

DeFi risks and the decentralisation illusion¹

Decentralised finance (DeFi) is touted as a new form of intermediation in crypto markets. The key elements of this ecosystem are novel automated protocols on blockchains – to support trading, lending and investment of cryptoassets – and stablecoins that facilitate fund transfers. There is a “decentralisation illusion” in DeFi since the need for governance makes some level of centralisation inevitable and structural aspects of the system lead to a concentration of power. If DeFi were to become widespread, its vulnerabilities might undermine financial stability. These can be severe because of high leverage, liquidity mismatches, built-in interconnectedness and the lack of shock absorbers such as banks. Existing governance mechanisms in DeFi would provide natural reference points for authorities in addressing issues related to financial stability, investor protection and illicit activities.

JEL classification: G18, G23, O39.

Crypto markets are underpinned by various forms of intermediation. While some forms of crypto intermediation have direct analogues in traditional finance, others – known as decentralised finance, or “DeFi” – are fundamentally new and have recently gained more traction. DeFi provides financial services without centralised intermediaries, by operating through automated protocols on blockchains. The DeFi ecosystem revolves around two elements: (i) novel protocols for trading, lending and investing, and (ii) stablecoins, which are cryptoassets that facilitate fund transfers and aim to maintain a fixed face value vis-à-vis fiat currencies, mainly the US dollar.

While the main vision of DeFi’s proponents is intermediation without centralised entities, we argue that some form of centralisation is inevitable. As such, there is a “decentralisation illusion”. First and foremost, centralised governance is needed to take strategic and operational decisions. In addition, some features in DeFi, notably the consensus mechanism, favour a concentration of power.

In principle, DeFi has the potential to complement traditional financial activities. At present, however, it has few real-economy uses and, for the most part, supports speculation and arbitrage across multiple cryptoassets. Given this self-contained nature, the potential for DeFi-driven disruptions in the broader financial system and the real economy seems limited for now.

¹ The authors thank Mike Alonso, Raphael Auer, Marcel Bluhm, Claudio Borio, Stijn Claessens, Sebastian Doerr, Jon Frost, Anneke Kosse, Asad Khan, Ulf Lewrick, Benoît Mojon, Benedicte Nolens, Tara Rice, Hyun Song Shin, Vladyslav Sushko and Nikola Tarashev for helpful comments and discussions, and Ilaria Mattei for excellent research assistance. The views expressed in this article are those of the authors and do not necessarily reflect those of the Bank for International Settlements.

Key takeaways

- Decentralised finance (DeFi) aims to provide financial services without intermediaries, using automated protocols on blockchains and stablecoins to facilitate fund transfers.
- There is a “decentralisation illusion” in DeFi due to the inescapable need for centralised governance and the tendency of blockchain consensus mechanisms to concentrate power. DeFi’s inherent governance structures are the natural entry points for public policy.
- DeFi’s vulnerabilities are severe because of high leverage, liquidity mismatches, built-in interconnectedness and the lack of shock-absorbing capacity.

DeFi would need to satisfy a number of conditions if it is to become a widely used form of financial intermediation. For one, blockchain scalability and large-scale tokenisation of traditional securities would need to be improved. No less importantly, DeFi will need to be properly regulated. Public authorities would need to interface with DeFi’s inherent governance structures, so as to ensure sufficient financial stability safeguards as well as to enhance trust by addressing investor protection issues and illegal activities.

This special feature examines DeFi mainly from a financial stability perspective, drawing attention to vulnerabilities that stem from leverage and liquidity mismatches. As a key attribute of crypto markets, leverage amplifies their volatility and procyclicality. In addition, the crypto ecosystem lacks internal shock absorbers, such as banks, that can provide liquidity at times of stress. This increases the potential for stablecoin runs that could sever links across investors and platforms, eroding the “networked liquidity” that is a defining feature of DeFi.

The rest of this special feature is organised as follows. The first section provides an overview, focusing on the building blocks of the DeFi ecosystem. The second outlines the decentralisation illusion. The third discusses key vulnerabilities from a financial stability perspective. The final section concludes with policy considerations.

The DeFi ecosystem

An overview

Decentralised finance (DeFi) is a fast-growing part of the crypto financial system. The rise of cryptoassets can be traced back to a whitepaper (Nakamoto (2008)) outlining a peer-to-peer transaction mechanism – blockchain – and the creation in 2009 of the first consequential cryptoasset – Bitcoin (BTC). Numerous blockchain technologies, as well as the respective cryptoassets that serve as mediums of exchange, have mushroomed since then. A key milestone was the development of Ethereum and its associated cryptoasset Ether (ETH). This technology supports automated contracts with pre-defined protocols hosted on blockchains, commonly referred to as “smart contracts”,² and was instrumental to spurring on the DeFi ecosystem.

² Blockchains like Ethereum enable the execution and validation of more elaborate contracts than simply user A pays a certain amount of cryptoassets to user B (which is an accounting system first operationalised by the Bitcoin blockchain). For instance, an automated trading contract allows A and

Function	Service	Crypto financial system		Traditional finance
		Decentralised finance (DeFi)	Centralised finance (CeFi)	
Trading	Funds transfer	DeFi stablecoins (DAI)	CeFi stablecoins (USDT, USDC)	Traditional payment platforms
	Asset trading	Crypto asset DEX (Uniswap)	Crypto CEX (Binance, Coinbase)	Exchanges and OTC brokers
	Derivatives trading	Crypto derivatives DEX (Synthetix, dYdX)		
Lending	Secured lending	Crypto decentralised lending platforms (Aave, Compound)	Crypto centralised lending platforms (BlockFi, Celsius)	Broker-dealers active in repo and securities lending
	Unsecured lending	Crypto credit delegation (Aave)	Crypto banks (Silvergate)	Commercial banks and non-bank lenders
Investing	Investment vehicles	Crypto decentralised portfolios (yearn, Convex)	Crypto funds (Grayscale, Galaxy)	Investment funds

CEX = centralised exchanges; DEX = decentralised exchanges; OTC = over-the-counter; USDC = USD Coin; USDT = Tether.

¹ Illustrative examples are given in parentheses.

Source: Authors' elaboration.

The term DeFi refers to the *financial applications* run by smart contracts on a blockchain, typically a permissionless (ie public) chain.³ Table 1 juxtaposes DeFi with centralised finance (CeFi) in crypto markets, as well as with the traditional financial system. The key difference between DeFi and CeFi lies in whether the financial service is automated via smart contracts on a blockchain or is provided by centralised intermediaries. While DeFi records all the contractual and transaction details on the blockchain (ie on-chain), CeFi relies on the private records of intermediaries, such as centralised exchanges and other platforms (ie off-chain).

