Navigating the dangers and risks in your digital asset product launch

November 2022

pwc

www.pwc.ch

Navigating the dangers and risks in your digital asset product launch

A digital asset offering is now a prerogative for traditional banks, given the consumer demand for this burgeoning asset class. But how do banks ensure that they are ready to launch their offering, be it cryptocurrency exposure or trading for clients, NFT marketplace, custodial services, or a combination of the business opportunities the technology brings?

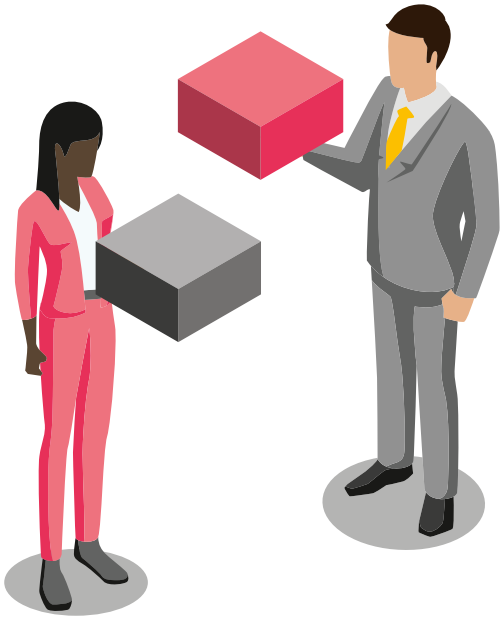
Offering products and services in digital assets is not without its challenges, with the below highlights barely scratching the surface:

- Blockchain technology brings transparency, traceability and 24/7 availability, but also demands an 'always-on' customer offering and real-time settlement processes, and relies upon the consensus and validation mechanism of the layer one protocol.
- Digital assets have unique characteristics and functionality, bringing with them a unique set of risks, such as the irreversibility of transactions and private key safeguarding.
- Smart contracts enable automated transactions and trusted, straight-through processing, provided you can rely upon the quality of code underpinning the contract and all relevant permutations have been considered.
- With a growing value of assets secured on chain and in wallets, and transferred between protocols via bridges, there is a greater incentive for malicious actors to penetrate weak spots in the value chain and drain funds, and therefore a significant focus on cyber and information security is required.

Financial institutions have established and proven risk and compliance policies and frameworks for the traditional products and services they offer. Given the regulatory environment and lack of specific licences for offering digital assets, financial institutions may in theory already have the required permission to support these new products or asset classes. Nevertheless, a proactive discussion with the regulator is highly recommended, if not essential, before launching the products and services, in order to discuss and clear the newly introduced risks and maintain a good relationship with the regulator.

How should a traditional financial institution wanting to offer digital asset services **adapt its existing risk and compliance policies** and frameworks? What are the new risks that need mitigation and monitoring? And what are the **market best practices**?

Given the complexity and constant change in the industry, with newly emerging technologies and risks, we believe it is important to work with partners who can not only provide challenge and assurance to the business approach, but also solve problems along the way and allow businesses to take advantage of the vast opportunities.



Focus risks for digital asset banking

Digital asset activities expose businesses to traditional risks as well as new types of risk. Given the maturing nature of the products and services, the list of potential risks is extensive and growing, with new risk typologies being uncovered as the technology and ecosystem evolve. Once established, careful monitoring of the external environment is essential to manage completeness of the risk landscape.

It is important to note that risks faced by companies will vary in terms of type and exposure, based on their business model and where they operate in the crypto ecosystem. For example, a core blockchain technology provider is likely to be more exposed to infrastructure risk compared with a pure crypto lender, whose primary risks are lending and counterparty risk. Hence, it is important that firms set up and tailor their own Enterprise Risk Management Framework to correctly define their firm-specific risks and taxonomy for a robust risk management process.

