

DIGITAL CURRENCIES: UNDERSTANDING EXPECTATIONS AND MANAGING YOUR RISK

FAQ eBook

Digital currencies are facing the perfect storm.

With increased regulator focus and greater interest from traditional financial services organizations (FSOs), businesses and individual investors, digital assets are now mainstream. It's time for FSOs to catch up – fast.

This clash of more regulation and increasing commercial interest in digital currencies results in escalated risks for FSOs in understanding and monitoring their direct and indirect exposure to digital currencies.

NICE Actimize recently teamed up with CipherTrace to discuss how to address the risk associated with cryptocurrencies.

Read on for answers to all your questions on cryptocurrency and how it can affect your organization.

**Do all banks have
crypto exposure?**



Even if a bank doesn't directly provide cryptocurrency services, in reality, the risk crypto presents is everywhere.

Illegal Money Service Businesses (MSBs) use their demand deposit accounts (DDA) as a conduit for the illegal trade of fiat for crypto by accepting cash payments in exchange for cryptocurrency. They often do this with a simple ACH transfer, wire transfer, or counter cash deposit at a depository institution. Peer-to-peer (P2P) crypto marketplaces also exist specifically designed to help people buy and sell cryptocurrencies using in-branch cash deposits or discrete wire transfers.

Because illegal MSBs and P2P crypto marketplaces constantly leverage the banking system, even banks not looking to onboard or bank Virtual Asset Service Providers (VASPs) must identify their crypto risk exposure.

CipherTrace uncovered that individuals are operating illicit crypto MSBs at **eight out of every 10 U.S. retail banks.**

To conceal unregistered MSBs, buyers are often told not to inform bank tellers that they are making deposits to purchase bitcoin but rather tell them they are purchasing "digital services."

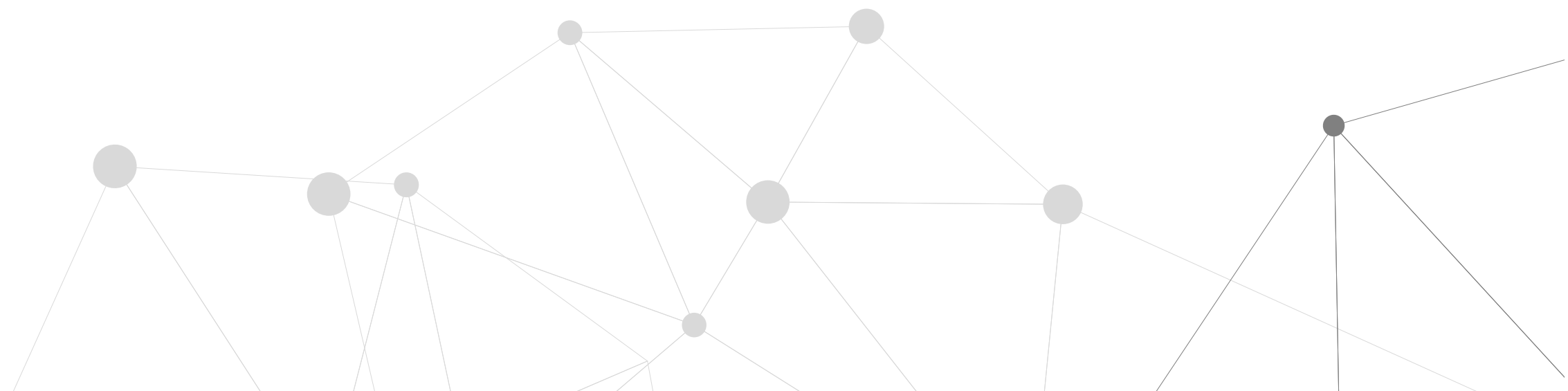
**How many crypto assets
are used for illicit purposes,
and what is the trend?**

The majority of cryptocurrency is not used for criminal activity.

That being said, there is evidence that cryptocurrencies are used for illicit activity and are used for illegal activity and as a means to launder illicit wealth around the globe; you only need to read recent media articles about law enforcement seizing millions of dollars' worth of cryptocurrencies from criminals.

It's globally recognized that virtual assets are not as extensively used for illicit purposes as fiat currency. However, all FSOs need to have appropriate and effective monitoring in place to identify those transactions that are suspicious.

