protiviti®
Global Business Consulting

COMPLIANCE INSIGHTS

The New Value Chain: How Digital Assets Are Reshaping Financial Crime, Compliance and Financial Transparency

By Carol Beaumier and Bernadine Reese

Are financial institutions prepared to address the risks of the new value chain?

Financial crime has entered a new era. The issue is no longer how criminals move money, but how they move **value**. Increasingly, that value moves across an expanding network of bank accounts, wallets, blockchains, tokenised instruments and digital platforms.

Understanding digital assets

The term *digital asset* is often used interchangeably with *cryptocurrency*, but this increasingly fails to reflect the reality of today's financial markets. Digital assets are best understood as the digital representation of value. That value may take many forms: money, securities, commodities, deposits, ownership interests, contractual rights or access to services.

Cryptocurrencies are only one subset of a much broader ecosystem that is rapidly becoming integrated into mainstream finance. Banks are experimenting with tokenised deposits that enable traditional bank money to move over blockchain infrastructure. Asset managers are exploring tokenised funds.

Capital markets participants are testing the issuance and trading of tokenised bonds and securities. Central banks across the world continue to examine the role of central bank digital currencies. At the same time, stablecoins are becoming an increasingly important mechanism for transferring value across borders and between financial ecosystems.

> ***In banking today, digital assets are best thought of as the digital representation of value, whether value is money, an investment, a claim, ownership of an asset, or a right to access a service.***
>
> ***The Evolution of Digital Assets, J.P. Morgan***

What links these developments is not the type of asset being represented, but the underlying infrastructure used to record ownership and transfer value. Distributed ledger technology allows assets to be issued, transferred, and settled through shared digital records that can be updated in near real time. In many cases, transactions can occur 24/7 rather than being constrained by traditional banking hours, settlement windows or geographic boundaries.

For financial institutions, this requires a shift in mindset. Historically, compliance programs have focused on monitoring different financial products, payment channels and customer relationships. Increasingly, institutions must focus on understanding how value moves across multiple ecosystems and infrastructures. The distinction between a payment, security, deposit, and digital asset is becoming less meaningful than the mechanisms through which value is created, transferred and controlled.

This shift is particularly important because the digital asset ecosystem will no longer be separate from traditional finance. Banks, payment firms, broker-dealers, custodians, exchanges, technology providers and investors are becoming increasingly interconnected. As these boundaries continue to blur, institutions that view digital assets solely as a niche or specialist asset class risk overlooking broader strategic, operational and financial crime implications.

Ultimately, digital assets should not be viewed as an entirely new category of financial activity. They are better understood as the next phase in the ongoing digitisation of value itself.

Why do criminals use digital assets?

A common response to this question is that digital assets provide anonymity. That is a misconception. Anonymity means a person's identity and financial details are kept secret. Public blockchains — where most digital asset activity occurs — offer pseudonymity, not anonymity. That's because:

- Transactions are recorded on a public ledger.
- Every transaction is linked to a wallet address, which serves as a pseudonym or digital identifier.
- Anyone can see the complete transaction history associated with a wallet address.
- Transaction histories are permanently recorded and often more traceable than cash.

Anonymity: **Little to no traceability**	**Pseudonymity:** **A trail that can be analysed**
The real identity of an individual is unknown and cannot reasonably be determined.	An individual's real identity is hidden behind an identifier but can be discovered.
No persistent identifier exists.	A persistent identifier exists (for example, a blockchain wallet address).
Activities cannot easily be linked back to a real-world person.	Activities can often be linked together through the pseudonym and potentially tied to a real-world person through investigation.

In fact, financial crime's great irony may be that digital assets are more traceable than cash.

More work is required to de-pseudonymise the available information and determine the real identity of the parties. (See "Methods of De-pseudonymisation" on this page.) But the critical question is not whether an identity can be uncovered, but whether a financial institution has developed the capabilities necessary to uncover it. The criminals hope that it has not, or at least that the time required to de-pseudonymise will provide them some advantage.

If it isn't anonymity that is the main draw for criminals, what are the advantages of digital assets criminals value?

There are several and they are generally the same advantages that appeal to legitimate users, including:

- Speed of near-instant settlement
- Cross-border capabilities
- 24/7 market access
- Peer-to-peer transactions, eliminating the need for traditional banks

Methods of De-pseudonymisation

- Exchange KYC records
- Blockchain analytics and address clustering to group wallets controlled by the same entity.
- Behavioral analysis through identification of transaction patterns
- Open source Intelligence (OSINT)
- Travel rule information
- Device, IP and metadata analysis

Criminal methods include using multiple wallets, moving funds across multiple addresses, leveraging multiple blockchain networks, using mixers and tumblers, and routing transactions through jurisdictions with weak controls or lax enforcement. In short, the goal of the criminals is to make attribution time-consuming and costly.

