BANK FOR INTERNATIONAL SETTLEMENTS

The crypto ecosystem: key elements and risks

Report submitted to the G20 Finance Ministers and Central Bank Governors

July 2023

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-670-5 (online)

The crypto ecosystem: key elements and risks

BIS report to be submitted ahead of the July 2023 G20 FMCBG meeting

Contents

1. Introduction

The market capitalisation of the crypto ecosystem – notwithstanding a significant decline in 2022 – lies in the trillions of dollars, and there are thousands of crypto coins in circulation. The spread of crypto has been global in nature and driven by a wide range of investors.

In theory, the crypto universe builds on the premise of decentralisation. Rather than relying on central bank money and trusted intermediaries, crypto envisages that the recordkeeping of transfers is provided by a multitude of anonymous validators. Decentralised finance, or "DeFi", seeks to replicate conventional financial services in a decentralised way within the crypto universe, often underpinned by the medium of exchange role of stablecoins. DeFi incorporates innovations such as programmability and composability on blockchains.[1] Such systems are "always on", allowing for worldwide transactions 24 hours per day, seven days per week.

Recent events revealed a wide divergence between the crypto vision and reality. Although crypto operates under the banner of decentralisation, in practice new centralised intermediaries have played a key role in channelling funds into the crypto universe and intermediating within it. The implosion of the FTX crypto exchange is only the most notable manifestation of the sector's vulnerabilities. Rather than providing a more resilient financial architecture, crypto displayed the same well known vulnerabilities of traditional finance, but in amplified ways.

This report reviews the key elements of the crypto ecosystem and assesses its structural flaws. It then goes over the risks that it poses and discusses options for addressing them. It also identifies data gaps and discusses ways to alleviate them.

The report has three key takeaways. First, the crypto ecosystem is subject to a high degree of fragmentation and is characterised by congestion and high fees. This would have been the case even if it had stayed true to its original decentralised ethos. These structural flaws derive from the underlying economics of incentives of validators rather than from technology. And while crypto has offered some elements of genuine innovation, these can be replicated or embedded in the safer and more trusted traditional finance system (BIS (2023)). Second, despite an original ethos of decentralisation, crypto and DeFi often feature substantial de facto centralisation, which introduces various pain points. A prime example concerns stablecoins, which piggyback on the credibility of the central bank's unit of account and may pose risks to monetary sovereignty. Third, while DeFi mostly replicates services offered by the traditional financial system, it does not finance any activity in the real economy but amplifies known risks. As growth is driven mainly by the speculative influx of new users hoping for high returns, crypto and DeFi pose substantial risks to (especially retail) investors. In sum, crypto's inherent structural flaws make it unsuitable to play a constructive role in the monetary system (BIS (2022)).

2. The key elements of the crypto ecosystem

This section describes the main components of the crypto ecosystem. It begins by tracing the development of Bitcoin and blockchain technology. It then discusses the growing role of centralised intermediaries in

[1] A blockchain is a digital ledger (like a spreadsheet) that records transactions in a way that is secure, transparent and immutable. Information is stored across a network of computers. In contrast to the centralised nature of traditional databases, every participant has a copy of the same ledger. When a new transaction is made, it is broadcasted to the network and verified by multiple computers using complex algorithms. Once verified, the transaction is added to the ledger as a "block" and cannot be altered without consensus from the network.

the ecosystem. In particular, it discusses stablecoins, which are most often issued by centralised entities and grew from a bespoke solution to the inherent volatility of crypto assets to becoming a pillar of the crypto ecosystem. The section concludes with a discussion of smart contracts and the decentralised finance applications that build on them. The technical terms used throughout this report are defined in the Glossary.

2.1 Unbacked crypto

The birth of crypto dates to the introduction of Bitcoin in 2009: a decentralised, peer-to-peer means of transferring value on a shared public ledger (ie a public blockchain using distributed ledger technology (DLT)). In its original formulation, crypto was characterised by not being backed by any asset, as well as by a stated claim to reduce the influence of intermediaries through decentralisation (Nakamoto (2008)).

Ownership of crypto assets and transactions with them are verified by decentralised validators and recorded on the public ledger. If a seller wants to transfer cryptoassets to a buyer, the buyer (identified through their cryptographic digital signature) broadcasts the transaction details, eg transacting parties, amount or fees. Validators (in some networks called "miners") then compete to verify the transaction, and whoever is selected to verify appends the list of transactions to the blockchain and is compensated in fees paid in cryptoassets. The updated blockchain is then shared among all miners and users. In this way, the history of all transactions is publicly observable and tied to specific wallets, while the true identities of the parties behind transactions (ie the owners of the wallets) remain undisclosed. In this sense, transactions on blockchains are pseudo-anonymous. By broadcasting all information publicly, the system verifies that every transaction is consistent with the history of transfers on the blockchain, eg that the cryptocurrency actually belongs to the seller and has not been spent more than once.

As cryptoassets started attracting broader attention from potential investors, centralised entities played a greater role in channelling funds into crypto coins. In particular, centralised exchanges, which facilitated the conversion between Bitcoin, other cryptoassets and fiat money, contributed to rising crypto prices by attracting new participants, in a self-reinforcing loop. Centralised intermediaries (notably platforms such as Mt Gox in the early days, and more recently Binance, Coinbase, Kraken and FTX until its sudden collapse in late 2022) have reasserted their key role in the crypto ecosystem time and time again. This system has come to be known within the crypto space as centralised finance (CeFi), and its ups and downs have contributed to the volatility of cryptoasset prices (Graph 1.A).

2.2 Stablecoins

Stablecoins have established themselves as the main medium of exchange within the crypto ecosystem and as a gateway into it. They are so-called because they aim to maintain a stable value relative to a specified asset or pool of assets. Stablecoins are usually pegged to a numeraire, almost always the US dollar, but can also target the price of other currencies or assets (eg gold or even other cryptoassets). In this way, they seek to overcome high volatility and low liquidity to play the role of a medium of exchange in the crypto universe. Stablecoins also play a key role in the DeFi ecosystem (see next section).[2]

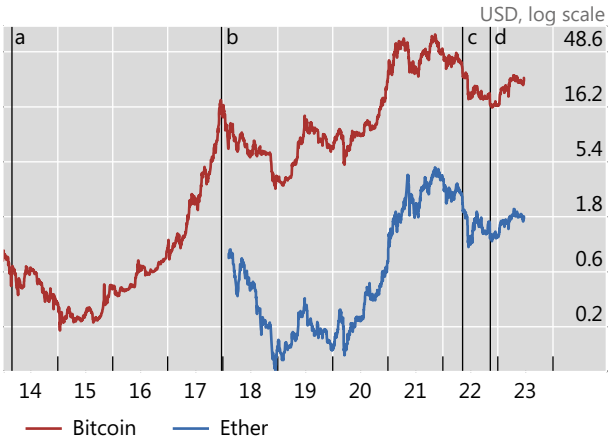
Stablecoins come in two main types, depending on how they attempt to maintain their peg (FSB (2022)). Most stablecoin arrangements are managed by a centralised intermediary and are "asset-backed". The underlying assets can include US government bonds, short-term corporate debt or bank deposits. The centralised intermediary invests the underlying collateral and coordinates the coins' redemption and

[2] The use of stablecoins avoids frequent and costly conversion between crypto and bank deposits in sovereign currency and allows users to leave their wealth within the crypto ecosystem, without exposing it to substantial volatility risk.

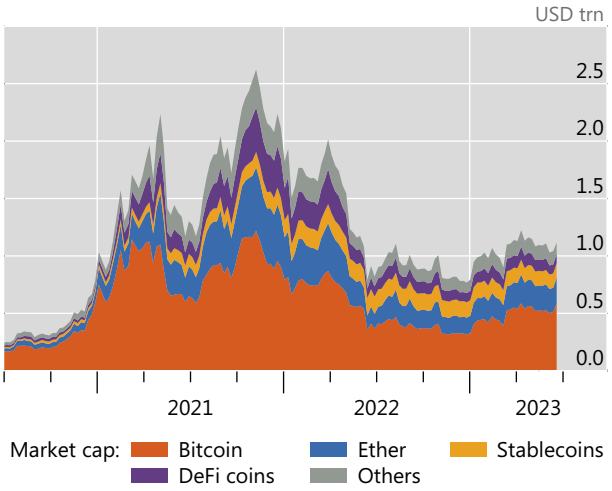
creation. The most prominent stablecoins are Tether, USD Coin (USDC) and Binance USD. "Algorithmic stablecoins", in contrast, aim to automatically rebalance supply via arbitrage with a paired volatile token to maintain the peg. They are typically not backed by real world assets, with the most prominent example being the failed TerraUSD stablecoin.[3]

Despite repeated setbacks and outsize volatility, crypto grew until late 2021 Graph 1

A. Long-term price of crypto assets



B. Market size of crypto and DeFi[1]



[a] Bankruptcy of Mt Gox. [b] Bursting of ICO bubble. [c] TerraUSD and Luna collapse. [d] Bankruptcy of FTX.

[1] End-of-week values. Categories comprise the largest seven stablecoins, 59 DeFi coins and 64 other cryptocurrencies. DeFi coins correspond to cryptocurrencies issued by DeFi platforms and with a market capitalisation-to-total value locked ratio smaller than 50, as reported by DeFiLlama. Total value locked refers to the size of capital pools underpinning DeFi protocols. For more details, see Table A2 from Auer (2022).

Sources: BIS (2022); Bloomberg; CoinGecko; BIS.

2.3 Smart contracts and decentralised finance

Since the advent of Bitcoin, many other blockchains and associated crypto coins have entered the scene, most notably Ethereum and its associated native coin Ether in 2015 (Graph 1.B). Ethereum and many of the newer blockchains allow for "programmability", ie they give developers the option of building applications on top of their blockchain through the use of so-called smart contracts.

