vinciworks

The state of cryptocurrency compliance in 2025: **Key risks and challenges**

How regulated entities can navigate the money laundering and financial crime risks in the new era of cryptocurrency

The state of cryptocurrency in 2025

The cryptocurrency landscape is evolving at an unprecedented pace, and 2025 is poised to bring significant challenges for businesses dealing with cryptocurrency—the money laundering avenue of choice for criminals, gangsters and terrorists. At the same time, President Trump's second administration is stuffed full of 'crypto-bros,' advocates of decentralised, high risk 'currencies' like Bitcoin, and many more weird and wonderful digital tokens.

Complicating compliance efforts is the potential for a more lenient regulatory approach toward cryptocurrency, with less emphasis on enforcement and oversight. Such policies and decision making from the US authorities could embolden bad actors, further increasing the risks for businesses and financial institutions.

Cryptocurrency's inherent features are a money laundering risk—anonymity, decentralisation, and rapid cross-border transactions. From drug cartels stuffing blood-soaked dollar bills into Bitcoin ATMs on the streets of Venezuela, to Iran funding proxy terrorist groups via crypto transfer, the risks of crypto are going nowhere.

For any organisation that has a regulatory obligation to understand source of funds or source of wealth, or conduct client due diligence, cryptocurrency is a serious and significant risk. 2025 is only to make compliance more complicated.

What's in this guide?

The return to **power of the crypto-bros**

The return to power of the crypto-bros

After a steady collapse of the cryptocurrency world from 2021-2022, the swaggering success of tech-enabled crypto-bros is back in 2025.

Why is cryptocurrency having yet another moment?

In an unexpected twist of fate, cryptocurrency is having its second (or perhaps third?) heyday. The crypto market all but collapsed in 2022 with the bankruptcy of FTX and the arrest and conviction of Sam Bankman-Fried, who is now serving a 25-year sentence for fraud.

This decline was sparked by the collapse of Celsius Network, a former cryptocurrency lending company, who announced it was pausing all withdrawals and transfers between accounts in order to "honor, over time, withdrawal obligations." Celsius has nearly 2 million customers and held more than $10 billion in assets when it paused trading. Much like a run on the banks, this sparked a wave of panic in the crypto world in 2022.

Stablecoins, a more recent crypto innovation which was backed by another currency or commodity like the dollar or gold, also took a hit. The TerraUSD stablecoin fell from $116 in to a fraction of a penny in 2022, despite it once having a market capitalisation of over $40 billion.

Core Scientific, one of the largest publicly traded crypto mining companies in the U.S., which primarily mints bitcoin, filed for bankruptcy, citing falling crypto prices and rising energy costs. BlockFi, a cryptocurrency lender, filed for Chapter 11 bankruptcy protection in November 2022, itself a casualty of the collapse of FTX.

Bitcoin's volatile growth

Since its inception in 2009, bitcoin has been characterised by significant price fluctuations. Over the past decade, it has seen both meteoric rises and sharp declines:

- **2017**
  From $1,000 in January to nearly $20,000 in December.
- **2018**
  A steep drop below $4,000.
- **2020–2021**
  A surge from $7,000 to a peak of $69,000 in November 2021.
- **2022**
  A "crypto winter" brought bitcoin below $20,000.
- **2023**
  A recovery to $42,000 by year-end.
- **2024**
  The year Bitcoin bounced back to over $90,000.
- **2025**
  Where will Bitcoin go next?

On 1 January 2023, the 'value' of a single Bitcoin, the most widely traded and recognised cryptocurrency, had slunk to $16,625.08. As 2024 began, Bitcoin was valued at $45,000. By November 2024, just after the re-election of Donald Trump, Bitcoin had soared to an all-time high of $90,000. On 1 January 2025, Bitcoin had reached $93,300. Much like President Trump, 2025 is the year that, for better or worse, Bitcoin is back.

What made cryptocurrency bounce back?

Bitcoin's dramatic rise throughout 2024 and into 2025 was influenced by several major developments:

January 2024

The US Securities and Exchange Commission (SEC) approved cryptocurrency exchange-traded funds (ETFs), including spot bitcoin ETFs, to operate in the United States.

An **ETF (Exchange-Traded Fund)** is a type of investment fund that is traded on stock exchanges, similar to shares of individual companies. It pools money from investors to invest in specific assets, such as stocks, bonds, commodities, or, in this case, cryptocurrencies.

A **spot bitcoin ETF** specifically allows investors to gain exposure to Bitcoin's actual market price (the "spot price") without needing to directly own or handle Bitcoin. Instead of buying and storing Bitcoin themselves, investors can buy shares in the ETF, which tracks the real-time price of Bitcoin.

Approval of these ETFs meant that traditional investors—like those using stock market accounts—can invest in Bitcoin and other cryptocurrencies more easily and securely, without needing to navigate cryptocurrency exchanges or manage digital wallets. This broadened accessibility, potentially increasing mainstream adoption and investment in cryptocurrencies while also subjecting them to the oversight and regulation of the SEC.

April 2024

A **bitcoin halving event** drew renewed interest, further driving up value. A Bitcoin halving event is a pre-programmed occurrence in Bitcoin's protocol that happens approximately every four years (or after 210,000 blocks are mined). During a halving, the reward that miners receive for successfully adding a new block to the blockchain is cut in half.

For example, before the April 2024 halving, miners might have earned 6.25 bitcoins per block. After the halving, the reward would be reduced to 3.125 bitcoins per block.

Halving limits the rate at which new bitcoins are created, effectively reducing the supply of new coins entering the market. Bitcoin has a fixed maximum supply of 21 million coins, and halving events are designed to make Bitcoin scarcer over time.

As the supply growth slows, demand can outpace the available supply, leading to upward pressure on Bitcoin's price. Historically, halving events have been associated with price increases, as the reduced reward makes Bitcoin scarcer. Halving events often generate significant media coverage and investor interest, bringing more people into the cryptocurrency market and increasing buying activity. The next halving is expected to occur in 2028, when the block reward will fall to 1.625 BTC. This will occur during the final year of Trump's presidency.

November 2024

Bitcoin hit a record high of $90,000, with a market capitalisation of approximately $1.8 trillion as Donald Trump won his second, non-consecutive election as President of the United States. He'd led the polls throughout much of the year. Bitcoin hit $108,000 on 17 December, 2024.

This has been the single biggest factor behind Bitcoin's 2024-2025 surge. His victory sent ripples through financial markets, cementing confidence in a more crypto-friendly regulatory environment under his administration. This political development has invigorated both cryptocurrency enthusiasts and institutional investors, driving Bitcoin to unprecedented highs.

What are Donald Trump's policies on cryptocurrency?

During his campaign, Trump positioned himself as a staunch advocate for cryptocurrencies, pledging to make the US "the crypto capital of the planet." He had previously called them a scam in 2021. His platform included several bold proposals designed to bolster the adoption and legitimacy of digital assets. Key among these was his plan to appoint a cryptocurrency-friendly chairperson to lead the US Securities and Exchange Commission (SEC). This move is a game-changer for crypto, as the current SEC leadership has been criticised for taking a cautious and, at times, adversarial approach to cryptocurrency regulation.

Paul Atkins was announced as the nominee to lead the SEC on 4 December, 2024. Atkins is a former SEC commissioner—widely seen as its most conservative, anti-regulatory member—and has also called for increased enforcement against fraud. Since 2017, Atkins has been a member of the Token Alliance, a cryptocurrency advocacy organisation.

Trump also proposed the creation of a **presidential advisory council for digital assets**, a body that would bring together key stakeholders in the cryptocurrency industry to shape policy and advise on regulatory frameworks. Trump appointed 29-year-old Bo Hines, a failed Congressional candidate, to lead the Cryptocurrency Council.

Another critical aspect of Trump's platform was his staunch opposition to the creation of a US central bank digital currency (CBDC). While many countries are exploring or developing CBDCs, Trump has argued that such initiatives pose a threat to financial freedom and decentralisation. His administration's rejection of a government-controlled digital currency is viewed as a win for private cryptocurrencies like Bitcoin, which operate outside of traditional centralised financial systems.

