Occasional Studies
Volume 20 – 5

Crypto-assets: evolution and policy response

DeNederlandscheBank
EUROSYSTEEM

Crypto-assets: evolution and policy response

Authors: Vera Lubbersen and Peter Wierts, with contributions from Luc Blommers, Menno Broos, Annemone Heijn, Menno Martens, Hugo Prince, Milan de Reede and Stan Verweij. Colleagues at DNB, the Dutch Authority for the Financial Markets (AFM) and the Netherlands Ministry of Finance are gratefully acknowledged for sharing their valuable views. Any remaining errors are our own.

De Nederlandsche Bank N.V.
P.O. Box 98
1000 AB Amsterdam
www.dnb.nl
info@dnb.nl

Contents

Summary

Crypto-assets have shown a remarkable evolution over the past two years that highlights their relevance for society as a whole. There have been large inflows and outflows in these markets. There have been polarised debates between crypto believers and sceptics. There have been warnings by authorities that investors could lose their money. In spite of those warnings, crypto-assets continued to exert a strong attraction to a substantial proportion of the population; approximately 14% of the Dutch population holds them. This raises questions: what makes crypto-assets so attractive? What opportunities and risks do they pose for society? And how can policymakers ensure that societal risks will be mitigated while leaving room for innovation?

As crypto-asset markets evolve, so does the regulatory response. More than a decade after crypto-assets were first introduced, their development is still at an early stage. Their future evolution is uncertain. But whatever one's view on the pros and cons, it seems plausible that these assets and markets are here to stay. Since crypto ecosystems try to replicate existing financial, payment and monetary functions, their relevance for financial regulation, payment systems and financial stability is a given. During the past years, DNB's crypto-asset supervision was geared towards legislation regarding anti-money laundering, countering the financing of terrorism and sanctions screening. Tailored crypto-asset regulation was not yet in force for the other traditional objectives of financial regulation related to financial stability, prudential supervision and consumer and investor protection. This will change over the coming years as new crypto-asset regulations enter into force. However, regulation and supervision are still evolving and will not eliminate all risks. Consumers and investors should remain aware of the risks before investing in these markets.

The aim of this study is therefore to: (*i*) deepen our understanding of the underlying technology and functions of crypto-assets; (*ii*) revisit their main opportunities and risks, and (*iii*) summarise our view on regulation, supervision and enforcement. In DNB's view, the main implications are the following.

First, the future path of innovation driven by the underlying technology is uncertain, which calls for continuous monitoring. More than a decade after its introduction, Distributed Ledger Technology (DLT) has facilitated the emergence of entire crypto-asset ecosystems, with their own issuers, assets, service providers and users. DLT has been a major innovation since it facilitates the storage and transfer of tokenised assets without a trusted central intermediary. The technology has its flaws, as illustrated by cases of high energy use and settlement congestion although newer releases show improvements. This may help to deliver on what are widely regarded as the main opportunities: (*i*) to improve the efficiency of global cross-border payments, and (*ii*) as a platform for innovation, to facilitate the storage and transfer of tokenised-assets. New use cases are being explored, such as those related to Web3 and Decentralised Finance, which brings new challenges. The path of future innovation is uncertain, as always, and it is rarely the case that major breakthroughs are predicted in advance. It remains important to continue to monitor the evolution, opportunities and risks of crypto-ecosystems as a whole as well as their constituent parts.

Second, unbacked crypto-assets are not suitable as money, and mainly serve as a speculative investment. While traditional analyses on the attraction of crypto-assets emphasise the "crypto promise" of disintermediated payments and finance, recent research highlights a complementary explanation: the desire to gamble. Unbacked crypto-assets have no underlying assets, which makes it difficult to value them. A large part of supply is taken out of circulation by investors and developers, which increases price volatility due to shifts in demand. Large price swings and strong social media attention trigger psychological factors such as fear of missing out and the difficulty to disengage. On the one hand, the volatility of unbacked cryptos increases their attractiveness as a speculative investment. On the other hand, it implies that they lack the stability that is needed for money. In

advanced economies, unbacked cryptos are hardly ever used as a means of payment. They are too volatile, and national and European payment infrastructures already support instant payments. There is no monetary authority to stabilise their value, no prudential regulation and no deposit guarantee fund. Buyers should be very cautious and aware of the risks before investing in these markets, and market conduct authorities should be given adequate tools to monitor and mitigate related risks.

Third, stablecoins may have the potential to function as a means of payment for specific use cases, but only if risks are adequately mitigated. Stablecoins aim to solve two of the major flaws of unbacked cryptos, i.e. to create a verifiable stable value, and to use the same unit-of account-function as fiat money. Both of these features may increase their suitability as a means of payment. This could improve the efficiency of cross-border payments and the settlement of tokenised assets. It could facilitate new use cases related to Web3. However, stablecoins also give rise to significant risks to monetary policy (since they fall outside the monetary policy framework), and financial stability, due to their link with the real economy, vulnerability to runs, and risks related to settlement. A major issue concerns the transparency, composition and redeemability of the asset backing, and inherent incentives for issuers to dilute it or restrict redeemability. Regulation is therefore needed to mitigate these risks.

Fourth, market participants must adhere to relevant existing requirements and prepare for forthcoming requirements. Due to their complexity, anonymity and opaque governance structures, crypto markets are more prone to market failures than traditional financial markets. Users and developers are largely anonymous, which makes crypto-assets vulnerable to money laundering, scams, theft, market manipulation and Ponzi schemes. This is exacerbated by the fact that there is no central entity that can be held responsible for the security and integrity of the network, while service providers can operate remotely without complying with regulations. Crypto-assets fulfil different functions, e.g. as (speculative) securities, electronic money or derivatives, which are subject to existing regulation in line with the principle: "same activity, same risk, same regulation". To further clarify the regulatory regime, a broad international consensus has emerged on the need for a coordinated regulatory response due to the cross-border reach of crypto-assets. International regulatory standard setting bodies have issued recommendations, such as the Financial Stability Board's consultative report on the regulation, supervision and oversight of crypto-asset activities and markets of October 2022. In the EU, the Market in Crypto-Asset Regulation (MiCAR) was agreed at the political level in the summer of 2022. MiCAR represents a welcome first step towards clarifying the regulatory approach. DNB calls on market participants to prepare for the new regulations, such as the MiCAR rules, which are expected to take effect in 2024.

Fifth, forthcoming regulatory changes continue to affect the objectives and tasks of DNB as an integrated central bank and supervisory authority. At the international level DNB will continue to contribute to the development of international standards by the Financial Stability Board (FSB) and other standard-setting bodies such as the Basel Committee on Banking Supervision (BCBS) and the Committee on Payments and Market Infrastructures (CPMI). DNB's mandate will be affected by forthcoming changes to European and national financial supervision, including those related to MiCAR (in close cooperation with the Dutch Authority for the Financial Markets, the AFM) and legislation regarding AML/CFT related supervision. Moreover, proposed changes to international standards will also continue to affect supervisory tasks, such as the proposed revisions to bank capital adequacy rules for crypto-asset exposures, and international standards for the transfer function of systemically important stablecoin arrangements. In sum, DNB stands ready to continue to monitor crypto-asset ecosystems and to contribute to the ongoing elaboration of the regulatory regime as well as its implementation.

1 Introduction

Crypto-assets have shown a remarkable market evolution over the past years: strong inflows and price increases since 2020, a rapid development in market structures, followed by strong outflows and contracting markets during the spring of 2022. Markets evolved rapidly due to the further development of DLT technology, stablecoins, exchanges and decentralised finance, invoking regulatory attention for these markets at a global, European and national level well before the downturn of crypto-markets in early 2022. Over the years, it became increasingly clear that these markets offer not only opportunities, but also risks: crypto-asset markets are not free from market failures, alongside the regulatory attention for risks related to illicit finance that have been on the radar for some time already (DNB/AFM, 2018).

The rapid evolution of crypto-asset markets affects the tasks and objectives of an integrated central bank and supervisory authority such as DNB. Crypto-assets can be seen as an attempt to rebuild monetary and financial infrastructures from scratch. Traditional financial functions such as investing, paying, lending, borrowing and risk management have evolved over long periods of time, and the same holds for the regulatory approach. Crypto communities have recreated these functions in an alternative way, in little more than a decade. As such it is no surprise that, while this is impressive by itself, the emerging risks and market failures have also confirmed why financial regulation remains needed to protect society at large. Due to their wide scope, crypto ecosystems also affect central bank functions related to financial stability, the orderly functioning of payment systems and monetary policy. The principal challenge is to balance the opportunities presented by this innovation with the risks to society, in a fast-evolving world and accompanied by a large degree of uncertainty.

The rapid evolution of crypto-asset markets implies that the opportunities and risks are evolving as well. As an underpinning for DNB's policy position, this study aims to: (*i*) deepen our understanding of the functioning of crypto-assets and their attractiveness; (*ii*) revisit their main opportunities and risks, and (*iii*) summarise our views on ongoing efforts regarding regulation, supervision and enforcement.

The rest of this report is structured as follows. Section 2 introduces crypto-assets, who invests in them, and how markets have evolved. Section 3 revisits the main opportunities and risks of the technology (hype or the future?), unbacked crypto-assets (money or security?), stablecoins (how stable?) and the monetary implications, including the differences between crypto-assets and central bank digital currency. Section 4 analyses why and how crypto-assets should be regulated. Section 5 presents the main findings and conclusions. The summary contains the implications for DNB's policy position. The Annex provides background information on the underlying technology, market infrastructures and decentralised finance.

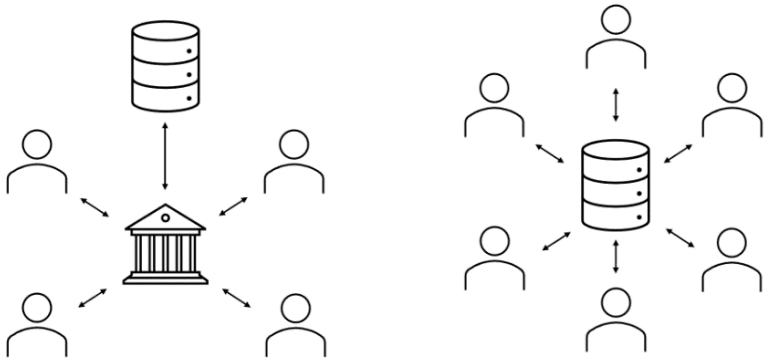
2 Crypto-assets evolution

2.1 What are crypto-assets?

Crypto-assets are a digital representation of value or rights designed to transfer value in a decentralised network, without the need for intermediaries such as (central) banks.[1] At the time of the invention of the internet, developers created the "HTTP 402 payment required error" to indicate that the requested content would not be available until the client would make a payment through a digital cash payment system. However, such a system did not render itself profitable. As national banking payment infrastructures had weak interoperability worldwide, it was not possible to create a digital cash payment system for such worldwide payments. This historical context illustrates the significance of the invention of crypto-assets. In principle, crypto-assets can be used by anyone around the world without using a trusted intermediary and are therefore seen by some as the ultimate fulfilment of the promise of the internet.

A defining feature of crypto-assets is the type of recordkeeping applied: distributed ledger technology (or similar technology). Digital money mostly exists as electronic entries in a digital ledger – a database of balances. As digital data can be copied, traditionally there had to be a trusted third party that would debit the balance of the payer and credit the balance of the payee, otherwise money could be spent twice. To cut out banks and settlement institutions, the crypto programming communities came up with an innovative idea: to give each computer access to the same synchronised database – hence the name "Distributed Ledger Technology" (DLT) (see Figure 1). There are different types of DLTs, but what they all have in common is that the ledger is controlled by users. The underlying software protocol specifies how and when entries can be created or added.

Figure 1. Traditional technology (left) versus Distributed Ledger Technology (right)



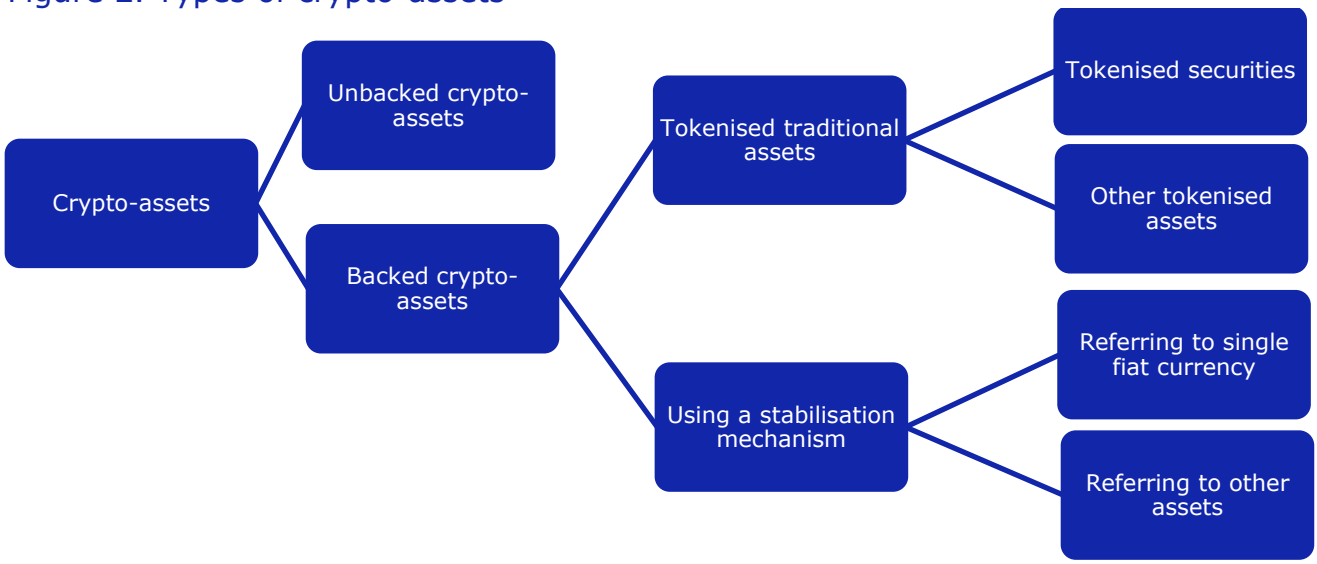
Source: own construction.

For the purpose of this report we take a financial perspective to distinguish between different types of crypto-assets. The definition of crypto-assets specifies the technology, but not the type of asset (i.e. "a digital representation of value or rights"). In principle, any asset which is transferred or stored electronically using DLT (or similar technology) is a crypto-asset. From a regulatory perspective, the same asset should be regulated in the same way – regardless of its technology. Therefore, we distinguish between what we call unbacked crypto-assets and backed crypto-assets (Figure 2). An unbacked crypto-asset is a value or right that only exists in the DLT: an entry in a distributed ledger. Backed crypto-assets refer to an underlying asset that exists outside the DLT. They

[1] The full official definition is: 'crypto-assets are a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology (DLT) or similar technology' EC (2020a).

are issued and redeemed by entities that promise to buy and sell the underlying asset backing in the traditional economic or financial system. Backed crypto-assets can be further subdivided into tokenised traditional assets, such as tokenised securities, and crypto-assets that use a stabilisation mechanism (BCBS, 2022). The latter are also called "stablecoins". They seek to link the value of a crypto-asset to the value of a traditional asset or a pool of traditional assets through a stabilisation mechanism.

Figure 2. Types of crypto-assets



Note: Based on BCBS (2022) and EC (2020a). Other distinctions would be possible as well, e.g. IOSCO (2020a) uses three categories (security token, payment token, utility token).

There is no globally accepted taxonomy of crypto-assets; the crypto community sometimes makes a distinction between native coins and tokens, but tokens could also specify the use case of a crypto-asset. Typically, a native coin is issued in its own DLT. For example, bitcoin (with lowercase b) and Ether are the native coins that are issued on the Bitcoin blockchain (with uppercase B) and Ethereum blockchain respectively. According to this taxonomy, a token represents ownership of an asset or right and is issued in a pre-existing DLT. For example, Tether issues stablecoin tokens on different blockchains. At the same time, tokens are also used to specify different use cases of crypto-assets more generally, as summarised in Table 1. These use cases are not mutually exclusive, i.e. a crypto-asset can serve different use cases at the same time.

Table 1. Use cases of crypto tokens

Payment tokens	Crypto-assets used as a means of exchange
Governance tokens	Crypto-assets that give holders the right to vote on issues related to a crypto project
Utility tokens	Crypto-assets intended to provide digital access to a specific good or service
Security tokens	Crypto-assets issued as a means to fund crypto projects, which typically provide rights (e.g. in the form of ownership rights and/or entitlements similar to dividends).
Non-fungible tokens	Crypto-assets that give ownership right to unique assets, such as a picture, song, ticket or house
Liquidity provider tokens	Crypto-assets that provide a claim in a crypto investment fund

Source: own construction, based on IOSCO (2020a) and EC (2020a).

2.2 Investor base

Crypto-assets are highly attractive to specific groups of retail investors, especially those who are highly educated, young and male. Several crypto surveys are available, both nationally and internationally. They generally provide the same overall message, while the specific results obviously differ. According to Cryptovaluta Monitor (2022), almost 2 million Dutch people over the age of 18 (or 14% of the population) invested in crypto-assets in June 2022, up from 900,000 people in 2018. IPSOS (2021) finds that Dutch men were more than twice as likely to invest in crypto than women. Moreover, young people (18-34) were five times more likely to invest in crypto-assets than senior people. Lastly, highly educated people were more than four times more likely to invest in crypto-assets than those with less education. A study using Finish data also confirms that crypto trading is associated with younger age and male gender (Oksanen et al., 2022).