Smart contracts are self-executing code that triggers an action if certain pre-specified conditions are met. They can automate some market functions and to some extent obviate intermediaries that are traditionally required to make decisions. They are therefore better thought of as *unattended* contracts (Neilson (2021)). The underlying code is publicly available (ie open source) and can be scrutinised. As smart contracts cannot directly access information that resides "off-chain", ie outside the specific blockchain, they require so-called oracles as mediators to provide such data.

[3] For example, an algorithmic stablecoin X could aim to keep a one-for-one peg to the US dollar by being convertible into one dollar's worth of another cryptocurrency Y and vice versa. Should X fall to 99 cents, a user could purchase X on an exchange for 99 cents and then exchange their X for $1 worth of new units of Y. There are of course exceptions to the broad categorisation used in this report. The most prominent is DAI, which is non-algorithmic and is backed by a mix of unbacked crypto (eg Ether) and stablecoins (eg USDC).

An important feature of smart contracts is their "composability", ie the capacity to combine different components in the system. Users can perform complex transactions on the same blockchain by combining multiple instructions within one single smart contract – like "money lego".

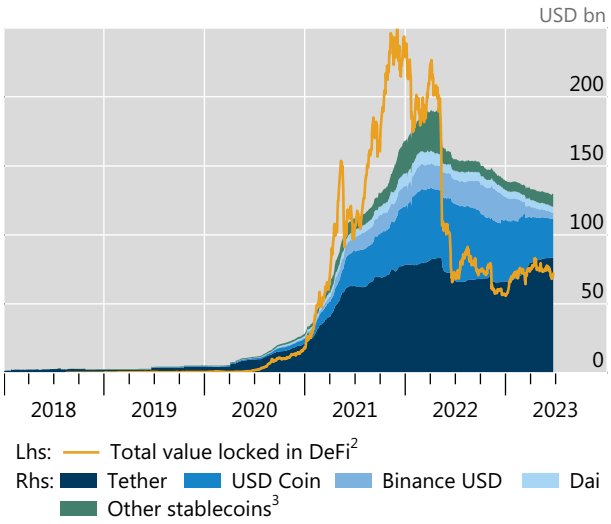
Programmability also opened the door to DeFi, a new ecosystem for the provision of crypto services. DeFi aims to offer traditional financial services and products on the blockchain, with the declared objective of greater transparency and cutting out the middlemen to lower costs. DeFi protocols combine multiple smart contracts to provide lending, borrowing and trading services within the crypto ecosystem. Decentralised applications (dApps) are graphical interfaces that allow users to interact with protocols from their computers or smartphones. While they are not strictly necessary to interact with the DeFi ecosystem, as users could set up their own interface, they are the entry point to DeFi for all but the savviest participants.

Stablecoins play an important role in the DeFi ecosystem by serving as a medium of exchange in a wide range of activities (Graph 2.A).[4] For one, they provide liquidity to the DeFi ecosystem by allowing users to move in and out of decentralised applications. Relatedly, stablecoins serve as trading pairs for other cryptoassets in decentralised exchanges, thereby allowing users to trade crypto without having to convert back to fiat currency, hence reducing transaction costs. Moreover, stablecoins are widely used on DeFi lending and borrowing platforms, where users borrow and lend stablecoins against collateral in the form of other cryptoassets. Because of this key role, turnover in stablecoins generally dwarfs that of other cryptoassets (Graph 2.B).

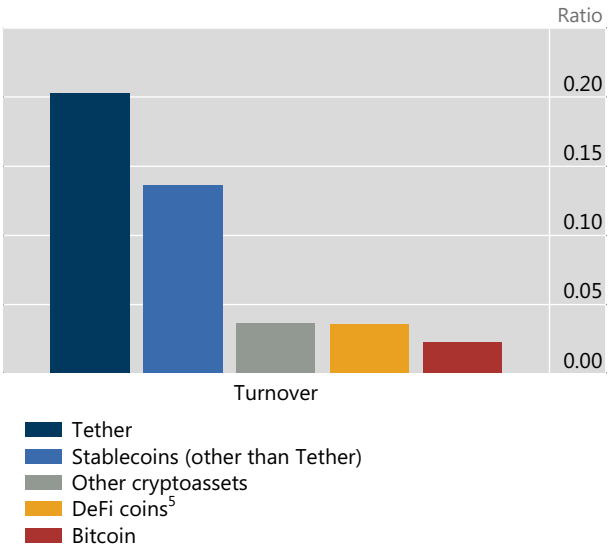
Stablecoins and DeFi grew in tandem

Graph 2

A. Stablecoins gained ground as capital in DeFi apps climbed[1]



B. Turnover of stablecoins dwarfs that of other cryptoassets[4]



[1] Stacked areas plot stablecoins' value in circulation. The selected stablecoins are those ranked as the top four by market capitalisation as of 21 June 2023. [2] Total value locked refers to the size of capital pools underpinning DeFi protocols. The sample includes 2,939 protocols. [3] Includes 61 other stablecoins. [4] Based on the top 20 cryptoassets by market capitalisation as of 21 June 2023 (four stablecoins, seven DeFi coins and nine other cryptoassets). Turnover is the monthly average of the daily volume-to-market capitalisation ratio from 21 May to 21 June 2023. [5] Cryptoassets issued by DeFi platforms.

Source: Aramonte et al (2021).

[4] See Aramonte et al (2021) and Schär (2021).

The main types of financial activity in DeFi, such as lending, trading and insurance, are the same as those already available in traditional finance. Lending platforms allow users to lend out their stablecoins with interest to borrowers that post other cryptocurrencies as collateral. Decentralised exchanges (DEXs) represent marketplaces where transactions occur directly between cryptocurrency or stablecoin traders, and prices are determined via automated mathematical formulas. On DeFi insurance platforms, users can insure themselves against some risks within the crypto system, eg the mishandling of private keys, exchange hacks or smart contract failures, receiving cryptoassets as compensation.

Yet, DeFi activities almost exclusively involve exchanging one stablecoin or crypto coin for another, and do not finance activity in the real economy. In this sense, the system is mostly self-referential and used for speculation in coins.[5] Growth is driven mainly by the continuous influx of new users hoping for high returns. Indeed, recent evidence suggests that rising crypto prices are followed by significantly higher adoption of crypto trading apps, as new users are lured by the prospect of further gains.[6]

3. Structural flaws and risks

This section highlights that, despite the potential for genuine technological innovation, crypto has inherent structural flaws that pose serious risks not only to its own stability and safety, but also to the traditional financial system. The section first reviews the main structural flaws of the crypto ecosystem, including congestion, fragmentation and the need to borrow credibility from sovereign money. It also discusses the problems arising from the need for centralisation. The section then summarises the main risks, splitting them into risks within the crypto ecosystem (including risks to market integrity, consumer protection and privacy), risks specific to DeFi and risks arising from the interconnectedness with the traditional financial system. The section then discusses options for addressing the risks posed by crypto, before closing with a discussion of the data gaps that currently hinder monitoring.

3.1 Structural flaws

3.1.1 Fragmentation and congestion

Crypto – even in its original, fully decentralised, form – suffers from inherent limitations of permissionless blockchains that lead to fragmentation of the system, accompanied by congestion and high fees.[7] Tracing the reasons for fragmentation highlights why the limitations are not technological but rather stem from incentive structures.

On the blockchain, self-interested validators are responsible for recording ownership and transactions. However, in the pseudo-anonymous crypto system, they have no reputation at stake and anonymity impedes accountability. Instead, they must be incentivised through sufficiently high monetary rewards to report truthfully and sustain the system of decentralised consensus. Honest validation must

[5] In April 2023, the Crypto Council for Innovation issued an open call for case studies "to tell clear stories of how this innovation has created a positive impact". The Crypto Council for Innovation provided three examples, with the most important being the ability to send financial aid through the use of stablecoins slightly faster than using standard financial institutions.

[6] See Auer, Cornelli, Doerr, Frost and Gambacorta (2022) and Cornelli et al (2023). Note that in some cases, cryptocurrency can be used to buy products in non-crypto businesses. For example, El Salvador made Bitcoin legal tender in 2021, yet usage remains low (Alvarez et al (2022)).

[7] See BIS (2018) and Boissay et al (2022).

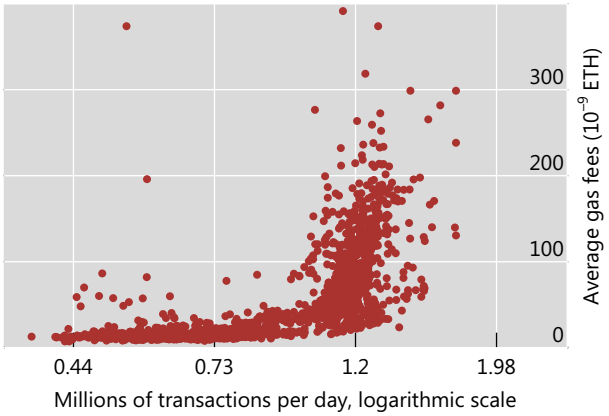
yield higher returns than the potential gains from cheating. Should rewards become too low, individual validators would have an incentive to cheat and steal funds, jeopardising overall security (Budish, 2022).

A common way to reward validators so as to maintain incentives is to limit the capacity of the blockchain, thereby maintaining high fees sustained by congestion (Huberman et al (2021)). As validators can choose which transactions are validated and processed, periods of congestion see users offering higher fees to have their transactions processed (Graph 3.A). Congestion and high fees also mean that payments systems based on decentralised blockchains will remain comparatively slow and expensive.