DeFi aims to provide financial services without using centralised entities. Namely, it digitises and automates the contracting processes, which – according to its proponents – could in the future improve efficiency by reducing intermediation layers. Importantly, it also provides users with much greater anonymity than transactions in CeFi or traditional finance. Such propositions have been key drivers of the heightened interest in DeFi platforms and the strong price rises of the attendant cryptoassets (Graph 1 left-hand panel). The expansion of DeFi in turn has hastened

B to exchange their assets according to an agreement on the terms of the transfer, contingent on pre-specified conditions. This is essentially an over-the-counter (OTC) trade without the traditional intermediaries, such as dealer banks.

³ A permissionless blockchain allows anyone to participate in the validation of transactions, while a permissioned one allows only a pre-selected group of participants to validate transactions.

the emergence of alternative blockchain designs that host smart contracts and seek to rival Ethereum.⁴

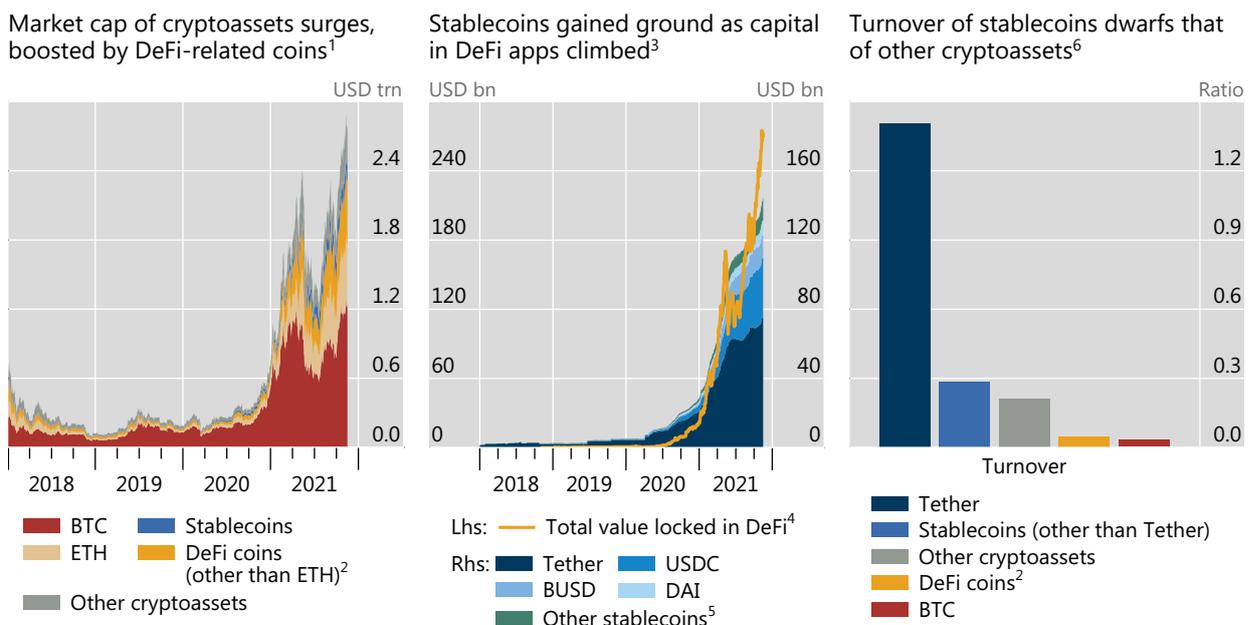
The building blocks of DeFi

DeFi differs from traditional finance not so much in terms of the types of service it seeks to provide, but rather in how it performs them. Each row in Table 1 represents a specific service, grouped under three broad functions: trading, lending and investment. This section analyses the main building blocks of these services, and how the underlying mechanisms compare with those in CeFi and traditional finance.

Stablecoins are cryptoassets that strive to tie their values to fiat currencies, such as the US dollar. They play an important role in the DeFi ecosystem, facilitating fund transfers across platforms and between users. Stablecoins allow DeFi market participants to avoid converting to and from fiat money at every turn. They also act as a bridge between the crypto and the traditional financial systems, which share a common numeraire – ie fiat currencies.

DeFi underpins the rapid growth in crypto activities

Graph 1



BTC = Bitcoin; BUSD = Binance USD; ETH = Ether; USDC = USD Coin.

¹ Market capitalisation of top 100 cryptoassets as of 15 November 2021 (seven stablecoins, 36 DeFi coins and 55 other cryptoassets). ² Cryptoassets issued by DeFi platforms. ³ Stacked areas plot stablecoins' value in circulation. The selected stablecoins are those ranked as the top four by market capitalisation as of 15 November 2021. ⁴ Total value locked refers to the size of capital pools underpinning DeFi protocols. The sample includes 679 protocols. ⁵ Includes 57 other stablecoins. ⁶ Based on the top 20 cryptoassets by market capitalisation as of 15 November 2021 (three stablecoins, 10 DeFi coins and seven other cryptoassets). Turnover is the monthly average of the daily volume-to-market capitalisation ratio from 15 October to 15 November 2021.

Sources: CoinGecko; Defi Llama; authors' calculations.

⁴ Transactions are validated and added to a blockchain via consensus, ie a network of "validators" need to expend resources to agree on which transactions are legitimate. Bitcoin and Ethereum blockchains build on proof-of-work, which is energy-intensive and raises scalability issues (Auer (2019)). Alternative blockchain designs have sought to overcome these problems by relying on consensus among a majority of the holders of a blockchain's exchange medium (proof-of-stake).

The growth of stablecoins has been exponential since mid-2020, when DeFi activities started to take off. As of late 2021, the value of the major stablecoins in circulation reached \$120 billion (Graph 1, centre panel), as compared with the roughly \$200 billion size of the largest money market fund. In particular, USD Tether has gained substantial scale as a “vehicle currency” for investors who seek to trade in and out of cryptoassets (right-hand panel). Being the first stablecoin, its growth has benefited from a user base built up early on, which has attracted new adopters seeking ease of trading (network externalities).

The mechanism for assuring a stable value varies across different designs.⁵ The majority of stablecoins are CeFi – eg USD Tether – as they are managed off-chain. Others, such as DAI, are DeFi stablecoins that are managed on-chain. In the case of CeFi stablecoins, a designated intermediary manages issuance and redemption as well as the reserve assets backing the stablecoins. Some of these assets are bank deposits or their close substitutes. Other assets may comprise short-term securities – such as Treasury bills, certificates of deposit and commercial paper – as well as cryptoassets themselves. To the extent that DeFi relies on such stablecoins, it remains dependent on CeFi and traditional finance.

