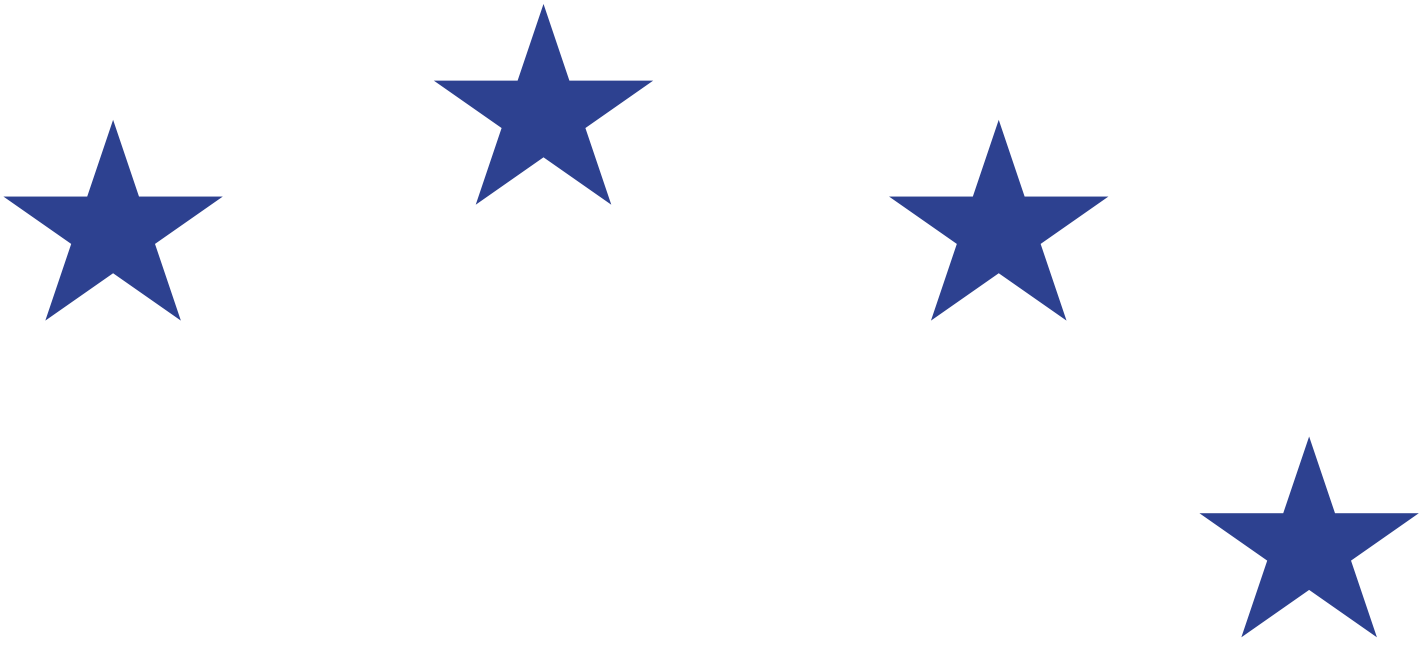
esma European Securities and Markets Authority

TRV Risk Analysis

Crypto-assets and their risks for financial stability



ESMA50-165-2251
Publication date: 4 October 2022

Luxembourg: Publications Office of the European Union, 2022

ISBN 978-92-95202-63-4, doi:10.2856/548378, ISSN 2599-8749, EK-09-22-431-EN-N

European Securities and Markets Authority
(ESMA)
Risk Analysis and Economics Department
201-203 rue de Bercy
75012 Paris
FRANCE
risk.analysis@esma.europa.eu

Financial stability

Crypto-assets and their risks for financial stability

Contact: claudia.guagliano@esma.europa.eu; steffen.kern@esma.europa.eu ([1])

Summary

Crypto-assets have gained increasing attention due to their rapid growth and so has the interest around their implications for the traditional financial system – including financial stability. ESMA has been following these developments closely for several years, including because of their risks to consumer protection ([2]), and outlines in this article the latest understanding of crypto-assets' risks and transmission channels to financial markets. While some sources of risk are well understood from traditional markets, others are novel and linked to the product design, technological development, or the complex infrastructures built around crypto-assets. We find that, at present, crypto-assets are still small in size and their interlinkages to traditional markets are limited. In future, this situation may change as market growth can occur suddenly and risk transmission is possible through various channels. Continuous monitoring of the crypto-asset market and its interconnectedness with the wider financial system is required to assess newly emerging threats in a timely manner, while regulations such as the EU proposal "Markets in Crypto-Assets" (MiCA) should be implemented swiftly to mitigate already identified risks.

Introduction

Since the publication of Bitcoin's (BTC) whitepaper in 2008 ([3]), the crypto-asset market has grown into a vast and inherently global system of over 20,000 coins ([4]), with features that increasingly resemble traditional financial markets and infrastructures.

After a sustained period of growing awareness and adoption of crypto-assets, deteriorating macroeconomic conditions have darkened the market outlook in recent months. Rising inflation and the end of the low interest rate era have undermined previously bullish investor sentiment, causing a dramatic sell-off in the crypto-asset market ([5]). By July 2022 the market had collapsed by over 60% in just half a year – showing its cyclicality and high volatility.

Despite the sell-off, the continued popularity of crypto-assets – not least among retail investors, their size, constantly evolving features, and growing interlinkages with the financial system are a source of concern for regulators globally.

This article:

a) identifies risks in the market for crypto-assets (which could serve as sources of financial instability); and
b) analyses the interlinkages with traditional markets (i.e. transmission channels that could create contagion risks).

It starts with: (i) an overview of recent market developments; continues with (ii) the analysis of specific sources of risk; along with (iii) potential transmission channels to traditional financial markets; (iv) sketches our approach to monitoring risks in the market; and (v) provides a brief overview of regulatory responses; followed by (vi) concluding remarks.

To assess crypto-asset related financial stability risks presented in this article, we draw inspiration from the criteria developed by the Financial Stability Board (FSB). The most relevant criteria include:

(i) size (i.e. crypto market size relative to the traditional market); and

([1]) This article was co-authored with Anne Choné, William Marshall and Paul Reiche.
([2]) The European Supervisory Authorities issued a warning to re-alert consumers to the high risks of many crypto-assets in March 2022.
([3]) Nakamoto, S. (2008), 'Bitcoin: A peer-to-peer electronic cash system'.
([4]) According to CoinMarketCap, as of July 2022.
([5]) Butterfill, J., 'There is more pain to come in the crypto markets', CoinShares, 6 July 2022; Ryder, C. and Aubert, D., 'How crypto might insulate from scary macro', Kaiko, 21 July 2022.

(ii) interconnectedness (i.e. the direct and indirect interlinkages between the various components of the crypto and traditional financial system).

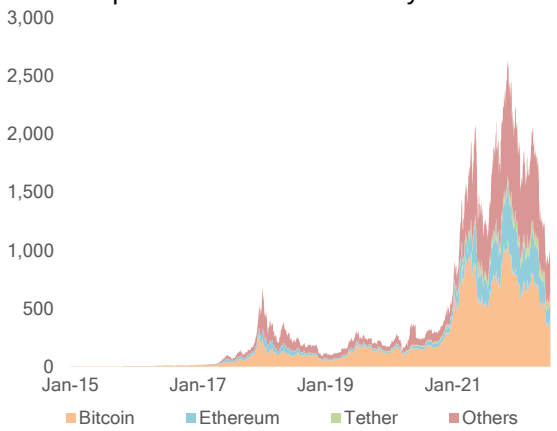
A third FSB criterion, substitutability (i.e. the ability to replace critical functions or infrastructures), will at this point not be central to our analysis given that crypto markets are still in a nascent state and do not form part of critical functions for the financial system as a whole. Substitutability issues are, nevertheless, likely to develop as these markets grow and may deserve dedicated attention in future (International Monetary Fund, Bank for International Settlements (BIS) and FSB, 2009) ([6]).