According to lawyer Hailey Lennon, who was regulatory counsel for cryptocurrency platforms Coinbase and bitFlyer, a "false narrative about cryptocurrency transactions has been created."



What risk do P2P exchanges pose, and how can organizations detect activity of unregistered P2P exchanges within bank deposit account activity?

P2P exchanges create exposure for banks because many are unlicensed MSBs. An unlicensed or unregulated business creates a sizeable risk for any FSO doing business with them, including the significant risk that the unregistered/unregulated organization has insufficient controls, or doesn't care whether or not they are transacting with criminals.

This means that any FSO doing business with them is potentially facilitating money laundering.

Continuous monitoring of P2P sites and dark markets is crucial for detecting P2P exchanges. To detect P2P activity in a bank deposit account, both the inflows and outflows of funds for that specific account need to be monitored.

Using intelligence obtained from CipherTrace data, NICE Actimize detection will identify and alert users to suspected P2P crypto exchanges.



**How much can FSOs trust the
AML procedures and policies at
regulated exchanges?**

FSOs should take comfort in the growing regulation of the industry and proposed regulation of Novel Institutions in the U.S. There are also tighter regulations in Europe in the form of the 5th Money Laundering Directive. These regulations and recent case laws make trading with regulated exchanges safer for all customers and financial institutions.

Recently, the UK Financial Conduct Authority (FCA) announced that they were extending their temporary register regime while working through the significant number of applications from VASPs. The FCA disclosed that several VASPs were not meeting AML regulatory standards, and as a result, a number withdrew their applications and ceased trading. This FCA enforcement shows that digital currency organizations have to meet the expected standards - or fall on the wrong side of regulatory enforcement.

There is still more work to be done, as not all countries regulate VASPs. To protect your organization, you must have a technology solution that can understand the risk associated with each VASP and have a way of monitoring your customers' activity for suspicious transactions.

For any bank that does not onboard VASPs and has no direct crypto activity, what are the minimum actions it should take?

Banks need to be asking themselves the following questions:

- What baseline controls do we have in place to identify customers dealing with virtual assets?
- Do we have institutional or peer-to-peer virtual currency customers?
- How does our financial institution interact with emerging payment systems?
- Do we have the tools we need to identify and report potentially suspicious activity occurring through our financial institution?

All these questions impact the policies and procedures banks need to put in place to mitigate risk.

At a minimum to manage risk, banks need the tools to understand the risk of a VASP and have visibility to which, if any, of their customers are transacting with a VASP.

"To be clear, exchanges are not the only ones with crypto risk exposure. These risks are not unique to money services businesses or virtual currency exchangers; banks must be thinking about their crypto exposure as well. These are areas your examiners, and FinCEN, will ask you about when assessing the effectiveness of your AML program."