The most important reason for retail investors to invest in crypto-assets is to gamble, mostly with small amounts. When asked why they invested in crypto, most cited they wanted "*to gamble*" (54%). Approximately 30% liked the excitement of investing. People also reported investing in crypto to earn some money because the return on their savings account was too low (42%), while few cited they wanted to use it as a payment method (7%). A similar finding is reported by Auer and Tercero-Lucas (2021), using US data: crypto-assets are not sought as an alternative to fiat currencies or regulated finance, but instead are a niche digital speculation object. Finally, while almost half (43%) of Dutch investors reported investing with small amounts (less than EUR 500), around a quarter said to invest with more than EUR 2,500. In fact, one out of eight (12%) said they would experience financial distress in case of severe value loss (IPSOS, 2021).

Young people are drawn by stories about of crypto millionaires on social media and in the gaming industry. The Dutch Ministry of Finance has therefore launched a campaign: "Smart with Crypto"[2]. Different studies suggest crypto trading is associated with excessive gambling, gaming and internet use by young people (Oksanen et al., 2022; Delfabbro et al., 2021). In a nutshell, their analyses suggests that large price swings and media focus on crypto millionaires trigger psychological factors such as overestimating the role of knowledge or skill, fear of missing out and the difficulty to disengage (Delfabbro et al., 2021). In fact, a lot of information is shared on social media about cryptos, but influencers are not always neutral and transparent on the topic. The "Smart with Crypto" website provides youngsters with information on crypto[3]. In addition, the campaign targets youngsters with short videos on YouTube, Snapchat and Twitch to make them aware of pitfalls and expectations that are too good to be true.

Crypto-asset use cases differ between Advanced Economies and Emerging Market and Developing Economies. In Advanced Economies (AEs), crypto-assets are most widely used for speculation and gambling. In Emerging Market and Developing Economies (EMDEs), crypto-assets (i.e. both unbacked crypto-assets and stablecoins) are used more often to send remittances, preserve savings in times of fiat currency volatility, or other needs specific to their country.[4] In countries with less developed monetary institutional frameworks, stricter limits on capital flows, more limited financial development and more costly remittance channels, crypto-assets are more commonly regarded as a viable alternative as an investment and as a means for cross-border payments.

---

[2] See Ministerie van Financiën start campagne om jongeren te wijzen op risico's van crypto's | Nieuwsbericht | Rijksoverheid.nl
[3] See Slim in Crypto - SIC - Wijzer in geldzaken
[4] See 2022 Global Cryptocurrency Adoption Index - Chainalysis, accessed on 21 September 2022.

While interconnectedness with the traditional financial sector is still limited, it is expected to increase over time (FSB, 2022a). Institutional investors in crypto-assets include hedge funds, while banks, pension funds and insurers keep a cautious approach. In a survey conducted among European institutional investors, approximately 23% of hedge fund professionals interviewed held crypto-assets in their funds, while other institutional investors reported small exposures. For example, only 3% of professionals interviewed from EU pension funds held crypto-assets (Fidelity Digital Assets, 2021). Most institutional investors see a limited role for crypto-assets in their portfolio due to their inferior risk/return profile, volatility and correlation with other markets (JP Morgan, 2021). However, institutional investors who control the cryptocurrency portfolios generally do believe crypto-assets will see mainstream adoption, but they also cite risk and volatility as the main barrier to investing in crypto (Bitstamp Crypto Pulse Report, 2022). In general, equity investments of large banks in crypto-assets represent a small fraction of their capital as of late 2021, i.e. for most around 0.3% (Aramonte et al., 2021). While the cryptoasset market remains small relative to the size of the global financial system, and banks' exposures to cryptoassets are currently limited, its absolute size is meaningful and there continue to be rapid developments (BCBS, 2022).

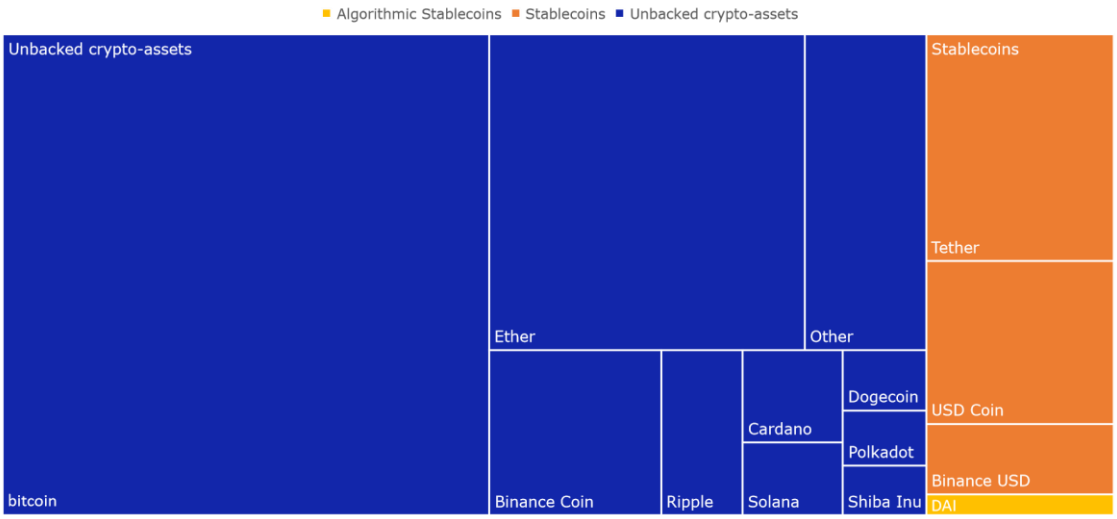
2.3 Market evolution

Crypto-asset markets have shown a volatile growth pattern over the past 13 years, predominantly driven by a few large crypto coins. The first trade of crypto for fiat happened on 22 May 2010, when a USD 35 pizza was traded for 10,000 bitcoin. The same pizza would cost around 0.00175 bitcoin in late 2022, when the price of bitcoin hovered around USD 20,000. Bitcoin dominates the crypto-asset market, followed by Ether (Figure 3). Bitcoin's share is decreasing, however: up to 2017, it has constituted approximately 85% of total crypto-asset market capitalisation, which has fallen to 44% since.[5] After bitcoin and Ether, a group of substantially smaller cryptos follow. At the time of writing, the vast majority of crypto-assets that reference traditional assets are dollar-denominated stablecoins (~99%).[6] Of the four biggest stablecoins, one is an "algorithmic" stablecoin and unbacked (Dai) (see Box 1), while the other three claim to be backed.

The past two years have shown a strong boom-bust pattern in the market capitalisation of crypto-assets. Crypto-asset market capitalisation grew by a factor of 3.5 in 2021 to USD 2.6 trillion, then almost halved again in mid-2021, after which it rose to a new record above USD 3 trillion the end of 2021, but fell back to less than USD 1 trillion during the spring of 2022 (see Figure 4), in the wake of the collapse of Terra Luna (see Box 1). Bitcoin in particular has seen a sharp boom-bust pattern. The price of bitcoin hovered around USD 8,000 until 2020, then reached a peak of USD 63,000 in April 2021, a low in around USD 30,000 in July 2021, a peak again of nearly USD 70,000 in November 2021, and a subsequent fall to around USD 20,000 as of summer 2022[7]. This period provides valuable lessons on the opportunities and risks of crypto-assets, and need for regulation, which will be discussed in Sections 3 and 4.

[5] See Global Cryptocurrency Market Charts | CoinMarketCap, accessed on 20th September 2022.
[6] See Top Stablecoins by Market Cap | CoinGecko, accessed on 19th September 2022.
[7] See Bitcoin price today, BTC to USD live, marketcap and chart | CoinMarketCap, accessed on 20th of September 2022.

Figure 3. Top 25 crypto-assets by market capitalisation in 2022



Note: The Other category contains the following coins: staked Ethereum (STETH), Polygon (MATIC), Tron (TRX), Avalanche (AVAX), Wrapped Bitcoin (WBTC), Uniswap (UNI), Leo token (LEO), Chainlink token (LINK), OKX utility token (OKB), Cosmos (ATOM), Ethereum Classic (ETC), Litecoin (LTC).
Source: Data obtained from CoinGecko.[8]

Figure 4. Total market capitalisation of crypto-assets over time (in EUR)

Source: own calculations based on data retrieved from CoinGecko.[9]

This boom-bust pattern could be amplified by a traditional leverage cycle. The correlation between growth in Decentralised Finance (DeFi)[10] and stablecoins was positive until May 2022 (see Figure 5) (IMF, 2022; BoE, 2022; IOSCO, 2022; FSB, 2022d). In DeFi, participants can deposit their unbacked crypto-assets as collateral and borrow stablecoins (see Figure 6). These stablecoins are used to invest in DeFi investment funds, which provides a return in unbacked crypto-assets. These can be further "staked" into other DeFi protocols, which issue new unbacked crypto-assets. This process is called "liquidity mining" by the crypto community, but also known as

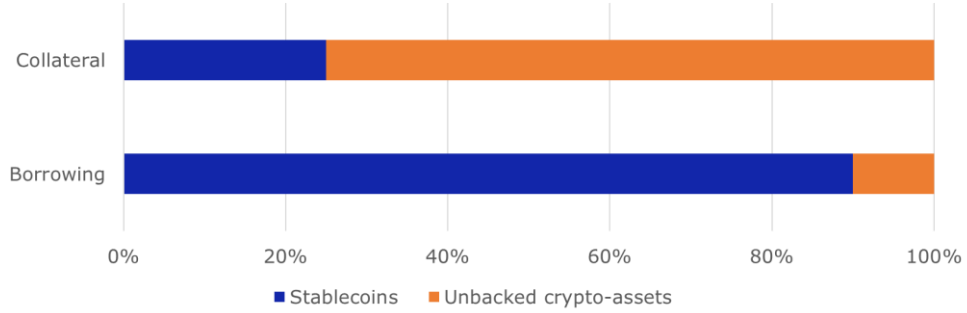
[8] Based on the first 25 crypto-assets with largest market capitalization, data has been retrieved from: Cryptocurrency-prijzen, grafieken, en marktkapitalisatie | CoinGecko, accessed on 28th September 2022.
[9] See De meest uitgebreide cryptocurrency-API | CoinGecko, accessed on 22nd of September 2022.
[10] Decentralised finance (DeFi) commonly refers to the provision of financial products, services, arrangements and activities based on crypto-assets (IOSCO, 2022) (see Annex).

"rehypothecation"[11] or in traditional finance as a leverage cycle. As unbacked crypto-assets increase in value, more investors are attracted by higher and higher returns. The process continues until holders want to redeem their unbacked crypto-assets back for stablecoins, which might not always be possible (ECB, 2022).

Figure 5. Growth in DeFi and stablecoins over time (in EUR)

Note: total market capitalisation of stablecoins and total value locked of crypto-assets (TVL) in DeFi protocols over time (in USD).
Source: own calculations based on data retrieved from CoinGecko and DeFi Liama[12]

Figure 6. Composition of borrowing and collateral in DeFi loans



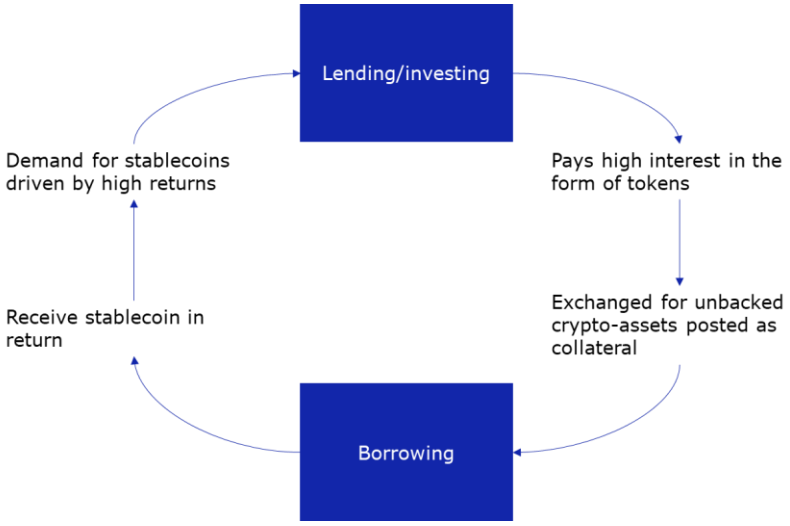
Source: IMF (2022).

A feedback loop emerges: as long as the value of volatile crypto-assets rises, it becomes attractive to borrow stablecoins which can in turn be invested (Figure 7). The process continues until the value of the volatile unbacked crypto-assets used as collateral declines. As soon as collateral value falls below certain thresholds, the contract will automatically liquidate and sell the underlying unbacked crypto-asset at a discount. In case this happens at a large scale, unbacked crypto-asset prices fall, triggering further liquidations. The high volatility of crypto-asset prices leads to frequent liquidation of DeFi loans (IMF, 2022; Aramonte et al., 2021). Holders of unbacked crypto-assets can redeem them for fewer stablecoins, so that risky algorithmic stablecoins fail (see Box 1), and only stablecoins deemed "safe" see an inflow (Liao & Caramichael, 2022). However, the emergence of

[11] Rehypothecation is when collateral for a loan can be re-pledged in other to obtain another loan, see ECB (2022).
[12] See Top stablecoins op marktkapitaal | CoinGecko and DefiLlama - DeFi Dashboard, accessed on 22nd of September 2022.

algorithmic stablecoins and risk-taking by stablecoins providers will likely lead to more failures and potentially larger sell-offs.

Figure 7. Leverage feedback loop between stablecoins and unbacked crypto-assets



Source: own construction.

This feedback loop has caused the failure of crypto companies that offered unsustainable returns, in some cases comparable to Ponzi schemes. Rehypothecation could cause liquidity to vanish quickly in case of a big shock (ECB, 2022). Examples are Celsius[13], Voyager[14], Vauld[15] and Three Arrows Capital.[16] Crypto "banks" are not regulated credit institutions, they do not fall under prudential supervision and deposits have no Deposit Guarantee Scheme (DGS). These companies invested crypto deposits in DeFi protocols while promising unsustainable returns. They were unable to accommodate withdrawals during market turbulence, forcing them to 'freeze' deposits. In essence, early investors benefited at the expense of later investors, which is reminiscent of Ponzi schemes. This reflects the lack of regulation and the complexity – both technically as well as financially - involved in the use of different tokens (ECB, 2022).

Box 1: Collapse of Terra USD (USTC) stablecoin

Terra USD (USTC) was an "algorithmic stablecoin". Unlike early stablecoins issued by centralised institutions – such as Tether Ltd (USDT), Paxos (PAX), Binance (BUSD) and Centre (USDC) – algorithmic stablecoins are issued in a decentralised way. USTC was issued by exchanging it for an unbacked crypto-asset named Luna.

The Luna Foundation Guard – a non-profit entity which was allocated a large amount of LUNA - could indirectly steer the issuance and redemption of USTC by selling and buying LUNA, because USD 1 worth of LUNA could be exchanged for 1 USTC and vice versa. As demand for USTC rose, the LUNA Foundation sold LUNA and used the

[13] See Cryptobank Celsius richting bankroet (fd.nl)
[14] See Klanten omgevallen cryptobedrijven zien hun geld mogelijk niet terug (fd.nl)
[15] See Ook cryptobank Vauld staat op omvallen (fd.nl)
[16] See Val van cryptohedgefonds Three Arrows voedt vrees voor domino-effect (fd.nl)

receipts to subsidise a crypto investment fund called the "Anchor Protocol Reserve", which in turn paid 20% interest on USTC deposits. This scheme effectively functioned as a Ponzi scheme. The returns from selling Luna were used to pay exorbitant interest rates in the Anchor Protocol Reserve. These returns attracted more and more investors who wanted to have USTC and therefore bought Luna (the only way to create new USTC was to "burn" LUNA). In fact, roughly 75% of outstanding USTC supply was held in the Anchor Protocol Reserve. In essence, early investors benefitted from late investors who lost almost all their money.

At its peak on 5 April 2022, LUNA had a market cap of USD 41 billion, while outstanding USTC peaked at USD 18.7 billion. Following broader price decreases in the crypto market, LUNA's market cap slid to USD 30 billion on 5 May 2022. Widespread withdrawals of USTC deposits from the Anchor Protocol Reserve over the weekend of 7 May caused panic and USTC lost its peg to the dollar (FSB, 2022d). Bitcoin and other assets that Luna Foundation Guard held were used to execute on-chain swaps and to prop up the price of USTC on exchanges.[17] As confidence was lost and crypto reserves were drained, LUNA and USTC lost more than 90% of their market caps as of mid-May 2022.

[17] See the Twitter reports of the Luna Foundation Guard in May: https://twitter.com/LFG_org/status/1526126703046582272.

3 Opportunities and risks

This section summarises the opportunities and risks of crypto-assets and their infrastructure. It provides the basis for the discussion of the regulatory response in Section 4, which should be aimed at balancing opportunities and risks. Our scope covers the role of an integrated central bank and supervisor, with objectives and tasks in the fields of financial stability, financial regulation and supervision, the payment system and monetary policy. We cover the technology (hype or the future?), unbacked crypto-assets (money or security?), stablecoins (how stable?) and the monetary implications, including the differences between crypto-assets and central bank digital currency

Crypto-assets often give rise to intense debates between crypto believers and crypto sceptics. Table 2 summarises some of the arguments that have been brought forward by different sides in these debates. The opportunities largely relate to the crypto-asset infrastructure (i.e. the storage and transfer of assets without trusted intermediaries), and the assets stored and transferred on these infrastructures. The risks largely follow the lines of the traditional market failures that provide a motivation for financial regulation and supervision, i.e. externalities (for financial stability objectives), asymmetric information and conflicts of interest (for consumer and investor protection and market functioning) and the need to protect the integrity of the financial system.