We also draw on the FSB for the **definition** of crypto-assets, namely "a type of private sector digital asset that depends primarily on cryptography and distributed ledger or similar technology" (FSB, 2022). This broad definition encompasses a wide variety of crypto-assets, ranging from "native tokens" (e.g. Bitcoin or Ether) and so-called "stablecoins" (e.g. Tether or USD-Coin) to "security tokens" and "non-fungible tokens" (NFTs) – all of them with different features and thus different implications for the traditional financial system, including its stability. We will focus on native tokens and so-called stablecoins that do not qualify as MiFID financial instruments or e-money, since they currently represent the largest part of the market by far.

A fast-moving and volatile market

When considering the entire scope of the development of crypto-assets in the last decade, it is clear that the strongest growth – both in terms of valuations and the number of coins in circulation – has occurred during the last 5 years. In the latest cycle from 2020 through to 1Q22, **crypto-asset prices soared** – driven by a high degree of speculation and the fear-of-missing-out among "cash-rich" consumers. Crypto-assets reached a combined valuation of around EUR 2.5 tn ([7]) in November 2021, marking a new all-time high, equivalent to five times the previous high in 2018. However, the market has since suffered a downturn, intensified by high-profile collapses of a large so-called stablecoin and lending platforms, dragging total market cap down to EUR 1 tn as of July 2022 (Chart 1). Even at its peak, crypto capitalisation remained at only 1 % of the combined capitalisation of global equity and bond markets (Kolchin, Podziemska and Hadley, 2022), underlining the so far limited relevance for financial stability at large.

Chart 1
Crypto-asset market capitalisation
Market capitalisations are extremely volatile



Note: Market capitalisation of Bitcoin, Ethereum, Tether and other crypto-assets, in EUR bn.
Sources: CoinMarketCap, ESMA.

Within the crypto-asset market, **so-called stablecoins** have recently established themselves as a distinct class, with a combined valuation growing from approximately EUR 5 bn in 2020 to EUR 152 bn in July 2022 (+ 3,000 %) – five times as fast as the overall crypto-asset market growth (+ 600 %). So-called stablecoins have gained popularity due to their promise to overcome crypto-assets' historically extreme volatilities by pegging their prices to an underlying value, such as the US dollar (USD) or a basket of crypto-assets, allegedly making them comparatively better suited to store value digitally without converting to fiat. This has enabled so-called stablecoins to evolve into a much-discussed component of the crypto-asset market, while also creating new linkages to the mainstream financial system (e.g. through directly holding traditional securities) ([8]).

Alongside the surge of capitalisations and issuance of new types of tokens, there has been a corresponding **increase in trading volumes**, bolstered by the emergence of specialised crypto-asset trading platforms with sizes and

([6]) The substitutability criterion might become relevant as soon as structures of the crypto-asset system reach systemic scale. For example, if a so-called stablecoin leads to the crowding out of an official currency in a certain jurisdiction, it might become difficult to revert to the official system should the so-called stablecoin fail.

([7]) Please note that crypto-assets remain largely unregulated at this point, meaning that available figures need to be considered with caution in the absence of comprehensive and reliable data.

([8]) We will further analyse so-called stablecoins in the "Risk transmission channels" section of this article.

volumes that now rival some of the smaller established markets. For comparison, the New York Stock Exchange and Binance (the largest trading platforms in the stock market and the crypto-asset market by volume) recorded total annual spot trading volumes of EUR 35 tn and EUR 8 tn respectively, until July 2022. But the key difference is that most trading platforms found in crypto markets operate outside of any regulatory oversight.

A noticeable development is the growth of **decentralised finance** (DeFi), commonly defined as "the provision of financial products, services, arrangements and activities that use distributed ledger technology to disintermediate and decentralize legacy ecosystems by eliminating the need for some traditional financial intermediaries and centralized institutions" ([9]). DeFi effectively purports to allow individuals and businesses to conduct financial transactions without intermediaries by leveraging on Distributed Ledger technologies (DLT). DeFi most developed applications as of today are decentralised exchanges (DEXs) and decentralised lending platforms. A key metric to evaluate the size of DeFi is total-value-locked (TVL), reflecting the capital committed to those protocols. As of July 2022, TVL is at around EUR 60 bn, equivalent to 7.5 % of the overall crypto-asset market ([10]).

Furthermore, we have observed an increasing usage of **crypto-asset derivatives**. Listed futures and options on crypto-assets are available on regulated exchanges such as the Chicago Mercantile Exchange (CME) or the Intercontinental Exchange (ICE), but most volumes of derivatives are transacted on unregulated crypto-asset trading platforms.

Market intelligence also points to a growing adoption by **institutional investors**, although reliable data are scarce and mostly survey based.

Structural risks in crypto-asset markets

In this section, we identify risks found in crypto markets, including the use of crypto-assets in financial applications and their associated infrastructures. We classify these risks into:

(i) traditional financial risks, which are similar to those found in established financial markets, although they may take somewhat different forms or be exacerbated in crypto-asset markets; and
(ii) those risks that are native to crypto-assets (i.e. arising from the unique properties of distributed ledgers and the application layer built on top of them).

Traditional financial risks

Many crypto-assets have no tangible value – contrary to traditional securities, such as stocks or bonds, which give holders rights to future cash flows or claims on firm assets in case of liquidation. As a result, most crypto-assets are **highly speculative**, meaning that their value depends exclusively on supply and demand dynamics. Speculative markets tend to be volatile (predominantly driven by news and technical indicators rather than fundamentals), susceptible to manipulation or fraud and often facilitate the emergence of bubbles that can eventually burst, causing a large redistribution of wealth.

Compounding the speculation in crypto-asset markets are **aggressive marketing** campaigns aimed at the public, including less sophisticated retail investors – in some cases advertising annual returns as high as 20 % (Shen, 2022). Crypto firms have also promoted increasingly **complex products**, often without adequately disclosing the risks and with little accountability for making misleading statements ([11]). The March 2022 joint ESA warning not only alerted consumers to the speculative nature of many crypto-assets but also the risks of misleading advertisements, including via social media and influencers ([12]).

Another factor behind the speculation is **leverage**, which is accessible to retail investors through margin accounts on crypto-asset exchanges, traditional derivatives (especially futures, options or contracts-for-difference) and through special crypto-asset derivatives (i.e. perpetual contracts known as "leveraged tokens") ([13]). Most major **crypto-asset exchanges** allow investors to make inordinately large investments compared to their capital base (up to 125 ×) and therefore take on risk in excess of their capacity to remain solvent (Table 1).

([9]) IOSCO, 'Decentralised Finance report, public report', March 2022.
([10]) See Defi Llama.
([11]) In the EU, Spain has dedicated new powers to regulators to address crypto promotions. See Dombey, D., Oliver, J. and Fleming, S., 'Spain leads European crackdown on crypto promotions', Financial Times, 17 January 2022.
([12]) The European Supervisory Authorities issued a warning to consumers on the risks of crypto-assets in March 2022.
([13]) See FTX's 'Leveraged token walkthrough'.

Many of the same exchanges offer leveraged tokens, which they claim provide the same potential for outsized returns with lower risk of liquidation than traditional leverage.