- Kenneth Blanco

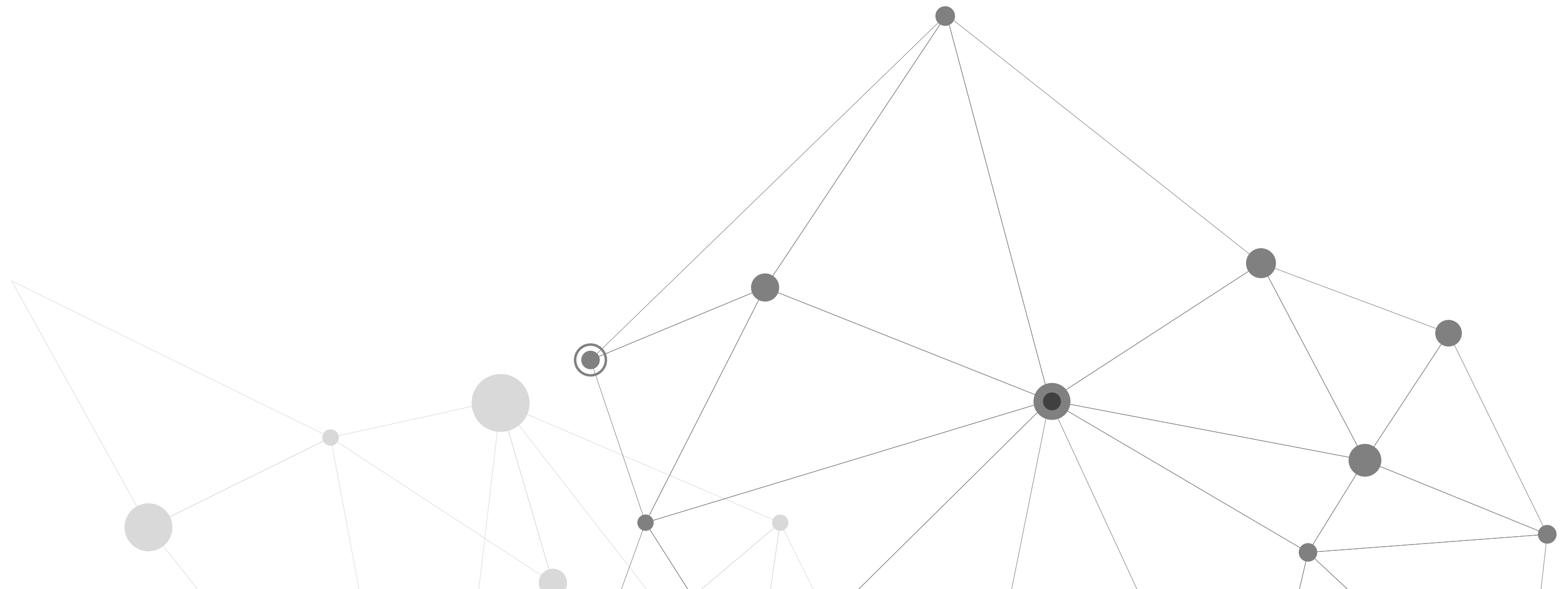
Director of the Financial Crimes
Enforcement Network

Are Decentralized Finance (DeFis) exempt from AML and KYC controls? How can a truly DeFi system be monitored by a government as far as BSA and AML?

We expect clarification on this issue to include decentralized cryptocurrency exchanges (DEXs).

Just like with centralized exchanges, the on/off ramps are the choke points where effective monitoring can be used to help identify BSA/AML suspicious activity.

DEX:
A decentralized exchange that operates in a decentralized way.¹



What happens when a sanctioned address uses mixing services to send coins to millions of random addresses to taint everyone?


This is identified via monitoring provided in the joint NICE Actimize and CipherTrace solution. By looking back at the hops when monitored at the receiving financial institution, the transaction(s) will be flagged as a high-risk transaction. An investigator can then review the information presented to them to make a disposition decision on the alert.

Did you know?

According to TechnoSports, the top three countries for crypto mining in 2021 include:

-  Sweden
-  Norway
-  Denmark

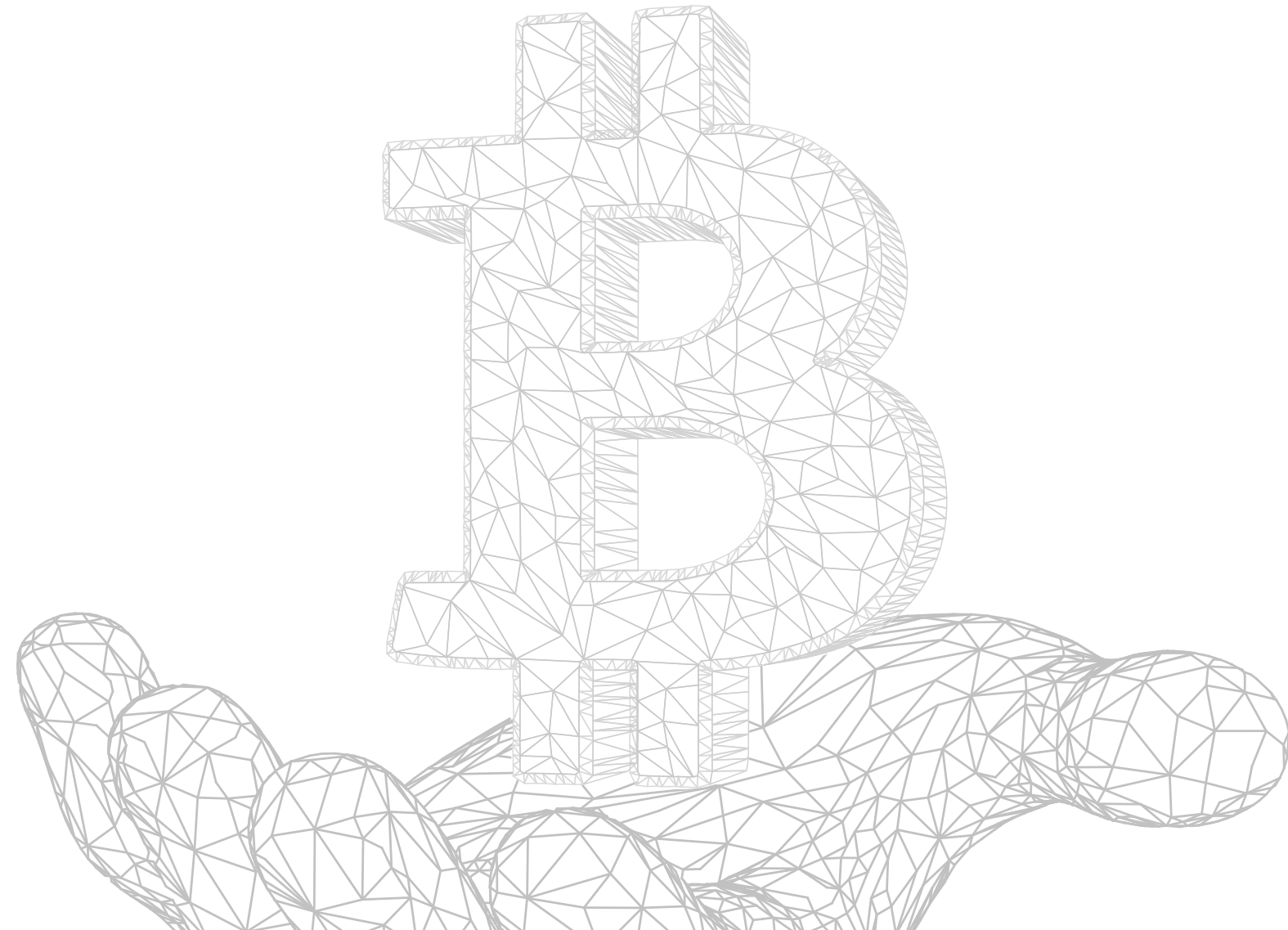


A diagram of a blockchain network on the left side of the slide. It shows a vertical chain of blocks labeled 'BLOCK 01' and 'BLOCK 02'. To the right of these blocks are several nodes labeled 'NODE 01' through 'NODE 05'. Lines connect the nodes to the blocks, illustrating a distributed ledger system. The background is a dark purple gradient with faint binary code (0s and 1s) and glowing red lines.

If blockchain analysis can be done and can identify the person(s) behind a cryptocurrency transaction, does that make the whole anonymity of crypto a myth?

Crypto transactions are typically classified as pseudonymous due to the publicly available ledger (the blockchain) that tracks all transactions and balances. U.S. courts have ruled that there is no expectation of privacy for individuals who use a public ledger cryptocurrency.

Crypto, specifically Bitcoin, has never been anonymous.





What are privacy coins, and how risky are they?

Privacy coins are a type of cryptocurrency that obscure each coin transaction's source and end destination.

These coins are said to provide privacy to owners and receivers by protecting their information - well-known privacy coins include Monero and Dash.

Privacy coins introduce risk into the financial system because the privacy they provide could allow for money laundering and counter-terrorist financing (CTF). For this reason, privacy coins have been delisted from several exchanges and have varying levels of legality depending on the jurisdiction you are in.

FATF recently published draft guidance that states, "If [a] VASP cannot manage and mitigate the risks posed by engaging in [activities that involve the use of anonymity-enhancing technologies or mechanisms], then the VASP should not be permitted to engage in such activities."

Balancing Expectations and Managing Crypto Risk

Understanding your customers' digital currency activities, your expectations and how to manage your digital currency risk are a start to addressing cryptocurrency.

Want the full story?

Watch Now



NICE
ACTIMIZE

¹ <https://defiprime.com/exchanges>

² <https://technosports.co.in/2021/03/29/top-10-countries-to-mine-cryptocurrency-in-2021/>

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

© Copyright 2021 Actimize Inc. All rights reserved.

www.niceactimize.com