Table 2. Overview of opportunities and risks

Opportunities	Risks

Crypto-asset infrastructures (see 3.1):
• Global electronic payment system for the internet:
  ○ Direct global access.
  ○ No reliance on platform providers or traditional financial intermediaries.
  ○ Anonymous, although transactions are traceable, identities are in principle not traceable.
  ○ Hard to seize or control by governments.
  ○ Operational resilience and reliance, i.e. no single point-of-failure and 24/7 availability.
• Potential for faster and cheaper retail payments for users, especially cross-border (e.g. remittances).
• Potential for more efficient wholesale payments, i.e. delivery-versus-payment (DvP) and payment-versus-payment (PvP) through disintermediation and automation (programmability).
• Potential for more transparent and accessible capital markets, as assets are tokenised and could be fractionalised into smaller assets, making them accessible to a wider set of investors.
 	
Unbacked crypto-assets (see 3.2):
Opportunities depend on the functioning of unbacked crypto-assets:
• Unbacked cryptos lack the stability needed to function successfully as money, but do provide the incentive structure behind the crypto-asset infrastructure, typically based on a fee in the
	Financial stability risks:
	• Risks of crypto-assets (impact through transmission channels):
	  ○ Financial cycle, i.e. leverage and asset price responses.
	  ○ Market illiquidity, i.e. crypto-assets cannot be sold.
	  ○ Price volatility, i.e. exchange rate risks make them unsuitable as money.
	  ○ Counterparty risk from crypto-asset issuers, custodians, brokers, trading platforms, custodial wallet providers and other intermediaries.
	• Specific risks from stablecoins:
	  ○ Settlement and run risk from improper asset backing.
	
	Monetary policy risks:
	• Monetary autonomy risks, i.e. risk of losing monetary control if crypto-asset with different unit of account than fiat currency is adopted.
	• Monetary transmission could be weakened in case of large-scale adoption of crypto-assets as money.
	
	Integrity risks:
	• Risks related to the anonymous nature of crypto-assets, which facilitates the use for money laundering/ financing of terrorism and other criminal purposes such as tax evasion.
	
	Market infrastructure risks:

native coin of the blockchain to the validators to secure the network and settle transactions. • Unbacked crypto-assets could function like unregulated securities, i.e. provide funding for a crypto project, but have no underlying assets or rights and are therefore harder to value. **Stablecoins (see 3.3):** Potential enabler of Web3, cross-border payments, and platform-based settlement of tokenised assets, i.e. by providing payment tokens on DLT platforms. Opportunities depend on the type of stablecoin: • Unbacked stablecoins lack the stability needed to function successfully as money. • Stablecoins intended to be volatile with respect to fiat currencies are unlikely to function as money in countries with a well-developed payment infrastructure. • Credibly backed stablecoins in fiat unit of account appear more suitable as settlement asset.	• Governance risks: unclear allocation of responsibilities and ability to intervene, resulting in settlement risk and illegal practices. • Data privacy and protection risks, i.e. although identities are hidden, all transactions are visible, while consumers cannot retrieve their funds in case of a loss of private key. • Operational risks, i.e. trade-off between scalability, decentralisation and security. • Environmental risks of proof-of-work consensus mechanisms. **Consumer and investor protection and market functioning risks:** • No gatekeeper, while complexity and anonymity aggravates risks, e.g. mis-selling and hacks. • Market manipulation and frontrunning based on inside information of anonymous computers and developers. • Anonymous nature of developers means information may be missing, inaccurate, incomplete and unclear with respect to the risks.

3.1 The technology: hype or the future?

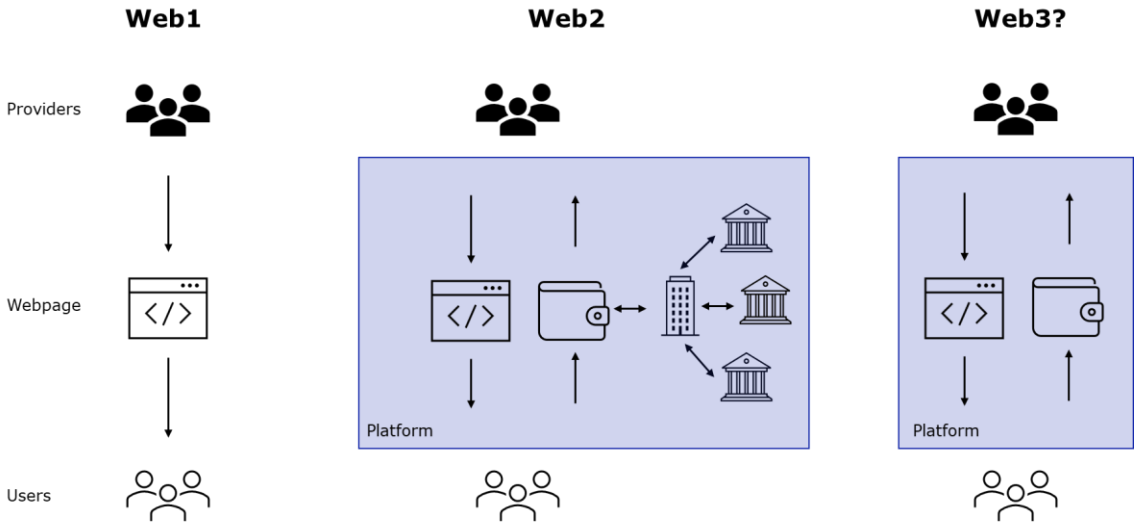
The original crypto promise was to lower the costs of commerce on the internet by creating electronic cash that would "*allow online payments to be sent directly from one party to another without going through a financial institution*" (Nakamoto, 2008). Given the global nature of the internet, this includes cross-border payments, which need to become faster, cheaper, more transparent and more inclusive (G20, 2021). The technology behind some crypto-assets provides opportunities in this respect, as they support feeless global transfers within a couple of seconds at low energy usage (Kappture, 2019). As soon as users have a wallet with crypto-assets, anyone can send and receive anonymously, without having to rely on an intermediary. Moreover, crypto-assets are difficult to seize by corrupt governments[18]. Lastly, crypto-asset infrastructures are available 24/7, as computers all over the world work together to maintain the platform, increasing robustness (no single point-of-failure) and limiting any single user from gaining dominant market power.

Some even refer to this opportunity as the fulfilment of the internet: Web3 (Figure 8). During the first generation of the internet (from 1991 to 2004), information on webpages was largely static and provided by its developers: Web1. Developers expected knowledge to be democratised; everyone could share knowledge and get paid for it by those who want to read it. Platforms emerged as an intermediary where users could pay each other for providing specific content, goods and services: Web2 (McKinsey, 2022; JPMorgan, 2022). These platforms gained dominant market power due to their two-sided market structure, economies of scale and network effects (DNB, 2021a). As crypto-assets were originally developed to be used without a platform provider or intermediaries, some believe they could be an enabler for Web3: a new era in which users can create, monetise, utilise and exchange information and assets for their own benefit (McKinsey, 2022). For example, instead of selling a product

[18] As an example, the Russian activist Navalny and his foundation are unable to receive donations through the traditional financial system as the Russian government has branded them an extremist organisation. Because of this, they have resorted to soliciting donations in crypto. See Navalny ally urges donors to use cryptocurrency due to crackdown | Reuters.

through an e-commerce platform, one issues a token on a blockchain which can be exchanged for payment tokens. Smart contracts define the conditions under which the transaction might be reversed, i.e. when the seller does not prove it has actually sent the product (Chainalysis, 2022). The key element is that this would remove the role of the platform provider, replacing it with computers in a decentralised network.

Figure 8. Digital cash for the internet



Note: During the first generation of the internet (Web1) information was largely static and provided by its developers. The second generation from 2004 onwards (Web2) has been characterised by platforms where users pay each other for providing specific content, goods and services. Some believe there will be a third generation (Web3) that will enable payment without a platform provider.

Source: own construction.

A key opportunity of crypto-asset infrastructures is that they do not rely on existing (national) financial infrastructures, but can be accessed and used for transfers from anywhere around the world. Banking payment infrastructures were mostly developed at a national level, and since the introduction of the euro also at the level of the euro area as a whole. Although payment infrastructures work well nationally or in a currency bloc like the euro area, they are not interoperable internationally. As an example, remittances have an average cost of 6.1%[19] and receipt of payment by the beneficiary is measured in hours or days, rather than seconds or minutes. One of the benefits of DLT is that different participants can transfer without having to rely on a central intermediary. Setting up a crypto wallet and making transfers only requires a smart phone and internet. Although older crypto-assets are relatively expensive and slow and cannot compete with traditional payment methods, some newer crypto-asset infrastructures are more competitive. Some even have zero or no fees and can complete transfers within 12 seconds (Kappture, 2019). This is mostly relevant for global payments, as Instant Payments within the Netherlands are completed within a maximum of 5 seconds (and mostly quicker), and within 10 seconds in the EU.[20]

Opportunities also arise in financial markets where financial assets could be tokenised and exchanged without using traditional financial institutions. Some institutions expect more and more assets to be tokenised

[19] See Remittance Prices Worldwide | MAKING MARKETS MORE TRANSPARENT (worldbank.org).
[20] See also What are instant payments? (europa.eu).

on DLTs, starting with tokenised securities. Over time, more illiquid and non-fungible assets (SME or real estate[21]) and even ownership or usage rights could also be tokenised (WEF, 2021). These tokens can be exchanged simultaneously, in what is known as delivery versus payment (DvP) or payment versus payment (PvP) transactions. In a DvP transaction, a fiat currency token is exchanged for a tokenised asset, such as a security. In a PvP transaction, two different fiat currency tokens are exchanged, possibly improving cross-border payments. Tokenisation could potentially make DvP and PvP transactions faster and cheaper through disintermediation and automation. Moreover, capital markets could potentially be made more transparent and accessible, as assets could be fractionalised into smaller assets, making them accessible to a wider set of investors (OECD, 2020 and 2022).

A key risk of crypto-asset infrastructures relates to their governance mechanisms, e.g. when there is no entity to hold accountable in case of a failure or if the infrastructure does not comply with regulatory requirements. The focal point in crypto governance is the open-source software protocol. It can be interpreted as a nexus of contracts that have been written in computer code. However, not everything can be written down in code, and contracts occasionally still need be interpreted or renegotiated by human beings (Davidson, 2021). For example, in case of a failure, crisis or emergency, changes will need to be made. Moreover, when the infrastructure is not compliant with regulations relating to the security and soundness of the infrastructure and its risk-management framework, the software protocol will also need to be changed (CPMI/IOSCO, 2022). However, crypto-assets rely on services provided by a network of computers, which are often incentivised through fees or stakes in the network (see Annex). Hence, there is no central entity to hold responsible for the security and integrity of the network. Therefore, it takes time before the whole network has reached consensus and transactions can be considered settled. Moreover, certain features favour the concentration of decision power, which facilitates collusion. This limits blockchain viability, because if someone controls more than 50% of the network, it is possible to change the underlying code and rewrite earlier transactions, creating settlement risk (Aramonte et al., 2021).

This governance structure facilitates illegal practices, because identities of malicious actors remain hidden. In conventional payment systems, users and intermediaries are identified, but their transactions remain private. This provides one possible balance between the need for identification and privacy. In a conventional DLT network, users and intermediaries remain anonymous (as they are represented by their public key, i.e. the crypto equivalent of a bank account number). This allows privacy with respect to trusted intermediaries, but it also facilitates misuse since identities are not known. It is easy to create new crypto-assets, which are susceptible to fraud and misleading/incomplete documentation.[22] Unsuspecting consumers are lured into misleading and false promises, being taken advantage of by other investors, intermediaries and developers who can affect market prices and engage in market manipulation (Auer et al., 2022; Eigelshoven *et al*., 2021). Moreover, risks of money laundering and terrorism financing have increased due to the constant growth in crypto markets (e.g. EBA, 2021).

At the same time, regular users are susceptible to privacy risk, since all transactions in crypto-assets are visible to anyone, and users cannot prove ownership in case of a loss of the private key. Although identities are hidden, all transactions in crypto-assets are in most cases completely traceable and can be seen by anyone. The moment someone obtains the public key (crypto equivalent of a bank account number) of a person when making a crypto transfer to this person, this person can see all previous transactions done on the blockchain. There are cryptos that hide such information, but this reduces the verifiability and hence security of the network. After all, the philosophy of cryptos is that one does not need a third party, because everyone can verify each other's

[21] See for example RealT Real Estate: RealToken_White_Paper_US_v03.pdf.
[22] See Initial Coin Offerings (ICO's): serious risks | Topics AFM | AFM Professionals

balances and transactions. The only way to hide payment history from transacting parties is to make a separate public key for each of them. This is how criminals are able to hide their identity while laundering money or financing terrorism (Makarov & Schoar, 2021), but for most people this is not doable. For example, each public key requires a private key (crypto equivalent of a pin code) and if an owner loses their private key, all funds are lost. Furthermore, these properties also make ownership impossible to prove if multiple people have access to the same private key and/or if private keys are stolen (CPAB, 2022).

A trade-off exists between decentralisation, scalability and safety of crypto-asset infrastructures (see Annex). Decentralised and secure DLTs are not scalable enough, because they require the majority of the network to validate each transaction. As centralised infrastructures can be settled by one party (i.e. without reaching consensus among a network), they are by definition more scalable. In fact, some DLTs use significant amounts of energy to reach consensus (DNB, 2021b), but this may change in the future. Major ecosystems such as Ethereum have already made the switch to more environmentally friendly technology.[23] Some new crypto-asset infrastructures are more scalable, but often less decentralised. Networks may become increasingly centralised over time to increase scalability as new intermediaries start to play an important role (Aramonte et al., 2021). As these scalable crypto-asset infrastructures are relatively new, their security in terms of operational resilience and reliance will only become clear over the years to come.

So far, traditional intermediaries have been largely replaced by new intermediaries such as crypto companies and exchanges, and at least some role for intermediaries will remain. Although the promise of Web3 is to provide financial services without using intermediaries, i.e. by using automated protocols and stablecoins to facilitate fund transfers, in practice new intermediaries will arise. Developers need funds to create the technology, and they often raise these finds by selling the crypto-asset on exchanges. In turn, users can transfer crypto-assets without relying on any intermediaries, but they first need to buy them and get access to a wallet. The future will tell to what extent it will be possible to run a platform on a decentralised network. It is impossible to predict the extent of innovation this technology will bring, just as it was impossible to predict the internet's potential two decades ago.

In any case, the main opportunity of crypto-assets could best be leveraged under a regulatory regime that addresses their societal risks. Currently, crypto-asset issuers, service providers and markets are weakly regulated. This implies that activities and practices can take place that would not be allowed in traditional, regulated financial markets. This is exacerbated by their complex, anonymous nature with untransparent governance structures. Buyers should therefore be very cautious and aware of the risks before investing in these markets, and market conduct authorities should be given adequate tools to monitor and mitigate these risks. Regulation not only protects consumers/investors and the wider financial system, but it also provides regularity clarity and certainty, which helps the opportunities of the crypto-asset infrastructure to materialise. However, regulation and supervision are still evolving and will not eliminate all risks. Consumers and investors should remain aware of the risks before investing in these markets.

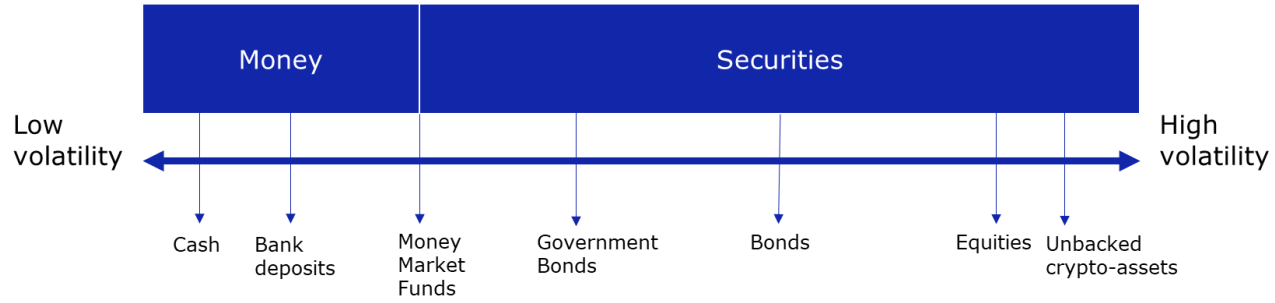
[23] See e.g.: The Merge: a blockchain revolution or just more hype? | Financial Times (ft.com).

3.2 Unbacked crypto-assets: money or speculative asset?

The opportunities and risks of the technology, or crypto-asset infrastructure, differ from those of the crypto-assets traded on the infrastructure. For example, people may say that they have bought Ethereum, while in fact they have bought Ether – the unbacked crypto-asset (or native coin) of the Ethereum blockchain. A relevant question is how such unbacked cryptos should be interpreted from an economic perspective. We start by discussing their ability to function as money. We then continue with an alternative explanation of unbacked crypto-assets as risky securities.

Unbacked cryptos lack the stability needed to function successfully as money. Money is anything people decide to accept as payment (means of exchange), use as saving (store of value) and use to communicate value (unit of account). Accepting unbacked crypto-assets as money is risky and costly, because the value of crypto-assets is volatile and exchanges may charge substantial fees. Figure 9 ranks different assets according to their volatility. On the left side of the figure is central bank money, which is backed by central banks and serves as an anchor for the monetary system. Next to it are bank deposits, which are interchangeable with central bank money and can be seen as private money. Unbacked crypto-assets are on the other side of the extreme. Hence, while unbacked cryptos have gained popularity as a speculative investment or even for gambling (as discussed in Section 2), their use in daily payments has remained limited.

Figure 9. "Moneyness" of financial assets



Source: own construction.