Table 1

Margin multiples offered on major crypto exchanges

Crypto exchanges offer leverage up to 125 ×

Exchange	Max. multiple (spot)	Max. multiple (deriv.)
Binance	20 ×	20 ×
FTX	20 ×	20 ×
Kraken	5 ×	5 ×
Bitmex	N/A	100 ×
Bybit	N/A	100 ×
Huobi Global	5 ×	125 ×
KuCoin	10 ×	100 ×

Source: Data as of July 2022 from CoinSutra.

Many of the same elements are reflected "on-chain" in the context of DeFi (i.e. with transactions recorded on the blockchain and settled in real time). Although over-collateralised lending (typically 110 %–150 % of debt value) is the norm throughout most of DeFi, **on-chain leverage** is accessible through a variety of methods with few (if any) gatekeepers. For instance, certain protocols offer the same derivatives and options products found on off-chain centralised exchanges. Other innovations have emerged, such as "leveraged yield farming" which allows users to supplement their deposited liquidity in a DeFi protocol with liquidity borrowed at lower collateral ratios from other protocols ([14]).

Risks native to crypto-assets

The **pseudonymity** that prevails in crypto-asset markets makes it virtually impossible to assess the creditworthiness or aggregate exposures of participants. Pseudonymity refers to the string of letters and numbers that constitute the "public keys" of self-custody wallets that often do not require any know-your-customer procedures to be created. Similarly, concentrations of asset holdings are difficult to identify because the same individual or entity may own several pseudonymous wallets (making their total balance impossible to trace). Estimates suggest there is a significant inequality in the distributions of certain assets (i.e. 2 % of wallets possess 94 % of all Bitcoins) ([15]), which has implications in terms of liquidity but also market integrity (i.e. in the case of large orders distorting price formation). More broadly, the current **lack of transparency and reliable data** to assess exposures and risks is a source of concern for consumer protection, market order and financial stability alike ([16]).

A second source of native risks is inherent to the use of **Distributed Ledger Technologies** (DLTs) on which crypto-assets are based. Attempts to manipulate the **consensus mechanisms** of distributed ledgers (i.e. through so-called "51 %" or "Sybil" attacks) can put the value on the entire blockchain at risk. If an attacker were to gain control of a majority (or a quorum) of network nodes (or hash power), he could deliberately change the ordering of transactions and enable a double spend ([17]). Since 2012, there have been 33 known attempts to attack consensus (both successful and unsuccessful), according to Makarov and Schoar (2022). In many cases, if the underlying consensus is compromised, stakeholders of the blockchain may vote to "hard fork" ([18]) the chain, which would allow them to salvage some value (depending on the acquiescence of the remaining nodes in consensus).

For a sense of the scale of value at risk to blockchain consensus attacks, as of July 2022, there was EUR 57 bn staked on the nodes of the 10 largest smart contract-enabled DLTs (Chart 2). In some cases, the percentage of total circulating token supply staked in consensus is as high as 80 % (as of July 2022). This figure does not include all of the total value in other assets that are also transacted on the blockchain (i.e. the ERC-20 tokens on Ethereum).

([14]) Verso Finance, 'Understanding leveraged yield farming', 5 November 2021.

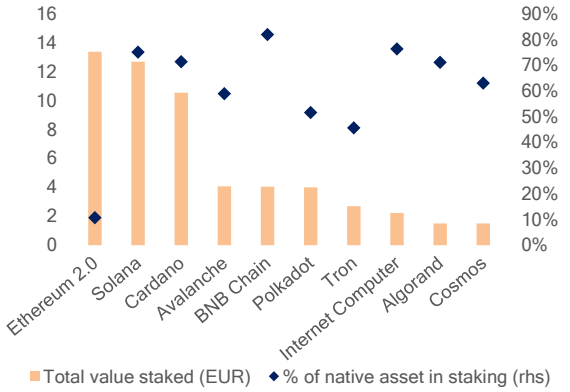
([15]) For a pure distribution of Bitcoin balances across wallets see: BitInfoCharts; Glassnode argues that this percentage is naturally skewed by cases of wrapped BTCs, custodian wallets or exchanges, and estimates it at around 70 % (Schultze-Kraft, 2021).

([16]) The markets in crypto-asset regulation (MiCA) introduces data reporting requirements intended to remedy this.

([17]) Double spending refers to the creation of new value where it did not exist before. An example would be when a single digital token (i.e. one BTC) is spent simultaneously more than once (and validated by the consensus mechanism).

([18]) Hard fork refers to a failure of nodes to reach consensus, which forces the creation of a new chain of transaction history (incompatible with the original blockchain).

Chart 2
Value staked on nodes of major blockchains
EUR 57 bn staked on top 10 blockchains



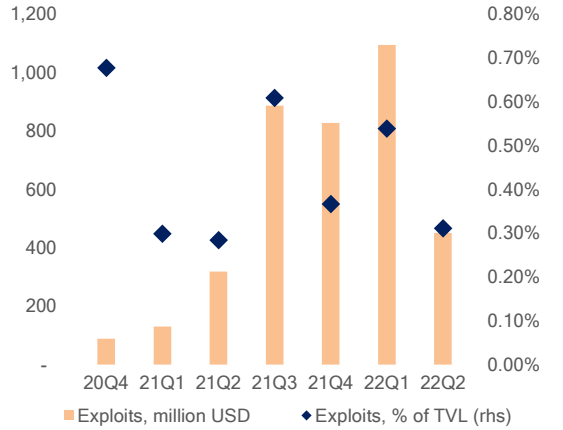
Note: Total value staked in consensus nodes on the 10 largest blockchains and the amount of native assets staked as a % of circulating supply (in EUR bn as of July 2022).
Sources: Staking Rewards; ESMA.

Adding to consensus-based risks is basic **network congestion**, which has halted services on several major blockchains in recent months ([19]). Though most blockchains use variable transaction fees to keep demand at sustainable levels, surges in traffic can cause consensus nodes to fall out of sync ([20]), leading to outages that may be devastating for investors' confidence in the blockchain. Sometimes, outages are deliberately caused by a malicious node within the network or by an external actor via a distributed denial-of-service (DDoS) attack ([21]).

DeFi shows similar types of **operational vulnerabilities**. These manifest themselves through a variety of so-called **"DeFi exploits"** – which refers to the range of code or governance-based attacks used to capture ill-gotten gains. In 2022 so far, EUR 1.4 bn have been lost to DeFi exploits (Chart 3). Most of the major exploited protocols (65 %) did not conduct a third-party audit of their code.

Governance attacks (in which an entity controls 51 % of governance tokens) are a source of vulnerability specific to DeFi. Unlike a Sybil attack, which targets the underlying blockchain consensus, governance attacks involve the accumulation of governance tokens that may enable attackers to manipulate **voting on DeFi protocol design parameters**. By doing so, they may allow certain transactions to steal liquidity from deposits in the protocol.

Chart 3
Value of losses to DeFi exploits
Losses of EUR 1.4 bn in 1H22



Note: Monthly losses from on-chain exploits (in million USD) and relative to the size of the overall DeFi ecosystem (% of TVL). Figures are notional at the time of the exploit.
Sources: Rekt, DeFiLlama, ESMA.

Another important feature unique to DeFi is **composability**, in which smart contracts native to different open-source protocols can interact with each other – similarly to APIs in the web-based economy (Xie, 2021). Composability enables **rehypothecation**, in which assets "staked" (i.e. deposited) on one protocol can be pledged as collateral (or liquidity) in another protocol (Hermans et al., 2022). Because this process involves no intermediaries who can monitor those collateral dependencies, the default of one actor can quickly propagate throughout the system.