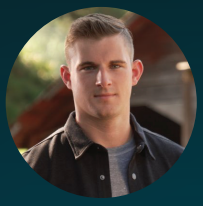
This pro-cryptocurrency stance has instilled a renewed sense of market confidence, not just in Bitcoin but in the broader cryptocurrency ecosystem. Investors view Trump's policies as a green light for growth, spurring significant inflows into digital assets. The optimism surrounding his re-election has also extended to traditional financial markets, with the US stock market experiencing a post-election rally. This alignment of bullish sentiment across markets has signalled a growing interconnection between cryptocurrency and mainstream finance, which did not exist to such a degree before.

Trump’s policies and rhetoric have positioned his administration as a catalyst for cryptocurrency adoption, setting the stage for a potential transformation of the US into a global hub for digital assets. But this presents unique risks for the rest of the world, with the potential for the US to become a new, powerful hub for laundering digital assets.

Trump’s crypto-bro cabinet

Trump has assembled a pro-crypto team to shape his administration’s policy. Key appointments include:

David Sacks, former PayPal COO, as White House AI and Cryptocurrency Czar, tasked with creating regulatory clarity for digital assets.



Bo Hines, Executive Director of the newly formed Crypto Council, focusing on balancing innovation with consumer protection.

Paul Atkins, a former SEC commissioner, as the new chair of the SEC, signalling a lighter regulatory touch.

Sriram Krishnan, Senior Policy Advisor for AI, who will align blockchain and AI strategies.

Stephan Miran, Chair of the Council of Economic Advisors, advocating for integrating blockchain into economic policy.

What caused Donald Trump's change of heart on crypto?

This newfound enthusiasm for cryptocurrency was not only driven by external factors but also by strategic support from key sectors, notably the cryptocurrency industry itself. Over the course of several months, the crypto market poured $245 million into the US election.

According to Stand With Crypto, an industry lobby group, 253 pro-crypto candidates were elected to the House of Representatives, compared to 115 anti-crypto candidates. In the Senate, 16 pro-crypto candidates won seats versus 12 anti-crypto candidates.

For many in the crypto community, Trump represented a potential ally in pushing for favourable regulatory treatment, especially as the industry was facing increased scrutiny from government regulators. The bet seems to have paid off.

In addition to the financial backing from the crypto industry, Trump's personal financial interests in the sector further fuelled his involvement in the space. In September 2024, he and his sons, Don Jr. and Eric, launched a cryptocurrency venture called World Liberty Financial, signalling the family's commitment to the burgeoning industry. The venture focused on developing blockchain-based financial products and services, with aspirations to create a platform for buying, selling, and trading digital assets. This move not only aligned with the broader trend of political figures engaging with emerging technologies but also positioned the Trump family as personal stakeholders in the rapidly evolving cryptocurrency landscape. The second Trump administration is ready to leverage his influence to shape the future of digital finance.

Institutional confidence: The impact of ETF inflows

The approval of Bitcoin exchange-traded funds (ETFs) in early 2024 marked a watershed moment for the cryptocurrency industry, opening the floodgates for institutional investment and bringing a new level of legitimacy to digital assets. For the first time, institutional investors—ranging from hedge funds to pension funds—had a regulated and straightforward avenue to invest directly in Bitcoin without the complexities and risks of holding the cryptocurrency themselves. This move not only made Bitcoin more accessible to traditional finance but also significantly boosted its appeal as a credible investment vehicle.

The momentum behind Bitcoin ETFs gained an even greater surge following Donald Trump's re-election. In the days immediately after his victory, inflows into Bitcoin ETFs skyrocketed, underscoring the newfound confidence in the asset class. On 11 and 12 November alone, a staggering $2 billion flowed into Bitcoin ETFs, reflecting the market's optimism about a cryptocurrency-friendly administration.

A key beneficiary of this surge has been BlackRock's iShares Bitcoin Trust, which has quickly emerged as a dominant force in the ETF market. Since its launch in 2024, the fund has attracted over $40 billion in capital, an unprecedented achievement that makes it the most successful ETF of the decade. BlackRock's involvement, as the world's largest asset manager, has further legitimised Bitcoin as an asset class, signalling to institutional investors that cryptocurrencies are no longer a fringe investment but a mainstream opportunity.

The success of Bitcoin ETFs represents more than just a milestone for the cryptocurrency industry—it highlights the growing convergence between digital assets and traditional finance. By providing a regulated and transparent investment vehicle, these ETFs have alleviated many of the concerns that have historically deterred institutional investors, such as custody risks and regulatory uncertainty. Furthermore, the accessibility of ETFs has enabled a broader spectrum of investors to participate in the cryptocurrency market, from retail investors to large-scale financial institutions.

BlackRock's dominance in the ETF space also reflects a broader trend: the increasing consolidation of cryptocurrency-related financial products under the umbrella of major financial institutions. This development has positive implications for the long-term stability and scalability of the cryptocurrency market—at least while the regulatory environment allows for it—as institutional participation brings not only capital but also a level of discipline and market maturity.

The approval and subsequent success of Bitcoin ETFs, particularly in the wake of Trump's election victory, underscore a pivotal shift in how digital assets are perceived and integrated into the broader financial ecosystem. With billions of dollars now flowing into these funds, Bitcoin has cemented its position as a critical asset in the portfolios of institutional and retail investors alike, paving the way for continued growth and adoption.

The impact of deregulation and tax incentives

Under Trump's second administration, the twin pillars of deregulation and tax reforms are poised to significantly bolster Bitcoin's growth and the broader cryptocurrency market. These measures signal a transformative shift in the US government's approach to digital assets.

Deregulation: A crypto-friendly environment

One of the key drivers behind the current optimism in the cryptocurrency market is the prospect of deregulation under Trump's leadership. During his campaign, Trump vowed to reduce regulatory barriers surrounding cryptocurrency trading and innovation, setting the stage for a more open and supportive environment. By scaling back restrictions imposed by federal agencies like the Securities and Exchange Commission (SEC), the administration is fostering an atmosphere that encourages investment and innovation in digital assets.

The anticipated deregulatory approach includes appointing a cryptocurrency-friendly SEC chair—Paul Atkins—to replace Gary Gensler, who had taken a more aggressive stance on crypto regulation. A less stringent regulatory framework could allow for the proliferation of new cryptocurrency-related products and services, making it easier for both businesses and consumers to engage with digital assets. Furthermore, Trump's establishment of a presidential Cryptocurrency Council and his commitment to making the US a hub for cryptocurrency innovation has signalled to investors there are four more years of a pro-crypto administration.

Tax cuts: Incentivising investment

In addition to deregulation, Trump's proposed tax reforms are another critical factor driving enthusiasm in the cryptocurrency market. By lowering the capital gains tax rate, the administration aims to make investing in assets like Bitcoin more attractive to both retail and institutional investors. A reduction in capital gains tax would allow investors to retain a larger share of their profits from cryptocurrency trades, encouraging increased participation in the market.

Even more impactful is Trump's proposal to eliminate taxes on US-based cryptocurrencies like Bitcoin and XRP. By making these digital assets tax-free, the administration is providing a powerful incentive for investors to favour American cryptocurrencies over foreign competitors, such as Ethereum, which is primarily based outside the US. This move not only aligns with Trump's "America First" agenda but also has the potential to drive substantial capital inflows into US-based crypto markets.

For businesses, these tax reforms offer an additional layer of incentive. Lower taxes on crypto-related transactions and holdings could reduce operational costs and increase profitability, making it more attractive for companies to integrate cryptocurrency into their operations. This could lead to wider adoption of Bitcoin and other digital assets as a means of payment, investment, and innovation.

A pro-crypto administration

Together, deregulation and tax reforms represent a powerful combination that could redefine the trajectory of the cryptocurrency market in the US. By removing regulatory barriers and providing tax incentives, the Trump administration is laying the groundwork for accelerated growth and adoption of digital assets. These measures are not only enticing existing investors but are also likely to attract new market participants, ranging from retail investors to institutional giants.

The broader implications of these policies extend beyond Bitcoin. A crypto-friendly regulatory and tax environment could stimulate innovation across the blockchain ecosystem, driving advancements in decentralised finance (DeFi), tokenisation, and Web3 technologies. As the US positions itself as the “crypto capital of the planet,” the impact of these reforms will likely ripple across global markets, influencing how other nations approach cryptocurrency regulation and adoption. While the full implementation of these policies will take time, the early signs of market confidence reflect the transformative potential of Trump’s pro-crypto agenda.