DeFi stablecoins record all transacting histories directly on-chain, without the involvement of centralised intermediaries. They rely on an overcollateralised pool of cryptoassets, ie the underlying assets are worth more than the stablecoins in circulation. Since crypto collateral has a very high price volatility, as measured in the reference fiat currency, DeFi stablecoins incentivise users to actively monitor the collateralisation ratio. To do so, the smart contracts behind these stablecoins allow any user to seize the collateral when the collateralisation ratio falls below a certain threshold (which is higher than 100%) and to redeem the stablecoins.⁶ Such a design ensures that the value of stablecoins remains tied to the fiat currency. Other DeFi stablecoins have attempted to minimise their price volatility vis-à-vis a fiat currency by relying solely on algorithms (ie dispensing with collateral). They do so by adjusting the supply of stablecoins to match their demand. So far, no purely algorithmic stablecoin has been widely adopted.

In sum, stablecoin issuers receive assets (collateral) in exchange for their own liabilities (stablecoins). While this mechanism looks superficially similar to how banks operate, there are fundamental differences. Issuers lack public backstops, such as deposit insurance, and rely on private backstops (collateral) to ensure that stablecoins maintain a steady value and are suitable as mediums of exchange. As such, the expansion of the balance sheets of stablecoin issuers, at least currently, is driven more by the appetite of investors to hold the stablecoins than by any desire of the issuers to acquire more assets. In other words, this growth is liability-driven, while the expansion of bank balance sheets is commonly asset-driven (McLeay et al (2014)).⁷

⁵ See G7 Working Group on Stablecoins (2019), IMF (2021) and PWG (2021) for more details.

⁶ Given that the collateralisation ratio is still above 100%, users who seize the collateral and redeem the stablecoins would earn a profit as long as the collateral value remains above the stablecoin's.

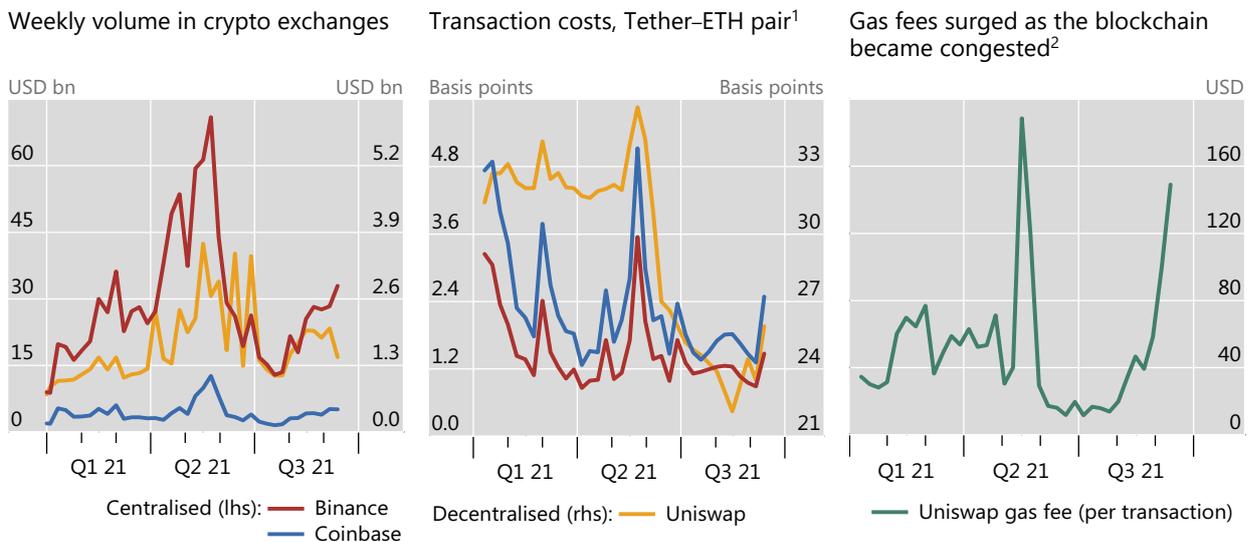
⁷ At present, the “business model” of stablecoins implies that they are passive vehicles that issue liabilities only upon user demand. However, financial history shows that, when their liabilities become widely accepted as a means of payment, intermediaries usually tend to actively expand liability issuance to finance asset purchases, especially when a regulatory framework is lacking. See eg Frost et al (2020) comparing stablecoins with the Bank of Amsterdam (1609–1820). A key feature of the Bank of Amsterdam that eventually led to its collapse was that the shift towards a more opportunistic issuance of liabilities was unchecked by regulation and lacked a public backstop.

Trading of cryptoassets can take place on both **centralised exchanges (CEXs)** and **decentralised exchanges (DEXs)**. The former are structured around the same principles as their conventional counterparts. CEXs maintain off-chain records of outstanding orders posted by traders – known as limit order books. By contrast, DEXs work in substantially different ways, by matching the counterparties in a transaction through so-called automated market-maker (AMM) protocols. AMMs follow mathematical formulas to determine prices based on transaction volumes. Box A discusses how AMMs incentivise liquidity provision; it also looks at their susceptibility to market manipulation. Both CEXs and DEXs have seen substantial growth since 2020, although the share of DEXs in the overall transaction volume on crypto exchanges has remained below 10% (Graph 2, left-hand panel).

At present, it seems to be costlier to trade on DEXs than on CEXs, especially for smaller transactions. For instance, the relative bid-ask spread for the Tether-ETH pair on a popular DEX has been up to 30 basis points wider than on a CEX (Graph 2, centre panel). In addition, trading on DEXs incurs execution costs when transactions are validated on the blockchain. These stem from so-called gas fees, which are designed to compensate validators. Gas fees increased markedly as cryptoassets gained popularity and blockchains such as Ethereum became more congested (compare left- and right-hand panels). Although transaction costs are higher in DEXs, some traders still prefer these platforms, in part due to their greater anonymity and interoperability with other DeFi applications (the so-called “DeFi Lego”).⁸

Centralised and decentralised exchanges: volumes and trading costs

Graph 2



¹ Transaction costs are measured as the relative bid-ask spread, defined as $2 \times (\text{ask price} - \text{bid price}) / (\text{ask price} + \text{bid price})$ for Tether-Ether in Coinbase, Binance and Uniswap. ² Gas fees are payments made by users to compensate validators for the computing power required to process and validate transactions on the Ethereum blockchain. The time series is calculated for Tether-Ether in Uniswap.

Sources: Bitquery, Binance; CoinGecko; Coinbase Pro; authors' calculations.

⁸ A trader wishing to combine CEX trading with DeFi lending or investing would incur round-trip gas fees, first transferring cryptoassets off-chain and then moving them back on-chain after trading on the CEX. The combined fees would limit the appeal of CEXs that offer lower spreads.