Limits to the supply of crypto-assets boosts price volatility. In principle, the supply of unbacked cryptos, as mere entries in a digital ledger, is limitless. Some unbacked crypto-assets therefore create artificial scarcity. The source code of bitcoin, for example, stipulates a maximum issuance of 21 million bitcoins. Crypto proponents see this as a better alternative for fiat money, as its prevents monetary policy from becoming overly expansive (Slagter & Slagter, 2021). The counterargument is that money supply, and monetary policy more generally, should respond to economic conditions. A fixed money supply leads to price volatility in case of demand shocks, and would be deflationary in a growing economy. Such price volatility is boosted further by the habit of crypto investors to hold their speculative investments for longer periods of time. By doing so, they effectively take coins out of circulation, which increases volatility and limits their use as a of form of money. In sum, the smaller the supply of a crypto, the more a change in demand affects the price, hence the more volatile that crypto is (Bolt & van Oordt, 2019).

Unbacked crypto-assets may function like unregulated securities. Successful new coins based on new DLT networks are typically created by traditional corporate entities (Ripple, BNB Chain, Algorand) or foundations

(Ethereum, Solana, Avalanche) that hire developers and might subsequently be transferred to Decentralised Autonomous Organisations (DAOs).[24][25] Developers often raise funds by collaborating with venture capital firms and by selling tokens or coins through initial coin offerings (ICOs)[26] (IOSCO, 2022). One might argue that an ICO could be compared to an initial public offering (IPO), implying that the crypto-assets issued classify as equity in the company. However, in many cases holders have no ownership, governance or profit rights in the entity, and suffer from weak legal protections and lack of control (Zetzsche et al., 2019). Only around 3% of ICOs have such rights attached and could classify as a security (Momtaz, 2020). In the end, only few unbacked crypto-assets may therefore fall under securities law[27] (ESMA, 2019).

As a security, unbacked crypto-assets are harder to value than traditional securities. The price of traditional securities such as equity shares depends on the potential of the underlying company, i.e. the business model and assets of the company. Unbacked crypto have no underlying assets or rights, which means their price is driven by the probability that the technology will gain a network of users (see Figure 10). The initial open source developers create a DLT protocol, which after its launch is supposed to function autonomously (see the Annex for an explanation). The DLT protocol thus has no owners and its code can be copied and reproduced by anyone. Its value lies in the network of people that use, develop and maintain the infrastructure. Hence, holders of unbacked crypto-assets have no shareholder or debtholder rights and there are no assets to resort to in case of a loss of confidence. Traders often have to rely on arbitrary technical analysis of price developments instead of expectations of future cashflows (Delfabbro et al., 2021).

Figure 10. Traditional financial assets (left) versus unbacked crypto-assets (right)

Company

Assets	**Capital**
	Traditional financial securities: equities & liabilities

?

Assets	**Capital**
	Unbacked crypto-assets

Source: own construction.

Therefore, the value of unbacked crypto-assets as securities is (also) uncertain and volatile. Prices of securities such as equities, bonds, derivatives, and exchange traded funds are determined based on supply and demand, which is fuelled by public information (and private estimations) about the value of the underlying assets, future cashflows and trustworthiness of issuing entities. As anyone can create new crypto-assets, according to some sources up to 80% of ICOs may be fraudulent, i.e. where crypto-assets either do not exist or the developers disappear after the ICO (ESMA, 2019). But even when ICOs are not fraudulent and the coin gets listed on a crypto exchange, about 40% still reportedly fail and get delisted, after which the coin becomes worthless (Momtaz, 2020). For example, the underlying technology could fail (hacks, coding errors etc.) or the investors could abandon the

[24] A DAO is an entity structure in which there is no central management. Instead, holders of distributed governance tokens vote on decisions which are posted on a blockchain (IOSCO, 2022).
[25] For example, Cardano positions itself like a DAO, but is supported by the Cardano foundation to set standards, by an enterprise arm called EMURGO to boost the platform through commercial ventures, and by a technology and engineering company (IOHK) to design, build and maintain the Cardano platform. See the Cardano website: Cardano | Discover Cardano.
[26] In an ICO, developers usually first issue a token to raise funding, which may later be changed into a coin or other utility related to the project (IOSCO, 2022). ICOs are often unregulated, untransparent and susceptible to fraud, misleading/incomplete documentation, and market manipulation, see: Initial Coin Offerings (ICO's): serious risks | Topics AFM | AFM Professionals.
[27] The SEC argues that the issuance of Ripple coins classifies as unregistered security issuance, but the outcome of the lawsuit is uncertain, see SEC.gov | SEC Charges Ripple and Two Executives with Conducting $1.3 Billion Unregistered Securities Offering, accessed on 5 October 2022.

project because of limited interest. Finally, even successful ICOs present important risks as developers and venture capitalist firms can exploit investors. Issuers often hold around 10% - 50% of total coins themselves (Auer et al., 2022; Aramonte et al., 2021), which allows them to benefit from future price increases and influence the price of their coin by changing the amount of coins in circulation.

As a speculative asset, crypto-assets present significant risks with respect to consumer and investor protection and the functioning of markets. Consumer and investor protection organisations and market conduct authorities – such as the AFM in the Netherlands – regularly warn for a partial or total loss of the invested amount (IOSCO, 2020a). The main risks for investors in crypto markets include market illiquidity (meaning crypto-assets cannot be sold), price volatility and counterparty risk from crypto-asset brokers, trading platforms, custodial wallet providers and other intermediaries. Moreover, there are risks to market integrity (fraud, theft, market abuse) as crypto markets and infrastructures do not operate fairly and securely. Information may be missing, inaccurate, incomplete and unclear with respect to the risks. This could lead to certain investors being disadvantaged compared to others. Retail investors in particular may be at risk, also since crypto exchanges often offer crypto-assets directly to consumers. There may be no proper on-boarding to prevent illegal and fraudulent sellers along with investors with insufficient knowledge or unsuitable risk-appetite from trading on the exchange (see Annex).

Crypto-assets could reach a point where they represent a threat to global financial stability due to their scale, structural vulnerabilities and increasing interconnectedness with the traditional financial system (FSB, 2022a). The IMF (2021) also reports that financial stability risks from the crypto ecosystem are not yet systemic, but this could change over time if growth continues and interconnectedness with the traditional financial sector increases. Risks should be closely monitored given the global implications and the inadequate operational and regulatory frameworks in most jurisdictions. Moreover, the rapid growth in Decentralised Finance has been compared to the growth in shadow banking as it happened before the Global Financial Crisis (Allen, 2022). The FSB (2022a) highlights four potential transmission channels between crypto-assets, the broader financial system and the real economy: (1) financial sector exposures, (2) wealth effects for crypto owners, (3) confidence effects, and (4) the use of crypto-assets in payment and settlement systems.

3.3 Stablecoins: stable?

Stablecoins add a stabilisation mechanism to unbacked crypto-assets. Asset backing implies that a balance sheet is added and that the assets back-up the value of the stablecoins (see Table 3). This gives stablecoins a financial design comparable to existing forms of money or investment, depending on their exact balance sheet structure. It also leads to financial risks and creates a direct link with the broader financial system, which creates risks for financial stability. However if some stablecoins managed to live up to their promise of stability both sustainably and credibly, the crypto opportunities would be closer to becoming realities, e.g. in relation to Web3, cross-border payments, and settlement of tokenised assets.

Table 3. Stylised stablecoin balance sheet

Assets	**Liabilities**
"Safe and liquid" assets [Regulatory option: liquidity buffer]	**"Stablecoins"** [Regulatory option: capital buffer]

Source: Bolt *et al*. (2022).

The stability of stablecoins is influenced by their peg and backing. Although most current stablecoins reference a single fiat currency, some may also reference other assets or multiple fiat currencies. In this case, they are not stable relative to the official fiat currency. At the same time, they could have a credible backing. Table 4 classifies crypto-assets based on these two perspectives on their stability. The horizontal axis shows the difference between backed and unbacked crypto-assets. The vertical axis shows the difference between those crypto-assets that are volatile vis-à-vis a fiat currency and those that are intended to be stable vis- à-vis a fiat currency.

Although most stablecoins are pegged to a stable fiat currency, the backing of stablecoins is not necessarily credible. As discussed, almost all existing stablecoins reference the dollar, although they may not have the same amount of assets in dollars in custody at all times. Moreover, key issues revolve around the presence of these assets, redemption rights (e.g. when and whether the stablecoins can be exchanged for the underlying assets) and whether fees apply (FSB, 2022d; PWG, 2021). Most current stablecoins are issued by unregistered and unlicensed entities and do not have credible mechanisms to support their promise of price stability (FSB, 2022d). Moreover, "algorithmic stablecoins" are intended to be stable vis-à-vis a fiat currency, but are issued through an algorithm created on a blockchain and are not backed by assets outside the crypto ecosystem. Algorithmic stablecoins are therefore essentially unbacked crypto-assets (see Table 4).

Table 4. classification of crypto-assets

	(Supposedly) backed crypto-assets	Unbacked crypto-assets
Volatile vis-à-vis single fiat currency	Asset-referenced tokens (ARTs), e.g. Libra, Tether Gold	Unbacked crypto coins/tokens, e.g. Bitcoin, Ethereum
Intended to be stable vis-à-vis a single fiat currency	E-money tokens (EMTs), e.g. USD Tether, USD Coin	Algorithmic stablecoins, e.g. Dai, Terra USD (which collapsed, see Box 1)

Source: own construction based on EC (2020a).
Note: The European Commission further distinguishes between backed crypto-assets using a stabilisation mechanism that refer to a fiat currency – e-money tokens (EMTs) – and those that refer to other assets[28] – asset-referenced tokens (ARTs) (EC, 2020a).

History has shown that stablecoin constructions are risky (Frost *et al*., 2020). Once adoption and trust have initially been established, a private entity may have an incentive to increase the return on its assets, e.g. by moving to higher yielding, more risky assets (or even loans), decreasing coverage, and restricting redeemability (e.g. imposing redemption fees or limiting – "not at par" – convertibility). The asset backing may be deliberately opaque to avoid revealing that full backing may be lacking. However, panics arise when information-insensitive debt turns into information-sensitive debt. This usually happens following a negative shock, when investors start to doubt whether the net asset value is enough to cover all withdrawals and they begin to fear that they might not get their full claim back (Gorton & Zhang, 2021; Holmstrong, 2015).

Nevertheless, some stablecoins function as money within crypto ecosystems. Buyers often use stablecoins to pay for unbacked crypto-assets and sellers to sell unbacked crypto-assets. (Liao and Caramichael, 2022). In this process, stablecoins effectively function as money and facilitate a large volume of digital asset trading. In fact, approximately 75% of trading on centralised exchanges involves a stablecoin (BoE, 2022). The same holds for

[28] More specifically: "the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets".

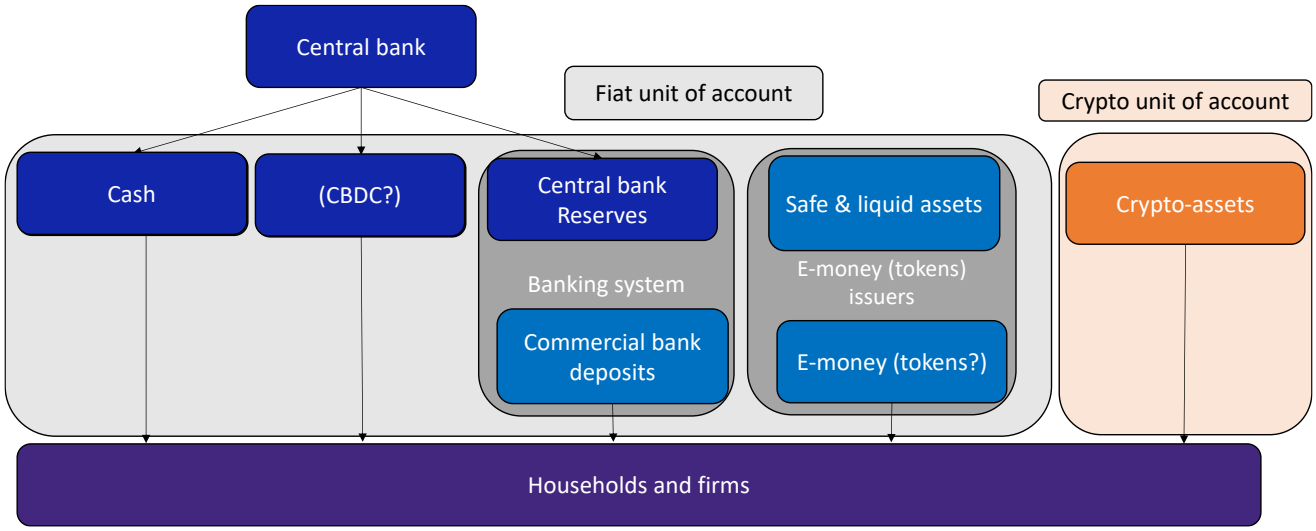
crypto borrowing/lending, where borrowers often borrow stablecoins against volatile collateral in the same way as money is borrowed from banks with assets as collateral.

Further adoption of unregulated stablecoins would therefore carry risks for the functioning of financial market infrastructures. Stablecoins may perform a transfer function similar to other types of financial market infrastructures. The same risks therefore apply: systemic risk, legal risk, credit risk, liquidity risk, general business risk, custody and investment risks and operational risk. Stablecoin arrangements present new ways for such risks to materialise, e.g. due to uncertainty about their backing (run risk), the lack of identifiable legal entities that assume responsibility for the transfer function, and uncertainty as to when settlements on DLTs can be considered final. A tailored application of the Principles for Financial Market Infrastructures is therefore needed to address risks in systemically important stablecoin arrangements, since disruption of critical financial market infrastructures could undermine financial stability (CPMI/IOSCO, 2022, and section 4).

3.4 Monetary implications

We now investigate the implications for the monetary system as a whole. The previous sections discussed the potential adoption of new technologies and the "moneyness" of crypto-assets. The next question is how it all fits together. Our discussion is centred on Figure 11, which provides an overview of current and potential forms of money available to households and firms.

Figure 11. Implications for the future monetary system



Central bank digital currency (CBDC) can be seen as a technological update of cash. We start on the left-hand side of Figure 11, which contains central bank money. Central bank money is the most safe and liquid form of money. It is supported by the fiat of the government, the balance sheet of the central bank (Broeders and Wessels, 2022), and central bank institutions geared towards public policy objectives. Cash is central bank money in a physical form, but its use is declining due to the digitalisation of payments (DNB, 2022a). To safeguard access

to central bank money, central banks around the world are developing CBDC. This includes the Eurosystem (see Eurosystem, 2020 or the ECB website[29] for more in-depth analyses of the digital euro). Like cash, the digital euro would be central bank money, but now in an electronic form. A digital euro would not be defined by its technology but by its issuance by the ECB and the national central banks. The investigation phase for a digital euro started in 2021 and will be concluded by the end of 2023. At the end of 2023 a decision will be made on the further development of a digital euro.

Central bank reserves and commercial bank deposits are used to transmit monetary policy. Moving one step to the right in Figure 11, we see the interplay between central bank reserves and commercial bank deposits. Banks hold reserve accounts at the central bank[30], while households and firms hold accounts at commercial banks. This is the two-tier banking system that provides the backbone of the payment system and monetary policy. The monetary policy stance determines the conditions under which commercial banks can get funding from the central bank, which in turn transmits to households and firms. Public policy objectives play an important role, as banks are subject to regulation, supervision, resolution policies and monetary policy, to maintain the trust and stability of the monetary and financial system.

Most crypto-assets fall outside this regulated monetary system. The unlikely adoption of these assets as money would thus put the uniformity of money at risk. When we look at the right side of Figure 11, we see that most crypto-assets fall outside this regulated monetary system. They do not use a fiat unit of account such as a euro or dollar. Brunnermeier and Landau (2022) argue that if households and firms were to adopt a crypto unit of account, the uniformity of money could be put at risk. Central banks would risk losing their monetary sovereignty. Monetary policy would become blunted by the proportion of products priced in this unit of account. We have argued that it is unlikely that unbacked crypto-assets will be used as money at a significant scale, but rather that they will function as risky securities. The likelihood of multi-currency stablecoins becoming a unit of account is also estimated to be low, at least in developed countries with a comparatively well-developed payment infrastructure and low inflation levels (ECB, 2020). Adoption may be higher in high-inflation countries, however, where unbacked crypto-assets may rival the local currency.

Well-backed stablecoins that use the fiat money unit of account are functionally equivalent to electronic money. We now turn to the middle of Figure 11, to arrive at the lesser known and least used asset that currently takes on functions of money: electronic money. E-money is functionally equivalent to stablecoins that are intended to be stable vis-à-vis a single fiat currency. The difference is the technology used. Stablecoins are based on DLT, while e-money is based on conventional technology. It is defined as an electronic store of monetary value on a technical device that may be used for making payments to entities other than the e-money issuer. E-money can only be issued by credit institutions or e-money institutions, which are regulated under the E-money directive (EC, 2009). Among other things, this directive requires backing by safe assets and one-to-one convertibility with a fiat currency (often the euro if it is issued in the European Union). This is why those stablecoins that function like e-money are called e-money tokens (see Table 4). Section 4 on the regulatory response discusses how the regulatory regimes for e-money and e-money tokens will be aligned.