Cryptocurrency for the people

Bitcoin and other cryptocurrencies accessibility has undergone a profound transformation over the years, breaking down the barriers that once limited its adoption to tech-savvy early adopters. Today, a combination of user-friendly platforms, regulatory advancements, and innovative financial products has opened the doors for retail investors of all experience levels to participate in the cryptocurrency market. This democratisation of access has been a major factor in Bitcoin’s recent surge in popularity and value.

User-friendly platforms: Cryptocurrency for the masses

Platforms like Coinbase, Binance, and Kraken have played a pivotal role in making Bitcoin and other cryptocurrencies more accessible to the general public. These platforms offer intuitive interfaces, robust security measures, and educational resources that simplify the process of buying, selling, and managing digital assets.

With features such as automated recurring purchases, portfolio tracking, and mobile apps, even those with limited investment experience can easily navigate the cryptocurrency market. Additionally, these platforms often include educational tools that help new users understand Bitcoin's potential as an asset, as well as the risks involved, further encouraging adoption.

Moreover, the rise of integrated payment systems and partnerships with traditional financial services has bridged the gap between traditional and crypto finance. For instance, services like PayPal and Cash App now allow users to purchase Bitcoin directly through their platforms, enabling millions of users to invest with just a few clicks.

The ETF revolution: A game-changer for retail investors

As mentioned before, the approval of Bitcoin exchange-traded funds (ETFs), particularly spot Bitcoin ETFs in 2024, was a watershed moment for accessibility. ETFs have transformed how retail investors can participate in the Bitcoin market by providing a familiar and regulated vehicle for investing in cryptocurrency without needing to directly own or manage digital wallets.

For investors who may have been hesitant to deal with the complexities of cryptocurrency wallets, private keys, or exchanges, ETFs offer a simple and secure alternative. By purchasing shares of a Bitcoin ETF, investors gain exposure to Bitcoin's price movements while benefiting from the protections and oversight of traditional financial markets. This accessibility has dramatically expanded the pool of participants, bringing more mainstream investors into the fold.

Breaking down stereotypes with accessibility

The ease of access provided by platforms and ETFs has been instrumental in reducing the stereotypes that cryptocurrency held as a high-risk, speculative investment. For retail investors, the process of entering the market has never been simpler. No longer do individuals need to navigate complex technical processes or rely on niche platforms to purchase Bitcoin. Instead, they can buy Bitcoin through the same apps or brokers they already use for traditional stocks and bonds.

This increased accessibility has also coincided with rising public awareness of Bitcoin as a legitimate investment option. As Bitcoin and other cryptocurrencies gain coverage in mainstream financial media, they are being perceived less as a speculative gamble and more as a viable component of a diversified investment portfolio.

Gains beyond bitcoin

Bitcoin’s surge has been accompanied by gains in other cryptocurrencies, as shown below:

Cryptocurrency	Price (Pre-election, USD)	Price (13 Nov 2024, USD)	% Change
Bitcoin (BTC)	$67,811.51	$90,584.17	33.58%
Ethereum (ETH)	$2,397.03	$3,192.60	33.19%
Dogecoin (DOGE)	$0.1583	$0.3995	152.37%
Solana (SOL)	$157.75	$215.18	36.41%

A global market for cryptocurrency

The surge in cryptocurrency accessibility is not limited to developed markets like the US and Europe. Platforms and products designed to cater to emerging markets are also driving global adoption. Mobile-friendly platforms, fractional purchasing options, and expanding internet access have made it easier for individuals worldwide to invest in crypto, even with smaller amounts of capital.

Additionally, Bitcoin's inherent features, such as borderless transactions and financial sovereignty, make it particularly appealing in regions with unstable currencies or limited access to traditional banking services. Platforms that offer local language support and integrations with regional payment systems are further broadening Bitcoin's reach.

Of course, this is also where the risk lies. As the entrypoint to crypto becomes so low that anyone with a mobile phone can buy crypto—anonymously—what's left to stop North Korean agents buying missile parts, or Iran-backed terror groups funding mass murder? Very little.

The money laundering **risks of cryptocurrency**

The money laundering risks of cryptocurrency

Cryptocurrencies, with their decentralised nature and pseudonymous transactions, present unique challenges in combating money laundering and terrorist financing.

One primary risk lies in the anonymity that some cryptocurrencies, such as Monero or Zcash, offer through advanced privacy features. Even with widely-used cryptocurrencies like Bitcoin, where transactions are recorded on public blockchains, the lack of stringent identity verification can enable bad actors to obscure the origins of funds. Cryptocurrencies can be used to launder money through a process known as "layering," wherein illicit proceeds are moved across numerous wallets and exchanges to create a complex trail that becomes challenging for authorities to trace. Moreover, decentralised finance (DeFi) platforms, peer-to-peer (P2P) exchanges, and mixers further complicate detection by facilitating transactions outside regulated frameworks.

Terrorist organisations have also shown interest in cryptocurrencies as a tool for fundraising and transferring funds internationally. Unlike traditional banking systems that are closely monitored, cryptocurrencies can bypass geographic and regulatory barriers. Social media and encrypted messaging apps have been used to solicit donations in cryptocurrency, often leveraging the perception of these assets as untraceable.

The rapid evolution of cryptocurrency markets adds another layer of complexity. Emerging technologies, such as non-fungible tokens (NFTs) and metaverse economies, open new avenues for illicit activities. Criminals may use these assets to hide money laundering operations by purchasing, trading, or selling digital goods with opaque pricing mechanisms. Meanwhile, regulators face challenges in keeping pace with these innovations, as jurisdictional inconsistencies and gaps in enforcement allow exploitation of the system.

To mitigate these risks, regulatory bodies worldwide are implementing stricter oversight. Measures like the Financial Action Task Force's (FATF) Travel Rule require virtual asset service providers (VASPs) to collect and share information about the identities of senders and recipients for transactions above a certain threshold. Additionally, many jurisdictions now mandate registration and compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) protocols for cryptocurrency businesses. However, enforcement remains inconsistent, with varying levels of adoption across countries. This makes cryptocurrency a risky venture, and all regulated entities should be aware of the risks.

The AML risks of Decentralised Finance (DeFi)

Decentralised Finance (DeFi) leverages blockchain technology to create an open-source financial system, but it presents unique challenges for Anti-Money Laundering (AML) due to its decentralised nature, pseudonymity, and reliance on smart contracts. The lack of central authority and intermediaries makes it difficult to implement and enforce traditional KYC/AML procedures.

Transactions often occur between anonymous wallets, hindering the tracking of fund origins and destinations. Furthermore, automated protocols can execute transactions without human oversight, potentially facilitating illicit activities without raising red flags. These factors create vulnerabilities for money laundering within DeFi, such as the use of decentralised exchanges (DEXs) and automated market makers (AMMs) to mix funds, the exploitation of stablecoin mechanisms to launder funds, and the potential for yield farming and lending protocols to generate profits from illicit funds.

Cross-chain bridges, which enable the transfer of assets between different blockchains, introduce additional AML risks. By facilitating the movement of funds across chains, they can further obscure the origin and destination of illicit funds. This increased anonymity can be exploited by criminals to circumvent regulations in jurisdictions with weaker AML/CFT controls. Moreover, hacks and exploits on cross-chain bridges can be leveraged to steal and launder substantial sums of cryptocurrency.

Enhanced due diligence measures for DeFi platforms and cross-chain bridges, including thorough background checks and transaction monitoring, are crucial. International cooperation between regulatory bodies is essential to track and combat cross-border money laundering activities. Technological solutions, such as blockchain analysis tools, can be employed to trace the flow of funds across different chains and identify suspicious activities.

How Russia uses crypto to evade sanctions

In the wake of Russia's invasion of Ukraine, international sanctions have been one of the most powerful tools used by Western governments to restrict Russia's access to global markets. However, as sanctions tightened, many Russian entities and individuals began turning to cryptocurrency as a means of evading these financial restrictions. The decentralised and pseudonymous nature of digital currencies has made it increasingly difficult for authorities to track and block illicit financial flows.

Russian oligarchs and their enablers have used and abused elements of cryptocurrency, along with the use of cryptocurrency exchanges and P2P trading, to evade sanctions.

Following the imposition of international sanctions, Russia has turned to cryptocurrencies to conduct trade with countries that have been less supportive of Western sanctions, such as Iran, Venezuela, and North Korea. For instance, Russia has reportedly used cryptocurrency to facilitate oil transactions with Iran, a country also subject to heavy sanctions.