Composability is also a fundamental requirement for one common attack vector in DeFi: the "**flash loan**". Flash loans are special transactions that allow users to borrow an asset without providing any upfront collateral (as long as the borrowed amount and a fee are returned before the end of the transaction) ([22]). Most of the large lending protocols and decentralised exchanges offer flash loans. The term "flash" denotes the speed with which they are executed: often within seconds based on pre-coded parameters. The appeal of flash loans for DeFi arbitrageurs is in the risk-free lending they offer: the loan is only valid within a single transaction (or block), which reverts to the pre-transaction state with no loss to

([19]) Somraaj, S., 'Solana plummets double-digits amid another network halt', Decrypt, 2 June 2022.
([20]) When consensus nodes fall out of sync: it increases centralisation among the remaining nodes, rendering the chain less Sybil resistant; and the remaining nodes may not be able to reach a quorum, which is necessary to approve new transaction blocks (a "kill switch" some blockchains have built in by design).
([21]) Certik, 'What is a DDoS attack? How can it affect crypto?', 8 February 2022.
([22]) Flash loans are attractive to some traders because they enable them to pre-code complex arbitrage trades and execute them quickly before prices equalise – all without the risk of losing their initial capital.

the borrower (or lender) if they are unable to repay the loan within the same block. This is only possible on a blockchain because of **atomicity**: actions can be executed collectively in sequence or fail collectively (Qin et al., 2021).

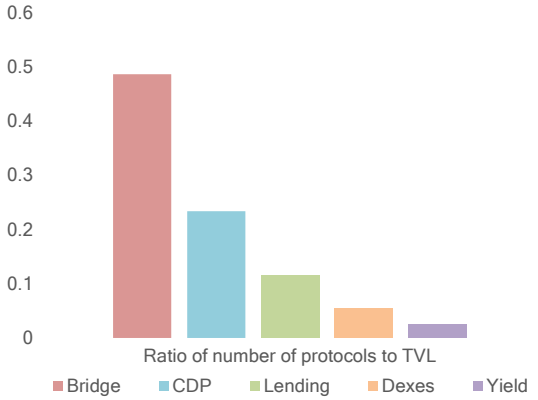
Market participants may use flash loans to exploit the liquidity pools of DeFi protocols (called "flash-loan attacks") in two ways. The first method is an **artificial arbitrage** or a "pump attack" that capitalises on market inefficiencies (low liquidity) and fragmentation. Without instant synchronisation of prices between DEXs or across blockchains, the same asset can be traded at marginally better prices in different venues. However, in a pump attack, the objective is to manipulate the relative price of two assets in a DEX liquidity pool to maximise this mismatch between liquidity pools before prices synchronise. The second method involves the **manipulation of "oracles"**, which are an on-chain source for verified price data (often, an oracle is simply a price feed determined by pair liquidity held in a DEX and broadcasted to the rest of the blockchain) ([23]).

The victims in both instances are the liquidity providers on the DEX, i.e. depositors who place a pair of crypto-assets in a "liquidity pool" which is then used to facilitate trading between the pair ([24]). These liquidity providers realise losses on their positions because they may be forced to buy an asset at a massive premium (or sell at a massive discount) due to unnatural price slippage incurred by the flash loan. Value stolen in flash loan attacks in 1H22 is estimated at EUR 300 m, or 1 % of the total year-to-date volume of EUR 26 bn. Flash loan attacks also account for 22 % of all year-to-date exploit value ([25]), though the majority of flash loans are understood to be used in legitimate arbitrage.

The current crypto market is characterised by extreme fragmentation between blockchains (in terms of liquidity and operability). But efforts to solve **interoperability** issues have introduced new points of failure and sources of abuse in the nascent network of public blockchains. **Bridge protocols** that serve as conduits for the transfer of funds between otherwise incompatible blockchain-specific assets are especially prone to exploits (Boissay et al., 2022). Bridges work by "burning" or "locking" the tokens destined for one chain and minting "wrapped" versions of the tokens with the same underlying value on the other chain (i.e. a token bridged onto the Ethereum blockchain is "burned" on the original chain and re-minted as an ERC-20 ([26]) token).

Due to their deep liquidity (EUR 11.2 bn held across 23 bridges – the highest average value deposited of any type of DeFi protocol (Chart 4)) and their complexity, they are prime targets for exploitation. In fact, the two largest DeFi exploits ever recorded have involved cross-chain bridges. The most high-profile attack was that against Ronin Network in March 2022, in which hackers stole EUR 582 m after gaining control of five of the nine nodes needed to control the chain consensus ([27]). The next most significant example is the February 2022 exploit of the Ethereum–Solana bridge, Wormhole, which suffered a EUR 304 m loss (in notional value of ETH at the time) ([28]).

Chart 4
Average TVL per protocol type
Bridges hold the highest average liquidity



Note: Ratio of TVL to the number of protocols in each of the top 5 protocol categories in DeFi (as of July 2022). CDP refers to collateralised debt positions (i.e. crypto-collateralised stablecoins).
Sources: DeFi Llama, ESMA.

In summary: crypto markets are susceptible to both novel and familiar risks. Novel risks originate either from the underlying design principles of the blockchain technology (i.e. pseudonymity, consensus mechanisms, interoperability issues)

([23]) Adams, H. et al. (2021), 'Uniswap v3 core', Uniswap, pp. 3–4. Other oracle providers (e.g. Chainlink) rely on decentralised network consensus to determine prices; See Chainlink, March 2021.

([24]) Certain DEX features also expose liquidity providers to what is known as an "impermanent" loss, i.e. the opportunity cost of placing crypto-assets in a liquidity pool instead of holding them. An impermanent loss is effectively the result of arbitrageurs being in a position to arbitrage the pair in the liquidity pool at their advantage, before the depositor recoups the crypto-assets. The more volatile the crypto-assets in a liquidity pool, the higher the risk of an impermanent loss.

([25]) See The Block's 'Exploits'.

([26]) ERC-20 is the nomenclature for the Ethereum token standard. Any ERC-20 token can be transacted on the Ethereum network for a gas fee paid to a miner.

([27]) Ronin Network, 'Back to building: Ronin security breach postmortem', 27 April 2022.

([28]) Extropy.IO, 'Solana's Wormhole hack post-mortem analysis', 8 February 2022.

or the fast-evolving DeFi-market (composability, governance, disintermediation). And while speculation is not a new concept, the lack of inherent value of most crypto-assets and new ways to access leverage (especially for less sophisticated investors) makes volatility more acute. Combined, these risks can render boom and bust cycles in crypto more pronounced than those of traditional markets. Given the unique vulnerabilities present in the crypto-asset market, it is prudent for supervisors to understand whether large contractions in the market could adversely affect the traditional financial system. Hence the next chapter analyses spillover risks by examining potential transmission channels and assessing the overall scale of current threats to wider financial stability.

Risk transmission channels

While crypto-asset and traditional financial markets are still considered as two largely separate systems, the transmission of shocks from one system to the other can occur as **connections between both markets** exist and are likely to grow. One prominent example is the scenario in which entities concurrently hold assets in one system and liabilities in the other, and (directly or indirectly) use the assets as collateral for the liabilities – creating a direct link between systems. As soon as those interdependencies exist, material value changes in one market may spill over into the other market, as entities might not be able to sustain a mismatch between their assets and liabilities through time.

We further distinguish below between:

(i) entities with a net-asset in the crypto system and a net-liability in the traditional system; and

(ii) entities with a net-liability in the crypto system and a net-asset in the traditional system.