Financial institutions, however, cannot afford to let complexity and attempts at obfuscation become excuses for inaction. Effective controls, analytics, and investigative capabilities are essential to modern financial crime risk management, and the ability to identify the actors behind digital asset activity is a defining competency. Even institutions that do not offer digital asset products today are increasingly exposed through their customers, counterparties and payment flows, making this a capability no financial institution can afford to ignore.

Digital assets changed money laundering

Criminals have always sought the fastest, cheapest, and least detectable ways to move illicit funds. In fact, financial institutions have faced a persistent challenge: criminals are frequently the first to recognise how new technologies can be exploited for illicit purposes. In the digital asset ecosystem, where innovation can occur in weeks rather than years, that reality imposes an even greater burden on the financial services industry to keep pace with innovation.

The following illustrates some current digital asset laundering typologies:

- **Cross-chain laundering** — In cross-chain laundering, criminals may use bridges, swaps and asset conversions to develop a fragmented transaction trail, making it more difficult for financial institutions to follow funds from source to destination. While not impossible to trace, each additional blockchain adds complexity and increases the investigative effort.
- **Stablecoin laundering** — Stablecoin laundering exploits the speed, liquidity and growing acceptance of stablecoins to move illicit value globally. Criminals convert volatile cryptocurrencies into stablecoins to reduce price risk while continuing to transfer funds across exchanges, wallets and jurisdictions. Because stablecoins are often well integrated into the digital asset ecosystem, they can facilitate rapid movement of funds at scale.
- **Layered wallet networks** — Layered wallet networks involve dispersing funds through numerous wallets and transactions to conceal the relationship between the originator and ultimate beneficiary. Similar to layering in traditional money laundering, each additional wallet and transfer is designed to make transaction analysis more challenging and to obscure ownership. Sophisticated networks can involve hundreds or even thousands of interconnected addresses.

Lazarus Harmony Horizon Bridge Hack

In June 2022, hackers linked to North Korea's Lazarus Group, a state-sponsored cyber threat organisation linked to North Korea's primary intelligence agency, the Reconnaissance General Bureau (RGB), stole $100 million from the Harmony Horizon Bridge. The Harmony Horizon Bridge was a California-based blockchain and crypto firm that functioned as a cross-chain crypto tool, providing for the movement of digital money between the Harmony network, Ethereum and Binance.

Investigators reported the stolen funds were moved through numerous intermediary wallets (layered wallet networks), routed through decentralised exchanges (DEXs), transferred across multiple blockchains using cross-chain bridges (cross-chain laundering), and passed through PES in an effort to obscure the transaction trail. Despite the hackers' efforts, blockchain analytics and international law enforcement cooperation enabled investigators to trace significant portions of the funds and attribute the activity to the Lazarus Group.

Only a small amount of the $100 million was ever recovered. Harmony Horizon Bridge opted to suspend operations after the hack.

- **Decentralised exchanges (DEXs)** — Decentralised exchanges allow users to exchange digital assets directly through smart contracts without relying on a traditional intermediary. They do not require user identity checks (KYC), and allow instant trading across different blockchain networks, hiding the link between illegal funds and the criminal.

- **Self-hosted wallets** — Self-hosted wallets are digital wallets controlled directly by the user rather than by a financial institution or exchange. While they serve many legitimate purposes, they can reduce the visibility that regulated institutions have into the ownership and movement of digital assets. Criminals often transfer funds to self-hosted wallets to place assets beyond the immediate reach of traditional compliance and monitoring

- **Privacy-enhancing services (PES)** — Technologies such as cryptocurrency mixers, coin-joining services and privacy protocols make it more difficult to trace digital asset transactions and identify the individuals involved. These services may obscure transaction flows, break the visible link between a sender and recipient, or conceal wallet relationships that would otherwise be visible on a public blockchain.

Digital asset money laundering rarely relies on a single concealment technique. Criminals increasingly combine multiple typologies together, creating complex networks of wallets, exchanges, blockchains and intermediaries designed to stay one step ahead of traditional financial crime controls.

For financial institutions, the answer is not to avoid digital assets; that may not even be possible. Rather, financial institutions must get better — ideally at least as good — at understanding digital assets as the criminals who seek to exploit them.