State-sponsored sanctions evasion

Garantex remains a central player in Russia's crypto market despite its designation by the Office of Foreign Assets Control (OFAC) and Office of Financial Sanctions Implementation (OFSI) in the US and UK, respectively. This centralised exchange (CEX) has processed a substantial volume of transactions by designated actors in Russia and Iran, demonstrating its utility for sanctions evasion. The Russian government has passed legislation to officially leverage services like Garantex, given its deep liquidity across major blockchains. Garantex has processed nearly $100 billion in transactions since 2018.

This has the hallmarks of large-scale, state-sponsored sanctions evasion at scale. Worryingly for regulated business, not all Garantex users are Russian nationals or Russia-based, nor do they operate on behalf of the Russian government. Meaning some non-Russian users may be at risk of facilitating sanctions evasion. Additionally, a great deal of sanctions evasion activity occurs outside official government channels and takes place through traditional off-chain methods, such as private investment vehicles and offshore shell companies.

In 2022, OFAC sanctioned BitRiver, one of the largest cryptocurrency mining companies in Russia. The company was accused of providing the infrastructure and services needed for sanctioned Russian individuals and entities to mine cryptocurrencies, facilitating the movement of illicit funds. BitRiver's activities demonstrate how cryptocurrency mining and related services can be used to create a financial ecosystem that operates outside the reach of global sanctions enforcement.

There are also reports of Russian companies using cryptocurrency exchanges based in countries with weak anti-money laundering regulations. These exchanges often provide an easy entry point for sanctioned entities to convert their cryptocurrency into fiat currency or other assets that can be moved across borders without attracting attention.

Another method for evading sanctions involves the use of crypto wallets, which allow individuals and organisations to store and manage their cryptocurrency holdings. OFAC also imposed sanctions on Russian-linked cryptocurrency wallets and addresses associated with money laundering operations. These sanctions targeted crypto wallets that were used to launder funds through multiple transactions and exchanges, ultimately enabling the sanctioned individuals to access capital despite the restrictions.

The global response to Russian sanctions evasion

In response to the growing use of cryptocurrency for sanctions evasion, global regulators have ramped up efforts to close loopholes. The US Treasury Department has targeted cryptocurrency exchanges and wallet addresses linked to Russia, warning them that they could face penalties for facilitating transactions that evade sanctions. In addition, international regulators are working to tighten the regulation of cryptocurrency exchanges, calling for more transparency and compliance with AML and KYC requirements.

Despite these efforts, the global nature of cryptocurrency and the decentralised nature of many blockchain networks make it difficult to fully control. The ability to move digital assets across borders without intermediaries makes cryptocurrency an attractive option for those seeking to evade financial sanctions. While some countries have taken action to restrict the use of cryptocurrency for illicit activities, others remain less vigilant, allowing Russian entities to find alternative routes to bypass sanctions. As the US pushes ahead with a crypto-friendly regulatory environment, Russian sanctions evaders could be emboldened.

Terrorism and crypto-currency: The Hamas digital wallet

Before its destruction, Hamas was the second richest terror group in the world, after Iranian-backed Hezbollah in Lebanon. Hamas had an annual budget of around $2 billion, and a lot of that came via crypto.

Research by blockchain analytics firm Elliptic showed that Hamas had potentially received more than US$7.3 million worth of crypto by July 2021, holding funds in Bitcoin, Tether stablecoin, Ether, Dogecoin and other crypto assets.

Hamas and the world of crypto-hawala

Zuhair Shamlakh, the head of the Hamas cryptocurrency arm, sent money mules abroad, swapping cryptocurrency for hard cash in a well-used hawala network of financing. With dozens of accounts in the former Binance crypto exchange, Shamlakh orchestrated funds used to finance the October 7 atrocities.

Shamlakh's Al Mutahadun exchange advertised on its Facebook page conversions for dollars, shekels and other local currencies at its streetfront office in Gaza. The use of crypto by the Gaza money exchanges was more sophisticated than Hamas's earlier fundraising efforts in bitcoin. Digital wallets connected to the companies moved funds overwhelmingly in the form of the stablecoin tether on a blockchain system called Tron, which has heightened user privacy.

This pivot to crypto helped Hamas and affiliates such as Palestinian Islamic Jihad to receive large sums from Iran during the two years that preceded the October 7 attacks on Israel. It was an attempt to use a new financial technology to lessen the risks of moving physical money and goods.

In June 2021, Israel's National Bureau for Counter Terrorist Financing seized a number of virtual currency wallets in connection to a Hamas fundraising campaign. One of the seized wallet addresses belongs to Buy Cash Money and Money Transfer Company (Buy Cash), a Gaza-based business that provides money transfer and virtual currency exchange services, including Bitcoin.

As well as involvement in Hamas fundraising, Buy Cash has also been used to transfers funds by affiliates in other terrorist groups, including for payment of large amounts of online infrastructure for ISIS.

Digital wallets identified by the Israeli counter-terror bureau found Hamas had received $41 million in crypto, according to research by Tel Aviv-based analytics and software firm BitOK. Wallets linked by the bureau in another order to Palestinian Islamic Jihad have received a further $93 million.

Some of the money and crypto exchanges look like typical storefront operations that offer international money transfers. Part of their businesses involved legitimate activity such as trade payments and remittances in order to generate sufficient cash flow to obscure Hamas' financing.

Shamlakh, owner of the Al Mutahadun exchange, which was cited in five sanctions cases as Hamas's main money changer. He arranged the transfer of Iranian money through crypto hawala networks. Around 2020, crypto became a method of large-scale transfers between Iran and the group within the hawala networks, instead of the massive tunnel network used to smuggle cash. Iran often swaps houses as a method of swapping cash for crypto. Shamlakh was sanctioned through asset freezes and travel bans in January 2024.

Fundraising and news outlets sanctioned for supporting terror

The US and UK sanctioned a terrorism-promoting media channel 'Gaza Now' alongside several individual executives of the channel, for providing direct financial support to Hamas via cryptocurrency.

One of the issues highlighted by the sanctions was Gaza Now's exploitation of the British and American financial system to support terrorism. The entity had received tens of thousands of dollars in cryptoasset donations, with the sanctioned individuals seeking to raise more cash for terrorism through crypto. Worryingly for sanctions compliance, most donations were under $500, with 40% under $100.

Crypto wallets added to US sanctions list

A series of crypto wallet addresses including Bitcoin (BTC), Ethereum (ETH) and Tether (USDT) were added to the US SDN sanctions list by OFAC in September 2024. The addresses belong to Iranian ransomware attackers and a neo-Nazi Russian paramilitary group Task Force Rusich. Task Force Rusich is known to be affiliated with The Wagner Group, which is also sanctioned by OFAC.

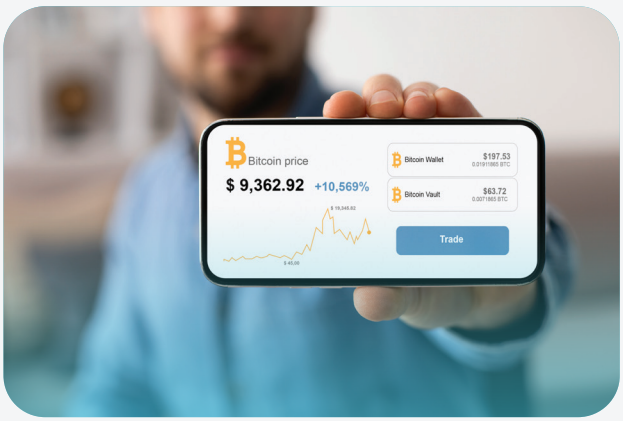
Sanctions evasion via crypto is known as cross-chain crime, and has been made easier as the decentralised exchanges, known as DEXs, do not apply AML controls. For example, using DEXs, criminals can readily exchange Ether for other assets – such as Tether – to attempt untraceability. In June 2022, North Korean ransomware attackers did this to launder funds they stole in a hack.

Another emerging risk factor are cross-chain bridges. These are services that allow a user to transfer assets from one blockchain, such as Bitcoin, to another, such as Ethereum.

Before these bridges, users could not easily move across blockchains. But these have become important parts of the crypto ecosystem.