Lending in DeFi tends to be overcollateralised. The reason is similar to that underpinning the overcollateralisation of DeFi stablecoins – the inherent lack of trust in anonymous transactions, together with the high volatility of the cryptoassets used as collateral. To protect the lender, loans can be automatically liquidated when the collateralisation ratio falls below a threshold. At present, the need for crypto collateral stands in the way of lending to households and businesses, eg for house purchases or productive investment. Nonetheless, outstanding loans on the major lending platforms have increased rapidly, to \$20 billion in late 2021 (Graph 3, left-hand panel). Rudimentary forms of unsecured lending, known as “credit delegation”, are available on some platforms. This often involves entities with established off-blockchain relationships, making collateral unnecessary.

DeFi lending platforms also offer a unique financial instrument, typically referred to as **flash loans**. These allow arbitrageurs to act without their own capital by taking out a loan for the entire arbitrage trade and then repaying the loan. Such loans are of zero duration and are essentially risk-free (requiring no collateral), as they are granted only if the arbitrage trade ensures the repayment of both principal and interest. Crucially, this is possible as all legs of the transaction can be attached to the same block (ie settled) simultaneously on the blockchain.⁹ Flash loans have increased in popularity, with the largest platform granting a total of about \$5.5 billion of such loans between their inception in mid-2020 and late 2021.

The growth of DeFi lending platforms has also encouraged the development of applications similar to investment funds in traditional finance. These **decentralised portfolios** follow pre-determined investing strategies, eg aggregating funds from investors and automatically shifting them across crypto lending platforms to profit from the best yields. As of late 2021, the funds held by two popular decentralised portfolios stood at around \$10 billion (Graph 3, centre panel).

The “decentralisation illusion” in DeFi

DeFi purports to be decentralised. This is the case for both blockchains and the applications they support, which are designed to run autonomously – to the extent that outcomes cannot be altered, even if erroneous.¹⁰

But full decentralisation in DeFi is illusory. A key tenet of economic analysis is that enterprises are unable to devise contracts that cover all possible eventualities, eg in terms of interactions with staff or suppliers. Centralisation allows firms to deal with this “contract incompleteness” (Coase (1937) and Grossman and Hart (1986)). In DeFi, the equivalent concept is “algorithm incompleteness”, whereby it is impossible to write code spelling out what actions to take in all contingencies.

This first-principles argument has crucial practical implications. All DeFi platforms have central governance frameworks outlining how to set strategic and operational

⁹ Besides facilitating arbitrage, flash loans open the door to market manipulation. Using a large volume of flash loans, an attacker can, for instance, manipulate the number of tokens in an AMM – which is a critical parameter in determining the prices of such tokens. In October 2020, the crypto trading platform Harvest was exploited by a flash loan attack, incurring losses of \$27 million.

¹⁰ For instance, in October 2021, an update to the lending platform Compound introduced an error that incorrectly distributed rewards worth \$90 million. The platform’s founder posted on Twitter that “There are no administrative controls or community tools to disable the [...] distribution” of rewards. In traditional finance, erroneous transfers can be challenged in court.

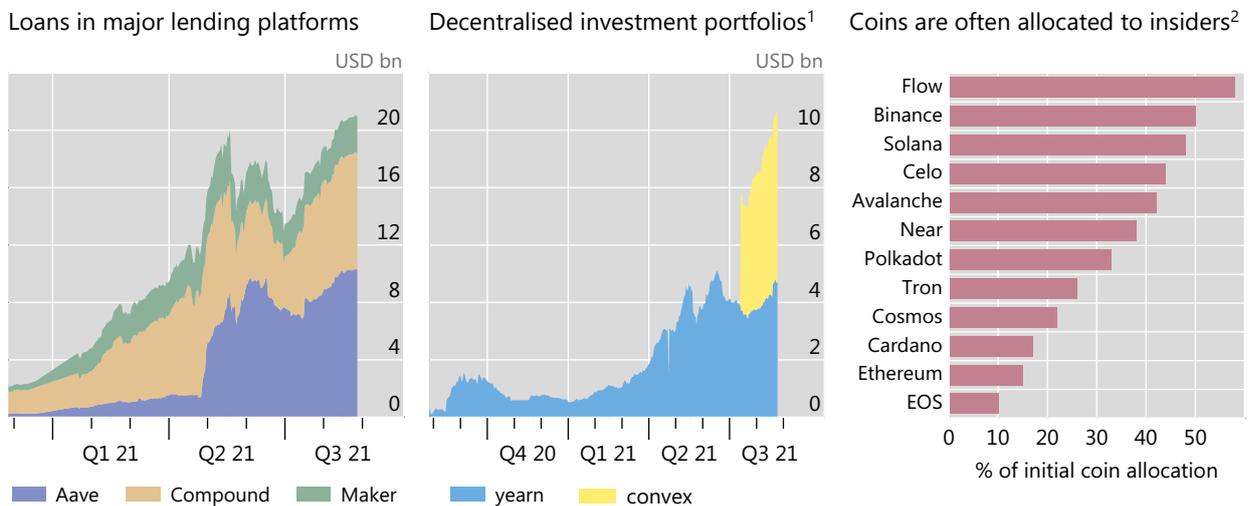
priorities, eg as regards new business lines.¹¹ Thus, all DeFi platforms have an element of centralisation, which typically revolves around holders of “governance tokens” (often platform developers) who vote on proposals, not unlike corporate shareholders. This element of centralisation can serve as the basis for recognising DeFi platforms as legal entities similar to corporations. While legal systems are in the early stages of adapting, decentralised autonomous organisations (DAOs), which govern many DeFi applications, have been allowed to register as limited liability companies in the US state of Wyoming since mid-2021.

In addition, certain features of DeFi blockchains favour the concentration of decision power in the hands of large coin-holders. Transaction validators need to receive compensation that is sufficient to incentivise them to participate without committing fraud. Blockchains based on proof-of-stake, which are expected to improve scalability, allow validators to stake more of their coins so that they have a higher chance of “winning” the next block and receiving compensation. Since the associated operational costs are mostly fixed, this setup naturally leads to concentration (Auer et al (2021)).¹² Many blockchains also allocate a substantial part of their initial coins to insiders, exacerbating concentration issues (Graph 3, right-hand panel).

Concentration can facilitate collusion and limit blockchain viability. It raises the risk that a small number of large validators can gain enough power to alter the blockchain for financial gain. Furthermore, large validators could congest the blockchain with artificial trades between their own wallets (“wash trades”), steeply raising the fees that other traders pay them. Another concern is that validators can

DeFi applications take off, while blockchain insiders are likely to reap the gains

Graph 3



¹ Size of capital pools in these DeFi investment portfolios. ² Initial coin allocation to insiders for major public (ie permissionless) blockchains as of 9 May 2021. Insiders includes development teams as well as early investors such as venture capital.