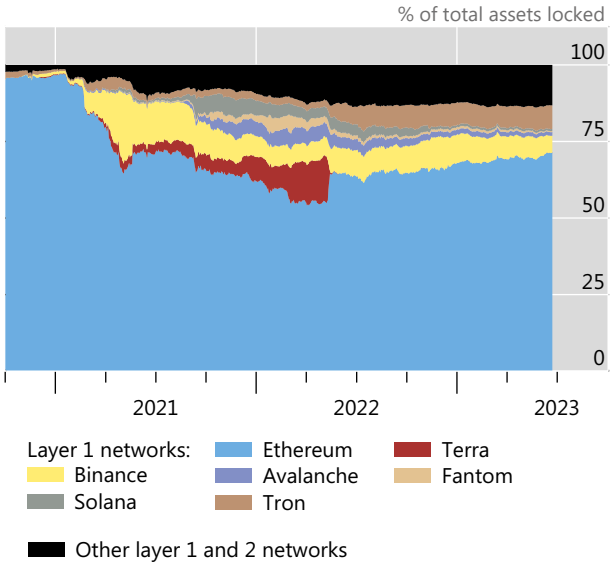
Blockchain congestion leads to fragmentation

Graph 3

A. Network congestion leads to high gas fees on the Ethereum network[1]



B. Fragmentation of layer 1 blockchains[2]



[1] Outliers larger than 450 Gwei (10^{-9} ETH) are excluded from the graph. [2] Based on total value locked which corresponds to the aggregate of all funds locked in a DeFi smart contract.

Source: Boissay et al (2022).

The blockchain capacity problem is a manifestation of the so-called scalability trilemma (Buterin (2021)). By their nature, permissionless blockchains can achieve only two of the three properties: security, decentralisation and scalability. Security – in the sense of truthful reporting and preventing manipulation of the transaction history – is enhanced through incentives and decentralisation. But sustaining incentives entails congestion, which limits scalability. It is this incompatibility between three key attributes that impairs blockchains' ability to serve as an efficient payment system and crypto's ability to serve as money.

Limited scalability has resulted in the fragmentation of the crypto universe, as newer blockchains with more capacity that possibly cut corners on security entered the fray. These newer blockchains often aim for higher transaction limits, even if these come at the cost of greater centralisation and weaker security. Simply put, on blockchains that rely on a larger network of validators and where each validator has only limited influence over the consensus, it is harder for one validator to manipulate the ledger. But this also means that every transaction takes longer to be validated, implying higher costs for users, and hence higher required rewards. Such blockchains therefore become congested more rapidly. On blockchains with fewer validators, on the other hand, there is more potential for a smaller group of validators to manipulate the network.

The Terra blockchain was just the most glaring example of a large number of new entrants (Graph 3.B). As recently as the beginning of 2021, Ethereum accounted for almost all of the total value locked in DeFi protocols. By May 2022, this share had dropped to 50%. The widening wedge (red area) accounted for by the failed Terra blockchain is particularly striking, as the collapse of the Terra blockchain highlights the tendency to fragmentation through crypto's vulnerability to new entrants who prioritise market share and capacity at the expense of decentralisation and security.

A system of competing blockchains that are not interoperable introduces new risks of hacks and theft. In this context, interoperability refers to the ability of protocols and validators to access and share information, as well as validate transactions, across different blockchains.[8] Interoperability of the underlying settlement layers is not achievable in practice, as each blockchain is a separate record of settlements. Nevertheless, so-called cross-chain bridges have emerged to permit users to transfer coins across blockchains. Yet, most bridges rely on only a small number of validators, which – in the absence of regulation and legal accountability – users need to trust not to engage in illicit behaviour. As the number of bridges has risen, they have stood at the centre of several high-profile hacks, highlighting vulnerabilities to security breaches stemming from weakness in blockchain governance. Such hacks could further lower trust in the broader fintech sector, standing in the way of greater adoption (Chen et al (2023), Doerr et al (2023)).

The fragmentation of the crypto universe stands in stark contrast to the network effects that take root in traditional networks. Crypto's reliance on decentralised validators and the attendant fragmentation leaves no role for money as a coordination device, making crypto unsuitable as a monetary system. Traditional networks, on the contrary, are characterised by the "winner takes all" property, whereby more users flocking to a particular platform beget even more users. Such network effects are at the heart of the virtuous circle of lower costs and enhanced trust in traditional platforms.

3.1.2 Stablecoins and the search for a nominal anchor

Fiat-backed stablecoins, the dominant form of stablecoin, piggyback on the credibility of the central bank's unit of account. Having a unit of account means that everyone uses it as a common measure of the economic value of products and services, greatly facilitating financial and economic transactions. In the real world, providing the unit of account for the economy is the primary role of the central bank. While there is no such thing as a central bank in the crypto universe, it needs to have a unit of account, like any monetary system. Stablecoins attempt to serve this unit-of-account function, but they do so by tying their value to fiat currencies, such as the dollar, whose value is guaranteed by a central bank. In this sense, stablecoins are the manifestation of crypto's existential search for a nominal anchor.

Yet stablecoins suffer from a number of shortcomings that threaten their claim to stability. For one, they are subject to an inherent conflict of interest whereby issuers are incentivised to invest in risky assets. The robustness of stablecoin stabilisation mechanisms hence depends crucially on the quality and transparency of their reserve assets, which are often lacking.[9] In addition, they benefit neither from the regulatory requirements and protections of bank deposits and e-money, nor from the credibility of the central bank defending the peg. Moreover, as stablecoins are transferable liabilities and transactions do not settle on the central bank balance sheet, their exchange rate can fluctuate away from par.[10]

[8] See Buterin (2016).

[9] See Arner et al (2020); Catalini and de Gortari (2021); Frost et al (2020); Gorton and Zhang (2022); Ahmed et al (2023).

[10] In other words, stablecoins cannot guarantee the "singleness of money" (see Garratt and Shin (2023)).

Box A

The collapse of the TerraUSD stablecoin

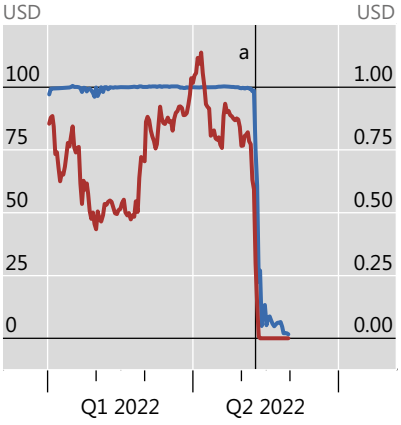
The use of TerraUSD (UST) grew rapidly over 2021–22 so that, prior to its collapse in mid-2022, it was the third largest stablecoin, with a peak market capitalisation of almost $19 billion. An *algorithmic stablecoin*, UST aimed to keep a one-for-one peg to the US dollar by being convertible into one dollar's worth of another cryptocurrency, Luna, on the Terra blockchain, and vice versa. For example, should Terra fall to 99 cents, a user could purchase UST on an exchange for 99 cents and then exchange their UST for $1 worth of new units of Luna on the Terra platform. A crucial aspect of this arrangement was that users would be willing to exchange UST into Luna only if Luna's market capitalisation exceeded that of UST. As Luna had no intrinsic value, its valuation stemmed primarily from the influx of speculative users into the Terra ecosystem. To attract new users, the associated lending protocol Anchor offered a deposit rate of around 20% on UST. As long as users had confidence in the stable value of UST and the sustained market capitalisation of Luna, the system could be sustained.

However, once investors lost confidence in the system's sustainability, the arrangement unravelled. In May 2022, the value of UST plummeted to almost zero (Graph A1.A). As UST dropped below its peg, a classic run dynamic took hold as investors sought to redeem their funds. Users burned their UST on a large scale to mint one dollar's worth of new Luna, in the hope of selling Luna while it still had some value. However, given the size and speed of the shock, confidence evaporated, meaning that there were not enough parties willing to buy all the newly minted Luna coins – and so the price of Luna collapsed.

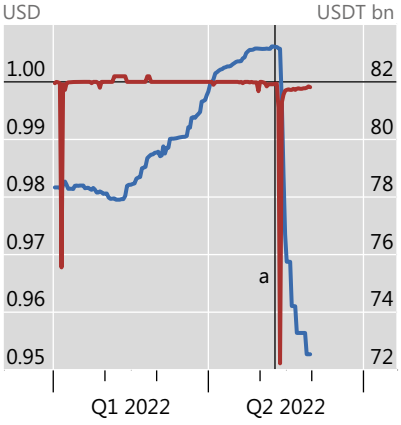
The TerraUSD implosion and fragilities in stablecoins

Graph A1

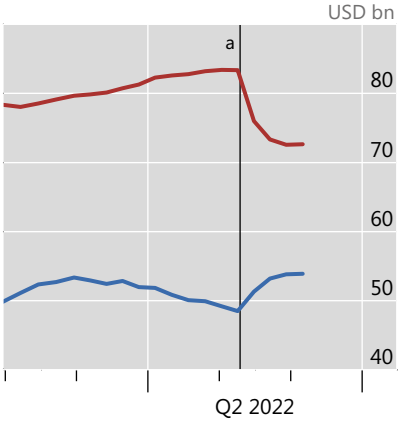
A. Terra and Luna coins dropped in value rapidly



B. Tether briefly lost its peg and suffered $10bn in outflows[1]



C. Investors moved to USD Coin and other asset-backed stablecoins



[a] TerraUSD and Luna collapse starting on 9 May 2022.

[1] The price corresponds to the low price.

Source: BIS (2022).

The UST/Luna implosion spilled over to the largest stablecoin, Tether, which dropped to a value of $0.95 before recovering. It saw outflows of over $10 billion in the subsequent weeks (Graph A1.B). The de-pegging has been linked to Tether's unwillingness to provide details about its reserve portfolio: investors worried about whether Tether had enough high-quality assets that could be liquidated to support the peg. This argument is supported by the inflows experienced by the regulated stablecoin USDC (with better documented reserves), with funds probably coming from Tether (Graph A1.C).