Criminals and state actors have found these bridges another way to launder crypto through blockchains. Similar to how cash can be laundered through the financial system by being rapidly sent around the world or swapped into different currencies.

Just one cross-chain bridge called RenBridge, is believed to have facilitated over half a billion dollars in illicit crypto transactions already. This includes over $150 million from ransomware attackers and $33 million traced to a North Korean attack.



North Korean hackers stole $1.3 billion in crypto in 2024

A staggering $2.2 billion in cryptocurrencies has been stolen globally in 2024, with North Korean hackers responsible for over half of the total, according to a study by research firm Chainalysis. Hackers affiliated with North Korea looted $1.3 billion in digital assets, more than doubling their haul from the previous year.

The study suggests that some of these thefts were linked to North Korean cybercriminals posing as remote IT workers to infiltrate cryptocurrency and technology firms. This tactic has allowed them to exploit vulnerabilities and gain access to sensitive systems.

While the amount of cryptocurrency stolen in 2024 represents a 21% increase compared to 2023, it remains below the record-breaking levels seen in 2021 and 2022. *"The rise in stolen crypto in 2024 underscores the need for the industry to address an increasingly complex and evolving threat landscape,"* the report noted.

A significant portion of the stolen crypto was traced to compromised private keys—digital credentials essential for accessing and managing crypto assets. *"Given that centralized exchanges manage substantial amounts of user funds, the impact of a private key compromise can be devastating."*

Among the major incidents this year were the theft of $300 million in Bitcoin from Japanese exchange DMM Bitcoin and the loss of nearly $235 million from India-based exchange WazirX.

The US has accused North Korea of using cryptocurrency theft to evade international sanctions and fund its weapons programs. In December 2024, a federal court in St Louis indicted 14 North Koreans for their alleged involvement in a long-running scheme to extort funds from U.S. companies and funnel the proceeds to Pyongyang.

What does the FATF say about crypto currency red flags?

In 2020, the Financial Action Task Force (FATF) published a comprehensive report aimed at guiding cryptocurrency wallet providers, exchanges, and other virtual asset service providers (VASPs) in developing robust AML programs. Recognising the unique risks associated with cryptocurrencies, FATF outlined key red flags to help identify and mitigate money laundering activities. These indicators focus on specific behavioural, transactional, and technological patterns that may suggest illicit activity.

Technological features that Increase anonymity

Cryptocurrencies and exchanges offering enhanced anonymity can be a haven for criminals. Features such as privacy-focused coins (e.g., Monero, Zcash), mixers, and tumblers allow users to obscure the origins of funds and make tracking transactions more difficult. Similarly, the use of decentralized exchanges (DEXs) and peer-to-peer trading platforms, which often lack robust KYC measures, can be exploited for illicit purposes.

Geographical risks

Jurisdictions with weak or non-existent AML regulations are a significant red flag. Criminals often channel funds through countries with limited oversight, leveraging gaps in international AML standards. These high-risk regions may also serve as "hubs" for setting up shell companies or fraudulent exchanges, complicating efforts to trace illicit funds.

Transaction size and frequency

Unusual transaction patterns, such as making several high-value transfers over a short period or repeatedly clearing transactions just below record-keeping or reporting thresholds (known as "structuring" or "smurfing"), may indicate attempts to evade scrutiny. These patterns are often used to launder large sums of money while avoiding detection by AML systems.

Transaction patterns

Behavioural anomalies in transaction patterns are another key indicator. Red flags include:

- Multiple transactions with no clear commercial rationale.
- Frequent large-value cryptocurrency transfers from numerous unrelated accounts to a single wallet within a specific timeframe.
- Cryptocurrency account activity that deviates significantly from the customer's known profile or declared purpose.
- Numerous small transactions from unrelated accounts, which are later consolidated into fiat withdrawals.

Source of funds and source of wealth

Suspicious activities related to the source of funds include:

- Single cryptocurrency wallets linked to numerous bank cards or accounts, indicating potential layering activities.
- Large deposits of cryptocurrency being converted into fiat currency shortly afterward without an apparent business justification.
- Customers actively concealing the origins of their funds, including those who utilise third-party intermediaries to obscure their financial history.

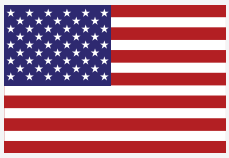
Sender or recipient profiles

Characteristics of senders or recipients can also signal potential money laundering risks. These include:

- Users who refuse to comply with KYC or provide incomplete or false identification.
- IP addresses that do not match declared locations, or frequent changes in IP address or personal information.
- Accounts exhibiting inconsistent or unexplained behaviour, such as switching between multiple wallets or addresses without a clear purpose.

Cryptocurrency regulation **around the world**

Cryptocurrency regulation around the world



Crypto regulation in the United States

As the US government grapples with how to regulate and integrate cryptocurrency into its broader financial system, some in Congress think they have the answer. **The Strategic Bitcoin Reserve and Bitcoin Act of 2024** stand out as a pivotal proposal in reshaping the US approach to digital assets.

This concept, which would see the US government accumulate a reserve of Bitcoin to hedge against financial instability and devaluation of the dollar, has gathered significant momentum. Initially championed during the 2024 Bitcoin conference by Senator Cynthia Lummis, the proposal gained further traction with support from President Donald Trump's incoming administration, which envisions making the US the global leader in cryptocurrency adoption.

This legislation, which outlines the purchase of 1 million Bitcoins over five years, presents a concrete plan for creating this reserve. Inspired by traditional central bank practices of holding gold and foreign currency reserves, these proposals aim to position Bitcoin as a core asset for the US Treasury.

The Strategic Bitcoin Reserve: A bold hedge against cryptocurrency

Under this vision, a Strategic Bitcoin Reserve would mirror the function of gold reserves, serving as a hedge against dollar devaluation, inflation, and potential economic instability. Proponents argue that as Bitcoin's supply is capped at 21 million coins, its scarcity makes it an attractive alternative to fiat currencies that can be devalued through overproduction. Establishing a reserve would signal the US government's confidence in Bitcoin as a critical financial asset, potentially setting a precedent for other nations.

Advocates believe this move could help mitigate the risks of mounting national debt and declining purchasing power of the dollar. By incorporating Bitcoin into its reserve portfolio, the US could diversify its financial holdings, leveraging Bitcoin's appreciation potential to strengthen its fiscal position.

The Bitcoin Act of 2024: Cementing bitcoin's role in national policy

Introduced by Republican Senator Cynthia Lummis, the Bitcoin Act of 2024 proposes a structured approach to acquiring and integrating Bitcoin into the US financial system. The legislation outlines a plan for the Treasury to purchase 200,000 Bitcoins annually over five years, potentially amassing 1 million Bitcoins, worth hundreds of billions of dollars at current prices.

This aggressive acquisition strategy would not only bolster the strategic reserve but also reinforce market confidence in Bitcoin. By committing to large-scale, predictable purchases, the US government could stabilise Bitcoin's value and encourage institutional and retail investors to follow suit.

Beyond its financial implications, the Bitcoin Act would mark a turning point in cryptocurrency regulation and adoption. It could establish a legal framework for incorporating digital assets into national financial systems, potentially paving the way for further legislation supporting innovation and growth in the crypto sector. While the full details and execution of these proposals remain to be seen, their mere introduction demonstrates the confidence the incoming US administration has on cryptocurrency.

Crypto regulation in the European Union

In May 2023, the European Union introduced MiCA (Markets in Crypto-Assets), establishing the world's first comprehensive framework to regulate the burgeoning cryptocurrency market. Designed to foster innovation while ensuring market stability and investor protection, MiCA integrates cryptocurrencies into existing financial systems and addresses the unique challenges posed by digital assets.

It fully came into force on 1 January 2025. MiCA sets clear and stringent requirements for all entities operating within the crypto ecosystem. Companies involved in issuing, trading, or providing services related to cryptocurrencies must obtain a license to operate within the EU. This licensing aims to ensure compliance with the EU's extensive AML rules.

A key aspect of MiCA is its categorisation of crypto assets, distinguishing between currencies primarily designed for value transfer (such as Bitcoin), asset-backed tokens (like stablecoins), and security-like tokens that resemble traditional investment instruments. By doing so, the regulation seeks to apply appropriate rules and oversight mechanisms tailored to the characteristics of each asset type.

