained.

Conclusion

The way forward for effective KYC and AML regulations over the cryptocurrency market will be built on two pillars: international consensus on regulations and prevention, and greater participation by cryptocurrency businesses themselves. Just like in the fight against money laundering and terrorist financing in fiat currencies, banks should lobby for cross-border consistency in laws and faster sharing of information. This can plug a lot of loopholes and reduce the avenues for illegal funds to enter and exit the cryptocurrency markets.

Blockchain, with its tamper-proof ledgers and cryptographically secured data, holds promise as a tool to apply KYC and AML regulations with greater certainty. However, this is possible only through greater participation by cryptocurrency businesses. More open dialogues between crypto exchanges and regulators can yield the desired results, and in turn, ease some of the apprehensions of banks.

A stronger working relationship between banks and crypto exchanges — with consecutively modeled KYC and AML programs — can become a strong deterrent to the criminal use of cryptocurrencies.

References

1. https://www.moneylaunderingwatchblog.com/2018/05/the-fifth-anti-money-laundering-directive-extending-the-scope-of-the-european-unions-regulatory-authority-to-virtual-currency-transactions/#more-3789
2. https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/
3. https://www.coindesk.com/information/is-bitcoin-legal/
4. https://coinmarketcap.com/all/views/all/
5. https://www.coindesk.com/mario-draghi-european-central-bank-has-no-power-to-regulate-bitcoin/
6. https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I
7. https://www.trulioo.com/blog/top-5-crypto-exchanges/
8. https://darknetmarkets.co/category/btc-mixer-tumber/
9. https://masterthecrypto.com/privacy-coins-anonymous-cryptocurrencies/
10. https://www.wns.com/insights/whitepapers/whitepaperdetail/460/counter-money-laundering-with-financial-data-analytics---wns
11. https://www.ccn.com/british-cryptocurrency-trade-group-seeks-fca-oversight/
12. https://news.bitcoin.com/canadian-crypto-exchanges-push-greater-regulatory-clarity/
13. https://kyc360.com/article/compliance-kyc-link-exchanges-banks-mass-adoption-bitcoin/
14. https://www.inc.com/will-yakowicz/startups-law-enforcement-agencies-catch-criminals-who-use-cryptocurrency.html

WNS (Holdings) Limited (NYSE: WNS) is a leading global Business Process Management (BPM) company. WNS offers business value to 350+ global clients by combining operational excellence with deep domain expertise in key industry verticals, including banking and financial services, consulting and professional services, healthcare, insurance, manufacturing, media and entertainment, retail and consumer packaged goods, telecommunications and diversified businesses, shipping and logistics, travel and leisure, and utilities and energy. WNS delivers an entire spectrum of business process management services such as customer care, finance and accounting, human resource solutions, research and analytics, technology solutions, and industry-specific back-office and front-office processes. WNS has delivery centers world-wide, including China, Costa Rica, India, the Philippines, Poland, Romania, South Africa, Sri Lanka, Turkey, UK and US.

To know more, write to us at marketing@wns.com or visit us at www.wns.com

WNS

Extending Your Enterprise