Sources: Messari Report, *Power and Wealth in Cryptoeconomies*, May 2021; Skew.

¹¹ Walch (2019) reviews DeFi from a securities regulation perspective, focusing on how decentralised it is in practice. She finds elements of centralisation, particularly in governance protocols.

¹² The trade-off between the blockchains’ ability to handle large transaction volumes, stakeholder concentration and blockchain security is known as Buterin’s “scalability trilemma”.

front-run large orders for higher trading profits (see Box A). Although front-running also occurs in traditional finance, it incurs punitive measures from regulators. These rent-seeking behaviours are detrimental to investors and may erode DeFi's appeal going forward.

Discussions about changes to governance protocols, in particular to rein in collusion, have gained momentum in the DeFi community.¹³ However, adopting these changes would not alter the basic fact that some centralisation is unavoidable.

Vulnerabilities and spillover channels

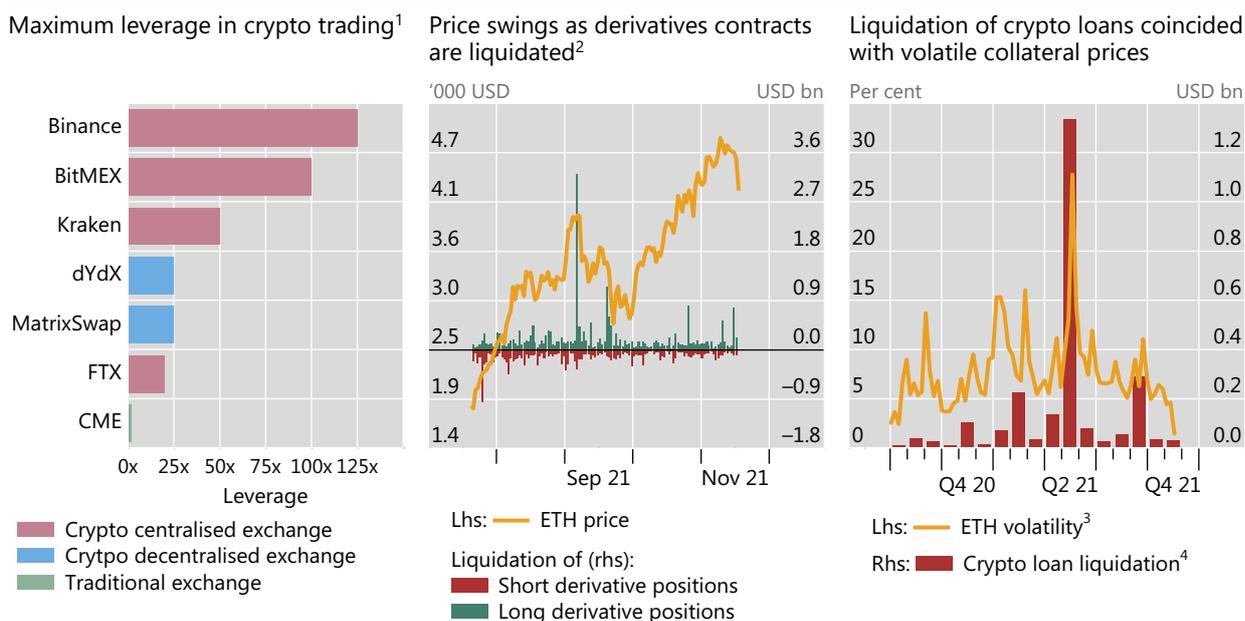
While DeFi is still at a nascent stage, it offers services that are similar to those provided by traditional finance and suffers from familiar vulnerabilities. The basic mechanisms giving rise to these vulnerabilities – leverage, liquidity mismatches and their interaction through profit-seeking and risk-management practices – are all well known from the established financial system. Some features of DeFi could make them particularly destabilising, though. In this section, we focus first on the role of leverage and run-risk in stablecoins due to liquidity mismatches, before covering spillover channels to the conventional intermediaries.

Leverage

DeFi is characterised by the high leverage that can be sourced from lending and trading platforms. While loans are typically overcollateralised, funds borrowed in one instance can be re-used to serve as collateral in other transactions, allowing investors to build increasingly large exposure for a given amount of collateral. Derivatives trading on DEXs also involves leverage, as the agreed payments take place only in the future. The maximum permitted margin in DEXs is higher than in regulated exchanges in the established financial system (Graph 4, left-hand panel). And unregulated crypto CEXs allow even higher leverage.

High leverage in crypto markets exacerbates procyclicality. Leverage allows more assets to be purchased for a given amount of initial capital deployed. But when debt eventually needs to be reduced, eg because of investment losses or depreciating collateral, investors are forced to shed assets, putting further downward pressure on prices. Such procyclicality can be amplified by the trading behaviour typical of markets at an early stage of development – eg the outsized role of momentum trading, which can add to price swings. In addition, the built-in interconnectedness among DeFi applications can also amplify distress, since the system's stability hinges on the weakest links.

¹³ Proposals to overcome the issues associated with token voting include vote delegation to trusted members, which resembles proxy voting in traditional finance, and extending voting rights to all participants irrespective of their holdings of governance tokens, similar to firms organised as consumer cooperatives. See <https://vitalik.ca/general/2021/08/16/voting3.html>.



¹ Maximum leverage for derivatives contracts as of 2021. For crypto exchanges, perpetual futures. For CME, standard futures. ² Includes positions in the following crypto exchanges: Binance, Bitfinex, Bitmex, Bybit, Deribit, FTX, Huobi and Okex. ³ Volatility is defined as the weekly average of (highest price – lowest price)/close price at minute level. ⁴ Monthly liquidation volume in the largest DeFi lending protocols: Aave, Aave v2, bZx v2, Compound, Maker, Polygon Aave and Venus.

Sources: bybt; CoinGecko; CryptoCompare; The Block, www.theblockcrypto.com/data/decentralized-finance/cryptocurrency-lending-exchanges/ websites; authors' calculations.

Financial intermediation in DeFi relies exclusively on private backstops, ie collateral, to mitigate risk and enable transactions when participants cannot trust each other. Thus, there are no shock absorbers in DeFi that can cut in during stress periods. By contrast, in traditional finance, banks are elastic nodes that can expand their balance sheets (extending loans or purchasing distressed assets) via the issuance of bank deposits, which are a widely accepted medium of exchange. The ability of banks to do so rests on their access to the central bank balance sheet (Borio (2019)).