To enhance transparency and security, MiCA mandates the identification of both senders and recipients for all cryptocurrency transactions, regardless of transaction value, aligning with the EU's broader efforts to clamp down on illicit financial activities. The regulation also introduces stricter measures for wallets holding assets exceeding €1,000, requiring full identity verification processes akin to those used in traditional banking systems. This reflects the EU's commitment to harmonising crypto regulations with existing financial protocols to mitigate risks and promote trust in digital assets.

Crypto regulation in the United Kingdom

The United Kingdom has long expressed aspirations to establish itself as a global hub for cryptocurrency innovation and adoption. Former Prime Minister Rishi Sunak championed this vision, launching initiatives such as the potential launch of a "digital pound" (a central bank digital currency) and even government-issued NFTs as part of efforts to signal the UK's commitment to embracing the digital economy.

The UK is supposed to announce a draft regulatory framework for crypto assets early in 2025. Economic Secretary to the Treasury, Tulip Siddiq emphasised the importance of removing legal uncertainties, particularly around staking services, which the government does not intend to classify as "collective investment schemes."

The Financial Conduct Authority (FCA) serves as the primary regulator for the crypto market, overseeing activities related to AML. licensing, and consumer protection. The FCA has taken a cautious yet proactive stance, requiring all crypto businesses operating in the UK to register and comply with stringent AML requirements. This includes ensuring transparency in operations and safeguarding against illicit financial activities.

Additionally, the UK's Crypto Asset Taskforce (CATF), a collaborative effort between HM Treasury, the FCA, and the Bank of England, plays a pivotal role in shaping the country's cryptocurrency strategy. The task force focuses on developing comprehensive regulatory frameworks to address the unique challenges posed by digital assets while fostering growth in the sector. These efforts include integrating cryptocurrencies into the broader financial ecosystem through tailored adjustments, such as recognising the differences between traditional financial instruments and blockchain-based assets.

Crypto regulation in China

China, once a global leader in cryptocurrency mining and trading, has taken a starkly different approach in recent years by imposing a blanket ban on all crypto-related activities. However in November 2024, a Shanghai judge clarified that personal ownership of cryptocurrency is legal in China. The ruling did make it clear that business activities involving cryptocurrencies remain banned.

During the 2010s, the country was at the forefront of the cryptocurrency boom, with Chinese miners contributing to the majority of Bitcoin's global hash rate. Additionally, several of the world's largest cryptocurrency exchanges, such as Binance and Huobi, were founded in China, making it a pivotal player in the early development of the crypto ecosystem.

However, the Chinese government began clamping down on the sector in 2017, initially banning Initial Coin Offerings (ICOs) and restricting domestic cryptocurrency exchanges. By 2021, the crackdown intensified, culminating in a comprehensive prohibition on all crypto trading, exchanges, and mining operations within the country. Authorities cited concerns over financial stability, illicit activities such as money laundering, and the environmental impact of energy-intensive mining practices as reasons for the sweeping measures.

The ban effectively forced crypto exchanges and mining companies to shut down or relocate their operations abroad. Many mining firms moved their activities to countries with more favourable regulatory environments and abundant energy resources, such as the United States, Kazakhstan, and Canada. Meanwhile, Chinese citizens were barred from accessing foreign crypto exchanges and participating in trading through rigorous enforcement of internet firewalls and financial monitoring systems.

Despite the ban, blockchain technology remains a key focus for the Chinese government. China has promoted the development of its state-backed digital currency, the Digital Yuan (e-CNY), which is issued and controlled by the People's Bank of China (PBOC). The Digital Yuan serves as the centrepiece of China's vision for a cashless society and reflects the government's preference for centralised digital financial systems over decentralised cryptocurrencies.

Despite the previous clampdown on cryptocurrency, the clarification of the law in November 2024 that personal ownership is lawful could spur renewed interest—or another clampdown—on cryptocurrency in China.

Crypto regulation in India

India has had a complex and evolving relationship with cryptocurrencies, marked by both enthusiasm and regulatory apprehension. The country saw rapid adoption of digital assets during the late 2010s, with millions of investors and numerous startups entering the crypto space. However, the Indian government and regulatory bodies have expressed persistent concerns about the potential misuse of cryptocurrencies for money laundering, tax evasion, and funding illegal activities, as well as the risks they pose to financial stability.

In 2018, the Reserve Bank of India (RBI), the nation's central bank, took a hard stance by prohibiting financial institutions from providing services to cryptocurrency businesses. This effectively choked the burgeoning industry, leading many exchanges and investors to suspend their operations. However, the Supreme Court of India overturned this ban in 2020, ruling that it was disproportionate and lacked adequate legal grounds. This decision reignited activity in the crypto market, sparking a surge in trading volumes and the entry of global and domestic players into the sector.

Despite the Supreme Court's ruling, regulatory uncertainty continues to cloud the future of cryptocurrencies in India. The government has signalled its intent to introduce legislation to ban all private digital assets, citing concerns over investor protection and systemic risks. The proposed bill, which aims to outlaw trading, mining, and holding of cryptocurrencies while potentially promoting the development of a state-backed Central Bank Digital Currency (CBDC), has faced delays due to political and logistical challenges.

The delays have left India's crypto market in a state of limbo. While the government deliberates, exchanges and investors operate in a largely unregulated environment, with many relying on self-regulation and compliance with general financial laws. The uncertainty has created a paradox: on one hand, India has emerged as a major player in the global crypto economy, with a rapidly growing user base and innovative startups; on the other hand, the looming threat of a ban discourages long-term investment and stifles broader innovation in the sector.

Adding to the complexity, the government has introduced stringent taxation policies, including a 30% tax on cryptocurrency profits and a 1% tax deducted at source (TDS) on all crypto transactions above a certain threshold. These measures, while seen as a step towards formalizing the sector, have led to reduced trading volumes and driven some investors to explore international platforms.

Crypto regulation in Japan

Japan has adopted a cautious yet progressive approach to cryptocurrency regulation, shaped significantly by its early experiences in the sector. A defining moment came in 2014 with the collapse of Mt. Gox, a Tokyo-based cryptocurrency exchange that, at its peak, handled over 70% of global Bitcoin transactions. The exchange filed for bankruptcy after losing approximately 850,000 Bitcoins—then worth over $450 million—due to hacking and mismanagement. This scandal highlighted the vulnerabilities of the nascent crypto market and underscored the need for robust regulatory oversight.

In response, Japan became one of the first countries in the world to introduce formal cryptocurrency regulations. In 2016, the Japanese government amended its Payment Services Act to recognise Bitcoin and other digital currencies as legal forms of payment. This legislation established a licensing system for cryptocurrency exchanges, requiring them to adhere to strict AML and customer protection standards. This move not only restored confidence in the market but also positioned Japan as a pioneer in creating a regulated environment for cryptocurrencies.

Further updates to the regulatory framework followed in 2018 after another high-profile hack involving Coincheck, a major Japanese exchange. The Financial Services Agency (FSA), Japan's financial regulator, introduced stricter security requirements for exchanges, mandatory cold storage for assets, and enhanced compliance protocols. These measures aimed to fortify the industry against cyber threats and ensure better safeguards for investors. At the same time, Japan continues to innovate, exploring areas like Central Bank Digital Currencies (CBDCs) and blockchain applications in industries such as supply chain, healthcare, and finance.

Crypto regulation in South Korea

South Korea has been a prominent player in the global cryptocurrency market, known for its early adoption and significant trading volumes. However, the country has also faced challenges in balancing its dynamic crypto industry with the need for regulatory oversight and user protection. In response, South Korea has taken significant steps to formalise its cryptocurrency sector, most notably with the recent implementation of the Act on the Protection of Virtual Asset Users (VASPs). Enacted in the summer of 2024, this law represents a landmark regulatory framework designed to enhance accountability and protect investors in the digital asset space.

Under the VASPs Act, cryptocurrency exchanges and other virtual asset service providers are required to conduct thorough due diligence, including robust Know-Your-Customer (KYC) and Anti-Money Laundering (AML) protocols. The act also mandates that exchanges maintain adequate capital reserves, segregate customer funds, and implement comprehensive security measures to safeguard user assets against cyber threats. These provisions aim to instil greater confidence in the market while mitigating risks associated with fraud, hacking, and financial instability.