E-money as issued by e-money institutions falls outside the monetary policy framework. E-money can be issued by credit institutions or e-money institutions. E-money institutions do not have access to central bank

[29] A digital euro (europa.eu).
[30] Financial market infrastructures and governments also hold accounts at the central bank.

money. They do not hold loans or extend credit either, but instead hold safe and liquid assets like short term government bonds or bank deposits. Since e-money falls outside the monetary policy framework, the question arises of how this impacts its effectiveness. The ECB has expressed concerns about the issuing of e-money by non-credit institutions (ECB, 1998, 2008, 2021a). The main argument against it is that implementation of monetary policy in the euro area would become increasingly difficult and the desired policy outcomes more uncertain. So far, this discussion has not become urgent in practice, given that e-money was intended for small scale use and never became systemic. However, technological developments now raise the possibility that the use of e-money tokens (a type of stablecoin) may grow in the future, as a result of their specific use cases.

Adoption of e-money at a larger scale would have less far-reaching consequences than adoption of other crypto-assets, but would still have implications for monetary and financial stability. Inflows and outflows of bank deposits to and from stablecoins that use the fiat unit of account also have an impact on banks' liquidity and credit intermediation. Banks may need to shift to more expensive sources of funding, thereby potentially increasing the cost of credit for households and smaller, bank-dependent firms. The actual effects depend on the type of backing, such as bank deposits, government bonds or central bank reserves (BoE, 2021). In the scenario where stablecoins are backed by bank deposits, this could create a system in which stable retail deposits are replaced with institutional stablecoin deposits. A run on the stablecoin would also lead to a sudden deposit withdrawal from these banks. In the scenario where stablecoins are backed by safe assets, such as euro-denominated government debt, runs on a stablecoin would translate to price and interest volatility in these markets (ECB, 2020).

Different solutions have been brought forward to avoid a potential loss of monetary policy effectiveness due to possible stablecoin adoption. In the US, the President's Working Group proposed to "*limit stablecoin issuance, and related activities of redemption and maintenance of reserve assets, to entities that are insured depository institutions*." This solution would bring stablecoins directly within the remit of monetary policy. However, this may not be the most appropriate solution for entities that only want to provide payment services related to e-money, but not issue loans (as they are not banks) (Bolt et al, 2022). In the EU, the EC (2020a) proposes a different solution: to align e-money and stablecoin regulation. It proposes to include limits and more stringent requirements for systemically important issuance of e-money tokens. The next section on the regulatory response therefore includes the main proposals from this perspective.

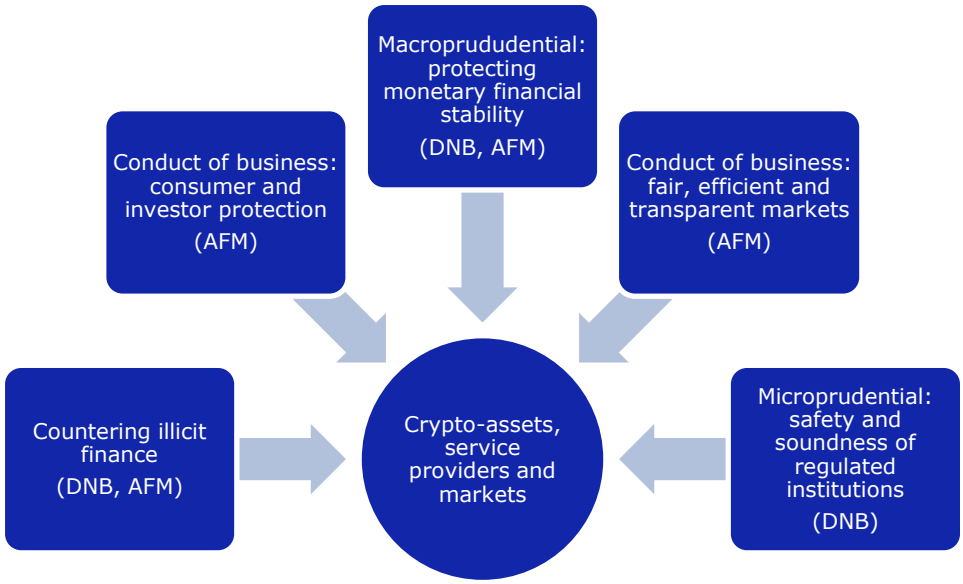
4 Regulatory response

4.1 Objectives

In view of the size and impact of crypto markets, the need for regulation is evident. As in any financial market, market failures will occur – and have occurred – in crypto markets. The need to protect financial stability, consumers and investors, market functioning and the integrity of the financial system applies in crypto markets just as it does in traditional parts of the financial system. The form and intensity of financial regulation will need to be proportional to the underlying risks. The main challenge is to achieve a balance between the benefits that crypto-assets and underlying technologies can bring, and the risks they pose to society.

To the extent that crypto-assets provide similar functions and pose similar risks as traditional financial instruments, they should be subject to similar regulation. Crypto-assets do not operate in a regulation-free space and must adhere to relevant existing requirements to address the risks they pose (FSB, 2022b). Regulation therefore applies to the different functions of crypto-assets. For example, crypto-assets could be designed to function as a electronic money, but they could also be a digital representation of a security and/or derivative. As a result, they may be incorporated into existing regulation (e.g. anti-money laundering and countering the financing of terrorism (AML/CFT), securities and banking law), or may require new regulation (e.g. the Markets in Crypto-Assets Regulation, see below). Figure 12 provides a high-level overview of applicable objectives of financial regulation, and the authorities responsible for financial supervision and oversight in the Netherlands. For all these objectives, international standards have been adopted or are under development, which helps to provide more clarity as to which crypto-asset functions fall under which legislation. (He *et al*., 2022).

Figure 12. Objectives of financial regulation applied to crypto-assets (and relevant supervisory authority in the Netherlands)



Source: own construction.

Table 5. Recent reports from International Standard Setting Bodies

Topic, institution		**Report**	**Main output**
Macroprudential: Financial stability	FSB	Regulation, supervision and oversight of crypto-assets and markets (2022c)	High-level recommendations to authorities to ensure that crypto-assets and markets fulfil general requirements, e.g. as regards governance, risk management and transparency.
		Review of the FSB high-level recommendations of the regulation, supervision and oversight of "global stablecoin" arrangements (2022d)	Review of the high-level recommendations for stablecoin arrangements, including how any gaps identified could be addressed, considering recent market and policy developments.
		Regulation, supervision and oversight of "global stablecoin" arrangements (2020)	High-level recommendations to address the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements.
	CPMI/ IOSCO	Application of the PFMI to systemically important stablecoin arrangements (2022)	Final guidance on the application of the PFMI to systemically important stablecoin arrangements.
Microprudential: regulated institutions	BIS/BCBS	Consultative document on prudential treatment of crypto-asset exposures (2022)	Standards for the prudential treatment of crypto-assets.
Conduct-of-business: investor protection and fair, efficient and transparent markets	IOSCO	Decentralised finance report (2022c)	Overview and risks of the decentralised finance market.
		Issues, risks and regulatory considerations relating to crypto-asset trading platforms (2020b)	Summary of IOSCO principles and regulatory approach to crypto-asset trading platforms.
		Investor education on crypto-assets (2020a)	Overview of risks for retail investors investing in crypto-assets. Guidance on investor education materials and risk warnings.
Illicit finance: anti-money laundering and countering-terrorist financing	FATF	Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers (2022)	Targeted review and update of implementation of FATF recommendations, as well as emerging risks and market developments that FATF monitors, such as Decentralised Finance (DeFi), Non-Fungible Tokens (NFTs), and unhosted wallets.
		Virtual asset and virtual asset service providers. Updated guidance for a risk-based approach (2021)	Guidance on the application of the FATF recommendations to virtual assets and virtual asset service providers.

Source: own construction.

International standards play an important role in harmonising the regulation and supervision of crypto-assets across sectors and countries. International cooperation is crucial due to the international reach of crypto activities. Cooperation has intensified recent years at the level of the international standard setting bodies (SSBs), which the Financial Stability Board (FSB) coordinates and to which DNB actively contributes (DNB, 2022a). Table 5 provides a high-level overview of the results produced so far, for different standard setters with different mandates.

International standards produced by SSBs are influenced by the input from all participating jurisdictions. The SSBs' guidance in turn influences local legislation, including EU legislation.

4.2 Countering illicit finance

AML/CFT regulations have been adjusted over the past years to address the use of crypto-assets for criminal purposes. The anonymous and cross-border nature of crypto-assets raises the risk of money laundering and the financing of terrorism, as well as sanctions evasion. A consistent implementation of the Financial Action Task Force (FATF) standards across jurisdictions is therefore essential. The FATF monitors progress made by FATF participating countries in implementing the AML/CFT standards (FATF, 2021 and 2022). It concludes that – although many jurisdictions have continued to make progress – most of them still have not implemented the full extent of the standards. These gaps facilitate regulatory arbitrage, because crypto-asset service providers can operate remotely from anywhere around the world. In response, the Anti-Money Laundering Directive (AMLD) has been adjusted in recent years so that it applies to: i) crypto-asset service providers engaged in exchange services between virtual currencies and fiat money; and ii) crypto custodial wallet providers that provide services to safeguard private cryptographic keys on behalf of their customers to hold, store and transfer virtual currencies.

As of the end of October 2022, DNB has granted 34 registrations to crypto service providers, while 9 are still being processed, and 41 requests for registration have been retracted. DNB is responsible for risk-based supervision of compliance by crypto-asset service providers and custodial wallet providers (as mentioned above) with the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft*), more specifically regarding topics such as customer due diligence, transaction monitoring and the reporting of unusual transactions to the Financial Intelligence Unit (FIU-NL). DNB is in close contact with public partners such as the prosecution office, the police and the FIU-NL to further the goals of the *Wwft*.

DNB has also taken action against providing services without a registration. Most breaches were stopped before a formal measure was imposed, while in some cases, a process of enforcement was started. On 18 August 2021, DNB issued a warning against Binance[31], and on 25 April 2022, DNB imposed a fine of EUR 3,325,000 to Binance for offering crypto services in the Netherlands without a registration.[32] Last but not least, DNB is responsible for supervision of compliance with the Sanctions Act 1977 (*Sanctiewet 1977*), which requires registered crypto service providers to identify clients on the sanctions list and to prevent breaches of sanctions legislation.

The AML framework is currently under revision, and Europe has recently reached agreement on a revised Transfer of Funds Regulation (TFR). The proposed changes widen the range of crypto-asset service providers (CASP) in the scope of the AML framework (including all CASP services under MiCAR, see below), put in place a European supervisory authority for high-risk entities, and include a direct regulation to strengthen harmonisation across countries. These changes should foster a level playing field and overcome regulatory arbitrage across countries within the European Union. In addition, the transfer of crypto-assets has been brought into the scope of the TFR regulation. TFR will require crypto-asset service providers to send information about the sender and receiver with the transaction, for all transactions in crypto-assets. The extent to which unhosted wallets will be

[31] DNB warns against Binance
[32] Boete voor Binance Holdings Ltd. vanwege het zonder de wettelijk vereiste registratie aanbieden van cryptodiensten (dnb.nl)

subject to these requirements is still under discussion. This obligation is new to crypto-asset service providers but information about the counterparty is already gathered to a certain extent in order to comply with the Sanctions Act (existing regulation). However, there is currently no requirement to send the information to the beneficiary's CASP. The TFR requirements already apply in full to transactions facilitated by banks or payment institutions and aim to make criminal money flows traceable. The TFR requirements are impactful for crypto service providers, as this requirement poses a technological challenge and may affect transaction speed.

4.3 Prudential and conduct of business regulation

Existing security, payment and banking regulation

Crypto-assets are also incorporated into existing banking, payments and securities regulation. Existing financial services legislation aims to protect monetary and financial stability, the security and soundness of regulated institutions, consumers/investors and fair efficient and transparent markets. In principle, new regulation is only needed where issuers, service providers and crypto-assets are not covered elsewhere under financial regulation.

Firstly, issuers and service providers of crypto-assets that qualify as securities are in principle subject to securities law, but new regulation is needed for the majority of crypto-assets. The European Commission has clarified that the existing definition of financial instruments, which is of key importance for defining the scope of EU financial services legislation (including the Market in Financial Instrument Directive/Regulation (MiFID/MiFIR) and other securities legislation), includes financial instruments based on DLT (EC, 2020c). Hence, in case backed crypto-assets qualify as tokenised financial instrument in the EU, they are to be treated as financial instrument. Complementarily, the new DLT pilot regime should allow DLT market infrastructures to be temporarily exempted from some specific requirements that could prevent the development of solutions for the trading and settlement of transactions in crypto-assets that qualify as financial instruments. This gives regulatory clarity, while the relevant authorities can gain experience with the opportunities and risks created by crypto-assets that qualify as financial instruments, and with their underlying technology (EC, 2020c). However, the majority of existing crypto-assets do not qualify as financial instrument and thus require new regulation (EC, 2020a).

Secondly, issuers of stablecoins that qualify as electronic money will be subject to the e-money directive. Due to the functional equivalence between e-money and e-money tokens (EMTs) [33], the MiCAR proposal clarifies that EMTs are to be deemed electronic money as defined in the existing e-money directive. Moreover, the scope of the Eurosystem oversight framework for electronic payment instruments, schemes and arrangements (PISA) has been extended to representations of value backed by claims or assets denominated in euro or redeemable in euro (ECB, 2021b). PISA in turn is based on the Principles for Financial market infrastructures (PFMI), which have been applied to systemically important stablecoin arrangements (CPMI/IOSCO, 2022, see Table 5).

Lastly, crypto-assets will also be incorporated in European banking legislation, following finalisation of international standards. The BCBS consultation proposal differentiates the prudential treatment for exposures to two groups of crypto-assets: (*i*) tokenised versions of traditional assets (including securities) and stablecoins,

[33] 'electronic money token' or 'e-money token' means a type of crypto-asset whose main purpose is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender, see EC (2020a).

and (*ii*) crypto-assets that fail to meet the classification requirements for group 1 (BCBS, 2022). According to these proposed standards, unbacked crypto-assets have conservative risk weights (i.e. 1250% of risk weighted assets), while the risk weights of backed crypto-assets depend on the asset that is tokenised. DNB is in favour of such a simple and conservative prudential treatment of banks' holdings of crypto-assets. More risk sensitivity could be added to the proposed standard, but without compromising on the conservative nature of the prudential treatment of crypto-assets. A next step is to update international standards for banks that issue stablecoins. After finalising the global standards, these are still to be incorporated in European legislation.

Tailored crypto-asset regulation

New tailored regulation is also needed, since many issuers and crypto-assets are not covered elsewhere under financial regulation. The European commission has highlighted three main reasons why a tailored crypto-asset regulation is necessary (EC, 2020a). Firstly, the majority of unbacked crypto-assets falls outside the scope of securities regulation, as they have no rights or assets attached. Secondly, stablecoins may become systemic in nature and/or may have a different unit of account, which poses additional risks for monetary and financial stability compared to e-money (see also Section 3.4). Thirdly, the services offered by crypto-asset service providers, such as wallet providers and exchanges, differ from traditional financial services, because the technology differs.

The Markets in Crypto-Asset Regulation (MiCAR) is therefore a welcome step in the regulation of crypto-assets (DNB, 2022b)[34]. It provides uniform rules for crypto markets, which is important for investors in crypto-assets and for the stability and integrity of the crypto ecosystem. DNB calls on market participants to prepare for the new MiCAR rules, which are expected to take effect in 2024. Under MiCAR, issuers of stablecoins or anyone offering crypto services must obtain a licence to do so from a financial supervisor. This licence allows MiCAR-regulated activities to be undertaken in all countries in the European Economic Area. In this respect, it is essential that the transition from current national regimes to the MiCAR regulation is carefully structured.

MiCAR regulates those crypto-assets outside the scope of securities regulation. It contains a clear separation for tokenised financial instruments such as securities, for which MiFID/MiFIR will be applied, and crypto-assets that fall under the new MiCAR regime. Those crypto-assets in turn are then separated into stablecoins, i.e. e-money tokens (EMTs) and asset-referenced tokens (ARTs), and other crypto-assets.

Actors in the crypto-assets market will be required to declare information on their environmental and climate footprint.[35] The European Securities and Markets Authority (ESMA) will develop draft regulatory technical standards on the content, methodologies and presentation of information related to principal adverse environmental and climate-related impact. Within two years, the European Commission will have to provide a report on the environmental impact of crypto-assets and the introduction of mandatory minimum sustainability standards for consensus mechanisms, including the proof-of-work

Unbacked crypto-assets are subject to requirements that include transparent information provision. MiCAR regulates the liability of crypto-asset issuers, imposes some basic disclosure requirements and prohibits any form of market manipulation and insider trading. However, risks remain and requirements appear lighter than under

[34] The Council Presidency and the European Parliament reached provisional political agreement in June 2022, See Digital finance: agreement reached on European crypto-assets regulation (MiCA) - Consilium (europa.eu), accessed on September 30th 2022. It should be noted that the final version of MiCAR is not yet available, this analysis is based on the public proposal (EC, 2020a) which is susceptible to change – no rights can be derived from this analysis.

[35] See Digital finance: agreement reached on European crypto-assets regulation (MiCA) - Consilium (europa.eu).

existing securities regulation. For example there are no requirements related to the development and distribution of crypto-assets (AFM, 2022). MiCAR also contains a ban on activities that may lead to market manipulation and insider trading and requires crypto-asset service providers (CASPs) to put in place surveillance and enforcement mechanisms to deter potential market abuse. However, enforcement issues remain as crypto-asset issuers have limited obligation to report data, which makes market manipulation difficult to trace and sanction (AFM, 2022).

Issuers of stablecoins require authorisation and are subject to stricter requirements than other crypto-assets (EC, 2020a). EMTs are backed by fiat currency and regulated as e-money[36], while asset-referenced tokens (ARTs) are backed by a combination of other assets. In both cases, stablecoin issuers are subject to general obligations, i.e. to issue a whitepaper, make sure assets are segregated and are not encumbered, have minimum own funds, disclosure, behaviour, governance, and communication requirements, prevention of conflict of interest, prohibition to provide interest, and to have a complaint handling procedure in place. However, EMTs and ARTs differ with respect to the claim, authorisation, investment of funds, redemption rights and limits as a means of exchange, which are summarised in Table 6.