The rise of digital asset fraud

While money laundering has historically dominated discussions about financial crime risk in digital assets, fraud has increasingly emerged as the most significant threat affecting both consumers and financial institutions. The combination of global reach, rapid settlement, relative ease of access and often irreversible transactions creates an attractive environment for fraudsters seeking to exploit victims at scale. In many cases, digital assets are not the root cause of fraud but rather the preferred mechanism for receiving, transferring, and dispersing illicit proceeds. Some of the more significant digital asset fraud threats include the following:

- **"Pig-butchering" scams** combine social engineering, relationship-building and fake investment opportunities, convincing victims to transfer funds into fraudulent platforms. Digital assets enable criminals to move and layer proceeds quickly across jurisdictions, making recovery difficult.

- **Investment fraud** has evolved in digital asset markets through fake token offerings, fraudulent trading platforms, impersonation scams and misleading promotions. These schemes increasingly use professional-looking websites, social media campaigns, AI-generated content and sophisticated customer support to appear legitimate.

- **Business e-mail compromise (BEC) and cyber-enabled fraud** now frequently involve compromised email accounts, deepfakes, and social engineering to redirect payments into digital asset wallets. The speed and global reach of digital asset transactions can significantly hinder recovery efforts.

A distinguishing characteristic of digital asset fraud is that victims frequently have no practical means of reversing a transaction once it has been executed. Unlike traditional payment mechanisms, which may offer dispute resolution, chargeback rights or intervention by financial institutions, many digital asset transfers are effectively final. While blockchain transparency may assist investigators in tracing funds, it does not guarantee recovery.

For financial institutions, this shift has important implications. Fraud prevention can no longer be viewed solely through the lens of traditional payment controls. Institutions increasingly require visibility into digital asset exposure, customer interactions with crypto asset platforms, wallet-related activity, and emerging fraud typologies. Effective fraud management now requires collaboration among traditional fraud teams, cyber specialists, sanctions professionals, and anti-money laundering investigators.

Sanctions evasion and national security risks

Fuelled by the geopolitical tensions across the globe, policymakers view digital assets not only as a financial crime concern, but also as a national security issue. The ability to transmit value globally, rapidly and outside traditional banking channels has not gone unnoticed by nation-states, cybercriminal organisations, terrorist groups and sanctions evaders seeking alternatives to conventional financial networks.

One of the most significant concerns involves state-sponsored actors, including North Korea, as illustrated in the Lazarus Harmoney Horizon Bridge case (see “Lazarus Harmony Horizon Bridge Attack,” page 4). Policymakers are concerned not only about the theft itself, but the potential use of the proceeds to support the goals of unfriendly nations.

Another concern is exchanges and service providers that may facilitate transactions involving sanctioned individuals, entities, or jurisdictions. (The Garantex case is a prime example.) These platforms can become conduits for illicit financial activity. In the same way that traditional financial institutions are prohibited from facilitating transactions involving sanctioned parties, digital asset service providers are expected to maintain robust sanctions compliance programs. Failure to do so can create the means through which sanctioned actors gain access to global financial markets despite economic restrictions.

The growth of the ransomware ecosystem also is receiving attention. Ransomware actors frequently demand payment in cryptocurrency because it can be transferred quickly across borders and layered through multiple wallets, exchanges and blockchain networks, complicating investigations and decreasing the likelihood of recovering stolen funds.

Policymakers also continue to monitor the potential use of digital assets for terrorist financing and proliferation financing. Although these activities reportedly represent a small fraction of overall digital asset activity, the ability to raise, transfer, and store value outside traditional financial channels nonetheless creates concerns. This has prompted regulators and international standard setters to issue warnings and advisories about the potential for terrorists to exploit digital assets.

The bottom line is that digital assets have made sanctions compliance significantly more complex. As a result, financial institutions must expand their sanctions compliance capabilities beyond conventional name screening and customer due diligence to include network analysis, blockchain analytics, and a clear understanding of sanctions-evasion typologies. Institutions that fail to expand their sanctions compliance program this may risk not only regulatory scrutiny, but also exposure to some of the most significant financial crime and national security threats of the digital age.

The emerging risks of stablecoins, DeFi, NFTs and gaming ecosystems

The evolution of financial crime risk in digital assets is not being driven solely by cryptocurrencies. Increasingly, attention is shifting toward emerging ecosystems that facilitate the creation, transfer, and exchange of value in new ways.

One area receiving substantial regulatory attention is stablecoins. Unlike many cryptocurrencies, stablecoins are designed to maintain a relatively stable value through reference to fiat currencies or other assets. Their price stability, growing liquidity and increasing integration with both digital asset and traditional financial markets have made them attractive for legitimate commerce ─ but they have also made them attractive to criminals seeking an efficient mechanism for moving value internationally.