The destabilising role of leverage came to the fore in the latest cryptoasset crash in September 2021. Forced liquidations of derivatives positions and loans on DeFi platforms accompanied sharp price falls and spikes in volatility (Graph 4, centre and right-hand panels).

Liquidity mismatches and run-risk in stablecoins

Stablecoins are inherently fragile. They are designed to target a fixed face value using various types of reserve asset. This arrangement gives rise to mismatches between the risk profiles of these assets (the underlying collateral) and the stablecoin liabilities. The vulnerability is similar to that of traditional intermediaries, such as money market funds, whose investors expect to be able to redeem in cash at par. Thus, contrary to what their name suggests, stablecoins are not money substitutes, since they lack a “no-questions asked” status (Gorton and Zhang (2021)).

The exact nature of stablecoins' vulnerabilities depends on their design. Coins backed by short-term securities with illiquid secondary markets, such as commercial paper, feature *liquidity* mismatches. Those backed by volatile collateral, such as cryptoassets, are exposed to *market risk*, because the value of these assets can quickly drop below the face value of stablecoins. Even though overcollateralisation generally offsets such risks, it can be exhausted when volatility spikes.¹⁴

Liquidity mismatches and exposure to market risk raise the possibility of investor runs. The viability of stablecoins hinges on investors' trust in the value of the underlying assets. Opaqueness and lack of regulation can easily erode this trust. If investors have doubts about the quality of the assets, they have an incentive to be the first to sell stablecoins or convert them to fiat currency. In turn, such a first-mover advantage can set off runs, leading to fire sales of the collateral.¹⁵ Furthermore, an evaporation of trust in stablecoins could have wide repercussions for DeFi. Transfers of funds across investors and platforms would become more costly and cumbersome, impinging on the "networked liquidity" that is a key feature of DeFi.

Linkages with the traditional financial system

While DeFi is largely separate from the traditional financial system at present, connections could increase. This would raise the potential for spillovers, which would stem from linkages through both the asset and liability side of banks, as well as the activities of non-bank institutions that bridge the two systems.

A conservative regulatory approach has, so far, restricted banks' participation in the crypto ecosystem. On the asset side, banks' exposures are limited, in terms of both loans and equity investments (BCBS (2021)). The equity investments of large banks in crypto-related firms range from \$150 million to \$380 million in size as of late 2021, representing just a small fraction of their capital (Graph 5, left-hand panel).¹⁶ On the liability side, some banks could receive funding from DeFi, since stablecoins might hold their certificates of deposit or commercial paper. As a result, runs on stablecoins could generate a funding shock for banks – akin to the familiar implications of a run on money market funds.

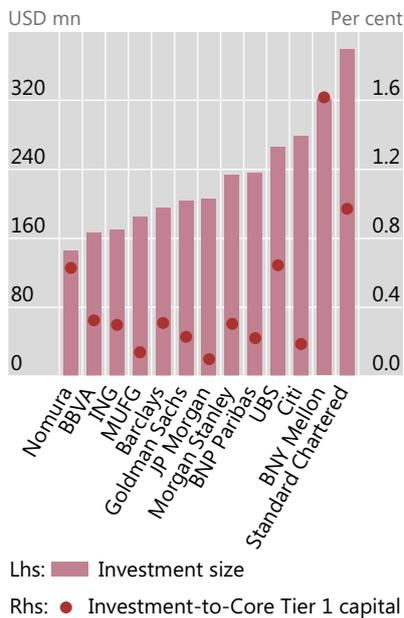
In addition, traditional non-bank investors are taking a growing interest in DeFi, as well as in the broader crypto markets. At present these investors include primarily family offices and hedge funds, which often receive credit from major dealer banks through prime brokerage. Funds with meaningful crypto exposure, some of which focus exclusively on DeFi while others are more diversified, have increased their assets from about \$5 billion in 2018 to about \$50 billion in 2021 (Graph 5, centre panel).

¹⁴ A recent example of losses on overcollateralised transactions relates to loans backed by the governance token of the most popular lending pool on the Binance smart chain (see <https://blog.venus.io/venus-incident-report-xvs-liquidations-451be68bb08f>).

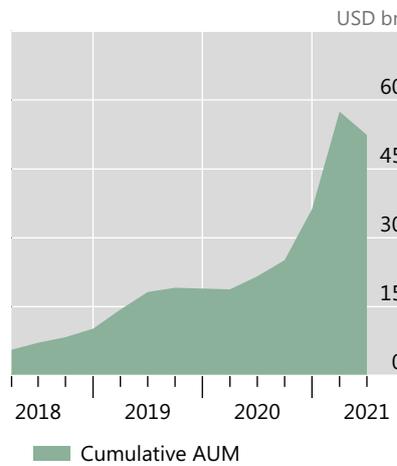
¹⁵ Indeed, such a run on a DeFi stablecoin (IRON) took place in June 2021. See Iron post mortem: <https://ironfinance.medium.com/iron-finance-post-mortem-17-june-2021-6a4e9ccf23f5>.

¹⁶ In October 2021, Société Générale announced plans to borrow \$20 million from MakerDAO – the issuer of the popular stablecoin DAI – using tokenised bonds as collateral.

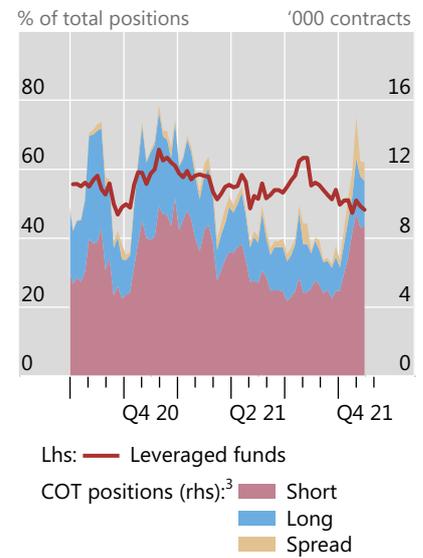
Major banks' equity investment in crypto-related companies¹



Assets under management of crypto funds²



Leveraged funds dominate in trading of CME Bitcoin futures



¹ Companies with a focus on cryptocurrencies technologies as of August 2021. The full list of the companies is available at www.blockdata.tech/blog/general/banks-investing-blockchain-companies. ² Includes crypto hedge funds, venture funds, hybrid funds, private equity funds, fund of funds and passive funds. ³ Commitment of Traders (COT) positions from CME.

Sources: Sam Wouters, Top Banks Investing in Crypto & Blockchain Companies, Blockdata, October 2021; CME Group, Commitment of Traders; Crypto Fund Research, *Crypto Fund Quarterly Report Q3 2020*; Fitch Solutions; Statista; authors' calculations.