Table 6. Specific requirements for ARTs and EMTs

Requirements	**ARTs**	**EMTs**
Claim	Holders have claim at market value	Holders have claim at par value
Authorisation	Authorisation under MiCAR	Credit/e-money institution
Investment of funds	Disclosure of tokens in circulation, value and composition of reserve assets every month, half-year audits. Investment of reserve assets in other assets (than referred to) is possible only in highly liquid instruments with minimal market and credit risk where profits/losses are borne by the issuer.	Safe & liquid assets denominated in the same currency as the one referenced by the EMT, i.e. government bonds, bank deposits, central bank reserves.
Redemption rights	Policy on redemption rights with minimum rights.	Holders may redeem at all times, at par value.
Use as means of exchange	Above a threshold, issuers of ARTs must report their use as a means of exchange within the euro area; their use will be restricted.	Use as means of exchange allowed for EMTs denominated in a currency which is the official currency of an EU Member state, use of EMTs denominated in other currency is restricted.

Source: own construction.

Stablecoins that may pose a risk to monetary and financial stability are subject to additional requirements and restrictions. This includes additional macro-prudential requirements for those e-money tokens that are deemed significant, since they could be used by a large number of holders and which could raise specific challenges in terms of financial stability, monetary policy transmission or monetary sovereignty. These will be supervised by the European Banking Association (EBA) and subject to higher requirements for own funds, stricter rules on custody and liquidity management, and stress tests. In addition, in view of the risks to monetary

[36] E-money is defined as an electronic store of monetary value that may be used for making payments to entities other than the e-money issuer. The e-Money Directive (EMD) requires, among other things, backing by safe and liquid assets and one-to-one convertibility with a fiat currency (EC, 2009).

sovereignty, the use of ARTs and non-euro EMTs as a means of exchange within the euro area will be monitored and restricted. Moreover, authorisation may be withdrawn in case the central bank issues an opinion that the ART poses a serious threat to monetary policy transmission, smooth operation of payment systems or monetary sovereignty.

Table 7. Crypto-asset services regulated under MiCAR compared to investment services and activities

Crypto-asset services under MICAR	**Existing regulation: with respect to investment services and activities under MiFID/MiFIR**	**Obligations under MiCAR**
The custody and administration of crypto-assets on behalf of third parties	Providing portfolio management for financial instruments	Contractual arrangements with clients, register of positions of clients, asset segregation, liability.
Operation of a trading platform for crypto-assets	Operation of a multilateral trading facility or organised trading facility	Operating rules, prohibition of trading on own account for the CASP, resilience of the trading systems, pre- and post-trade transparency, obligation to settle transactions in the DLT.
Exchange of crypto-assets for fiat currency that is legal tender; exchange of crypto-assets for other crypto-assets	Proprietary trading	Non-discriminatory commercial policy, obligation to publish a firm price, execution at the price displayed at the time of receipt, transparency on orders and transactions.
Execution of orders for crypto-assets on behalf of third parties	Execution of orders	Best execution, clear information to clients on the execution policy.
Placing of crypto-assets	Placing of financial instruments	Clear agreement with the issuer before the placing, specific rules on conflicts of interest.
Reception and transmission of orders for crypto-assets on behalf of third parties	Reception and transmission of orders for financial instruments on behalf of third parties	Prompt transmission of orders, prohibition of non-monetary benefits, no misuse of information related to client orders.
Providing advice on crypto-assets	Providing advice on financial instruments	Necessary skills and knowledge, assessment of crypto-assets with the needs of clients.

Source: own construction based on public sources such as EC (2020a).

Crypto-asset service providers (CASPs) will also need to apply for authorisation. The services they provide are to be regulated as stated in the EC proposal are listed in Table 7 (EC, 2020a). In this respect, MiCAR could be seen as a crypto version of the investment services and activities in MiFID/MiFIR. Next to the specific obligations listed in Table 7, CASPs will also have general obligations, such as behavioural, organisational and prudential capital requirements, rules related to the safekeeping and segregation of clients' crypto-assets and funds, complaint handing procedures, and rules regarding the prevention of conflict of interest and outsourcing. However, it should be noted that where MiFID/MiFIR already specify detailed level 2 regulation, level 2 regulations under MiCAR are still to be drafted. Moreover, as with most financial regulation, it seems likely that future revisions of MiCAR will be needed to adapt to the regulatory challenges that emerge over time.

4.4 Supervision and enforcement

Crypto-asset issuers and service providers must adhere to relevant existing requirements to address the risks they pose. Experience has now been gained with AML/CFT supervision with respect to crypto-assets, but enforcement of new legislation obviously only starts after it has been enacted. We list some of our preliminary considerations below, while recognising this early stage of development.

Requiring entities to report official data to supervisory and oversight authorities is key for supervision and enforcement. At the moment, data to properly assess risks and monitor compliance is lacking. Although blockchains provide public data, supervisory and oversight authorities need data on the specific parties in crypto markets, such as developers, crypto-asset service providers and issuing entities to monitor whether they comply with regulation. As long as there is no requirement for reporting underlying data to authorities, authorities cannot monitor compliance and enforcement becomes difficult (AFM, 2022).

One possible avenue that may foster supervision and compliance in the future, although not a "silver bullet", is to experiment with code-based regulation. Once the code has been written, protocol-based transactions have the potential to run autonomously (although human beings still run the computers, and intermediaries also play an important role). For such transactions, compliance will need to be reflected in the source code itself. As an example, some suppliers already offer solutions that integrate Know Your Customer compliance into decentralised applications. One way forward could be to encourage industry-based and regulatory standards for source code protocols, for instance with respect to anonymous transactions (He *et al*., 2022, of the IMF, raise a similar point). It would also require that supervisors develop deeper knowledge in the field of coding, and could pose difficulties given that there is no guarantee that regulatory standards will remain embedded in codes due to decentralised decision-making.

Direct supervision and enforcement on unbacked crypto-assets is possible through regulated entities that provide interaction points with the traditional financial system. Enforcing only direct regulation of unbacked crypto-assets might be challenging, because the legal entity behind many crypto activities may be unknown. However, enforcement is also possible indirectly through regulated entities that provide crypto-asset services. Important interaction points providing a regulatory anchor point are the issuers of backed crypto-assets and crypto-asset service providers (CASPs). For example, not allowing a crypto exchange to offer an unregulated crypto-asset might complement efforts to sanction unidentified developers in case they do not comply with the legal framework. The same applies to issuers of backed crypto-assets, which are the bridge between traditional assets and crypto-assets. This is also the approach taken under MiCAR, i.e. no crypto-asset may be offered via regulated crypto-asset service providers unless this crypto-asset meets specific requirements (in case of unbacked crypto-assets) or the issuer has been authorised (in case of backed crypto-assets).

At the same time, enforcing regulation for large, internationally active entities remains challenging, as they often offer their services remotely. Large, internationally oriented players may choose to be located in lightly regulated jurisdictions.[37] They offer their services remotely, which means it may be difficult to evaluate whether they target the Dutch market. Alongside intervention by the local supervisor (as mentioned above), this

[37] Based on daily turnover, the 10 largest exchanges are headquartered in the Cayman Islands, Bahamas, Belize, Seychelles, South Korea, Singapore, and the US. Source CoinMarketCap: Top Cryptocurrency Exchanges Ranked By Volume | CoinMarketCap, accessed summer 2022.

also requires enhanced international cooperation with respect to compliance. Crypto exchanges that operate in the Netherlands are already required to register with DNB and to comply with AML/CFT and sanctions legislation. DNB will start an investigation if there are indications that they serve the Dutch market without a registration. Most breaches were stopped before a formal measure was imposed, while in some cases, a process of enforcement was started.[38] When MiCAR enters into force, CASPs and issuers of stablecoins will need to apply for authorisation and comply with the relevant requirements, which will be jointly supervised by both the AFM and DNB.

4.5 Challenges for the regulatory regime

The evolution of crypto-assets regulation has only just begun. Given the observations described above, we identify three overarching challenges regulators will need to address in the coming years.

A first challenge is to continue international cooperation, especially in light of large, internationally active market players that operate remotely. While international consensus is emerging on the main requirements for crypto-assets, there are differences between jurisdictions, which is to be expected in view of the early stage of evolution of the regulatory approach. Crypto-asset service providers that provide cross-border services should comply with the regulations of the jurisdictions where they offer their services, even if they are themselves located in lightly regulated jurisdictions. Coordination also remains needed with respect to regulation itself. For example, the US Presidents' Working Group (PWG, 2021) proposed regulating stablecoins as bank deposits, while the EU approaches them as e-money. The underlying challenge may be that global standards for e-money have been lacking (Dobler et al., 2021). It is therefore important to continue coordination across borders to overcome regulatory arbitrage. This requires harmonised regulation across borders and enhanced international cooperation with respect to supervision and enforcement.

A second challenge is to further align MiCAR with existing regulation to promote uniformity, also in light of the monetary implications. For example, while macro-prudential requirements have been included for "significant" stablecoins, further clarification may be needed in case the use of e-money tokens as a regulated form of money grows. In that case, clarification may be needed with respect to the monetary implications, the level playing field with banking regulation, and the applicability of deposit guarantee schemes. Likewise, consumer and investor protection and market functioning regulation under MiCAR appear to be weaker than under existing European securities law regulation (AFM, 2022). Existing rules will therefore have to be developed further, also taking into account that level 2 regulations for MiCAR are still to be drafted. Tighter standards could level the playing field between investors in crypto-assets and those investing in traditional markets. If not, MiCAR could unintentionally give the impression that risks are adequately mitigated, while in practice this is not the case (AFM, 2022).

A third challenge is for regulation to keep pace with the rapid evolution of crypto ecosystems. Developments in crypto-asset markets continue at a rapid pace. Since the development of MiCAR, new forms of crypto-assets and services have emerged which remain out of its scope such as NFTs and DeFi. Regulating these decentralised networks might be challenging. It will be difficult to apply financial regulation and supervision if it is not clear who or what is responsible for compliance, including reporting standards. Regulation of decentralised

[38] See: Boete voor Binance Holdings Ltd. vanwege het zonder de wettelijk vereiste registratie aanbieden van cryptodiensten (dnb.nl)

finance may therefore imply that the governance of these crypto ecosystems needs to change. Regulatory discussions will continue at the global level to address the challenges posed by these new assets.

5 Findings and conclusion

This study has provided a broad overview of the evolution of crypto-assets, their main opportunities and risks, and summarised the international regulatory response. Throughout the study, a distinction has been made between the main types of crypto-assets, i.e. unbacked crypto-assets and stablecoins, their main functions, i.e. as a medium of exchange or speculative investment, and the underlying technology that provides for storage and transfer of these assets.

A key finding with respect to the underlying technology is that it could lead to innovative applications, but that it also carries additional risks compared to the traditional financial system. The technology behind some crypto-assets could support feeless global transfers within a couple of seconds. Anyone could potentially send and receive anonymously, without having to rely on an intermediary and without relying on any national government. Additionally, crypto-asset infrastructures are available 24/7, as computers all over the world work together to maintain the platform, increasing robustness (no single point-of-failure) and limiting any single computer from gaining dominant market power. At the same time, due to their complexity, anonymity and opaque governance structures, crypto-asset infrastructures are more prone to market failures than traditional financial markets. There is typically no central entity that can be held responsible for the security and integrity of the network, while anonymous participants can engage in all sort of illegal activities, and some large service providers are located in lightly regulated jurisdictions.

A key finding with respect to unbacked cryptos is that most people in Advanced Economies (AEs) buy crypto-assets as a speculative investment. The opportunities presented by the technology behind crypto-assets should be separated from the assets themselves. Even if crypto-asset infrastructures eventually fulfil their potential, unbacked crypto-assets will remain too risky to be recognised as money. In AEs in particular, unbacked cryptos are hardly ever used as a means of payment. They are too volatile, complete decentralisation seems an illusion and national and European payment infrastructures already support instant payments. Their volatility increases their attractiveness as a speculative investment. However, even as a speculative asset class, unbacked crypto-assets suffer from significant shortcomings that underline the need for regulatory intervention. For example, constructions emerge that resemble Ponzi schemes. where unsuspecting (often young) investors are misled by stories about crypto millionaires on social media websites.

A key finding with respect to stablecoins is that they have more potential to deliver on the main opportunities of crypto-assets – to improve the speed and efficiency of cross-border payments and to facilitate the storage and transfer of tokenised assets. Stablecoins have been developed to solve two of the major flaws of unbacked cryptos: to decrease their volatility and to avoid the creation of a new unit of account by using fiat money as backing. Both of these features may increase their suitability as a means of payment, especially across borders, on payment platforms that settle tokenised assets for tokenised money. Without proper regulation and supervision, however, stablecoins give rise to significant risks to financial stability due to their vulnerability to runs and settlement-related risks.

Based on these findings, we conclude that the main opportunity of crypto-assets can best be fulfilled under a regulatory regime that addresses the risks. A broad international consensus has emerged on the need for a regulatory approach beyond AML/CFT issues and which should addresses all the traditional objectives of financial regulation.

For DNB, this broadening of scope implies an expansion of activities in its roles as a central bank and supervisory authority. At the international level, DNB will continue to contribute to the development of FSB and BIS international standards, such as those that affect payment system oversight, due to the transfer function of systemically important stablecoin arrangements. Regulatory changes will also affect DNB's supervisory tasks, including those related to the drafting of level II legislation for MiCAR and its implementation (in close cooperation with the Dutch Authority for the Financial Markets, AFM). Moreover, amendments are forthcoming in European legislation that provides the foundation for DNB's AML/CFT supervision and banking supervision; these amendments will also cover crypto-asset exposures. Given that the regulation and supervision of crypto-assets is still in its early years, we expect that the regulation of crypto-assets will remain on the international policy agenda for years to come, also due to the expansion of financial functions in crypto-asset ecosystems resulting from the evolution of decentralised finance and non-fungible tokens.

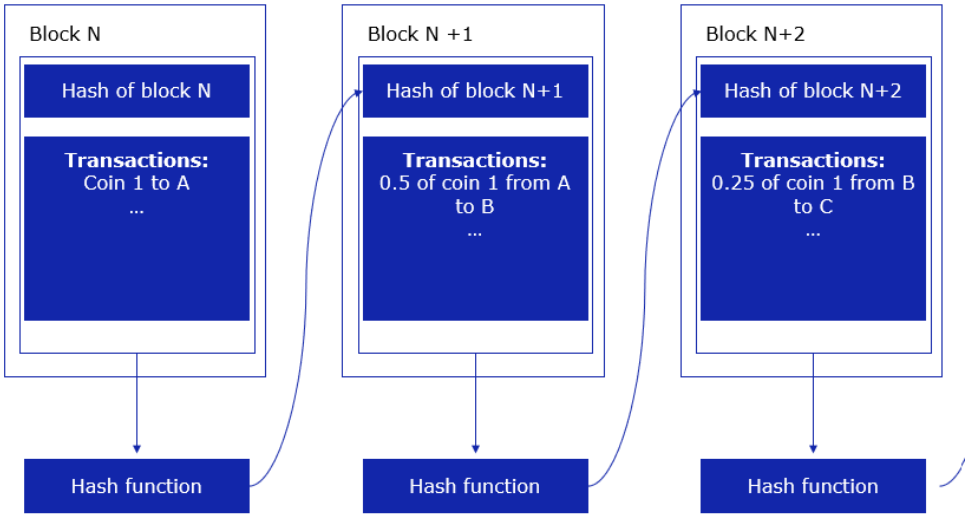
Annex

1 Distributed Ledger Technology

DLTs are organised as blockchains, although newer "chain-based" technologies have emerged. Transactions are chained, because the spender of a coin refers back to the previous spender from whom the coin was received (see Figure A.1). In a blockchain, ownership is proven by using the blockchain to reconstruct the history of all transactions ever made to and from a public key – the crypto equivalent of a bank account number. Users can prove ownership to a public key and initiate transactions only if they know the private key associated with that public key. Hence, a private key could be seen as the password or PIN code giving access to a public key. In most blockchains, all transactions are done with a public key and the amount of coins that correspond to each public key can be traced. Hence, once someone sends crypto to someone else and thus obtains the public key, all other transactions done by this person (and with this public key only) can be traced. Most cryptos, like Bitcoin, use a single blockchain and all transactions of all public keys are processed in this single chain. However, some cryptos use new technologies where each public key starts its own chain and these different chains interact.

Blockchains use hashing to allow verification of the history of transactions, giving blockchains their "immutable" character. A hash function encodes lengthy information in a simple code which makes it easy to verify but nearly impossible to reverse. For example, a very simple hash function would be to use the last 4 digits of a long and complex number. It is easy to verify that the last 4 digits are correct, but it is impossible to reveal the full number with only the last 4 digits. Blockchains use much more complicated hash functions, whereby even a minor change to the information in a block creates a completely new hash output in the next block. This makes previous transactions "immutable" – if someone makes changes to earlier transactions, there is a different hash output and all consecutive blocks in that chain become invalid.

Figure A.1. Blockchain illustration



Note: this is a stylised illustration of a UTXO (unspent transaction output) model blockchain, which states both the amount of crypto sent to someone else and the amount that remains after each transaction. In contrast, an account-model blockchain records accounts instead of transactions.
Source: own construction.

Through their joint efforts and a mechanism to achieve consensus, nodes create a chain of blocks, giving blockchains their "decentralised" nature. A blockchain network consists of nodes (basically computers) which write and validate transactions. Consensus needs to be reached among these nodes about which chain to accept. A blockchain could be public, which means anyone with a computer could be a node (called permissionless blockchains), or private, which means only specific entities are allowed to be nodes (called permissioned blockchains). In the strongest case of centralisation there is only one node that validates transactions. This would not be a distributed ledger anymore, but a traditional database instead.