A case in point has been the above-mentioned implosion of TerraUSD, which in May 2022 lost nearly its entire value over the course of a few days (Box A). In the aftermath, several fiat-backed stablecoins saw large-scale redemptions, temporarily losing their peg. Redemptions were more pronounced among stablecoins whose issuers did not disclose the composition of reserve assets in detail, presumably reflecting investors' worries that such issuers might not be able to guarantee conversion at par. Indeed, stablecoins have proved to be not that stable.

3.1.3 False decentralisation claims and their consequences

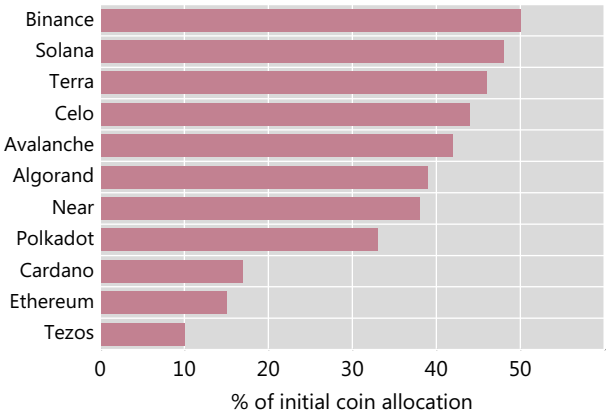
Crypto proponents argue that decentralisation guarantees the safety of the system. However, there is often a de facto concentration of decision-making power. While centralisation is not a structural flaw per se, it introduces new risks and invalidates arguments made by proponents of crypto and DeFi that stress its purportedly decentralised nature.

Concentration arises partly from congestion effects in decentralised platforms with proof-of-work systems. To reduce congestion, newer proof-of-stake blockchains require validators to post their coins as collateral, which gives them a better chance of being paid for validating the next block. However, this can lead to a concentration of power and coins among a small number of validators, since operational costs are mostly fixed (Auer, Frost and Vidal Pastor (2022)).

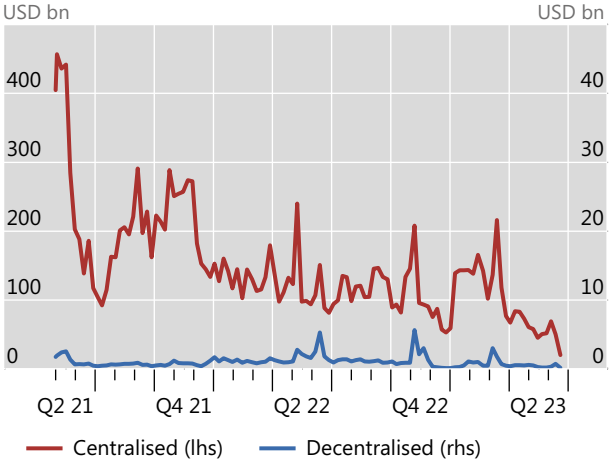
"Contract incompleteness", ie the inability to write contracts that can cover all future possible eventualities, is another reason for centralisation. It is recognised that centralisation can allow economic agents to overcome contract incompleteness. This has an analogue in the DeFi space in the concept of "algorithm incompleteness", namely the inability to write code that covers all potential situations and outcomes. Consequently, DeFi platforms must have some degree of central governance to address these gaps in code and outline strategic and operational priorities. This element of centralisation is typically represented by "governance tokens", held to a large extent by platform developers and early investors (ie insiders) who vote on proposals (Graph 4.A). With the increasing centralisation of validators, the risk of attacks and hacks increases, not least as these centralised nodes are often unregulated.[11]

Insiders control token allocation and centralised exchanges dominate volumes — Graph 4

A. Coins are often allocated to insiders



B. Weekly trading volume[1]



[1] Centralised = Binance and Coinbase; Decentralised = Curve.fi, PancakeSwap (v2) and Uniswap (V2). Weekly averages of daily values.

Sources: Auer, Frost and Vidal Pastor (2022); BIS (2022).

[11] See IOSCO (2022).

DeFi's inherent need to obtain information from the real world also represents an important impediment to decentralisation. While DeFi, in principle, relies on decentralised and consensus-based trust, the reporting of data that underpins smart contracts relies on oracles. Oracles process and source the data, ultimately transmitting this information to the blockchain. As oracles require trust and exhibit various degrees of centralisation, this gives rise to the "oracle problem" (Box B). In the extreme, some use a single data source or have a single person/entity in charge of transmitting information to the platform. This introduces a single point of failure and leaves room for untruthful reporting, as whoever oversees the

Box B

The oracle problem

Decentralised finance (DeFi) needs to import data from the real world, which creates a practical conundrum: it is impossible to import data into a blockchain without involving a third party (the oracle).

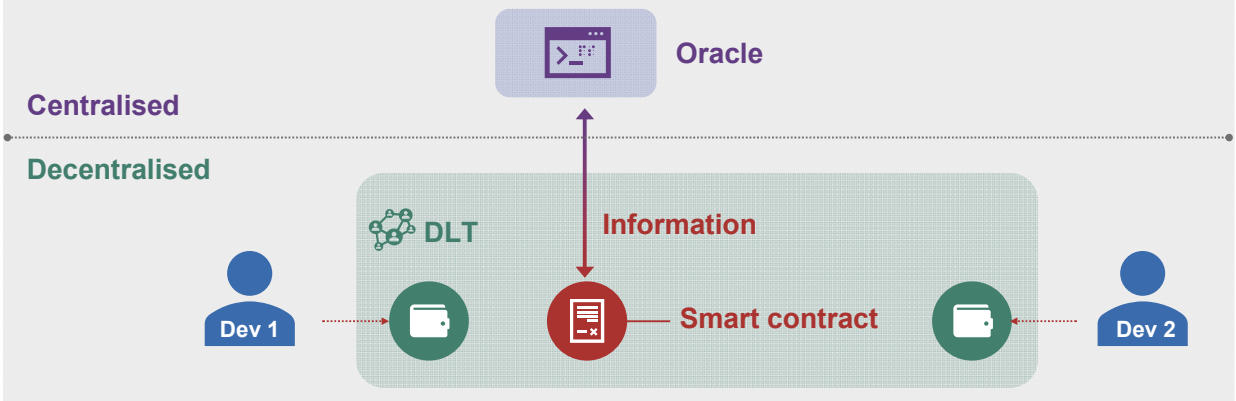
The oracle problem arises because oracles introduce centralisation to a decentralised system, overriding the reliance on consensus as a trust mechanism (Graph B1). Oracles with a high degree of centralisation rely on a single data source or have a single person/entity responsible for transmitting information to the platform. This reliance on one source introduces a single point of failure and leaves room for manipulation when the data source is not trustworthy.

Three main risks emerge. First, the anonymity of agents in a DeFi setting may increase incentives for malicious behaviour. In traditional finance (TradFi), when manipulations are detected, the identities of the manipulators are typically revealed, and those individuals are held accountable for malpractice by supervisory agencies and others. The open and transparent nature of DeFi may make detection of fraud easier, but the inability to identify and hold responsible individuals accountable makes DeFi systems more susceptible to manipulation. Second, the lack of regulation or oversight of oracle providers makes recourse less clear in DeFi. Although there are legal challenges surrounding information falsification in TradFi, established legal systems provide the basis for assigning penalties, compensating victims and, in some cases, clawing back funds. Third, the terms of smart contracts and the data inputs they reference on the blockchain are immutable, which makes errors or illegal actions more costly than in traditional financial settings. Once data are validated on the blockchain, they cannot be corrected, and all smart contracts that reference that data will continue to do so.

Technological efforts to decentralise oracles involve adding consensus mechanisms to information provision processes, for instance through a group of independent blockchain oracles. These solutions try to reintroduce decentralised trust at the expense of speed and efficiency, since the more networks are added to guarantee truth, the more delays will be introduced throughout the lifecycle of a smart contract.

The oracle problem

Graph B1



Source: adapted from Duley et al (2023).

oracle has the ability to corrupt the system by misreporting data. Currently, there are no clear rules as to how oracle providers are incentivised or vetted, or who is held accountable if a smart contract acts upon incorrect off-chain information.

Finally, centralisation is also present in crypto trading activities, where investors rely mainly on centralised exchanges (CEXs) rather than decentralised ones. While the latter work by matching the counterparties in a transaction through so-called automated market-maker protocols, CEXs maintain off-chain records of outstanding orders posted by traders – known as limit order books – which are familiar from traditional finance. CEXs attract more trading activity than DEXs because of their lower costs (Graph 4.B). Even though crypto CEXs mimic some functions of traditional exchanges, they are not subject to the same regulation and supervision.

Reliance on CEXs can jeopardise users' investments, as these exchanges have repeatedly shown to be lacking even basic risk management controls and governance standards. The most prominent examples include the failure of bitcoin exchange Mt Gox in 2014, which resulted in the loss of more than $400 million worth of bitcoin, and the bankruptcy of FTX in November 2022, which caused losses to its customers of billions of dollars, among many others.

3.2 Risks

When discussing the risks of crypto, it is important to note that, to date, the ecosystem is largely self-referential. Activities almost exclusively involve exchanging one stablecoin or cryptocurrency for another, without financing any activity in the real economy. In consequence, crypto currently poses significant risks mainly to investors in the crypto space, while links to the real world remain limited.

3.2.1 Within the crypto ecosystem

Crypto poses significant risks to investors. Rising crypto prices tend to lure retail investors into the space, with an expectation of quick and large capital gains (Graph 5.A).[12] These expectations are generally not met, however, as a large share of users in most economies tend to lose money (Graph 5.B).