Textbox 1

Derivation of “net-exposures”

To distinguish between different types of intersystem exposures we refer to the balance sheet of relevant actors (i.e. entities with exposures to both markets).

Assets	Liabilities
Crypto-asset (CA)	Crypto-liability (CL)
Financial-asset (FA)	Financial-liability (FL)

By definition, the values of assets and liabilities are greater or equal to zero ($CA \geq 0$, $CL \geq 0$, $FA \geq 0$, $FL \geq 0$) and have to balance (i.e. $CA + FA \equiv CL + FL$).

We define the **net-exposure** for the crypto-asset market and the traditional financial market as the difference between the corresponding assets and liabilities, leading us to two cases:

(i) $CA - CL > 0 \Leftrightarrow FA - FL < 0$
(ii) $CA - CL < 0 \Leftrightarrow FA - FL > 0$

We refer to case (i) as entities with a “net-asset” in the crypto-market and a corresponding “net-liability” in the traditional market, and to case (ii) as entities with a “net-liability” in the crypto-market and a “net-asset” in the traditional market.

This approach implicitly assumes that value changes of assets and liabilities in one system occur unidirectionally and in the same order of magnitude (i.e. are offsetting each other). While we are aware that this is a strong simplification, it helps to illustrate how price volatility and value changes in one system can affect the outstanding obligations in the other .

Crypto-asset investors

The first case with a **net-asset held in the crypto system** could be considered the base case, as almost every natural or legal person faces some kind of fiat-denominated obligations in the real economy, while crypto-assets are predominantly used for investments or speculative purposes. It encompasses retail and institutional investors with direct or indirect exposures (i.e. through direct holdings of crypto-assets or investment products with crypto-assets as underlying, i.e. derivatives or investment funds).

As already highlighted above, data on investors’ exposure to crypto-assets are incomplete and patchy. For **retail investors**, the European Central Bank’s November 2021 Consumer Expectation Survey indicates that as many as 10 % of European households may own crypto-assets. However, most respondents appear to invest only small amounts – below EUR 5,000 (Hermans et al., 2022). The United Kingdom’s Financial Conduct Authority’s 2021 consumer research on crypto-assets reached similar conclusions and estimated the number of British adults investing into crypto-assets at around 4 %, with a median investment of around GBP 300 (Karim and Tomova, 2021). And while the absolute number of retail investors is still small, both surveys indicate an increasing consumer interest to invest in crypto-assets.

Fidelity’s latest (2021) “Institutional Investor Digital Asset Study” finds that **institutional investors** globally are also showing greater acceptance of crypto-assets. The results suggest that 52 % of all respondents have invested into crypto, with an even higher rate (56 %) among European professionals. The survey also showed that ownership of crypto-assets was concentrated in Bitcoin and Ether and that

outside of crypto-native hedge funds and venture capital funds, adoption was led by high-net-worth investors, financial advisors, and family offices (Neureuter, 2021). While one argument for professional investors to participate in the crypto-asset market could be its potential portfolio diversification benefit, we note that crypto-assets seem to have established a relatively stable positive correlation with the stock market, in particular with technology stocks ([29]).

Both types of investors (retail or institutional) can have **direct crypto-asset exposure**, which refers to a situation where entities hold crypto-assets directly – either in self-custody or with a third-party custodial wallet provider. While pseudonymity hinders the analysis of who is directly exposed, the overall market capitalisation can be regarded as an upper bound. Comparing the size of crypto-assets to traditional assets, we find that they are still comparably small. At its peak in November 2021, the combined capitalisation of all crypto-asset reached EUR 2.4 tn before falling to a value of EUR 0.9 tn in July 2022 – significantly smaller than estimates for the capitalisation of precious metals (EUR 14 tn), equities (EUR 124 tn) and fixed income securities (EUR 127 tn) (Linciano et al., 2022; Kolchin, Podziemska and Hadley, 2022).

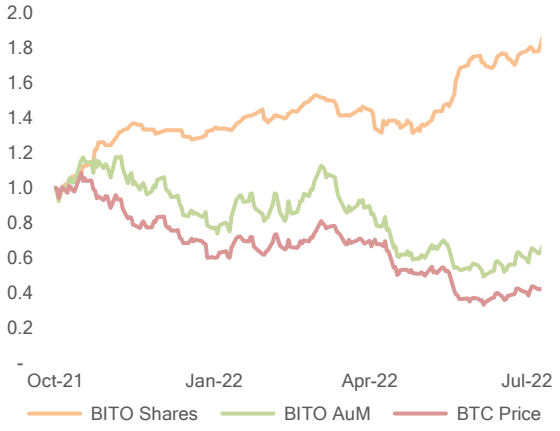
In addition to or in place of direct investments, investors might seek **indirect crypto-asset exposure**. Derivatives, funds and exchange-traded products (ETPs) can provide a way for investors to participate in crypto-asset markets without leaving their traditional habitat, as these products do not necessarily require them to build new skills or infrastructures (e.g. to execute transactions on crypto-asset trading platforms or to safekeep those assets). The use of regulated investment products, such as regulated derivatives or funds, provided by intermediaries, also helps mitigate certain risks attached to crypto-assets.

The first cornerstone of indirect exposure are **crypto-asset derivatives**. While most trading takes place on unregulated crypto-asset exchanges, the Chicago Mercantile Exchange (CME) as a regulated entity appears to have seized a market share for Bitcoin futures of around 10 % (measured by open interest), or around 4 % (measured by trading volume). According to data from "The Block", open interest of derivatives (futures and options) on Bitcoin and Ether across all major exchanges was EUR 20–25 bn in July 2022 ([30]). Compared to the European derivatives market with an outstanding notional amount of EUR 250 tn, the size of the global crypto-asset derivatives market appears, however, still small (EMIR database, trade repositories, ESMA).

The second cornerstone of indirect exposure are **crypto-asset funds and ETPs**, which to some extent rely on derivatives and funds themselves but can – depending on their regulatory status – also directly invest into crypto-assets.

A recent survey ([31]) by the European Supervisory Authorities has revealed around **90 Europe-based investment funds** that are directly exposed to physical crypto-assets, along with another 20 funds with indirect exposure (e.g. through crypto-asset derivatives or other funds). While the exact value of those funds' crypto-asset exposure could not be assessed, it can be regarded as marginal compared with a total of around 60,000 EU-domiciled investment funds (UCITS and AIFs) representing a net-asset value of EUR 18 tn (AIFMD database, national competent authorities, ESMA).

Chart 5
ProShares "BITO" Bitcoin ETF
Declining AuM but increasing number of shares



Note: ProShares BITO assets under management (AuM), shares outstanding and Bitcoin price, indexed to October 2021.
Sources: ProShares, Refinitiv, ESMA.

The financial sector has paid special attention to the **first SEC-regulated Bitcoin ETF in the United States** (ticker: BITO), which ProShares launched in October 2021 to offer investors exposure to Bitcoin futures. While BITO's assets

([29]) For an analysis of asset correlations, please refer to the "Financial innovation" section of ESMA's *Report on Trends, Risks and Vulnerabilities* (TRV) 1-22 and 2-22.

([30]) BTC futures: EUR 10 bn; ETH futures: EUR 5 bn; BTC options: EUR 5 bn; ETH options: EUR 3 bn; (The Block, July 2022).

([31]) The survey was conducted in April 2022 among national competent authorities supervising insurances, banks and financial markets in 28 European Economic Area member states.

under management reached the USD 1 bn mark within just 2 days of its launch, the ETF's value has since suffered during the overall decline of the crypto-asset market in 2022. However, as indicated by the stable number of outstanding BITO shares, investors' interest in this sort of regulated product appears to persist (Chart 5). No similar ETF exists in the EU today, but there are several ETPs that provide exposure to crypto-assets with a combined market value of around EUR 6.5 bn in July 2022 – to be compared with the total size of the European ETF sector of around EUR 1.3 tn ([32]).