Highlighted below are focus risks across selected categories:

Risks in focus for digital asset banking – products and services

Product/service offering
- Cannibalisation (of existing offering)
- Bifurcation of services
- Operational complexity

Tokens and tokenomics
- Issuance management (token issuance vs. sales)
- Tokenomic design and valuation approach
- Token classification

Market dynamics
- Macro market demand
- Target customer demand
- 'Scaling' risk
- Network effects

Product characteristics
- Volatility/leverage of intended digital asset and underlying
- Underlying characteristics of digital asset (native digital vs. tokenized traditional)
- Utility of product/tokens

Risks in focus for digital asset banking – operations

Technology
- Blockchain infrastructure
- Smart contracts
- Consensus protocol
- Network risk
- Bridging assets
- Data oracles

Custody
- In-house vs. vendor-managed
- On premise vs. ‘as a service’
- Hot, warm, cold custody
- HSM vs. MPC security approach

Business continuity
- BCP tailored to digital assets
- Blockchain, node and bridge monitoring tools
- Real-time escalation given 24/7 blockchain activity

Third party
- Critical third-party dependencies
- Supplier risk
- Lack of ‘long-standing’ record
- Internal knowledge to monitor and manage vendors

Risks in focus for digital asset banking – financial

Credit
- Regulated borrowing limits/ requirements
- Collateral valuation
- Margin calls and timing
- ‘Flash-loan’ market

Market
- Market volatility
- 24/7 market trading
- Black swan events
- Impermanent losses

Liquidity
- Market liquidity and depth
- Lock-up periods and staking
- Exchange and DeFi protocol liquidity
- Automated liquidation procedures

Counterparty
- Unregulated market participants
- ‘Rug-pull’ projects
- DAO and DeFi organisations
- Insurance gaps

Key considerations for the compliance function

The rise of cryptocurrency payments has increased trading volumes as well as the complexity of related money laundering activities. Despite bear market conditions in the second half of 2022, the 24-hour trading volume represents approximately 82 billion US dollars as of 20 September 2022. This reflects the fact that demand for cryptocurrencies remains high, even if at lower levels compared with the peaks in 2021.

Financial institutions are due to deliver on, at a minimum, the same regulatory requirements as for fiat currencies. Anti-money laundering for cryptocurrency payment solutions requires financial services organisations and virtual asset service providers to monitor transactions and counterparties, and to detect and intervene in money laundering activity. Below are some key compliance considerations related to AML, KYC and regulatory enforcement.

Anti-Money Laundering (AML)/Combating the Financing of Terrorism (CFT)

CFT and the related risk of sanctions and penalties is arguably the **biggest legal and compliance risk** for firms operating in the crypto space.

Allowing a transaction to sanctioned counterparties can result in **penalties years into the future**, and since transactions cannot be rejected counterparty monitoring and ex-ante remediation is essential.

As the transactions are near real-time and without geographical restrictions, cybercriminals **can obscure their identity, quickly transfer funds** into various locations or **exploit regulatory discrepancies** between jurisdictions. As such, counterparty monitoring and KYC are essential compliance matters.

Know Your Customer (KYC)

Due to the **anonymity provided by blockchain technology**, the counterparty in a DLT environment is not always easily identifiable and the **availability of personal data** on the network's participants may be very limited.

Loose KYC requirements, especially on unlicensed exchanges, are increasingly being exploited by cybercriminals, who conceal their identity or **assume fake identities to commit fraud**.

Screening customers against name lists can also be a challenge, particularly since pseudonymous accounts are / have been commonly used in DeFi.

Legal and regulatory enforcement

A key legal risk that firms face is the **enforceability of laws and regulations** in digital assets, especially relating to blockchain technology and smart contracts.