The events of 2022 illustrate vividly the risks faced by investors, especially smaller ones.[13] The aftermath of the collapses of TerraUSD and FTX saw a striking pattern: the number of daily active users across the major platforms increased markedly, suggesting that users attempted to weather the storm by shifting their portfolios away from stressed tokens into safer alternatives, including asset-backed stablecoins (Graphs 6.A and 6.B). However, behind this flurry of activity, large investors appear to have benefited at the expense of smaller holders. Indeed, owners of large wallets reduced their bitcoin holdings, whereas medium-sized and especially smaller holders increased their holdings (Graph 6.C).

The lack of control mechanisms in many crypto firms implies that investors' money is at high risk if these firms face funding challenges or the threat of bankruptcy. For instance, following its failure, it emerged that FTX owed more than $3 billion to its unsecured creditors – mainly users of the exchange who had transferred their funds there. FTX was not the only case in which this happened. Many of the customers of other crypto firms that failed in recent years have been unable to access their funds or have had to wait a very long time to do so.[14]

[12] See Auer, Cornelli, Doerr, Frost and Gambacorta (2022).

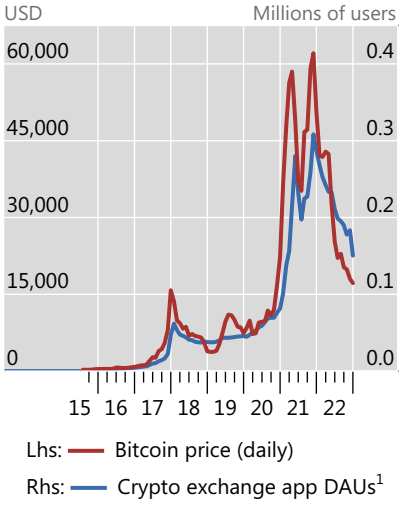
[13] See Cornelli et al (2023).

[14] With the start of the latest crypto winter and in the aftermath of the demise of TerraUSD, there were numerous failures beyond FTX, with those of Celsius, Voyager, BlockFi, Three Arrows Capital and Genesis being the most prominent.

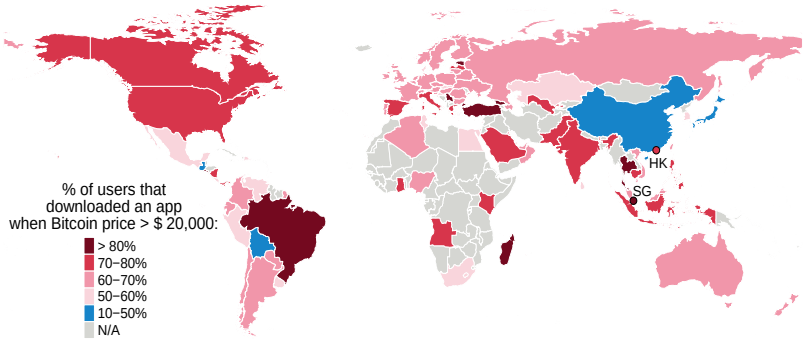
Retail investors have chased prices, and most have lost money

Graph 5

A. More users trade when the Bitcoin price increases…



B. …and a large share of users in nearly all economies probably lost money[2]



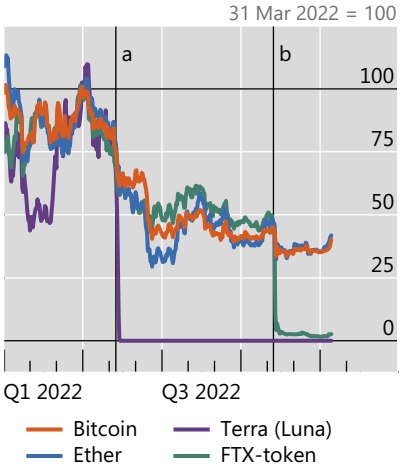
[1] Cross-country monthly average of daily active users (DAUs). Calculated on a sample of more than 200 crypto exchange apps over 95 countries. [2] The use of this map does not constitute, and should not be construed as constituting, an expression of a position by the BIS regarding the legal status or sovereignty of any territory or its authorities, the delimitation of international frontiers and boundaries and/or the name and designation of any territory, city or area. Based on data up to mid-December 2022.

Sources: Auer, Cornelli, Doerr, Frost and Gambacorta (2022); Cornelli et al (2023); CCData; Sensor Tower.

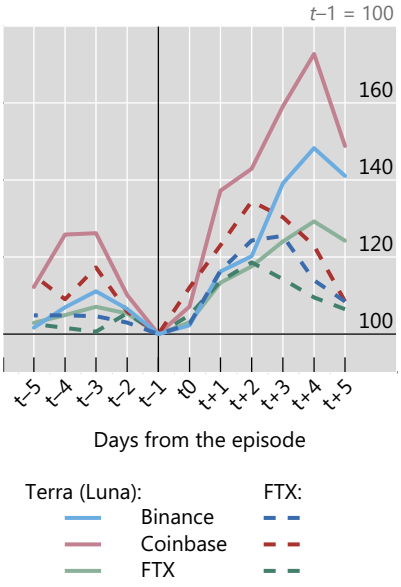
In stormy seas, "the whales eat the krill"

Graph 6

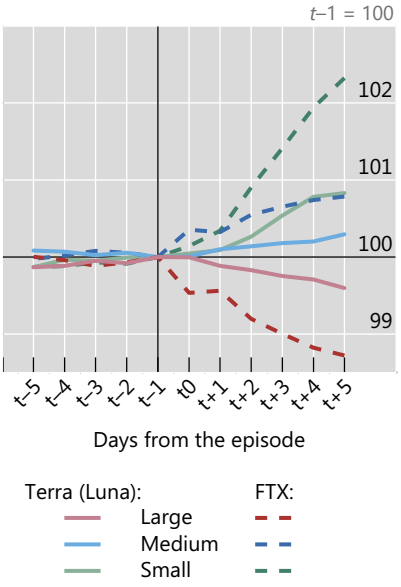
A. As prices tumbled…



B. …all users traded more…[1]



C. …but whales sold while krill bought[2]



[a] TerraUSD and Luna turmoil, 8 May 2022. [b] FTX collapse, 7 November 2022.

[1] Based on daily active users of crypto exchange apps. [2] Based on the number of BTC held in addresses with balances of less than 1 BTC (small), 1–1,000 BTC (medium) and more than 1,000 BTC (large).

Sources: Cornelli et al (2023); IntoTheBlock; Sensor Tower.

Crypto is probably also used for illicit activities such as money laundering, the financing of terrorism and tax evasion. Pseudo-anonymity and lack of oversight certainly contribute to these risks. The use of crypto thereby presents important challenges for regulators and law enforcement agencies, as they may find it hard to track and trace crypto transactions. To address these risks, measures aimed at better governance, anti-money laundering (AML) and combating the financing of terrorism (CFT) are needed. Effective governance frameworks can ensure that market participants are operating in a transparent and accountable manner, promoting the integrity of the financial system. The Financial Action Task Force has developed guidance on registration and licensing requirements for service providers in the crypto space (FATF (2021, 2022)).

3.2.2 Risks in DeFi

The DeFi ecosystem amplifies several risks that are also present in the traditional financial system (FSB (2023)). Of particular relevance are operational risks, its reliance on leverage and the complex web of interconnections within the system, which make it particularly prone to episodes of instability.

Operational risks

While all services are subject to operational risk, a number of DeFi features make such risks particularly acute. These may cause operational disruptions and hinder the ability to deliver services and products.

The first type of operational risks in DeFi are those linked to governance frameworks. As these frameworks are often unclear, opaque, untested and easy to manipulate, they can mislead users about the claims and safeguards of DeFi activities. In addition, there is uncertainty over what ex post remedial protections are available to participants. For instance, developers and founders at times lack the incentives to maintain DApps once they receive the initial investment. This may expose users to losing their money in "rug pulls" – a risk that is compounded by the difficulty of making developers and founders accountable for their actions, as their economic incentives are unclearly expressed and poorly disclosed and the system features a pseudo-anonymous structure.

The need for centralisation poses further problems. The holding of voting power across major decentralised autonomous organisations (DAOs) – which are responsible for managing many DApps – is highly concentrated, implying that in practice only a few controlling actors can propose, pass or implement initiatives (Feichtinger et al (2023)). Disagreements about governance decisions can occur, leading to forks and network splits. This can materialise in losses for investors and a loss of confidence in DeFi protocols, which could spill over to other markets.

The second type of operational risk in DeFi is linked to its dependence on the proper functioning of the underlying blockchains. Disruptions to the blockchain caused by outages, network congestion or consensus failure can affect the cost, functioning and performance of the blockchain and the DeFi services that rely on it.

A third source of operational risk is the use of smart contracts. Smart contracts need to account for many possible states of the world before they are deployed, creating complexity. In turn, such complexity increases the potential for coding errors and consequent unexpected behaviour. Immutability implies that it is not possible to correct mistakes and reinstate the status quo ante without the consensus of blockchain validators.

Fourth, oracles and bridges can be an additional source of operational risk in DeFi. The functioning of many DeFi protocols critically relies on oracles. Errors in, manipulation of, or attacks on oracles may trigger actions in one protocol (eg liquidations or margin calls) with unanticipated negative consequences in other protocols (eg in algorithmic reserve assets or collateral management). Therefore, oracles could be critical in initiating or propagating a shock.

A similar risk is related to cross-chain bridges. Separate blockchains are not interoperable, requiring bridges that connect protocols across various blockchains. Typically, a bridge will hold (collect) assets from one chain or protocol and issue or release assets on another chain or protocol for the same value. This allows asset holders to transact across chains or protocols but creates repositories potentially holding large amounts of assets, rendering them targets for theft and misappropriation.