Despite these regulatory advancements, public enthusiasm for cryptocurrencies in South Korea has shown signs of cooling. This contrasts with the country's previous reputation as a hotspot for crypto trading, where the "Kimchi Premium"—a phenomenon where Bitcoin prices in South Korea traded significantly higher than global averages—underscored the fervour for digital assets. Today, while the market remains active, broader interest has been tempered by global market volatility, regulatory scrutiny, and caution among retail investors.

The South Korean government's proactive approach to regulation reflects its dual objectives: fostering innovation in the blockchain sector while ensuring that investor protection and market integrity remain paramount. Alongside the VASPs Act, authorities are also exploring additional measures, including taxation policies for crypto earnings and enhanced oversight of Initial Coin Offerings (ICOs).

Case study: The crypto-bro president of El Salvador

El Salvador's 'crypto-bro' president, 40-year-old Nayib Bukele, has made Bitcoin (BTC) the central plank of his economic agenda. The populist leader has ruled the Central American country since 2019, racking up a litany of accusations from democratic backsliding to rampant corruption. But it's his flirtation with cryptocurrency that has hit headlines. Not only did he force through world-first reforms making Bitcoin legal tender in a midnight session of Congress, but he plans to build a geo-thermal powered city devoted to Bitcoin mining at the base of a volcano.

Meanwhile, the government gave away a new digital wallet app, Chivo, to each citizen, containing $30 worth of Bitcoin and installed hundreds of crypto cash machines across the country. Despite Bitcoin's steady rise, the average Salvadorian has—unsurprisingly—missed out. Meanwhile the risks remain, as does IMF opposition.

Making the tokens legal currency means everyday businesses may find it exceedingly difficult to undertake necessary KYC requirements expected of Bitcoin transactions. Bukele's hasty measures have made it far easier for criminals who have Bitcoins to exchange them for hard currency, or potentially launder tokens through luxury goods or real estate. Identifying deliberately structured transactions becomes exponentially more difficult when the currency can have double- or triple-digit value fluctuations against the dollar, sometimes daily.

Making sense of customer profiles could present a significant challenge too. Around 70% of El Salvador is unbanked, offering virgin territory for money launderers to open new accounts with wallets bursting with BTC. A rural farmer with millions in Bitcoin to their name is a textbook case for enhanced due diligence or increased monitoring anywhere else in the world. In El Salvador that farmer can currently fly under the radar.

One of the benefits of Bitcoin is that transactions are stored on blockchain, theoretically making every payment trackable and traceable. But the Chivo wallet, made available to every Salvadoran, has been plagued with problems from identity theft to disappearing coins. It's a worrying start for a national crypto experiment where trust in the technology is the gold standard.

The issue in El Salvador lies in the lack of sufficient AML and KYC regulations. In their assessment of El Salvador's Bitcoin roll out, Fitch has not yet downgraded their rating of the country's banks. But the credit appraiser stated: *"If technological infrastructure, controls, and the regulatory and supervisory framework are not adequately developed or implemented, it could expose banks to greater operational, cyber, and money laundering risks."*

As Fitch has noted, Salvadoran banks have yet to meet Basel II or Basel III standards. The country does not follow IFRS accounting standards and doesn't have capital requirements for market or operational risk. For correspondent banking services and regulated entities the world over, when presented with a transfer from El Salvador and the source of funds listed simply as BTC, what kind of money laundering risk does that present? Is a very high dollar amount in an average citizen's bank account simply the result of a Bitcoin induced economic boom, or the illicit proceeds of corrupt gains?

President Bukele's controversial adoption of Bitcoin comes amidst increasing concerns about democratic backsliding and corruption in the country. The US has recently banned dozens of Salvadoran officials from the United States for corruption, several of whom are senior members of President Bukele's administration. A number have also been indicted for money laundering and accepting bribes.

President Bukele shows no sign of stepping back from his controversial reforms. The self-proclaimed 'World's Coolest Dictator' has previously used the military to force legislation through congress and has ousted five supreme court judges and an attorney general who ruled against him. President Bukele's penchant for 'rule-by-tweet' and his popularity in cryptocurrency circles is raising serious red flags. FATF action against El Salvador could have serious consequences. Grey listing flags the country for increased monitoring, and is the first step towards black listing. If black listed, El Salvador would join only Iran and North Korea. The international community would be obliged to sanction El Salvador and automatically apply enhanced due diligence.

The trouble with President Bukele is he may be more interested in winning fans among cryptocurrency advocates—and his good friend Donald Trump—than assuaging the international community's concerns.

Conducting a cryptocurrency risk assessment **for regulated entities**

Conducting a cryptocurrency risk assessment for regulated entities

Should cryptocurrency always be treated as high risk? In VinciWorks opinion, yes. While not every cryptocurrency user presents a risk, there is no legitimate use for cryptocurrency. The only benefits it provides are to nefarious actors who may be attempting to launder money, evade sanctions, or fund acts of terror.

Whether you decide to conduct enhanced due diligence on any use of cryptocurrency is up to your own risk appetite, however there are a number of checks and questions to assess the risk factors if you are faced with a cryptocurrency-related transaction.

Client identification and due diligence

Know your customer (KYC): Have you conducted thorough KYC checks on clients involved in cryptocurrency transactions?

Source of funds: Have you verified the source of the funds being used for cryptocurrency transactions?

Beneficial ownership: Have you identified the true beneficial owner of the cryptocurrency wallet or account?

Sanctions screening: Have you screened the client and associated entities against relevant sanctions lists (e.g., OFAC, EU sanctions)?

Politically Exposed Persons (PEP): Have you assessed whether the client or associated individuals are PEPs, requiring enhanced due diligence?

Transaction monitoring

Transaction size and frequency: Have you evaluated the volume and frequency of cryptocurrency transactions to detect unusual or suspicious activity?

Cross-border transfers: Are there transactions involving cross-border transfers, and have you assessed the associated risks?

Peer-to-peer transactions: Are clients using decentralised exchanges or P2P platforms? How do you track and monitor these types of transactions?

Suspicious transaction reporting: Do you have procedures in place to identify and report suspicious cryptocurrency transactions to the appropriate authorities?

Risk assessment of crypto exchanges and platforms

Regulatory status: Is the cryptocurrency exchange or platform used by the client regulated in a reputable jurisdiction with proper AML/KYC controls in place?

Exchange location: Does the exchange operate in a jurisdiction with weak or insufficient anti-money laundering controls (e.g., a high-risk country)?

Operational transparency: Is the exchange transparent about its ownership, operational practices, and AML policies?

AML compliance: Does the exchange have an established AML program that includes monitoring, reporting, and record-keeping requirements?

Type of cryptocurrency involved

High-risk cryptocurrencies: Are clients using privacy coins (e.g., Monero, Zcash) or other cryptocurrencies with a high degree of anonymity that may complicate tracking?

Stablecoins: Are stablecoins being used, and have you assessed the risks associated with their backing, liquidity, and regulatory concerns?

Emerging cryptocurrencies: Are there any new or lesser-known cryptocurrencies involved that lack a clear regulatory framework or market oversight?

Technology and blockchain transparency

Blockchain transparency: Have you evaluated the transparency of the blockchain for the cryptocurrency in question? Public blockchains offer more transparency than private or permissioned blockchains.

Decentralised finance (DeFi): Are your clients interacting with decentralised finance platforms or smart contracts, and have you assessed the risks related to these decentralised ecosystems?

Anonymity features: Do the cryptocurrencies or platforms used offer built-in anonymity features (e.g., mixing services or coin tumbling)? How do these features impact risk assessment?

Geopolitical and legal considerations

Sanctioned countries and entities: Have you identified whether the cryptocurrency transactions involve any countries, entities, or individuals subject to international sanctions?

Jurisdictional risk: Are you aware of the legal and regulatory frameworks governing cryptocurrency in your jurisdiction and any countries where the client's activities may occur?

Cross-border regulations: Are you aware of the varying levels of cryptocurrency regulation in different countries where your clients operate or have assets?

Third-party services and intermediaries

Use of crypto custodians or wallet providers: Do clients use third-party custodians or wallet providers? Have you assessed the risk of these third parties in terms of security and regulatory compliance?

Crypto payment processors: Are clients using crypto payment processors or gateways? How do these services handle AML/KYC compliance?

Internal policies and staff training

AML policies: Does your organisation have up-to-date and comprehensive AML policies and procedures specific to cryptocurrency transactions?

Employee training: Have staff members received specific training on cryptocurrency risks and the relevant regulations for monitoring and reporting suspicious activities?