In summary, there has been an increasing acceptance of crypto-assets as a new asset class. However, while the number of investments has significantly increased, its overall **size is understood to be limited up to this point** – compared to the size of the overall financial system, and even more so after the recent drop in crypto-asset valuations. Therefore, while crypto-assets can undoubtedly lead to a redistribution of wealth when they are held as an asset, we have not seen any indication so far that this has caused systematic defaults in the real economy.

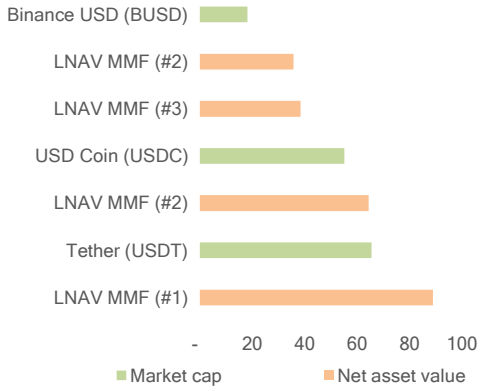
"Stablecoins"

The second case is characterised by a **net-liability held in the crypto system**. So-called reserve-backed stablecoins that are pegged to a fiat currency represent the most relevant example.

To date, the third and fourth largest crypto-assets by market capitalisation – Tether (USD 65 bn) and USD-Coin (USD 55 bn) – are **reserve-backed stablecoins** pegged to the US-Dollar. Their business model shares similarities with that of deposit taking banks or e-money institutions, to the extent that for every dollar collected, a token is being issued, with the general expectation on the part of investors that they will be able to redeem at par.

To meet redemption demand and support confidence in the peg, stablecoin issuers typically maintain a reserve of low-risk assets (e.g. fiat currencies and money market instruments), and can thus further be **compared to money market funds** (Gorton and Zhang, 2022). In fact, Tether and USD-Coin claim to have reserve assets that rival some of the largest money market funds.

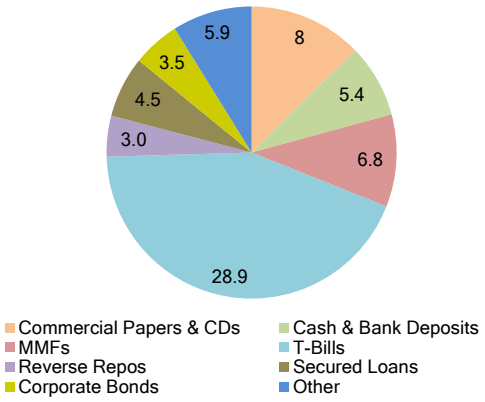
Chart 6
AuM of "stablecoins" and EU Money Market Funds
"Stablecoin" size comparable to large MMFs



Note: Comparison of largest stablecoins and Europe-domiciled prime MMFs (LVNAV) (in EUR bn) as of July 2022.
Sources: Fitch Ratings, CoinMarketCap, ESMA.

However, in the **absence of mandatory disclosures** on their reserve assets, doubts have been cast onto the existence of stated reserves – especially for the largest stablecoin Tether, essentially accusing it of fraud (Faux, 2021). Tether and Circle (the issuer of USD-Coin) have since started to voluntarily disclose the size and composition of reserves, revealing massive exposures to US-treasuries, commercial papers, and money market funds (Chart 7).

Chart 7
"Stablecoin" reserve composition
Tether with high exposure to US treasury bills



Note: Breakdown of Tether reserves (in USD bn) as of 30 June 2022.
Sources: Tether, ESMA.

Transmission of market stress between crypto-asset and conventional markets could occur in the **scenario of a run** on a large so-called stablecoin, forcing the issuer to liquidate reserves in the traditional market, which depending on the volume could cause serious strain on market liquidity and prices ("fire sales"). Given a daily

([32]) European Central Bank, 'Statistical release – Euro area investment fund statistics: First quarter of 2022', 23 May 2022.

trading volume of US-treasuries of around USD 150 bn and Tether's treasury-bill holdings of about USD 39 bn, those risks appear manageable at this moment. However, liquidations could cause ripples in less liquid markets, such as for commercial papers or certificates of deposit (Harris, 2022).

The run and subsequent collapse of the once third-largest so-called stablecoin Terra (TerraUSD) – with a peak market capitalisation of around EUR 16 bn – in May 2022 has shown that **fear can quickly spread within the crypto-asset market**. While Terra itself was an algorithmic stablecoin without a one-to-one fiat reserve backing, its collapse quickly affected Tether and several smaller stablecoins, causing them to temporary de-peg – while Bitcoin and Ether saw their prices plummet by more than 30 % within a week. The overall turmoil remained limited to crypto-assets. But it showed the strong links within the crypto-asset system.

Other channels

Based on the Terra collapse, another transmission channel becomes apparent, namely if a certain investor behaviour begins to occur in both crypto and traditional markets at the same time. Such spillovers are referred to as **confidence effects** – meaning a situation where with or without direct intersystem exposures, turbulences in one system would reflect in the other by undermining investors' confidence in both markets. Confidence effects usually result from and amplify existing wealth effects.

Infrastructures might represent another channel of contagion. First, largely unregulated crypto-asset service providers (CASPs) suffer from a range of market integrity issues (from front running of retail orders to wash trading and other forms of market manipulation), and from erratic operational risks (such as outages or exploits). Although those deficiencies do not directly affect the stability of traditional markets, they can cause or amplify the wealth redistribution within the crypto-asset system. Second, regulated infrastructures are increasingly offering crypto-asset related products and services, such as trading and clearing of crypto-asset derivatives or other investment products, meaning that those infrastructures are at least temporarily exposed to value changes of crypto-assets and the associated counterparty risks.

Another transmission channel mentioned in the existing literature is the use of **crypto-assets in payment and settlement** (FSB, 2022). Although itself a combination of possible wealth and confidence effects, this transmission channel represents the risk of a potential wide-spread adoption of unregulated assets and related risks, for the purpose of transactions. In fact, so-called stablecoins purposely aim to bridge the gap between volatile crypto-assets and traditional fiat currencies, thereby making them usable as stores of value and means of payment. Several corporate initiatives – such as the now defunct Diem project ([33]), which was originally initiated by Meta, or Mastercard's commitment to support some crypto-assets on its network ([34]) – suggest that crypto-asset based payments could indeed gain further traction.

It is worthwhile considering that today's payment service providers and big tech companies have a great impact on consumer behaviour. Therefore, under a scenario where one of those companies would actively promote crypto-asset payments, further **adoption could occur rapidly**. An example has already been provided by Tesla, which by first accepting payments in Bitcoin before withdrawing this decision only a few months later has caused several immediate price reactions (Roberts, 2021). Therefore, imagining a scenario in which a large retailer would enable crypto-assets as a payment option, or a leading tech company would introduce crypto-asset based peer-to-peer payments, consumer exposure could soar in a short period of time, strengthening the link between both systems.

We conclude that multiple transmission channels between the crypto market and the traditional financial system exist. However, their **scale remains limited at this time**. Risk transmission hinges largely on the interlinkages between both systems (i.e. the degree of crypto adoption). Given the extraordinary pace of developments in the crypto-asset market, along with the potential of some influential players to further accelerate adoption, continuous monitoring should be warranted to identify critical exposures should they emerge.