Collateral and leverage

Due to pseudo-anonymity, financial intermediation in DeFi largely rests on the re-use of collateral. The reason is that the identity of borrowers and lenders is hidden behind cryptographic digital signatures. Lenders thus cannot access information such as borrowers' credit scores, but require crypto collateral to align incentives.[15]

The ubiquitous presence of collateral leads to procyclicality and can trigger sharp adjustments in prices that have knock-on effects on other market segments. In booms, appreciating prices mean that collateral values increase, while collateralisation ratios fall. In busts, loans are liquidated as prices – and hence collateral values – decline sharply, suppressing lending activity. This mechanism is further amplified when borrowed cryptoassets are used as collateral for additional loans (akin to rehypothecation). The specific features of DeFi relating to the management of leverage – in particular, the automatic liquidation of collateral – are a primary reason why deleveraging dynamics in DeFi can be especially strong.

Automated risk management tools serve to protect the lender but raise financial stability concerns for the DeFi ecosystem due to their system-wide effects. In these protocols, loans for which collateral falls in value below a certain threshold trigger an automatic liquidation. If these liquidations occur under stressed conditions, collateral may be forcibly liquidated into a market with low liquidity, pushing collateral prices down further, leading to contagion. In the traditional financial system, such self-reinforcing dynamics can be alleviated via orderly liquidation at central counterparties or by human intervention, or it can be arrested by market circuit breakers. Such mechanisms are absent in DeFi.

Intra-connectedness and complexity

DApps are considerably interconnected with each other. Further, the DeFi ecosystem as a whole is closely intertwined with other parts of the crypto ecosystem. Thanks to the composability properties of DeFi, DApps often employ multiple smart contracts and interact with multiple protocols, which create strong interdependencies across smart contracts. As a result, problems in a single smart contract could propagate across the entire ecosystem. As such, composability can amplify the reach and speed of financial contagion within DeFi or lead smart contracts to interact in unexpected ways. Compounding this issue is the fact that smart contract code is widely re-used, such that seemingly independent contracts may in practice be subject to the same vulnerabilities. In sum, the various components of DeFi are highly interconnected, so that assessing one element of the crypto system in isolation falls short of assessing its role in the overall ecosystem.

3.2.3 Interconnectedness with the traditional financial system

The interplay between the crypto market, traditional finance and the real economy has remained limited so far (Auer, Farag, Lewrick, Orazem and Zoss (2022)). As crypto remains a largely self-referential vehicle used mainly for speculation, this is perhaps not surprising. In fact, the existing links result in large part from crypto's need to interact with traditional finance to sustain its growth. However, institutional investors and households continue to show interest in crypto despite the events of the past year. Hence the potential for these linkages to grow further cannot be ignored.

[15] Aramonte et al (2022) develop these arguments in more detail.

Among these linkages, the relationship between crypto and the core banking sector is of particular importance. The fall in crypto prices that started in the second half of 2022 did eventually spill over to the traditional financial system. In March 2023, for instance, California-based Silvergate Bank – widely touted as a key "crypto bank" – had to cease operations after haemorrhaging a large amount of client deposits. Similarly Signature Bank, which also specialised in serving the crypto industry, was wound down by authorities shortly thereafter. These cases highlight that a business model that is highly exposed to crypto can be problematic for the banking sector.

Banks could also increase connections to crypto through credit provision to counterparties with crypto exposures or through custody and other crypto-related services to their clients. Recognising those risks, the Basel Committee on Banking Supervision (BCBS) recently endorsed a global prudential standard for banks' exposures to cryptoassets (BCBS (2022)). Moreover, risks along the bank-crypto nexus extend beyond (direct and indirect) exposures because of the potential negative externalities associated with banks channelling funds into the crypto ecosystem, given their role as the mainstay of the monetary system. Along with banks, other financial entities such as family offices, hedge funds and asset managers could also increase their crypto investments, lured by the potentially high returns.

Tokenisation of claims on real-world assets, such as stocks or real estate, is another way through which the interconnections between traditional finance and crypto could grow. This could result in the growth of crypto itself, as new money gets channelled into such tokenised assets. It could also engender a more complex web of interconnections between crypto and traditional finance as the activities of the entities in these two ecosystems become more intertwined. In this scenario, the systemic importance of the crypto ecosystem could increase substantially.

Crypto's growing interconnectedness with traditional finance and the real economy may also pose a threat to monetary sovereignty. The availability of stablecoins, in particular, may facilitate cryptoisation, ie the substitution of local currencies with crypto-based ones.[16] During periods of macroeconomic instability and depreciating exchange rates, holders of domestic fiat currencies might shift into alternative currencies, putting additional pressure on the domestic currency itself. Such a behaviour may result in the loss of monetary sovereignty for domestic monetary authorities as well as the crowding out of funding for local financial institutions, with long-term consequences for the overall monetary and financial stability of these countries. To be sure, the risk of currency substitution is always present and it is incumbent upon each jurisdiction to manage it properly. However, the existence of crypto and stablecoins can substantially increase the likelihood of such scenarios materialising, as it makes currency substitution much easier in practice. Should stablecoins be issued by big tech companies, taking advantage of the self-reinforcing data-network-activities loop that enables them to exploit ever-growing network effects (Shin (2019)), the threat to monetary sovereignty may be greatly exacerbated.

Interconnections between crypto and the traditional financial system can work both ways. For instance, as a consequence of the bank turmoil in March 2023, some stablecoins lost their peg – most notably USDCoin after disclosing that a substantial amount of its cash reserve was deposited in Silicon Valley Bank. Stablecoins that used USDCoin as a reserve asset also broke par, whereas other stablecoins traded at a premium. These events demonstrated that it is likely not possible to develop truly stable stablecoins, ie stablecoins that can maintain their peg against all circumstances, even if they invest mainly or exclusively in safe assets.

3.2.4 Risks to emerging market and developing economies

Several risks related to crypto and stablecoins are exacerbated in emerging market and developing economies (Feyen et al (2021), UNCTAD (2023), Prasad (2023)).

[16] See IMF (2021).

First, stablecoins could pose severe risks to the integrity of the financial system, including for AML/CFT. While this risk is present in all countries, resource constraints in emerging market and developing economies (EMDEs) may make it more difficult for authorities to keep pace and adjust their surveillance, regulatory and supervisory frameworks.

Second, stablecoins pegged to foreign currencies would fluctuate in value against local currencies in EMDEs. If used for debt contracts, this would be a de facto new form of foreign exchange (FX) lending, which has been at the heart of many financial crises in EMDEs.

Third, stablecoins could import the monetary policies of the fiat currencies in the basket, which may not be optimal for most EMDEs and could thus impinge on their monetary autonomy (IMF (2023a)). Countries with large cross-border inflows in stablecoins may face difficulties in maintaining international reserves in hard fiat currencies. This has implications for the functioning of FX and interbank markets, which are shallower in EMDEs. Liquidity and redemption shocks may thus create disruptive spillovers.

Fourth, and related to the points above, the risks of cryptoisation outlined in the previous section are particularly acute for EMDEs. Stablecoins can facilitate currency substitution and the evasion of measures that EMDEs may use to defend their currencies during periods of elevated FX volatility.

Fifth, given reach, scale, network and "winner takes all" effects, EMDEs might end up as a "host" to entities in a stablecoin system that provide critical services such as governance and reserve asset management, which may be headquartered elsewhere. This could create a misalignment of incentives between "home" and "host" supervisors, impeding a holistic oversight. As such, EMDE authorities may lack control over the broader stablecoin arrangement and its operations that involve residents. When domestically adopted at scale, this could inhibit risk monitoring and effective oversight of payments to prevent illicit use and to safeguard financial stability.

3.3 Addressing the risks in crypto

The numerous risks posed by crypto have naturally generated a debate on the optimal policy strategies for mitigating them. A *BIS Bulletin* (Aquilina et al (2023)) outlined three non-mutually exclusive lines of action that could be pursued in the policy toward crypto – namely, a combination of *containment, regulation* and *bans*. The *Bulletin* contains details of the three approaches, together with specific examples.

Several jurisdictions are already taking various policy actions along the above spectrum. More concretely, this includes bans, restrictions, clarifications, bespoke requirements and initiatives to facilitate innovation.[17] Most initiatives adopted so far tend to target centrally managed activities (most notably, issuers of security tokens and stablecoins) and are a function of market developments in each jurisdiction.

Multilateral initiatives in this area, coordinated by the Financial Stability Board (FSB), are already taking steps to reach consensus on the appropriate regulatory actions. The FSB has already published a proposed framework for the international regulation of cryptoasset activities (FSB (2022)). This framework contains two core components. First, it makes recommendations that promote the consistency and comprehensiveness of regulatory, supervisory and oversight approaches to cryptoasset activities and markets, and strengthen international cooperation, coordination and information-sharing. Second, it sets out revised high-level recommendations for the regulation, supervision and oversight of "global stablecoin" arrangements to address the associated financial stability risks more effectively. The IMF has also published its view on the core elements of an effective policy framework for addressing the risks posed by cryptoassets (IMF (2023b)).

[17] See FSI (2023) for an overview of the crypto regulatory landscape across 19 jurisdictions.

More broadly, public authorities could also complement the above lines of action by encouraging sound innovation within the traditional financial system or through the use of central bank digital currencies (Aquilina et al (2023)). Improving the quality and reducing the costs of payments would be an important component of such a strategy. This could be achieved by introducing retail fast payment systems, such as the Unified Payment Interface (UPI) in India, Pix in Brazil, FedNow in the United States or initiatives such as the Single Euro Payments Area (SEPA). Another important component of this broader strategy would be issuing central bank digital currencies that meet real needs. If properly designed and implemented, such initiatives could support sound private sector innovation, while reducing the cost of payments, enhancing financial inclusion and bolstering the integrity of the financial system.

3.4 Addressing data gaps: Project Atlas

Data on crypto activities come from two sources: on-chain data from blockchains and off-chain data reported by market actors. Data are spread across a vast network of distributed ledgers, exchanges and other providers. Figures on basic indicators such as market size and crypto usage hence lack transparency, consistency and reliability (ESRB (2023)).