In a related sign of this increased involvement in crypto as an emerging asset class, leveraged investors, a category that includes hedge funds, are now a major participant in the trading of Bitcoin futures on the Chicago Mercantile Exchange (right-hand panel). Looking ahead, many intermediaries and infrastructures appear set to develop their business in crypto markets, including DeFi, alongside their traditional finance activities. This could potentially strengthen the links between the traditional and crypto systems. The recent popularity of a Bitcoin futures-based ETF is a tell-tale sign of this growing interest (see Todorov (2021) also in this issue).

Policy considerations and conclusions

Although it has grown rapidly, the DeFi ecosystem is still developing. At present, it is geared predominantly towards speculation, investing and arbitrage in crypto assets, rather than real-economy use cases. The limited application of anti-money laundering and know-your-customer (AML/KYC) provisions, together with transaction anonymity, exposes DeFi to illegal activities and market manipulation. On balance, DeFi's main premise – reducing the rents that accrue to centralised intermediaries – seems yet to be realised.

History shows that the early development of novel technologies often comes with bubbles and loss of market integrity, even while generating innovations that could potentially be of broader use down the road. With improvements to blockchain scalability, large-scale tokenisation of traditional assets, and most importantly,

suitable regulation to ensure safeguards and enhance trust, DeFi could yet play an important role in the financial system.

The growth of DeFi poses financial stability concerns. One is leverage-driven procyclicality, which arises from changes in collateral value and fluctuations in the associated margins. Since collateral prices fall and margins rise at times of distress, downward price spirals often arise and may spread to the rest of the financial system. Due to the largely self-contained nature of DeFi, episodes of rapid deleveraging have thus far had little effect outside crypto markets.

Another concern applies more specifically to one of DeFi's main building blocks – stablecoins. If the attendant risks are not well managed, stablecoins are prone to runs, which would compromise their ability to transfer funds within the DeFi ecosystem. In addition, possible fire sales by a stablecoin of its reserve assets could generate funding shocks for corporates and banks, with a potentially severe impact on the broader financial system and the economy.¹⁷ These risks are compounded by the fact that users treat stablecoins as a medium of exchange, although they are neither central bank money nor commercial bank money.

Since the main challenges in DeFi resemble those in traditional finance, established regulatory principles can serve as a compass. The basic tenet “same risks, same rules” should apply, not least to counter regulatory arbitrage. From a systemic perspective, policy measures should lead DeFi participants to internalise costs arising from the procyclicality of leverage. To address the run-risk in stablecoins and the associated possibility of wider contagion, policymakers can draw on precepts in bank regulation and supervision, on current initiatives in securities regulation about strengthening investment funds' prudential framework, and on international risk management standards for payment infrastructures.¹⁸ Likewise, authorities focused on market integrity and illicit financial activities will need to expand their realm to cover DeFi.

The decentralised nature of DeFi raises the question of how to implement any policy provisions. We argue that full decentralisation in DeFi is an illusion. And indeed, platforms have groups of stakeholders that take and implement decisions, exercising managerial or ownership benefits. These groups, and the governance protocols on which their interactions are based, are the natural entry points for policymakers. These entry points should allow public authorities to contain DeFi-related issues before this ecosystem attains systemic importance. Regulatory safeguards would also help to ensure that the innovative potential of DeFi brings overall benefits to finance.

¹⁷ Also see Arner et al (2020). As a better substitute for stablecoins, which are privately issued, central bank digital currencies (CBDCs) could support fund transfers with greater efficiency and safety.

¹⁸ See BCBS (2021) and PWG (2021). Also see CPMI-IOSCO (2021) for proposed guidance on the use of stablecoins as a settlement asset by a stablecoin arrangement.

Trading in the DeFi era: automated market-makers

Sirio Aramonte, Wenqian Huang and Andreas Schrimpf^①

Trading of cryptoassets in DeFi relies on new and unique matching mechanisms. One widely used mechanism in traditional finance is the centralised limit order book, which entails keeping electronic records of all outstanding orders. Likewise, crypto centralised exchanges (CEXs such as FTX, Binance or Kraken) rely on limit order books managed *off-chain*. But in DeFi, the sheer volume of orders would render the management of an *on-chain* limit order book very costly. Another mechanism in traditional finance – the dealership model, where dealers use inventories of assets in over-the-counter (OTC) trading – revolves around establishing trustworthy relationships with counterparties. Such intermediation is not feasible in DeFi due to the anonymity of transactions, and it also goes against the stated aim of building an intermediary-free ecosystem. To dispense with limit order books and the dealership model, decentralised exchanges (DEXs) resort to so-called *automated market-maker* (AMM) protocols.

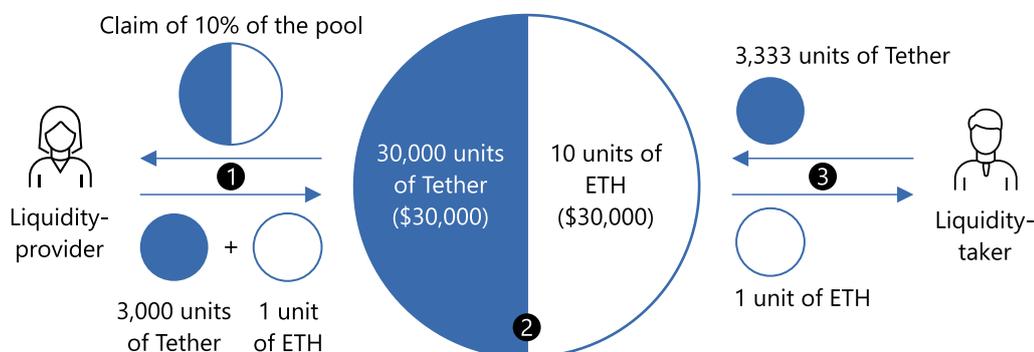
AMM protocols allow traders to exchange one cryptoasset for another automatically on a blockchain. They build on the idea that traders can become liquidity-providers by making their cryptoassets (eg ETH and Tether) available in liquidity pools. In turn, protocols allow other traders demanding liquidity (ie liquidity-takers) to buy or sell the cryptoassets in the pool, with relative prices set on the basis of quantities.^② One popular type of AMM sets the liquidity-takers' exchange rate between token X and Y on the basis of the following *constant product function* that links relative prices and quantities (also known as the *bonding curve*):

$$\text{Amount of token X} * \text{Amount of token Y} = \text{constant.}$$

DEX – constant product function market-maker

Graph A

- ① Suppose 1 Tether = \$1, 1 ETH = \$3,000
Initially, 27,000 units of Tether and 9 units of ETH, each worth \$27,000



Transactions:

- ① A liquidity-provider "deposits" 3,000 units of Tether and 1 unit of ETH
- ② After this deposit, the pool contains 30,000 units of Tether and 10 units of ETH
Following the bonding curve, the constant equals 300,000 (= 30,000 * 10)
The liquidity-provider has a claim of 10% of the pool's crypto-assets
- ③ A liquidity-taker wishes to buy 1 unit of ETH
The price for 1 ETH is $(30,000 + x) * (10 - 1) = 300,000$
Thus, $x = 3,333$, which is the amount of Tether the taker pays for 1 ETH
End result: the pool contains 33,333 units of Tether and nine units of ETH

Liquidity-provider's value (10% of the pool)

Before trade
3,000 units of Tether
+ 1 unit of ETH
= \$6,000

After trade
3,333 units of Tether
+ 0.9 units of ETH
= \$6,033

Source: Authors' elaboration.