([33]) See Diem project.
([34]) Dhamodharan, R., 'Why Mastercard is bringing crypto onto its network', Mastercard News, 10 February 2021.

Crypto risk monitoring

To summarise our assessment of crypto-assets' sources of risk and potential transmission channels to the traditional financial system, we apply ESMA's established risk monitoring framework to the crypto-asset market. The framework assesses risks across five dimensions (liquidity, market, credit, contagion and operational) and splits contagion risk into "internal contagion" (within the crypto-asset market) and "external contagion" (from the crypto-asset market to the traditional financial system). The risk assessment was conducted across four major components of the crypto-asset system:

(i) Unbacked crypto-assets;

(ii) Backed crypto-assets ("stablecoins");

(iii) Crypto-asset service providers (CASPs);

(iv) Decentralised finance (DeFi);

and aggregated to an overall level. The complete framework, with further explanations can be found in the appendix to this article.

Table 2

ESMA framework for crypto-asset risks

Medium-high risk with slightly negative outlook

	Level	Outlook
Liquidity	○	→
Market	○	→
Credit	○	↗
Contagion (internal)	○	→
Contagion (external)	○	↑
Operational	○	↗

Liquidity risk refers to blockchain congestion and the absence of minimum standards for liquidity provision at centralised exchanges or DEXs. It can also arise when confidence effects trigger runs on so-called stablecoins. As such, we assign a medium–high risk level. But since we have no reason to believe the current liquidity issues will either deteriorate or improve in the near-term, we maintain a stable outlook.

For **market risk**, we consider the value and liquidity concentration in a few crypto-assets along with the frequent and opaque use of leverage as the main vulnerabilities. And although the recent sell-off and de-leveraging in crypto markets may have slightly alleviated these concerns, we continue to see high risks with a stable outlook in the near-term.

Credit risk originates from the default condition of pseudonymity in the blockchain technology, preventing the adequate assessment of counterparty risk. Defaults of intermediaries such as stablecoin issuers or CASPs can have large-scale effects and new products and services (e.g. CeFi lending) continue to increase credit exposures. Therefore, we perceive a medium–high risk with a negative risk outlook.

Internal contagion risk appeared in the aftermath of the collapse of Terra/Luna and the bankruptcies of several large CeFi platforms (beginning with Celsius), which coincided with an overall market drawdown of around 50 %. Furthermore, the prominence of certain crypto-assets and intermediaries, along with the high degree of interconnectedness within the crypto-asset system, leads us to a stable outlook from a high risk level.

So far, markets have not yet seen serious signs of **external contagion risk**, which may for now be considered as "low". The outlook remains, however, uncertain as multiple transmission channels exist and crypto markets will continue to evolve quickly thereby testing regulators' ability to contain newly emerging risks. Hence, external contagion risks could increase rapidly on the back of wider crypto adoption.

Operational risk is marked as high due to the numerous vulnerabilities that are inherent to the blockchain technology and DeFi (i.e. consensus mechanisms, interoperability issues, and open-source nature). Further, CASPs and issuers, including issuers of "stablecoins", today are not obligated to adhere to standards for operational resilience. And while upcoming legislation in the EU, such as the European Digital Finance Package ([35]), will help to address certain concerns, DeFi's increasing complexity and rising adoption rates could exacerbate existing risks, leading us to a negative risk outlook.

([35]) The European Digital Finance Package comprises legislative proposals for MiCA and the digital operational resilience of financial services (Digital Operational Resilience Act – DORA).

Shaping a global regulatory response

Crypto-assets are **a global market** without national or regional borders, and most market participants do not even disclose their domicile. In most jurisdictions, crypto-assets do not fall within the existing regulatory perimeter, and no dedicated regulatory provisions are in force yet.

The EU is the first major jurisdiction worldwide to provide a comprehensive, dedicated regulatory framework for crypto-assets, the **EU Markets in Crypto-Asset Regulation (MiCA).** MiCA is set to regulate crypto-assets, including so-called stablecoins that do not already fall under existing EU rules, by setting regulatory requirements for the public offer and marketing of crypto-assets and the provision of services related to them. In addition, MiCA includes provisions to **prevent market abuse** involving crypto-assets. More specifically, with regard to stablecoins and with a view to mitigate risks to investors and financial stability, MiCA provides that issuers of stablecoins will need to be authorised (either as a credit institution or an e-money institution for e-money tokens, or under MiCA for asset-referenced tokens) and have in place a robust and segregated reserve of assets to support the peg, and in the case of e-money tokens enable holders to redeem at par. For issuers of significant so-called stablecoins, supplemental requirements and EU-level (instead of national) supervision apply. The final text of MiCA is expected to be published in the Official Journal in spring 2023 and will enter into application between 12 and 18 months thereafter.

Yet, while MiCA is intended to create a comprehensive regulatory framework for crypto-assets, **continuous monitoring** will remain necessary. As the system continues to evolve quickly, with novel business models and emerging risks, further regulatory actions may be required through time. A wider crypto adoption among European citizens and institutions may also expand intersystem exposures.

Pending EU rules, two **jurisdictions within the EU** (France and Malta) have established dedicated national regimes for CASPs ([36]). In Germany, some licencing and prudential requirements also apply to CASPs providing certain types of services (e.g. MiFID type or custody services).

Other **G7 countries** are also looking to contain crypto related financial market risks. In the US, for example, the SEC uses the “Howey Test” to determine which assets, incl. crypto-assets, qualify as a security. Regulatory scrutiny has mainly focused on stablecoins since they strike the most acute threat to financial stability and could disrupt monetary policy transmission (by potentially competing with fiat money). However, where scope exists, regulators have brought enforcement actions against several major CASPs over conflict-of-interest concerns and alleged sales of unregistered securities.

Given the cross-border nature of the crypto-asset market, the **importance of global standard setting organisations**, such as the Financial Stability Board (FSB) and the International Organization of Securities Commissions (IOSCO) cannot be understated. Both organisations provide essential venues to promote standardisation by convening supervisors from across jurisdictions to share information and promote regulatory convergence around a common set of principles ([37]).

Conclusion

Due to their volatile growth cycles, and as long as relevant regulatory provisions do not apply, crypto-assets entail numerous risks which may in future become relevant for financial stability. Until now, turmoil in the market for crypto-assets (much of which can be attributed to the inherent vulnerabilities in the market structure and underlying technology) has not spilled over into traditional financial markets or the real economy.

However, spillovers may occur, depending on how current risks can be contained and how interlinkages between both systems will develop. Though such threats have not yet materialised, understanding their root causes is an important first step in shaping an appropriate regulatory response and mitigating the fallout of market downturns in the future. ESMA is in the process of including crypto-assets in its risk monitoring framework, and will continue to analyse material risk issues as they emerge.

([36]) More information on the two national regimes can be found on the websites of the Autorité des marchés financiers and the Malta Financial Services Authority.

([37]) While the FSB focuses primarily on financial stability, IOSCO concentrates on global standard setting for securities markets. For more information on their activities around crypto-assets, please refer to the website of the FSB and IOSCO’s ‘Crypto-asset roadmap for 2022-2023’.

References

Boissay, F. et al. (2022), '*Blockchain Scalability and the Fragmentation of Crypto*', BIS Bulletin No 56, Bank for International Settlements, Basel.

Faux, Z., 'Anyone seen tether's billions?', Bloomberg, 7 October 2021.

FSB (2022), '*Assessment of Risks to Financial Stability from Crypto-assets*'.

Gorton, G. B. and Zhang, J. (2021), 'Taming wildcat stablecoins', *University of Chicago Law Review*, Vol. 90, Forthcoming.