Data gaps hamper efforts to develop a coherent monitoring framework for crypto at large.[18] These issues stem in large part from (i) the difficulty in aggregating, reconciling and analysing the data available on distributed ledgers; (ii) the pseudo-anonymity that inhibits the ability to ascertain the types of cryptoasset investors who may be the beneficiaries of multiple wallets; and (iii) the large number of off-chain transactions. These data gaps stand in the way of a proper assessment of potential risks.

In response to these data challenges, the BIS Innovation Hub Eurosystem Centre, the Deutsche Bundesbank and De Nederlandsche Bank have initiated Project Atlas, which will shed light on the macroeconomic relevance of cryptoasset markets and DeFi. The data will be based on a transparent methodology and tailored to the needs of public authorities. It will blend reported data gathered from crypto exchanges and stablecoin issuers with data from public blockchains. By attributing blockchain transactions to crypto exchanges and their geographic locations, Atlas will be able to derive and visualise cross-border flows around the globe.

Preliminary data from Project Atlas reveal that, although relatively small in comparison to total network traffic, flows between centralised crypto exchanges are substantial (Graph 7.A). Attributing geographic locations to exchanges (where possible) lays out the structure of cross-border flows and provides a starting point for evaluating the relative economic significance across jurisdictions (Graphs 7.A and 7.B). This indicates non-negligible – and growing – use of cryptocurrencies for cross-border capital flows.

Nevertheless, further steps are needed for a holistic assessment of crypto markets. Cooperation on data collection and monitoring by individual jurisdictions can facilitate the development of appropriate policy responses. Such cooperation could also help with enforcement actions for illicit activities. Currently the lack of standards implies that data on crypto are usually limited to what companies report voluntarily or dependent on companies whose business model is to sell data to market participants. For on-chain data, the choice of methodologies greatly influences the reported numbers while the exact heuristics and methodologies are often unclear. Accordingly, data are often reported differently by various analytics companies and are difficult to compare across time and space.

With respect to DeFi, the FSB (2023) highlights three types of indicators that authorities should be monitoring to assess vulnerabilities and risks. First, indicators that can help to gauge the overall size and evolution of the sector. Second, indicators especially designed to assess financial vulnerabilities. And

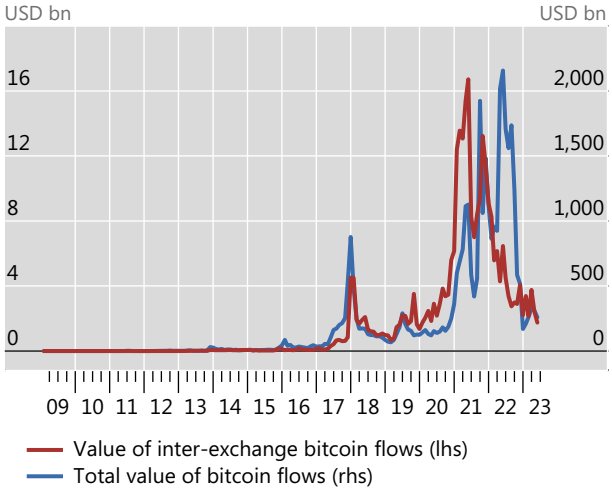
[18] See FSB (2023) and IMF (2023).

third, indicators that can help gauge the potential for spillovers by tracking and assessing interconnections between DeFi, CeFi, traditional finance and the real economy.

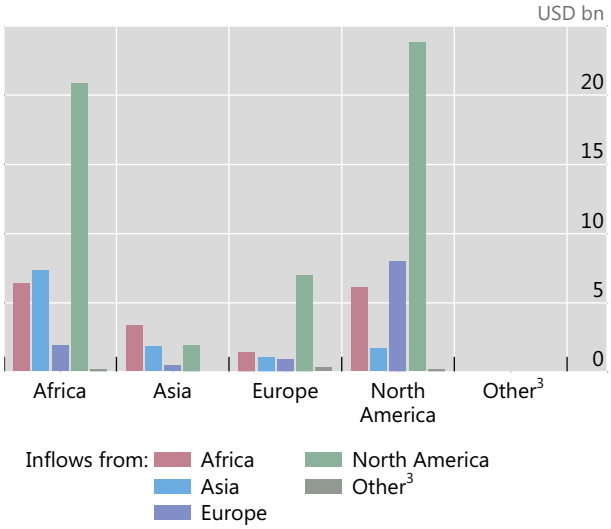
Bitcoin flows between exchanges[1]

Graph 7

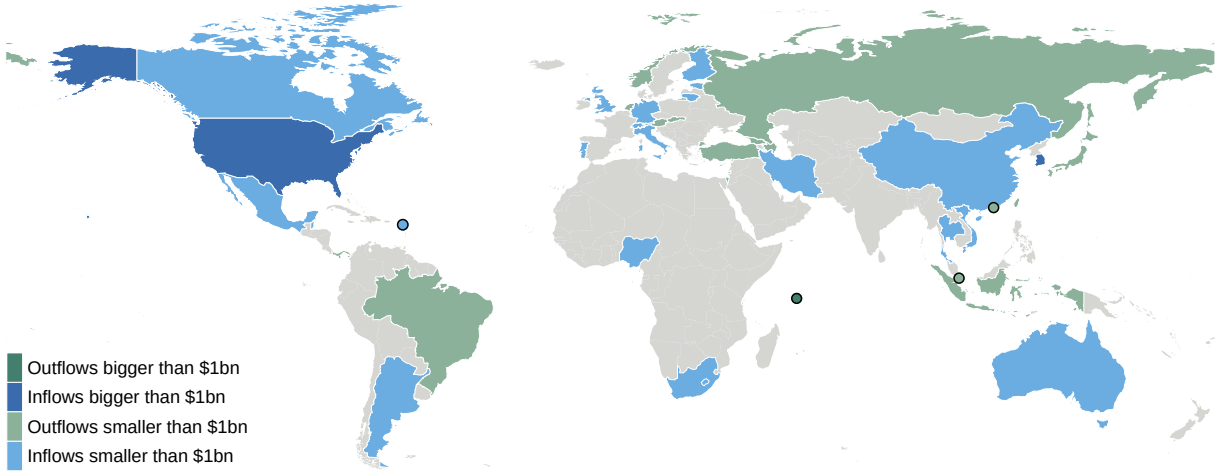
A. Inter-exchange and total flows[1]



B. Inflows by continent[2]



C. Net flows by country[4]



[1] Inter-exchange flows are a lower bound estimate. The calculation of total flows excludes certain transaction types (eg coinbase transactions), flows between the same addresses as inputs and outputs in a transaction and transactions between addresses attributed to the same crypto exchange. [2] Preliminary daily data for the period Jan–Dec 2022, based on the location of exchanges for which flows are identified, not on users' location. [3] Latin America and Oceania. [4] The use of this map does not constitute, and should not be construed as constituting, an expression of a position by the BIS regarding the legal status or sovereignty of any territory or its authorities, the delimitation of international frontiers and boundaries and/or the name and designation of any territory, city or area. The circles represent Antigua and Barbuda, Hong Kong SAR, Seychelles and Singapore. Preliminary daily data for the period Jan–Dec 2022, based on the location of exchanges for which flows are identified, not on users' location.

Source: BIS Innovation Hub Eurosystem Centre Project Atlas.

Developing an accurate picture of crypto and DeFi will require a considerable amount of work to standardise definitions, processes and approaches. Work on these issues is already ongoing in the Data Gaps Initiative, as welcomed by G20 leaders in November 2022.[19]

4. Conclusions

In just over a decade, crypto has gone from niche activity to something that impinges on the mainstream financial system. While initially it was the preserve of a small set of enthusiasts, millions of retail users as well as more and more institutional investors have entered the crypto ecosystem in recent years.

Crypto offers some elements of genuine innovation, such as programmability and composability. With these new functionalities, sequences of financial transactions could be automated and seamlessly integrated. Together with tokenisation, this has the potential to reduce the need for manual interventions that currently delay transactions and create costs (Carstens (2023), Aldasoro et al (2023)).

That said, crypto has so far failed to harness innovation to the benefit of society. Crypto remains largely self-referential and does not finance real economic activity. It suffers from inherent shortcomings related to stability and efficiency, as well as accountability and integrity. These structural flaws result from the underlying economics of incentives rather than technological limitations. Furthermore, while DeFi and crypto for the most part replicate services offered by the traditional financial system, they can exacerbate known vulnerabilities. Taken together, the key takeaways from this report suggest that crypto's inherent structural flaws make it unsuitable to play a significant role in the monetary system.

[19] See IMF (2022).

References

Ahmed, R, I Aldasoro and C Duley (2023): "Par for the course: public information and stablecoin runs", mimeo.

Aldasoro, I, S Doerr, L Gambacorta, R Garratt and P Koo Wilkens (2023): "The tokenisation continuum", *BIS Bulletin*, no 72, April.

Alvarez, F, D Argente and D Van Patten (2022): "Are cryptocurrencies currencies? Bitcoin as legal tender in El Salvador", *NBER Working Papers*, no 29968.

Aquilina, M, J Frost and A Schrimpf (2023): "Addressing the risks in crypto, laying out the options", *BIS Bulletin*, no 66, January.

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

Aramonte, S, S Doerr, W Huang and A Schrimpf (2022): "DeFi lending: intermediation without information?", *BIS Bulletin*, no 57, June.

Arner, D, R Auer and J Frost (2020): "Stablecoins: risks, potential and regulation", *Bank of Spain Financial Stability Review*, November.

Auer, R (2022): "Embedded supervision: how to build regulation into decentralized finance", *Cryptoeconomic Systems*, vol 2, no 1, June.