The oldest consensus mechanism used by the biggest crypto-assets, namely Bitcoin and Ethereum up to 2022[39], is Proof of Work (PoW). In this consensus mechanism, nodes attempt to guess a random number – called the nonce – correctly, as quickly as possible (this validation process is also known as "mining" in the case of PoW). The first miner to guess the number correctly adds a new block to the blockchain in which it writes transactions. The rest of the miners validate whether the transactions and the nonce are correct. If more than half agree, the block will be accepted and the chain continues. The miner is rewarded with new coins and transaction fees for writing the transactions. In case one or more transactions are invalid (i.e. transactions do not follow from the history of the blockchain and/or transactions are not signed with the private key), the rest of the network will notice (verifying is easy due to hashing), the block will not be accepted by the majority of the network and the miner will lose its reward. This creates economic incentives to secure the network while at the same time preventing misbehaviour.

Newer consensus mechanisms have emerged which use significantly less energy and are cheaper and faster than PoW (Macias, 2020). While Bitcoin and its associated Proof of Work involve high energy usage (Traspalacios and Dijk, 2021; De Vries *et al*., 2022), high transaction fees and low transaction speed, new consensus mechanisms can settle transactions at lower energy usage (Agur *et al*., 2022), within a second and with much lower fees. The key difference between these newer consensus mechanisms and PoW is the way in which economic incentives are created. In a PoW consensus mechanism, miners consume significant energy resources (computer power) to guess the nonce, which gives them skin in the game and prevents misbehaviour. In newer consensus mechanisms, nodes (called validators in these consensus mechanisms) are incentivised through other mechanisms. For example, in a Proof of Stake (PoS) consensus mechanisms, coin holders can "stake" coins to become a validator. The algorithm chooses which validator will write the next block; the more coins that are "staked", the higher the probability to write transactions and receive rewards. If a validator misbehaves, staked coins could be slashed off, providing a direct financial incentive to prevent misbehaviour without spending significant energy resources.

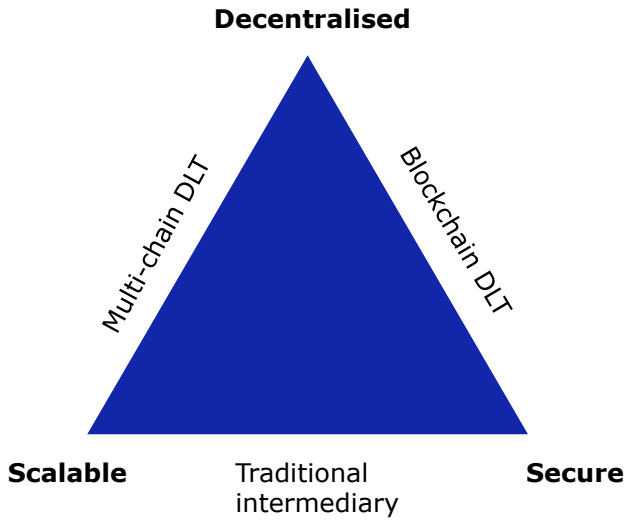
Since nodes work in a decentralised way, they can sometimes create several blocks at the same time. This means it takes time before transactions are far along enough in the chain to be considered final. When different nodes add different blocks to a chain, this is known as a temporary or soft "fork". Eventually, one of the chains will become the accepted chain after a subsequent block has been added, making it the longest chain. However, this also means that the network will not accept transactions on the other chains. Nodes will continue on the longest chain, because the rest of the network continues on this chain, and this involves the highest probability of reward. In PoW consensus mechanisms, for instance, adding blocks to shorter chains is discouraged as this would be a waste of mining power on a chain that the rest of the network will not accept, while in PoS consensus mechanisms a node would have a stake slashed off. The longer a recipient waits, the more blocks are added, and

[39] On 15 September 2022, Ethereum transitioned to a proof-of-stake consensus mechanism. See The Merge | ethereum.org, accessed 20 September 2022.

the lower the probability that the transaction will be reversed by a longer chain. For example, before Ethereum transitioned to proof-of-stake "*the recommended waiting time [was] six blocks or just over 1 minute*".[40] In case there is disagreement in the network, part of the network might also decide to continue on a different chain permanently – called a hard fork. Many coins have been created by such "hard forks" on Bitcoin and Ethereum chains, for example. The biggest are Bitcoin Cash, Bitcoin Gold and Ethereum Classic.

New multi-chain technologies have emerged in which multiple blockchains interact, so that new blocks are added asynchronously and simultaneously. Examples are chain-based Directed Acyclic Graph (DAG) technologies. In this case, multiple blocks on different blockchains are written simultaneously by different nodes and validated by the rest of the network. This leads to increased scalability, but comes at a cost of a loss of security. As there is no single blockchain of which all nodes hold a copy and validate transactions, there is no consensus among the full network either. A solution is to allow only some (credible) nodes to validate transactions. However, this makes the network less decentralised.[41] The tension between the objectives of decentralisation, scalability and security has also been referred to as the scalability trilemma (Figure A.2).

Figure A.2. Scalability trilemma of DLTs



Source: BIS (2022), Buterin (2021).

The security of the network depends on the rewards for validation and the size of the network. If an attacker controls more than 50% of the nodes, this attacker could rewrite the blockchain and reverse transactions.

[40] See Proof-of-work (PoW) | ethereum.org, accessed summer 2022. The Ethereum website does not specify a new recommended waiting time since it moved to a proof-of-stake consensus mechanism. In proof-of-stake consensus mechanisms, nodes are chosen by the algorithm to write a block with transactions. Therefore, when the network performs optimally and honestly, there is only ever one new block at the head of the chain, and all validators attest to it. However, it is possible for validators to have different views of the head of the chain due to network latency or because a block proposer has equivocated. In this case the algorithm chooses the chain to which most validators attested.

[41] For example, both Nano and IOTA are based on such technology. Each Nano represents a vote and holders of Nano choose where they delegate their voting right to. When a node has 0.1% of voting weight delegated to it, it becomes a Principal Representative. Principal Representatives get to vote first. As soon as more than 50% of the total voting weight of all nodes has validated, the transaction is irrevocable. Hence, decentralization of the network depends on how holders assign their voting right, see: Protocol Design - ORV Consensus - Nano Documentation. IOTA transactions are double-checked by a centralized node called "The Coordinator", see: The Coordinator | Network | Getting Started | IOTA Documentation.

These attacks are referred to as 51% attacks. The larger the network of nodes, the harder it gets to gain 50% of the network. The economic incentives behind launching a 51% attack have been modelled (Auer, 2019). For example, attackers could buy or rent mining equipment in the case of proof-of-work consensus mechanisms. The probability of success of such an attack depends on the rewards for "honest" validation, the costs to buy or rent the nodes, the amount of nodes in the network and the amount of crypto that could be stolen. These theories suggest that as the rewards for "honest" validation decline, the punishment for "dishonest" validation falls, and/or the network declines, such an attack becomes more profitable and the network less secure (Auer, 2019). A research project by MIT has detected over 40 attacks on several coins.[42] Attacks could go unnoticed, as they are often aimed at exchanges that have large transaction inflows, but do not have an incentive to disclose successful attacks due to the risk of being perceived as insolvent.

2 The crypto-assets infrastructure

Issuance

The open-source nature of DLT protocols implies that anyone can create new crypto-assets. DLTs are organised as blockchains (see Section 1 of this Annex). Anyone can copy the blockchain, change the underlying code and thus create a new crypto-asset coin. Tokens can then be issued on these blockchains. For example, the first stablecoins – the so-called Tether tokens - were issued on the Omni layer in 2014, a digital platform created for creating and trading tokens on the Bitcoin blockchain. This sparked the idea to develop blockchains with more complex applications. Examples are the Ethereum blockchain, the BNB Chain (previously Binance Smart Chain), Tron, Solana, and Avalanche. Open-source technical standards have emerged to aid developers in creating specific tokens that are compatible with a certain blockchain.

Backed crypto-assets are issued and redeemed by an entity that is supposed to buy and sell the underlying asset backing in the traditional financial system. Where crypto-assets represent ownership of an underlying traditional asset that exists outside the blockchain, the asset-backed cryptos should match the assets in custody at all times. Hence, an entity must buy these assets when backed crypto-assets are issued and sell these assets when backed crypto-assets are redeemed. For example, Tether issues different backed tokens (USDt, EURt, Tether Gold, etc.) on different blockchains, such as Ethereum, Tron, Solana, Omni (Bitcoin) and Avalanche. Each time someone buys a Tether token, Tether is supposed to acquire the corresponding asset on the market (and vice versa). As anyone can create new tokens, key issues revolve around the presence of these assets and the implications in case of loss (for example due to misrepresentation, theft, bankruptcy, damage etc.) (FSB, 2022d).

Access

Crypto-assets can be accessed and transferred by entering the private key (password) stored in a wallet. A crypto-asset wallet stores private keys. It can do this in different ways, e.g. on a piece of paper, on a USB stick or in an app created by developers. Initial private keys may be owned by developers, investors or exchanges. These private keys may then be used to transfer crypto-assets to other wallets. Developers of a crypto-asset usually also develop apps which can be used to store the private key and transfer crypto, but in principle

[42] See 51% Attacks — MIT Digital Currency Initiative.

anyone can create apps. Some apps allow for the storage of multiple private keys and can also be used to buy crypto-assets from exchanges.

Processing & settlement

Users typically offer a fee – called a gas fee – to the nodes for processing and settlement of transactions. These fees are paid in the native crypto coin of the respective blockchain. Fees strongly differ across different blockchains, but even within blockchains they depend on the timing and the difficulty of the transaction. Some transfers require more computer power than others, and sometimes blockchains are congested and there is a long backlog of transactions waiting to be settled. In some cases there are nodes that have a strong incentive to provide services for free. For example, exchanges may want to try to create network effects because they hold the crypto themselves and earn profits through their platform.

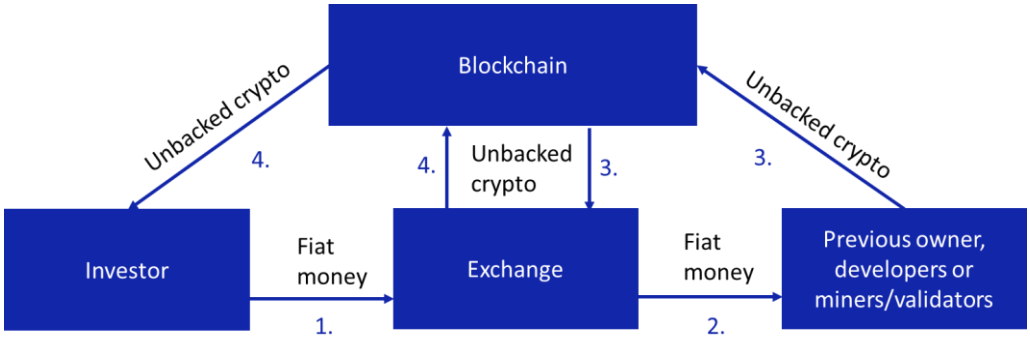
As nodes can choose which transactions they add to the ledger and in which order, they can affect market prices and engage in market manipulation. The amount they can earn from other investors – by influencing the choice and sequence of transactions – is called "miner extractable value" (MEV). For example, they can execute their own transactions before large transactions move market prices. The miner then earns a profit and delays other transactions. Such behaviour is deemed illegal in traditional markets, as brokers are supposed to act in the best interest of their clients. Front-running based on inside information induces an "invisible tax" and inhibits transparent price formation. Since the ledger is public, such behaviour has been observed at a large scale, but the identity of the respective nodes are generally unknown (Auer et al., 2022).

Exchanges

Crypto exchanges form a bridge between crypto-assets and fiat money, and thus the real economy. Direct crypto payments for goods and services are rare in the real economy. Centralised crypto exchanges form the bridge between crypto ecosystems and the real economy by providing a marketplace where crypto-assets can be exchanged for fiat money (IOSCO, 2022). Developers and miners/validators sell their crypto-assets via exchanges to consumers. Decentralised exchanges form no such link, since they only facilitate the exchange of crypto-assets.

A stylised exchange of an unbacked crypto-asset for fiat money follows approximately four steps (see Figure A.3). Step 1: An investor opens an account with a crypto exchange, deposits fiat money, and sends in a request to buy a certain crypto-asset. Crypto exchanges are usually linked to a multitude of blockchains and are active in a wide variety of crypto-assets. Step 2: the exchange buys the requested crypto-asset either from the previous owner, or in case of a newly issued unbacked crypto-asset, from developers through a so-called Initial Coin Offering (ICO) or from miners/validators. Step 3: the seller of the crypto-asset sends in a transaction on the blockchain from their own public key to the crypto exchange wallet public key. The crypto-assets are now in the wallet of the exchange, on behalf of the investor. Step 4: the investor may decide whether to hold the crypto-asset in the wallet of the exchange (also called a "hosted wallet") or to move it to a private wallet (also called an "unhosted wallet"). In the latter case, the exchange sends a request to the blockchain to transfer the crypto-asset from the exchange's public key to the investor's public key.

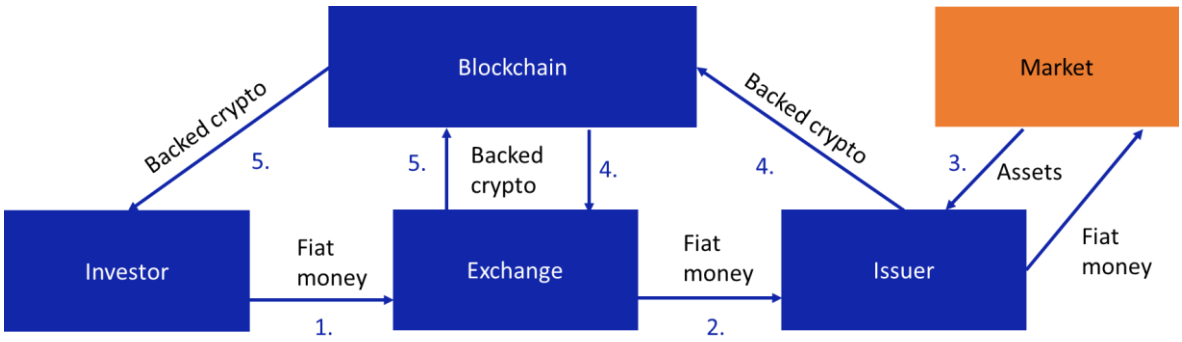
Figure A.3. Exchange of unbacked crypto-asset into fiat money



Source: own construction.

The issuance and redemption of backed crypto-assets follows approximately five steps (see Figure A.4). Step 1: an investor opens an account with a crypto exchange, deposits fiat money and sends in a request to buy this backed crypto-asset. Next, the exchange could either buy the requested backed crypto-asset from a previous owner and proceed as above (Figure A.3), or the backed crypto-asset will need to be issued by the issuer. In this latter case, step 2 follows: the crypto exchange has an account with the issuer, deposits fiat money, and sends in a request to buy the backed crypto-asset. Step 3: the issuer acquires the underlying asset and issues the backed crypto-asset on the blockchain. Step 4: the issuer sends a request to blockchain to transfer the backed crypto-asset from the issuer's public key to the crypto exchange wallet public key. Step 5: the investor may decide to move the backed crypto-asset from the exchange to investor's private wallet. Redemption follows the same steps in reverse order.

Figure A.4. Issuance of backed crypto-asset



Source: own construction.

Exchanges often provide different crypto-asset services that are traditionally separated in other markets, leading to potential conflicts of interest and market manipulation. Exchanges may: 1) provide custody of crypto-assets, 2) operate a trading platform, 3) be the counterparty of a transaction, including exchanging crypto-assets for other crypto-assets or fiat currencies and "placing" crypto-assets, and 4) be the broker, including the execution, reception and transmission of orders. Moreover, some exchanges also provide for

lending or borrowing of crypto-assets, run nodes in blockchain networks, and provide advice on crypto-assets. If all these functions are combined, conflicts of interest may arise and price discovery may lack transparency (IOSCO, 2020b). For example, as a validator or investment advisor, exchanges may be aware of upcoming orders before other parties, and they may use this information in their role as a market maker (which would be called frontrunning based on insider information in traditional markets). Moreover, conflicts of interest may also arise since there is no third party to verify ownership. In fact, it is unclear what arrangements are in place in event of a loss, including a loss due to theft from the exchange or its failure. Such events could even go unnoticed, as exchanges have no incentive to disclose successful attacks due to the risk of being perceived as insolvent.

Exchanges often provide crypto-asset services directly to consumers, which implies that there is no gatekeeper to protect consumers/investors and prevent illegal use. In traditional financial markets, access to trading venues is typically limited to intermediaries who act on behalf of their customers. There are four main reasons for this (IOSCO, 2020b). Firstly, limiting access to eligible parties protects investors from fraudulent buyers/sellers who engage in market manipulation, such as pump-and-dump schemes, wash trading, and manipulation of order books (Eigelshoven *et al*., 2021). Secondly, limiting access is important to prevent on-boarding of retail investors when trading is not suitable for them. Intermediaries are required to ensure that investors know the risks of trading in particular products. They should assist investors in choosing asset classes that match their individual financial situations/risk tolerances to help mitigate the risks of significant loss. Thirdly, limiting access contributes to preventing criminal or illegal trading activity, such as money laundering and financing of terrorism. Lastly, limiting access is important as there might be regulatory arbitrage if investors are permitted from jurisdictions where such activities are prohibited.