Technology solutions: Are you using specialised AML software or blockchain analytics tools to monitor cryptocurrency transactions effectively?

Regulatory compliance and reporting

AML/CTF compliance: Do the entities involved in the transaction comply with AML/CTF regulations as they pertain to cryptocurrency transactions? Are all required filings made in a timely manner?

Tax compliance: Does the transaction comply with all tax requirements? Have you completed all necessary steps to ensure the beneficial owners are not attempted to evade tax?

Audit trails: Do you maintain comprehensive and secure audit trails for cryptocurrency transactions that may be subject to regulatory inspection?

Reputation and red flags

Reputation check: Have you conducted a reputation check on the cryptocurrency platform or wallet provider to ensure they have a good standing in the market?

Red flags: Are there any indicators of potential illicit activity, such as connections to high-risk jurisdictions, prior legal issues, or known cases of financial crimes?

What to do if there is a cryptocurrency red flag?

If any of the checks on cryptocurrency transactions or clients raise a red flag, you must take prompt and appropriate action to mitigate risk and comply with regulatory requirements. Here's a step-by-step guide on what to do when a red flag is detected:

Conduct enhanced due diligence (EDD)

Review the transaction and client profile: If a red flag is identified, the first step may be to conduct enhanced due diligence (EDD). This involves gathering more detailed information about the client, the source of funds, and the nature of the transaction. For example, if the transaction is linked to a high-risk jurisdiction or involves large, unexplained transfers, further investigation is needed to understand the background and potential risks.

Verify KYC and AML information: Reassess the KYC documentation and ensure that all the information provided by the client is consistent and complete. This might include verifying identification documents, sources of wealth, and the legitimacy of business activities.

Assess the transaction context: Investigate the context of the transaction that triggered the red flag. For example, if the client is using privacy coins, examine whether the client's behaviour aligns with known money laundering techniques, such as using mixing services or anonymous wallets.

Consult with internal compliance experts

Escalate the matter: If a red flag arises, it's essential to escalate the issue to your internal compliance team or designated AML officer. They can assess the situation from a compliance and risk management perspective. If you make a report, do not act until you are notified further.

Determine the next steps: The compliance team should analyse the red flag in light of your organisation's AML/CTF policies and procedures. If necessary, they should consult with legal counsel or external experts to ensure the correct course of action is taken.

Conduct transaction monitoring

Monitor the transaction trail: Analyse the transaction history of the client or wallet address involved in the flagged activity. KYC analytics tools can track the flow of funds, identify any suspicious patterns, and determine whether the funds are linked to illicit activities or high-risk entities.

Check for additional red flags: Review previous transactions related to the customer or transaction to identify any recurring patterns of suspicious activity. If the entity is engaged in ongoing high-risk activity, it may indicate a more systemic issue.

Check for sanctions or legal violations

Sanctions screening: If the red flag involves a potential connection to a sanctioned entity or individual, immediately screen the client or transaction against relevant sanctions lists (e.g., OFAC, EU, UN) and other watchlists (e.g., PEP, AML blacklists).

Legal consultation: If the investigation uncovers potential violations of sanctions or other laws, seek legal advice to determine whether the transaction or client should be reported to authorities.

Report suspicious activity

File a Suspicious Activity Report (SAR): If the red flag involves a legitimate concern regarding potential money laundering, terrorism financing, or sanctions evasion, a Suspicious Activity Report (SAR) should be filed with the appropriate financial intelligence unit (FIU) or relevant authority. Do not file an SAR yourself. Notify your compliance officer. Do not act on the transaction if you make a report. Discussing this with the client could result in a tipping off offence.

Document all actions: Maintain a detailed record of the actions taken to investigate the red flag, including communications, reports, and decisions made. This documentation will be essential for regulatory audits and to demonstrate compliance with AML/CTF requirements.

Consider terminating or freezing the relationship

Assess the risk of continuing the relationship: If the enhanced due diligence or investigation reveals that the client is involved in illegal activities, sanctions evasion, or poses a significant regulatory risk, consider terminating the relationship. This may involve freezing the client's assets or blocking further transactions.

Notify the client if required: Depending on the jurisdiction and nature of the activity, you may be legally obligated to notify the client of the termination. However, if this would risk alerting the client to an ongoing investigation (e.g., in the case of suspected money laundering), then the client should not be informed. Always consult your compliance officer before taking any further action.

Review and strengthen internal controls

Analyse internal controls: After identifying and addressing a red flag, it's important to review your internal controls and procedures to ensure they are effective in preventing similar issues from arising in the future. This includes reviewing transaction monitoring systems, KYC processes, and staff training on cryptocurrency risks.

Update risk assessment procedures: Use the findings from the investigation to refine your risk assessment procedures. This could involve identifying new red flags specific to cryptocurrency transactions or ensuring that your staff is better equipped to detect emerging risks.

Discuss concerns with authorities

Engage with regulators: If the red flag involves a serious compliance issue, cooperate fully with regulators and law enforcement agencies. This may involve providing additional information, facilitating investigations, or sharing any relevant data.

Be transparent: Transparency with regulators will demonstrate a proactive approach to compliance and help ensure that your entity is not complicit in illicit activities.

Strengthen ongoing monitoring

Ongoing vigilance: Even if a red flag has been resolved, continue monitoring the client's activities to ensure that no further suspicious transactions occur. Periodically review their account and transaction behaviour to detect any evolving risks.

Periodic reassessment: Regularly reassess the risk level of cryptocurrency transactions, especially as regulatory environments and the technology itself evolve.

When a red flag is raised in relation to cryptocurrency transactions or clients, it's essential to take a measured, thorough approach. By conducting enhanced due diligence, escalating the matter internally, monitoring transactions, reporting suspicious activity, and engaging with regulators, you can mitigate the risks associated with cryptocurrency while ensuring compliance with regulatory frameworks. Proactive action is key to protecting your entity from legal, financial, and reputational risks.

What next?
Protecting your firm in the face of cryptocurrency risks

In 2025, regulated entities such as law firms and financial institutions face growing risks related to cryptocurrency transactions. As America moves towards cementing itself as the cryptocurrency capital of the planet under Donald Trump and his cabinet of crypto-bros, the ease and social acceptance of crypto will grow. This does not remove its risk, nor the fact crypto is the currency of choice for the world's gangsters, money launderers and terrorists.

All entities must stay vigilant and continuously update their compliance frameworks to align with shifting regulations, particularly in areas like AML and tax compliance.

The potential for financial crime, including money laundering and fraud, remains a significant concern, exacerbated by the rise of decentralised finance (DeFi) platforms, privacy coins, and peer-to-peer transactions that can be difficult to track. Entities must invest in advanced transaction monitoring systems and blockchain analytics tools to detect suspicious activities, perform thorough due diligence, and maintain strong reporting practices.

Another key risk involves exposure to high-risk jurisdictions, particularly those lacking robust regulatory frameworks or those subject to international sanctions. Transactions involving these regions or unregulated exchanges can pose compliance challenges, requiring enhanced scrutiny and due diligence.

Illicit cash can be converted to crypto in Moscow or Caracas, and spun around the world in seconds. Weapons can be bought in crypto stolen by hackers, and criminals paid off via online wallets without ever needing to convert their ill-gotten gains into real cash. In 2025, the crypto risk is vastly increasing.

By adopting a comprehensive risk assessment framework, regulated entities can mitigate these risks, stay compliant with evolving regulations, and better manage the exposure to illicit or non-compliant activities in the cryptocurrency space.

About us

We believe compliance enables business. Compliance is an opportunity to be one step ahead, so your organisation can focus on advancing the business.

For over 20 years, VinciWorks has been at the leading edge of re-envisioning compliance tools and training. Our creative and driven team works hard everyday, challenging the traditional compliance industry to become forward-thinking, interactive and engaging. From our vast library of 800+ courses, to the award-winning Omnitrack training and compliance management software, to a curated catalogue of world class resources, VinciWorks is here to support your organisation every step of the way.

We constantly have our finger on the pulse, being the first to adapt our products to new regulations and market changes that impact our customers' businesses. Our flexible solutions ensure that every one of our products is tailored to our customers' unique business needs, placing them at the heart of everything we do.

vinciworks

www.vinciworks.com
enquiries@vinciworks.com
+44 (0) 208 815 9308