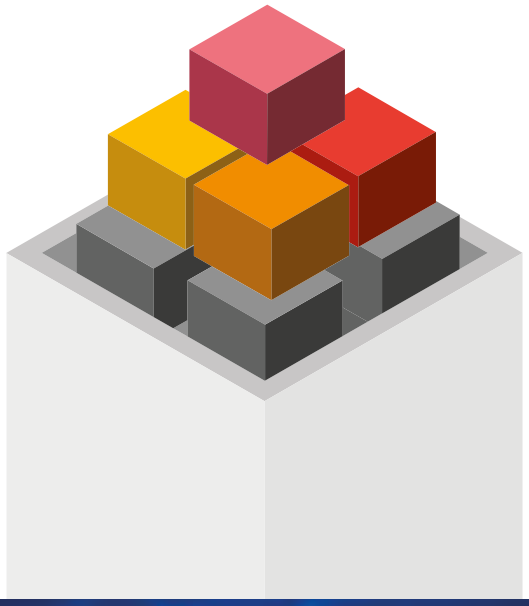
Blockchain technology generally cannot be allocated to a single jurisdiction as the **ledger does not have a physical location**, and a blockchain's nodes can be situated anywhere in the world. Any criminal activities on the blockchain are therefore harder to enforce, since it may present complex legal issues and involve many different jurisdictions.

Legal frameworks for smart contracts have **not been clearly defined** by lawmakers and regulators, which questions their enforceability and puts counterparties at risk.

Tax compliance

The OECD recently published (Oct 2022) a two-part document — the **Crypto-Asset Reporting Framework (CARF)** and Amendments to the **Common Reporting Standard (CRS)** — to establish a global tax transparency compliance framework (incl. rules for automatic reporting and exchange of taxpayer information between countries).

Adjustment of reporting, and any potential withholding, to adhere to these new rules is a **crucial compliance matter**.



Importantly, similar to the focus risks outlined in the previous section, new methods of laundering and obscuring transactions are prevalent in digital assets. This highlights once again the need to monitor the external environment, identify new patterns of criminal activity and regularly update the compliance framework. One recent example of tumbling and mixing in the digital asset space is the Tornado Cash platform, recently sanctioned by the US.

Case study: Tornado Cash

Background

Virtual currency mixer Tornado Cash has been used to launder more than **7 billion US dollars**[1] since its launch in 2019, with at least 1.5 billion US dollars being identified as proceeds from crimes.[2] Some prominent examples of laundering include:

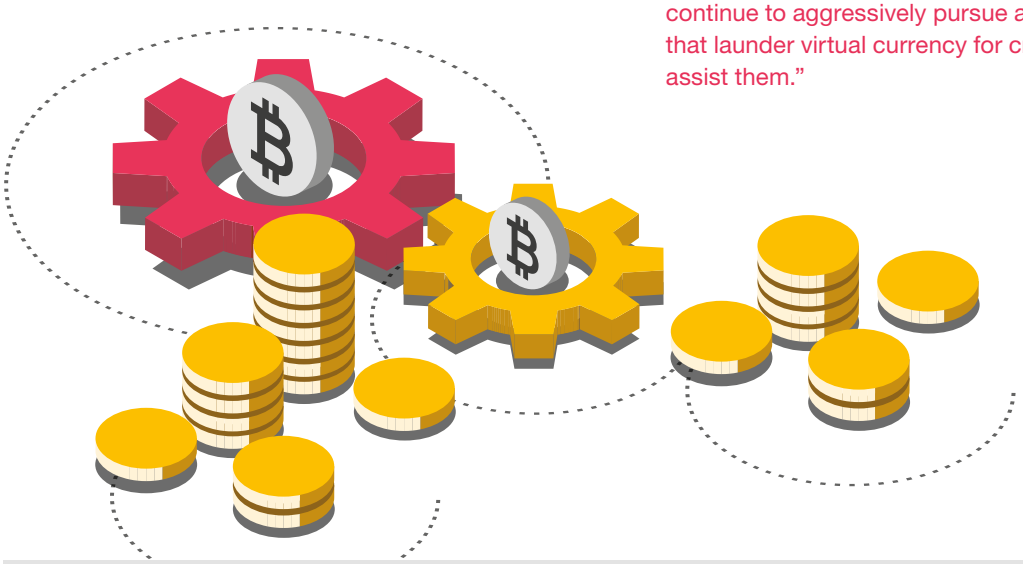
- 455 million US dollars stolen by the Lazarus Group, which is a state-sponsored hacker group from the Democratic People's Republic of Korea. It was sanctioned by the US in 2019, in the largest known virtual currency heist to date.
- 96 million US dollars that came from cyber attacks in June 2022: the Harmony Horizon bridge heist.
- 7.8 million US dollars in the Nomad heist in August 2022.