Graph A illustrates this AMM with an example of a liquidity pool comprising Tether and Ether. When a trader wishes to provide liquidity, they need to deposit Tether and Ether in proportion to the two cryptoassets' dollar values in the pool (which is one at step ❶). The liquidity-provider's claim on the pool is proportional to its contribution.❸

The AMM protocol incentivises liquidity provision in two ways. First liquidity-takers pay to the providers a fee that may range from a few basis points to several percentage points. Second, at each extraction of liquidity, the bonding curve generates an automatic transfer from the liquidity-taker to the providers. In the example in Graph A, the liquidity-taker pays a premium to acquire 1 ETH (equal to 333 units of Tether at step ❷). This makes the overall pool – and the claim of the liquidity-provider in particular – appreciate in value (bottom of right-hand panel).

That said, liquidity-providers can suffer losses if the relative price of the two cryptoassets on other exchanges diverges substantially from that implied by the bonding curve. The loss is realised when the liquidity-takers withdraw the cryptoasset that has increased in value, leaving the liquidity providers worse off than if they had kept their funds outside the pool. The transaction fees may not be high enough to offset this loss, which is commonly referred to as "impermanent loss".

Certain features of AMMs expose liquidity-takers to market manipulation on DEXs. The execution of trades in AMMs requires validations based on the blockchain's consensus protocol, ie buy and sell orders are stored in a public memory pool, so that validators (also known as "miners") can add them to the blockchain. When submitting orders, liquidity-takers are uncertain about the timing of their orders' execution and the execution prices, as these depend on the execution sequence. Importantly, the order quantities become public knowledge *before* their price impact has materialised – which is easily predictable from the bonding curve. This time lag opens the door to malicious activity, whereby a trader may try to place a buy and an offsetting sell order immediately before and after, respectively, the pre-announced buy order. When the latter order is large enough, the bonding curve implies that the malicious trader's sell order will be executed at a higher price than his buy order, thus generating a profit. Such front-running behaviour is particularly attractive to large validators because they have a higher chance to "win" the next block and time their front-running trades optimally. The profits sometimes are called "miner extractable value".

More and more analytical work on the pros and cons of AMMs is emerging. On the one hand, AMMs enable on-chain trading without intermediaries, improving interoperability with other DeFi platforms such as lending and investment platforms. Compared with a limit order book model, the bonding curve in AMMs also mitigates overcompetition between liquidity-providers on prices, potentially enhancing liquidity provision overall (Lehar and Parlour (2021)). On the other hand, the strict bonding curve in AMMs limits the flexibility of liquidity-providers and exposes them to impermanent losses, thus deterring traders from liquidity provision. The risk of being front-run may also push traders away from AMM protocols.

As the DeFi ecosystem remains in flux, AMM designs are still evolving. One emerging feature brings AMMs closer to the traditional limit order book model. Specifically, liquidity-providers can choose which range of the pricing curve they would like to provide liquidity to. When the transacted price falls within this range, the mechanics described above apply. Otherwise, the liquidity-providers' assets are removed from the active liquidity pool. In addition, the types of cryptoasset that can be traded via AMM protocols are also expanding, ranging from non-fungible tokens to tokenised equity shares.

❶ The views expressed in this box are those of the authors and do not necessarily reflect those of the BIS. ❷ The AMM trading mechanism shares similarities with the framework of Shapley and Shubik (1977), which ensures market-clearing. See L Shapley and M Shubik, "Trade using one commodity as a means of payment", *Journal of Political Economy*, vol 85, no 5, pp. 937–68, and H S Shin, "Comparing the robustness of trading systems to higher-order uncertainty", *Review of Economic Studies*, vol 63, no 1, pp. 39–59. ❸ Decentralised trading is often fragmented. If there are multiple pools trading the same asset pair, one may use a smart order router for the best prices.

References

Arner, D, R Auer and Frost (2020), "Stablecoins: risks, potential and regulation", *Financial Stability Review*, Banco de España, no 39, Autumn.

Auer, R (2019): "Beyond the doomsday economics of 'proof-of-work' in cryptocurrencies", *BIS Working Papers*, no 765.

Auer, R, C Monnet and H S Shin (2021): "Permissioned distributed ledgers and the governance of money", *BIS Working Papers*, no 924.

BCBS (2021): "Prudential treatment of cryptoasset exposures", Basel Committee on Banking Supervision, consultative document.

Borio, C (2019): "On money, debt, trust, and central banking", *Cato Journal*, no 39, pp 267–302.

Coase, R (1937): "The nature of the firm", *Economica*, vol 4, no 16, pp 386–405.

Committee on Payments and Market Infrastructures-International Organization of Securities Commissions (CPMI-IOSCO) (2021): "Application of the principles for financial market infrastructures to stablecoin arrangements", *CPMI Papers*, no 198, October.

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

G7 Working Group on Stablecoins (2019): "Investigating the impact of global stablecoins", *CPMI Papers*, no 187, October.

Gorton, G and J Zhang (2021): "Taming wildcat stablecoins", working paper, September.

Grossman, S and O Hart (1986): "The costs and benefits of ownership: a theory of vertical and lateral integration", *Journal of Political Economy*, vol 94, pp 691–719.

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

Lehar, A and C Parlour (2021): "Decentralized exchanges", working paper, August.

McLeay, M, A Radia and R Thomas (2014): "Money creation in the modern economy", Bank of England, *Quarterly Bulletin*, Q1, March.

Nakamoto, S (2008): "A peer-to-peer electronic cash system", White Paper.

President's Working Group (PWG) (2021): "Report on Stablecoins", President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, November.

Todorov, K (2021): "Launch of the first US bitcoin ETF: mechanics, impact, and risks", *BIS Quarterly Review*, December.

Walch, A (2019): "Deconstructing decentralization: exploring the core claim of crypto systems", in C Brummer (ed), *Cryptoassets: legal, regulatory, and monetary perspectives*, Oxford University Press.