Decentralised Finance (DeFi) introduces additional complexity. Through smart contracts, users can borrow, lend, exchange or invest assets without relying on traditional intermediaries. While DeFi platforms offer innovation and efficiency, they can also create challenges relating to governance, accountability, customer identification, sanctions screening, transaction monitoring and enforcement. As DeFi services increasingly replicate functions traditionally performed by regulated institutions, supervisors continue to examine how existing regulatory expectations should apply in decentralised environments.

Non-Fungible Tokens (NFTs) present a different set of considerations. Although attention has shifted away from the speculative NFT boom of recent years, questions remain regarding valuation, ownership, market manipulation, wash trading and the potential use of NFTs as mechanisms for transferring value between parties.

Gaming and virtual ecosystems represent another area of growing interest. Increasingly sophisticated online environments now contain digital currencies, virtual assets, marketplaces and peer-to-peer trading mechanisms that possess characteristics traditionally associated with financial systems. These ecosystems may create opportunities for value transfer, fraud and other forms of financial crime where controls have not evolved at the same pace as the underlying technology.

The common thread across these developments is the gradual expansion of digital asset ecosystems beyond the boundaries traditionally associated with financial services. As value becomes increasingly programmable, transferable and embedded across digital environments, financial institutions must broaden their understanding of where financial crime risk may emerge and how it can move between apparently unrelated ecosystems.

Implications for banks and financial institutions

For many financial institutions, the question is no longer whether digital assets will affect their risk profile, but how quickly those effects will materialise. Even institutions with no direct cryptoasset offering increasingly encounter digital asset exposures through customers, payment flows, counterparties, investments, correspondent relationships, investigations, sanctions reviews, fraud cases and third-party service providers. The growing integration of traditional finance and digital asset markets means that institutions can no longer assume that digital assets sit outside their control environment.

As a result, **financial crime frameworks must evolve beyond traditional product- and channel-based approaches**. Risk assessments should increasingly consider digital asset exposure across customer segments, products, jurisdictions, distribution channels, and business activities. Transaction-monitoring programs may require the integration of blockchain analytics and wallet intelligence alongside conventional monitoring solutions.

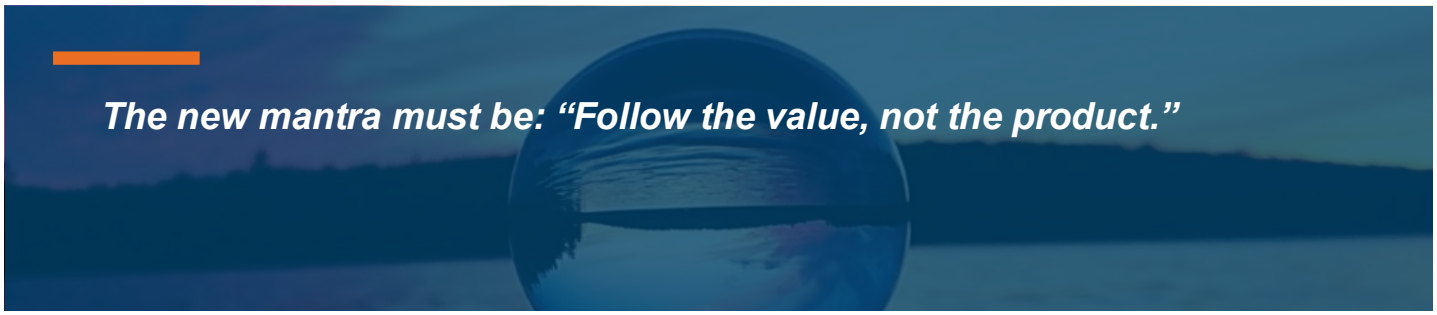
Sanctions-screening methodologies must adapt to incorporate wallet addresses, network analysis, and emerging sanctions-evasion typologies.

Governance will become equally important. Boards and senior management should ensure that digital asset risk is appropriately reflected within enterprise risk management frameworks, financial crime programs, fraud strategies, operational-resilience planning, and third-party risk oversight. The question is no longer whether a dedicated crypto team exists; it is whether the institution has developed sufficient organisational capability to understand how digital assets affect its broader risk profile.

Perhaps most importantly, institutions should resist viewing digital assets solely through the lens of compliance obligations. Digital assets, tokenisation, programmable finance, and blockchain-based infrastructure are reshaping how value moves throughout the financial system. The strategic institutions of the future are likely to be those that understand both the opportunities and the risks of this transformation.