Overview

The US Treasury has worked to expose components of the virtual currency ecosystem, like Tornado Cash and Blender.io, that cybercriminals use to obfuscate the proceeds from illicit cyber activity and other crimes. While most virtual currency activity is licit, it can be used for illicit activity, including sanctions evasion through mixers, peer-to-peer exchangers, darknet markets, and exchanges. This includes the facilitation of heists, ransomware schemes, fraud and other cybercrimes.

Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson:

"Today, Treasury is sanctioning Tornado Cash, a virtual currency mixer that launders the proceeds of cybercrimes, including those committed against victims in the United States. Despite public assurances otherwise, Tornado Cash has repeatedly failed to impose effective controls designed to stop it from laundering funds for malicious cyber actors on a regular basis and without basic measures to address its risks. Treasury will continue to aggressively pursue actions against mixers that launder virtual currency for criminals and those who assist them."



Consequences

All property and interests in property of Tornado Cash, in the United States or in the possession or control of US persons, were blocked and had to be reported to the Office of Foreign Assets Control (OFAC). Additionally, any entities that are owned 50% or more, directly or indirectly, by blocked persons were also blocked. All transactions by US persons or even persons in transit within the United States, involving any property or interests in property of designated or otherwise blocked persons are prohibited, unless authorised by a general or specific licence issued by OFAC, or exempt.

[1] US Treasury Department

[2] Eliptic Blockchain Analysis (https://hub.elliptic.co/analysis/tornado-cash-mixer-sanctioned-after-laundering-over-1-5-billion/)

How can PwC help

Digital asset transformation is a global priority for PwC. Our purpose, to build trust in society and solve important problems, motivates us to contribute to the development of a robust and well-managed digital asset ecosystem with risk management and compliance built in from day one.

We have a broad range of experience, having supported layer one technology providers and early digital asset banking clients, as well as stablecoin issuers and DeFi platforms.

We can help define or provide assurance on your risk and compliance strategy, focusing on what is relevant for your product and service offering, and working with you to remediate any gaps identified. Given our credentials, we are uniquely positioned to provide market insight and help you continue to monitor and assess emerging risks and challenges on your journey.

For more details on our service offering and the benefits of becoming a 'crypto bank', please see our prior publication.

Contacts

Patrick Akiki
Financial Services Markets Leader,
PwC Switzerland

+41 79 708 11 07
akiki.patrick@pwc.ch

Jean-Claude Spillman
Partner & Head Asset & Wealth Management and Banking Regulatory,
PwC Switzerland

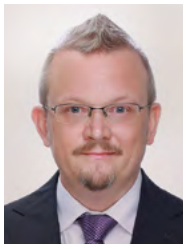
+41 58 792 43 94
jean-claude.spillmann@pwc.ch

Mark Hussey
Director, Blockchain, DLT and Token Business Advisory Lead,
PwC Switzerland

+41 79 549 07 59
mark.hussey@pwc.ch

Dario Orteca
Director, Business, Blockchain and Digital Asset Transformations,
PwC Switzerland

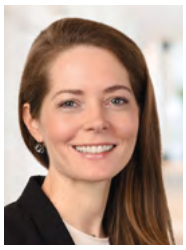
+41 79 238 62 78
dario.orteca@pwc.ch



Sebastian Ahrens
Director, Blockchain, Financial Crime Compliance Lead,
PwC Switzerland

+41 79 267 86 44
sebastian.ahrens@pwc.ch

With thanks to:



Beate Fessler
Senior Manager,
Financial Services Consulting,
PwC Switzerland

+41 79 783 59 10
beate.fessler@pwc.ch

Michel Moench
Manager, Financial Services Consulting,
PwC Switzerland

+41 78 822 45 87
michel.moench@pwc.ch

PwC, Birchstrasse 160, 8050 Zurich, +41 58 792 44 00