Harris, A., 'Money markets are insulated, for now, from the stablecoin mess', Bloomberg, 12 May 2022.

Hermans, L. et al. (2022), 'Decrypting financial stability risks in crypto-asset markets', *Financial Stability Review*, No 1, European Central Bank.

International Monetary Fund, BIS and FSB (2009), 'Report to G20 finance ministers and governors – Guidance to assess the systemic importance of financial institutions, markets and instruments: Initial considerations'.

IOSCO (2022), 'Decentralized finance report'.

Karim, M. and Tomova, G., 'Research note: Cryptoasset consumer research 2021', Financial Conduct Authority, 17 June 2021.

Kolchin, K., Podziemska, J. and Hadley, D. (2022), '*2022 Capital Markets Fact Book*', Securities Industry and Financial Markets Association, New York.

Linciano, N. et al. (2022), '*Emerging Trends in Sustainable Investing and Cryptoasset Markets*', Commissione Nazionale per le Società e la Borsa, Rome, p. 26.

Makarov, I. and Schoar, A. (2022), 'Cryptocurrencies and decentralized finance (DeFi)', *NBER Working Papers*, No 30006.

Neureuter, J. (2021), '*The Institutional Investor Digital Assets Study*', Fidelity Digital Assets.

Qin, K. et al. (2021), 'Attacking the DeFi ecosystem with flash loans for fun and profit', in Borisov, N. and Diaz, C. (eds), *Financial Cryptography and Data Security*, Springer, Berlin, Heidelberg, pp. 3–32.

Roberts, J. J., 'Bitcoin price smashes $44,000 as market reacts to Tesla purchase', Fortune, 8 February 2021.

Schultze-Kraft, R., 'No, bitcoin ownership is not highly concentrated – But whales are accumulating', Glassnode, 2 February 2021.

Shen, M., 'DeFi app promising 20 % interest on stablecoin deposits raises concerns', Bloomberg, 23 March 2022.

Xie, L., 'Composability is innovation', Future, 15 June 2021.

Glossary

Non-exhaustive list of terms used in this TRV article. Descriptions based on usage by official international institutions, incl. BIS, FSB, IMF and IOSCO. Terms and their definitions may change in future given the rapidly-evolving nature of crypto-asset markets.

51 % (or Sybil) attack: When a malicious actor is able to compromise more than half of the validators in a network, the actor can execute fraudulent transactions.

Algorithmic so-called stablecoins: A type of so-called stablecoins that use algorithms to defend their peg. Usually, this is done by automatically issuing more coins when their price is too high and buying coins off the market when their price is too low. Contrary to reserve-backed so-called stablecoins, they do not rely on a one-to-one reserve backing of issued coins.

Atomicity: An instantaneous exchange of assets, such that the transfer of one occurs only upon transfer of the other.

Blockchain: A form of distributed ledger in which details of transactions are stored in the ledger in the form of blocks of information. A block of new information is attached to the chain of pre-existing blocks via a computerised process by which transactions are validated.

Consensus: In DLT applications, the process by which validators agree on the state of a distributed ledger.

Composability: The capacity to combine different components in a system, such as DeFi protocols.

Crypto-asset: A type of private sector digital asset that depends primarily on cryptography and distributed ledger or similar technology.

Crypto-asset service provider (CASP): Any entity whose occupation or business is the provision of one or more crypto-asset services to third parties on a professional basis.

Crypto-asset trading platform: Any trading platform where crypto-assets can be bought and sold, regardless of the platform's legal status.

Decentralised finance (DeFi): A set of alternative financial markets, products and systems that operate using crypto-assets and smart contracts and are built using distributed ledger or similar technology.

Decentralised exchanges (DEXs): Marketplaces where transactions occur directly between crypto-asset traders.

Distributed ledger technology (DLT): A means of saving information through a distributed ledger (i.e. a repeated digital copy of data available at multiple locations).

Oracle: A service that provides outside (off-chain) information for use by smart contracts in a DLT system.

Rehypothecation: The practice that allows collateral posted by one entity to be used again as collateral by another entity for its own funding.

So-called stablecoins: A crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets.

Smart contract: A self-executing application that can trigger an action if some prespecified conditions are met.

Validator or validating node: An entity that verifies transactions in a blockchain. In some networks, this role is played by miners.

Appendix

Crypto-assets in the ESMA risk assessment framework

Risk overview

	Type of crypto entity				
	Backed	Unbacked	CASPs	DeFi	**Overall**
Liquidity	🟡	🟡	🟡	🟡	🟡
Market	🔴	🔴	🟡	🟡	🔴
Credit	🟡	🟡	🔴	🟡	🟡
Contagion (internal)	🔴	🔴	🔴	🔴	🔴
Contagion (external)	🟡	🟢	🟢	🟢	🟢
Operational	🟡	🔴	🟡	🔴	🔴

Note: **Backed** = Backed crypto-assets, **Unbacked** = Unbacked crypto-assets, **CASPs** = Crypto-asset service providers, **DeFi** = Decentralised finance.

Explanation and detailed risk driver

Risk categories	Type of crypto entity			
	Backed (SCs)	Unbacked	CASPs	DeFi
Liquidity	- Risk of runs on so-called stablecoins.	- Congestion of blockchain networks remains a common issue.	- No standards on liquidity provision. - Suspension of redemptions (e.g. Binance following Celsius).	- No minimum TVL on DEXs and in lending protocols.
Market	- Market concentration / prominence of some coins (e.g. USDT, USDC). - De-pegging is a common issue.	- Market concentration / prominence of some coins (e.g. BTC, ETH) / “everything is correlated with BTC”. - No inherent value compared to traditional securities. - High leverage and interlinkages create high price volatility.	- High leverage multiples available to unsophisticated investors.	- High leverage multiples available to unsophisticated investors. - Unsustainable yields and untransparent business models. - De-pegging of algorithmic stablecoins (e.g. Terra/Luna).
Credit	- Issuer defaults.	- Pseudonymity prevents evaluating the creditworthiness of counterparties.	- Frequent and opaque use of leverage. - Defaults of CeFi platforms (e.g. Celsius).	- Frequent and opaque use of leverage. - Defaults of algorithmic stablecoins (e.g. Terra/Luna). - Defaults of borrowers in lending protocols. - Usually relying on over-collateralisation.

Contagion (internal)	- Market concentration / prominence of some coins (e.g. USDT, USDC). - So-called stablecoins are the equivalent to cash in the crypto-market.	- Market concentration / prominence of some coins (e.g. BTC, ETH).	- Market concentration / prominence of certain CASPs (e.g. Binance).	- Composability creates significant interlinkages. - Defaults of large protocols can cause significant confidence effects (e.g. Terra/Luna).
Contagion (external)	- Fire sales in money markets. - Crowding out of high-quality liquid assets. - Still relatively small in size (compared to traditional markets).	- No evidence so far. - Limited interlinkages with the traditional financial system.	- Limited sizes compared to traditional infrastructures. - Limited interlinkages with the traditional financial system.	- No evidence so far. - Limited interlinkages with the traditional financial system.
Operational	- No regulatory requirements on operational resilience (compared to traditional deposit taking institutions).	- Inherent blockchain risks (consensus mechanism; fragmentation, i.e. interoperability issues).	- No regulatory requirements on operational resilience (outages, hacks, ransomware).	- Open-source code of protocols, and DeFi governance make it susceptible to hacks and exploits.

Note: **Backed** = Backed crypto-assets, **Unbacked** = Unbacked crypto-assets, **CASPs** = Crypto-asset service providers, **DeFi** = Decentralised finance.

esma European Securities and Markets Authority