Auer, R, G Cornelli, S Doerr, J Frost and L Gambacorta (2022): "Crypto trading and Bitcoin prices: evidence from a new database of retail adoption", *BIS Working Papers*, no 1049, November.

Auer, R, M Farag, U Lewrick, L Orazem and M Zoss (2022): "Banking in the shadow of Bitcoin? The institutional adoption of cryptocurrencies", *BIS Working Papers*, no 1013.

Auer, R, J Frost and J Vidal Pastor (2022): "Miners as intermediaries: extractable value and market manipulation in crypto and DeFi", *BIS Bulletin*, no 58, June.

Bank for International Settlements (BIS) (2018): "Cryptocurrencies: looking beyond the hype", *Annual Economic Report*, June, Chapter V.

——— (2022): "The future monetary system", *Annual Economic Report*, June, Chapter III.

——— (2023): "Blueprint for the future monetary system: improving the old, enabling the new", *Annual Economic Report*, June, Chapter III.

Basel Committee on Banking Supervision (BCBS) (2022): "Prudential treatment of cryptoasset exposures – second consultation", June.

Boissay, F, G Cornelli, S Doerr and J Frost (2022): "Blockchain scalability and the fragmentation of crypto", *BIS Bulletin*, no 56, June.

Budish, E (2022): "The economic limits of bitcoin and anonymous, decentralized trust on the blockchain", *University of Chicago, Becker Friedman Institute for Economics Working Papers*, no 83.

Buterin, V (2016): "Chain interoperability", R3 Reports.

——— (2021): "Why sharding is great: demystifying the technical properties", vitalik.ca/general/2021/04/07/sharding.html.

Carstens, A (2023): "Innovation and the future of the monetary system", keynote speech at the Monetary Authority of Singapore, 22 February.

Catalini, C and A de Gortari (2021): "On the economic design of stablecoins", mimeo.

Chen, S, S Doerr, J Frost, L Gambacorta and H S Shin (2023): "The fintech gender gap", *Journal of Financial Intermediation*, vol 54.

Cornelli, G, S Doerr, J Frost and L Gambacorta (2023): "Crypto shocks and retail losses", *BIS Bulletin*, no 69, February.

Doerr, S, L Gambacorta, L Guiso and M Sanchez del Villar (2023): "Privacy regulation and fintech lending", *BIS Working Papers*, no 1103.

Duley, C, L Gambacorta, R Garratt and P Koo Wilkens (2023): "The oracle problem and the future of DeFi", *BIS Bulletin*, forthcoming.

European Systemic Risk Board (ESRB) (2023): "Crypto-assets and decentralised finance. Systemic implications and policy options", May.

Feichtinger, R, R Fritsch, Y Volanthen and R Wattehofer (2023): "The hidden shortcomings of (D)AOs – an empirical study of on-chain governance", mimeo.

Feyen, E, J Frost, H Natarajan and T Rice (2021): "What does digital money mean for emerging market and developing economies?", in R Rau, R Wardrop and L Zingales (eds), *The Palgrave Handbook of Technological Finance*, pp 217–41.

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

——— (2022): *Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers*, June.

Financial Stability Board (FSB) (2022): "Assessment of risks to financial stability from crypto-assets", February.

——— (2023): "The financial stability risks from decentralised finance", February.

Financial Stability Institute (FSI) (2023): "Crypto, tokens and DeFi: navigating the regulatory landscape", *FSI Insights on Policy Implementation*, forthcoming.

Frost, J, P Wierts and H S Shin (2020): "An early stablecoin? The Bank of Amsterdam and the governance of money", *BIS Working Papers*, no 902, November.

Garratt, R and H S Shin (2023): "Stablecoins versus tokenised deposits: implications for the singleness of money", *BIS Bulletin*, no 73.

Gorton, G and J Zhang (2022): "Taming wildcat stablecoins", *University of Chicago Law Review*, vol 90.

Huberman, G, J Leshno and C Moallemi (2021): "Monopoly without a monopolist: An economic analysis of the bitcoin payment system", *The Review of Economic Studies*, vol 88, no 6, pp 3011–40.

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

——— (2022): "G20 Leaders welcome new data gaps initiative to address climate change, inclusion and financial innovation", Press Release, no 22/410, November.

——— (2023a): "G20 note on the macrofinancial implications of cryptoassets", February.

——— (2023b): "Elements of effective policies for crypto assets", IMF Policy Paper, February.

International Organization of Securities Commissions (IOSCO) (2022): *Decentralized finance report*, March.

Nakamoto, S (2008): "Bitcoin: a peer-to-peer electronic cash system", white paper.

Neilson, D H (2021): Stablecoins and DeFi: Banking for unattended contracts, *Soon Parted*, 12 October, https://www.soonparted.co/p/stablecoins-defi..

Prasad, E (2023): "Managing risks from crypto assets and decentralized finance: an emerging market and developing economy perspective", Background Note for G-20 Discussions on Regulation of Crypto Assets, June.

Schär, F (2021): "Decentralized finance: on blockchain- and smart contract-based financial markets", Federal Reserve Bank of St. Louis, *Review*, vol 103, no 2, April.

Shin, H S (2019): "Big tech in finance: opportunities and risks", speech at the BIS Annual General Meeting, June.

United Nations Conference on Trade and Development (UNCTAD) (2023): "Note on the macrofinancial implications of crypto assets for developing countries", April.

Glossary

This glossary sets out a (non-exhaustive) list of terms used in the report. The definitions are based primarily on previous reports by international organisations and standard-setting bodies.

Asset-backed token: A cryptoasset that represents an interest in a physical asset.

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

Bridge: A technique used to transfer cryptoassets between ecosystems by, typically, creating a synthetic representation of a blockchain-specific cryptoasset on a different blockchain.

Centralised exchange (CEX): A cryptoasset trading platform that facilitates the buying and selling of cryptoassets, either for fiat currencies or for another digital asset. The platform functions as an intermediary and sometimes provides custody and other services.

Centralised finance (CeFi): Centralised intermediaries (for example lending or trading platforms) within the crypto ecosystem that purport to offer some of the features of DeFi with some of the ease of use and security of traditional financial services products.

Composability: the ability to reuse existing software components to build new applications. The crypto industry refers to composability as akin to Lego blocks. Each block can be combined with another, allowing developers to build complex structures by combining different blocks.

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

Cryptoasset: A type of private sector digital asset that is expressed primarily through cryptography and distributed ledger or similar technology.

Cryptoisation: The risk of local currency substitution with cryptoassets, most likely dollar-denominated stablecoins. This is a particular risk for countries with unstable currencies and weak monetary frameworks.

Decentralised autonomous organization (DAO): In theory, a decentralised application consisting of rules of operation that dictate who can execute a certain behaviour or make an upgrade. Code helps create an organisational structure intended to function without a centralised management structure.

Decentralised applications (DApps): DeFi applications offering services such as lending or trading, predominantly between cryptoassets including stablecoins.

Decentralised exchange (DEX): Marketplaces built using distributed ledger or similar technology where transactions can occur directly between cryptoasset traders.

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

DeFi protocol: A specialised system of rules that creates a program designed to perform traditional financial functions.

Digital asset: A digital instrument that is issued or represented through the use of distributed ledger or similar technology. This does not include digital representations of fiat currencies. It is also called a coin or token.

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

Gas fees: Unit that relates to the amount of computational effort required to execute specific operations on the Ethereum network. Gas refers to the fee required to conduct a transaction on Ethereum.

Governance tokens: Tokens issued as an incentive, allowing the user the purported opportunity to become a partial owner and decision-maker in a DeFi protocol.

Mining: One means to create new cryptoassets, often through a mathematical process by which transactions are verified and added to the distributed ledger.

Native token: The base token of a blockchain which plays an integral part in the operation of the protocol it is issued on and that is created at the blockchain's genesis. It is usually used to pay transaction fees.

Oracle: A service that enables smart contracts to access, in real time, relevant external or off-chain data by means of queries typically through crypto exchange application programming interfaces and which provides inputs to smart contracts.

Order book exchange: A type of decentralised exchange (DEX) that uses smart contracts for transaction settlement and order books, which are usually held off-chain by a third party, for registration of buy and sell orders.

Proof of stake: A blockchain-specific consensus mechanism for validating entries into a distributed database and keeping the database secure based on validators' pledging or "staking" a certain amount of cryptoassets in order to have a chance to be chosen for the creation of a new block.

Proof of work: A blockchain-specific consensus mechanism for validating entries into a distributed database and keeping the database secure where potential validators compete with one another to solve cryptographic puzzles in order to be allowed to add transactions to the distributed ledger.

Pseudonymous data: Data that cannot be attributed to a specific individual, without the use of additional information.

Rug pull: A cryptoasset market scam in which a development team attracts investors into a project before disappearing with investor funds, leaving investors with a valueless asset.

Side-chain: A type of off-chain scaling solution that helps overcome capacity restrictions inherent to traditional blockchain networks by leveraging a separate and independently run blockchain network that is connected to the original one by a two-way bridge.

Smart contract: A cryptoasset term that refers to self-executing applications that can trigger an action if some pre-specified conditions are met.

Stablecoin: A cryptoasset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets.

Staking: Is the process of locking up cryptoassets for a set period of time to help support the operation of a blockchain in return for a share of transaction fees.

Tokenisation: The process of creating a digital representation (token) of an asset and putting it on a programmable ledger. The information stored in tokenised form can include asset type, ownership details, valuation, legal framework, optionality and settlement requirements

Total value locked: Industry-reported measure of the total value of assets deposited in a DeFi protocol.

Validator: An individual or entity responsible for verifying transactions on a blockchain.

Wallet: An application or device for storing the private keys providing access to the cryptoasset. Hosted wallets are typically held by a third-party provider, unhosted wallets by the user.

Wallet provider: A firm that offers storage services to investors in cryptoassets. These may be connected online ("hot" storage) or kept offline ("cold" storage).