The future: From financial crime controls to value movement controls

The emergence of digital assets is often described as a technological transformation, but its long-term impact may be broader. At its core, digital assets are changing how value can be represented, transferred, stored, and exchanged. Historically, financial institutions have occupied the centre of the money-transfer ecosystem. Today, value can move through public blockchains, tokenised assets, digital wallets, smart contracts, decentralised applications, and increasingly integrated financial platforms.



At the same time, embedded digital asset services are making blockchain-based functionality available through traditional financial products, creating new forms of interaction between traditional finance and digital finance. Meanwhile, advances in AI-enabled blockchain analytics are improving the ability of institutions to detect suspicious behaviour, identify wallet relationships, trace cross-chain activity, and uncover previously hidden financial networks.

Taken together, these developments suggest that the future of financial crime compliance may be less about determining whether activity involves fiat currency or digital assets and more about understanding how value moves. The new mantra must be: “Follow the value, not the product.”

If controls remain organised around product labels, they may miss how value moves across customers, counterparties, jurisdictions, payment channels, wallets, trade documents, and intermediaries — and leave financial institutions at the mercy of the criminals.

Conclusion

Cash remains attractive to criminals. Wire transfers continue to facilitate the movement of illicit proceeds. Shell companies still obscure beneficial ownership. Trade-based money laundering remains one of the most effective techniques for disguising the movement of value across borders. Many of the financial crime risks facing institutions today would be familiar to investigators from decades ago. Digital assets have not brought an end to these tried-and-true typologies.

What digital assets have done is expand the financial crime landscape. They have introduced new methods for moving, disguising, storing, and transferring value that operate alongside, and increasingly intersect with, traditional financial products. Cross-chain transfers, decentralised exchanges, self-hosted wallets, privacy-enhancing technologies, tokenised assets, and blockchain-based ecosystems have created new challenges for financial institutions, regulators, and law enforcement agencies seeking to identify and disrupt illicit activity.

But the story is not just one of increased risk. Digital assets have also created unprecedented opportunities for transparency, analytics and investigative insight. Unlike many traditional financial crime typologies that rely on opaque structures and fragmented records, blockchain activity often leaves a permanent and detailed trail of information. Institutions that develop the technology, expertise and investigative capabilities necessary to analyse that information can often uncover relationships and patterns that would be difficult to identify in traditional financial systems.

Ultimately, the institutions that succeed over the next decade will be those that recognise digital assets as part of a broader transformation in how value moves. The question is not whether digital assets will affect financial crime risk. Rather, the question is whether institutions will respond quickly enough to understand, monitor and manage the risk.

About the authors

Carol Beaumier is a senior managing director in Protiviti's Risk and Compliance practice. Based in Phoenix, she has more than 30 years of experience in a wide range of regulatory issues across multiple industries. Before joining Protiviti, Beaumier was a partner in Arthur Andersen's Regulatory Risk Services practice and a managing director and founding partner of The Secura Group, where she headed the Risk Management practice. Before consulting, Beaumier spent 11 years with the U.S. Office of the Comptroller of the Currency (OCC), where she was an examiner with a focus on multinational and international banks. She also served as executive assistant to the comptroller, as a member of the OCC's senior management team and as liaison for the comptroller inside and outside of the agency. Beaumier is a frequent author and speaker on regulatory and other risk issues.

Bernadine Reese is a managing director in Protiviti's Risk and Compliance practice. Based in London, Reese joined Protiviti in 2007 from KPMG's Regulatory Services practice. Reese has more than 30 years' experience working with a variety of financial services clients to enhance their business performance by successfully implementing risk, compliance and governance change and optimising their risk and compliance arrangements. She is a Certified Climate Risk Professional.

About Protiviti's Compliance Risk Management practice

There's a better way to manage the burden of regulatory compliance. Imagine if functions were aligned to business objectives, processes were optimised, and procedures were automated and enabled by data and technology. Regulatory requirements would be met with efficiency. Controls become predictive instead of reactive. Employees derive more value from their roles. The business can take comfort that its reputation is protected, allowing for greater focus on growth and innovation.

Protiviti helps organisations integrate compliance into agile risk management teams, leverage analytics for forward-looking and predictive controls, apply regulatory compliance expertise and utilise automated workflow tools for more efficient remediation of compliance enforcement actions or issues, translate customer and compliance needs into design requirements for new products or services, and establish routines for monitoring regulatory compliance performance. Learn more about Protiviti's Compliance Risk Management services.