Decentralised exchanges are blockchain protocols which only facilitate the exchange of crypto-assets. Examples are DyDx, Uniswap and OasisDEX. The daily trading volume of the largest centralised exchange (Binance) in 2021 was around EUR 20 billion. By way of comparison, the largest decentralised exchange, DyDx, had a relatively small trading volume of around EUR 1.5 billion per day in the same period.[43] Decentralised exchanges are built on self-executing smart contracts and have no identifiable entity behind them, even though there is a community of programmers which set up and maintain these exchanges. The crucial differences with centralised exchanges are that users of decentralized exchanges remain in full control of their own funds at all times. Rather than using an intermediary that matches buyers with sellers, this function is performed through code executed on a blockchain. This also means that only crypto-assets can be exchanged that are on this blockchain.

3 Decentralised finance

Decentralised finance (DeFi) commonly refers to the provision of financial products, services, arrangements and activities based on crypto-assets (IOSCO, 2022). These are offered to users via financial applications run by smart contracts[44] on a blockchain, called decentralised applications (DApps). In general, four different layers can be identified. At the base, or settlement layer, is the underlying blockchain. The second layer

[43] See dYdX Perpetual Trade Volume, Trade Pairs & Trust Score | CoinGecko and Binance Trade Volume, Trade Pairs & Trust Score | CoinGecko, accessed on 19th September 2022.

[44] Smart contracts are an algorithm coded to update records when a set of conditions are met , or simply "a set of coded computer functions". Such a smart contract is meant to enforce contract execution even though there is no judicial contract that could be enforced.

is the asset layer; only crypto-assets that have been issued on a blockchain can be exchanged on that blockchain. The third layer is the protocol layer; these are the computer codes, also called smart contracts, that create financial products and services. These smart contracts facilitate payments based on pre-set conditions defined in code. For example, a condition could be that a payment will only be made if the counterparty has deposited a certain crypto-asset first. Such a payment will be made without further intervention of a third party. The fourth layer consists of the end-user applications, such as web interfaces and apps, that make these financial products and services available to users.

The DeFi market is dominated by borrowing/lending applications, decentralised exchanges and asset management applications (BoE, 2022). Although different decentralised exchanges work in different ways, in general they involve depositing a crypto-asset in a smart contract in return for another crypto-asset. DeFi borrowing and lending applications do the same, albeit that the exchange can be reversed according to pre-set conditions. For example, the user deposits a volatile crypto-asset as collateral inside a smart contract and receives a stablecoin in return, but the transaction will be reversed if the value of the collateral drops below a certain threshold. Asset management applications aggregate multiple protocols to find investment opportunities with the highest return, also called yield farming or yield optimising. Again, an investor deposits a crypto-asset inside a protocol and receives a token which may be exchanged later for the crypto-asset on deposit, potentially at a profit.

Liquidity pools facilitate the exchange of different crypto-assets and therefore play an important role in DeFi applications. In order to facilitate the exchange of one crypto-asset for another crypto-asset, both crypto-assets need to be provided by someone and the exchange rate between these crypto-assets needs to be automatically determined. This happens through the use of so-called liquidity pools, which could be seen as a sort of crypto investment fund. Users "lock-in" crypto-assets in liquidity pools for which they receive liquidity provider (LP) tokens in return (see Aramonte et al. (2021) for a detailed explanation). LP tokens give a right to the liquidity fees that a pool generates and may also give certain voting rights on the protocol (i.e. governance tokens). The exchange rates between the crypto-assets in the liquidity pool are then determined automatically according to a formula based on the ratio of assets held in the pool. Thus, as the ratio of crypto-asset A to crypto-asset B increases, the liquidity pool price of crypto-asset A decreases and the price of crypto-asset B increases. The price in the liquidity pool may diverge from the price on other exchanges, called slippage, in which case arbitrageurs will buy the relatively cheaper crypto-asset until the price presumably converges again.

Liquidity pools often consist of stablecoins to reduce exchange rate risks. Investors in liquidity pools are susceptible to high exchange risk. Although the idea is that arbitrageurs will make sure that prices in the liquidity pool do not diverge too much from market prices, in practice the volatility of crypto-asset is such that prices across exchanges and liquidity pools diverge. In this case liquidity providers make a loss, because prices in the liquidity pool diverge from market prices. This loss is often referred to as an "impermanent loss", reflecting the hope that losses are not permanent as prices may converge again. However, in practice prices may not always converge. If prices diverge too much, investors might lose faith and withdraw their funds from the liquidity pool. The higher the volatility of a given crypto-asset inside a liquidity pool, the more the exchange rate in the liquidity pool may deviate from market exchange rates, hence the higher exchange rate risks. Many liquidity pools therefore consist for a large part of stablecoins. In fact, DeFi protocols host a significant portion of stablecoins in circulation. For example, USDT and USDC are the largest stablecoins by market capitalisation, of which approximately 20% and 40% are locked in DeFi protocols, respectively (IOSCO, 2022).

Complete decentralisation is an illusion, but the technology behind DeFi has potential to be used in more use cases if properly regulated like other financial activities. The open-source nature of DeFi facilitates worldwide cooperation between programmers who create algorithms and protocols which could make traditional financial services and activities potentially faster, more transparent and more inclusive (IMF, 2022). However, developers do not create these algorithms and protocols for free. Successful DApps require some form of organisation to receive funding and to set organisational and strategic goals (Aramonte et al., 2021). Exchanges and stablecoin issuers also play an important role. Users generally prefer a reliable organisational form, because DeFi protocols are not always as resilient and temper-proof as suggested. Since anyone can create new smart contracts and few investors have the skills to read them properly, exploits, bugs, and hacks are rampant (IOSCO, 2022). DeFi investors have been largely unprotected and are susceptible to market manipulation and exploitation. Regulatory discussions may therefore need to focus on the appropriate regulatory regime for DeFi applications, including the need for identifiable market entities that take on responsibility for ensuring the security, soundness and efficiency of the protocol.

References

AFM (Dutch Authority for the Financial Markets). (2022). *Rapport Financiële Stabiliteit: Ronde tafel Tweede Kamer.* Link

Agur, I., Lavayssière. X., & Bauer, G. V. (2022). *How Crypto And CBDCs Can Use Less Energy Than Existing Payment Systems.* IMF Blog. Link

Allen, H.J. (2022). *DeFi: Shadow banking 2.0?*. Forthcoming in William & Mary Law Review. Link

Aramonte, S., Huang, W., & Schrimpf, A. (2021). *DeFi risks and the decentralisation illusion*. BIS Quarterly Review, December 2021. Link

Auer, R. (2019). *Beyond the doomsday economics of "proof-of-work" in cryptocurrencies*. BIS Working Papers 765. Link

Auer, R., Monnet, C. & Shin, H. S. (2021). *Distributed ledgers and the governance of money*. BIS Working Papers 924. Link

Auer, R., & Tercero-Lucas, D. (2021*). Distrust or speculation? The socioeconomic drivers of US cryptocurrency investments*. BIS Working Papers 924. Link

Auer, R., Frost, J., & Vidal Pastor, J.M. (2022). *Miners as intermediaries: extractable value and market manipulation in crypto and DeFi.* BIS Bulletin 58. Link

BoE (Bank of England). (2021). *New forms of digital money: Discussion Paper.* Link

BoE (Bank of England). (2022). *Financial stability in focus: Cryptoassets and decentralised finance.* Financial Policy Committee*.* Link

BCBS (Basel Committee on Banking Supervision). (2021). *Consultative document: Prudential treatment of crypto-asset exposures.* BIS. Link

BCBS (Basel Committee on Banking Supervision). (2022). *Consultative document: Second consultation on the prudential treatment of crypto-asset exposures.* BIS. Link

Bitstamp. (2022). *Crypto Pulse.* Report 2022 Q1. Link

Bolt, W., & Van Oordt, M. R. C. (2019). *On the value of virtual currencies*. Journal of Money, Credit and Banking 52(4), 835-862. Link

Bolt, W., Lubbersen V., & Wierts, P. (2022*). Getting the balance right: Crypto, stablecoin and CBDC*. Journal of Payment Strategy & Systems. 16(1), 39-50. Link

Broeders, D. & Wessels, P. (2022). *On the capitalisation of central banks*. DNB Occasional Study Voume 20-4. Link

Brunnermeier. M. & Landau, J.P. (2022), The digital euro: policy implications and perspectives, Study requested by ECON Committee. Link

CPMI/IOSCO (Committee on Payments and Market Infrastructures, International Organization of Securities Commissions). (2022). *Application of the principles for financial market infrastructures to stablecoin arrangements*. BIS. Link

Chainalysis. (2022). The Chainalysis State of Web3 Report. June 2022. Link

Cryptovaluta Monitor. (2022). *Betalen, beleggen en sparen in een nieuwe economie.* Juli 2022. Link

Davidson, S. (2021). *From corporate governance to crypto-governance*. SSRN. Link

Delfabbro, P., King, D.L., & Williams, J. (2021). *The psychology of crypto trading: Risk and protective factors*. Journal of behavioural addictions, 10(2), 201-207. Link

De Vries, A., Gallersdörfer, U., Klaaßen, L., & Stoll, C. (2022). *Revisiting Bitcoin's carbon footprint*. Joule, 6(3), 498-502. Link

DNB (De Nederlandsche Bank). (2020). *Central bank digital currency: Objectives, preconditions and design choices.* Occasional Studies 18-1, Link

DNB (De Nederlandsche Bank). (2021a). *Changing landscape, changing supervision: Developments in the relationship between BigTechs and financial institutions.* link

DNB (De Nederlandsche Bank). (2021b). *The carbon footprint of bitcoin*. DNB Analysis by Trespalacios, J.P. & Dijk, J. Link

DNB/AFM (De Nederlandsche Bank, Autoriteit Financiële Markten). (2018). *Cryptos: Recommendations for a regulatory framework*. Link.

DNB (De Nederlandsche Bank). (2022a). *DNB payments strategy 2022-2025.* Link

DNB (De Nederlandsche Bank). (2022b). *MiCAR important step in regulation of crypto assets.* DNBulletin. Link

Dobler, M., Garrido, J., Grolleman, D., Khiaonarong, T., & Nolte, J. (2021). *E-Money: Prudential Supervision, Oversight, and User Protection.* International Monetary Fund, Departmental Paper. Link

EBA (European Banking Authority). (2021). *Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector.* Link

ECB (European Central Bank). (1998). *Report on electronic money*. Link

ECB (European Central Bank). (2008). *Opinion of the European Central Bank of 5 December 2008 on a proposal for a Directive on the taking up, pursuit and prudential supervision of the business of electronic money institutions (CON/2008/84)*. Official Journal of the European Union, 6 February 2009, pp. 1–9. Link

ECB (European Central Bank). (2020). *Stablecoins: implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area.* ECB Crypto-Assets Task Force, Occasional Paper 247. Link

ECB (European Central Bank). (2021a). *Opinion of the European Central Bank of 19 February 2021 on a proposal for a regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (CON/2021/4)*. Official Journal of the European Union, 29 April 2021, pp. 1–9. Link

ECB (European Central Bank). (2021b). Eurosystem oversight framework for electronic payment instruments, schemes and arrangements, November 2021. Link

ECB (European Central Bank). (2022). *Decrypting financial stability risks in crypto-asset markets.* Financial Stability Review, may 2022. Link

Eigelshoven, F., Ullrich, A., & Parry, D. A. (2021). *Cryptocurrency Market Manipulation—A Systematic Literature Review.* In ICIS 2021 Proceedings on Building Sustainability and Resilience with IS: A Call for Action (Austin, Tex.: International Conference on Information Systems, Dec. 12–15). Link

EC (European Commission). (2009). *Directive on the taking up, pursuit and prudential supervision of the business of electronic money institutions.* Official Journal of the European Union 2009/110/EC. Link

EC (European Commission). (2020a). *Proposal for a regulation on markets in crypto-assets, and amending Directive (EU) 2019/1937.* COM/2020/593 final, 29.9.2020. Link

EC (European Commission). (2020c). *Proposal for a regulation on a pilot regime for market infrastructures based on distributed ledger technology*. COM02020/594. Link

ESMA (European Securities and Markets Authority). (2019). Advice Initial Coin Offerings and Crypto-Assets. ESMA50-157-1391. Link

Eurosystem. (2020). *Report on a digital euro.* Link

FATF (The Financial Action Task Force). (2021). *Virtual assets and virtual asset service providers: updated guidance for a risk-based approach.* FATF/OECD. Link

FATF (The Financial Action Task Force). (2022). *Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers.* Link

FCA (Financial Conduct Authority). (2022). *Strengthening our financial promotion rules for high risk investments, including crypto-assets.* Consultation Paper 22/2. Link

Fidelity Digital Assets. (2021). *The Institutional Investor Digital Assets Study.* Link

FSB (Financial Stability Board). (2020). *Regulation, supervision and oversight of "global stablecoin" arrangements: Final report and high-level recommendations*. Link

FSB (Financial Stability Board). (2022a). *Assessment of risks to financial stability from crypto-assets.* Link

FSB (Financial Stability Board). (2022b). *Statement on international regulation and supervision of crypto-asset activities*. Link

FSB (Financial Stability Board). (2022c). *Regulation, supervision and oversight of crypto-assets and markets. Report by the Crypto-Assets Working Group.* Link

FSB (Financial Stability Board). (2022d). *Review of the FSB high-level recommendations of the regulation, supervision and oversight of "global stablecoin" arrangements.* Report by the Working Group on Regulatory Issues on Stablecoins. Link

Frost, J., Shin, H.S. & Wierts, P. (2020). *An early stablecoin? The bank of Amsterdam and the governance of money.* BIS Working Papers 902. Link

G7 Working group on stablecoins (2019*). Investigating the impact of global stablecoins*. Link

G20 (2021). *G20 Roadmap for enhancing cross-border payments. First consolidated progress report*. Link

Gorton, G.B. & Zhang, J. (2021). *Taming wild cat stablecoins.* SSRN. Forthcoming University of Chicago Law Review. Link

He, D., Kokenyne Ivanics, A., Lavayssière, X., Lukonga, I., Schwarz, N., Sugimoto, N., & Verrier, J. (2022). *Capital flow management measures in the digital age: challenges of crypto-assets.* IMF Fintech Notes 2022/05. Link

Holmstrong, B. (2015). *Understanding the role of debt in the financial system.* BIS Working Papers 479. Link

IMF (International Monetary Fund). (2021). *The crypto ecosystem and financial stability challenges.* Global Financial Stability Report, Chapter 2. Link

IMF (International Monetary Fund). (2022). *The rapid growth of FinTech: vulnerabilities and challenges for financial stability.* Global Financial Stability Report, Chapter 3. Link

IOSCO (International Organization of Securities Commissions). (2020a). *Investor education on crypto-assets: Final report*. Link

IOSCO (International Organization of Securities Commissions). (2020b). *Issues, risks and regulatory considerations relating to crypto-asset trading platforms: Final report.* Link

IOSCO (International Organization of Securities Commissions). (2022). *Decentralized finance report: Public report*. Link

Ipsos. (2021). *Attitudes van cryptobezitters: Ad hoc onderzoek voor AFM.* Link

JP Morgan. (2021). *Cryptocurrencies: bubble, boom or blockchain revolution*. Link

JP Morgan. (2022). *Opportunities in the metaverse: How businesses can explore the metaverse and navigate the hype vs. reality.* Link

Slagter, B. & Slagter, P. (2021). *Ons geld is stuk: En waarom bitcoin de oplossing is.* Hollands Diep. Amsterdam, 2021. Link

Kappture. (2019*). Accepting Cryptocurrency at the Point-Of-Sale.* Version 1, 29th June 2019. Link

Lannoo, K. (2021). *Regulating crypto and cyberware in the EU.* Policy brief, European Capital Markets Institute. Link

Liao, G.Y. & Caramichael, J. (2022). *Stablecoins: Growth Potential and Impact on Banking.* International Finance Discussion Papers, 1334. Washington: Board of Governors of the Federal Reserve System. Link

Macias, I. R. (2020). *Verity Ledger: a protocol for improving data quality and ensuring data authenticity in publicly-built open datasets* [Doctoral dissertation]. Massachusetts Institute of Technology. Link

Makarov, I. & Schoar, A. (2021). *Blockchain analysis of the bitcoin market.* NBER Working Paper 29396. Link

McKinsey. (2022). *Value creation in the metaverse: The real business of the virtual world.* Link

Momtaz, P.P. (2020). Initial Coin Offerings. PLoS ONE 15(5): e0233018. Link

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Link

OECD (Organisation for Economic Co-operation and Development). (2020). *The tokenization of assets and potential implications for financial markets.* OECD Blockchain policy series. Link

OECD (Organisation for Economic Co-operation and Development). (2022). *Regulatory approaches to the tokenization of assets.* OECD Blockchain policy series. Link

Oksanen, A., Mantere, E., Vuorinen I., & Savolainen I. (2022). *Gambling and online trading: emerging risks of real-time stock and cryptocurrency trading platforms.* Public Health 205, 72-78. Link

PWG (President's Working Group). (2021). *Report on stablecoins: President's Working Group on Financial Markets, the FDIC and the OCC.* Link

van Oordt, M.R.C. (2022). *The emerging autonomy-stability choice for stablecoins,* Tinbergen Institute Discussion Paper. Link

WEF (World Economic Forum). (2021). *Digital assets, distributed ledger technology and the future of capital markets.* Insight report in collaboration with Boston consulting group. Link

Zetzsche, D. Buckley, R.P. Arner, D.W. & Föhr. L. (2019). The ICO Gold Rush: It's a scam, it's a bubble, it's a super challenge for regulators. Harvard International Law Journal, 60(2), 267-315. Link

DeNederlandscheBank
EUROSYSTEEM

De Nederlandsche Bank N.V.
P.O. Box 98, 1000 AB Amsterdam
+31 20 524 91 11
dnb.nl