BIS

BIS Bulletin

No 56

Blockchain scalability and the fragmentation of crypto

Frederic Boissay, Giulio Cornelli, Sebastian Doerr and Jon Frost

7 June 2022

BIS Bulletins are written by staff members of the Bank for International Settlements, and from time to time by other economists, and are published by the Bank. The papers are on subjects of topical interest and are technical in character. The views expressed in them are those of their authors and not necessarily the views of the BIS. The authors are grateful to Louisa Wagner for administrative support and to Martin Hood for editing.

The editor of the BIS Bulletin series is Hyun Song Shin.

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

ISSN: 2708-0420 (online)
ISBN: 978-92-9259-562-3 (online)

Frederic Boissay Frederic.Boissay@bis.org
Giulio Cornelli Giulio.Cornelli@bis.org
Sebastian Doerr Sebastian.Doerr@bis.org
Jon Frost Jon.Frost@bis.org

Blockchain scalability and the fragmentation of crypto

Key takeaways

- *Permissionless blockchains work by providing monetary incentives to decentralised validators. Yet the mechanism for maintaining these incentives necessarily entails congestion effects and high fees. These high fees encourage the use of alternative chains, leading to a fragmentation of the crypto landscape.*
- *Newer blockchains have higher capacity, even if these come at the cost of greater centralisation and weaker security. Differences in the design also preclude blockchain interoperability.*
- *Limited scalability and a lack of interoperability not only prevent network effects from taking root, but a system of parallel blockchains also adds to governance and safety risks.*
- *Despite fragmentation, cryptocurrencies on different blockchains exhibit strong price co-movements, as they often share the same investor base, and growth is sustained by speculative buying of coins.*

The crypto universe saw explosive growth in the last two years. From January 2020 to November 2021, the value of cryptocurrencies rose more than tenfold, peaking at $2.8 trn, before crashing to $1.2 trn in June 2022. Assets locked in the decentralised finance (DeFi) space rose 180 times, to $109 bn.

As the system grew, it started to fragment. Initially, most DeFi protocols ran on the Ethereum blockchain, which has relatively high fees. Yet since early 2021 newer rival networks, touted as "Ethereum killers", have gained market share (Graph 1, left-hand panel). In particular, Binance, Avalanche and – until recently – Terra rapidly increased their footprints. In early May 2022, the total value of cryptocurrencies associated with protocols on Ethereum made up just half of the overall assets locked into DeFi.[1]

The fragmentation of the crypto landscape stands in stark contrast to traditional (payment) networks, which benefit from strong network effects. In the traditional system, the more users flock to a particular platform, the more attractive it becomes for new users to join that platform, creating a virtuous circle. This drives costs down, improves service quality and promotes financial inclusion (BIS (2021)). The recent launch and rapid adoption of Brazil's Pix instant payment system illustrates these dynamics. In just over a year since its launch, Pix has seen 114 million users sign up, or 67% of the adult population (Duarte et al (2022)).

This bulletin argues that fragmentation arises from inherent limitations of blockchains. To maintain a system of decentralised consensus on a blockchain, self-interested validators need to be rewarded for recording transactions. Achieving sufficiently high rewards requires the maximum number of transactions per block to be limited. As transactions near this limit, congestion increases the cost of transactions exponentially. While congestion and the associated high fees are needed to incentivise validators, users are induced to seek out alternative chains. This leads to a system of parallel blockchains that cannot harness network effects, raising concerns about the governance and safety of the entire system.

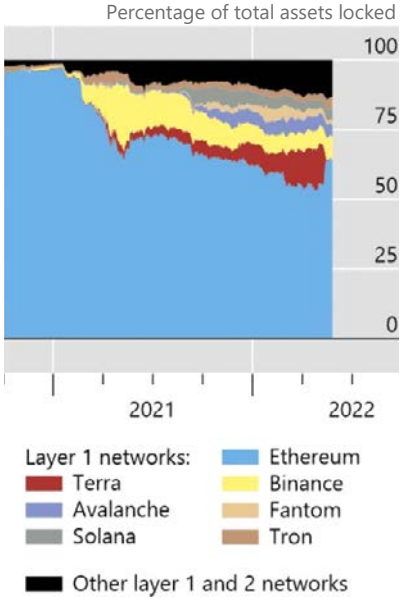
[1] In DeFi, a protocol refers to the code used for designing a decentralised application ("dApp") – or to the application itself, which allows transactions between users (eg lending, trading etc). Assets are "locked" in DeFi when they are used as collateral.

Blockchains, crypto and DeFi

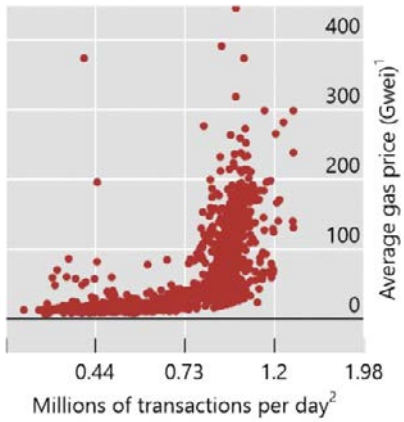
Crypto is built on permissionless distributed ledger technology (DLT), ie blockchains.[2] Crucially, rather than putting trust in centralised intermediaries, eg banks and the central bank, the blockchain is sustained by a multitude of pseudo-anonymous, self-interested validators incentivised via rewards and fees.

The more the sorrier: fragmentation rather than network effects — Graph 1

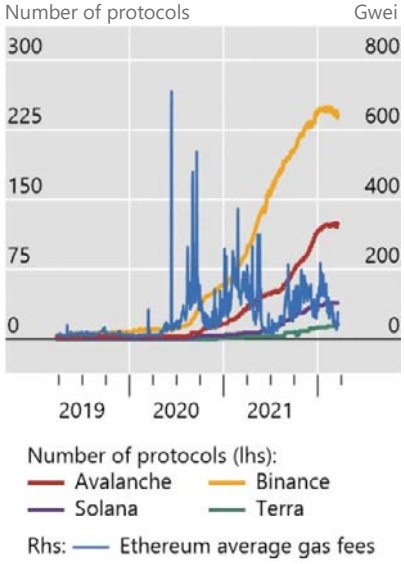
Fragmentation of layer 1 networks in decentralised finance (DeFi)



As transactions near the limit, gas fees on Ethereum spike



Periods of congestions are followed by growth of other blockchains



[1] One Gwei corresponds to 10^{-9} ETH (ie 0.000000001 ETH). Outliers larger than 450 Gwei are excluded from the graph. [2] Transactions per day are shown on a logarithmic scale.

Sources: CoinGecko; Defi Llama; Etherscan; authors' calculations.

The use of blockchains and cryptocurrencies is essential in the move towards a decentralised system. With a blockchain, any participant can transact on a public ledger – whether in the form of fund transfers, locking of assets as collateral or other functions – without the need for a centralised intermediary that keeps track of transactions. Since all transactions are public, blockchains must feature pseudo-anonymity. As the history of transactions is publicly observable and tied to a specific wallet with a corresponding address, the true identity of the party behind transactions (ie the owner of the address) remains hidden.[3]

Cryptocurrencies are the means of exchange among users and are also essential to reward validators for running and maintaining the decentralised system. Suppose Juanita wants to sell cryptocurrencies to Hiro. The buyer, Hiro (whose identity is hidden behind his cryptographic digital signature), would first broadcast the transaction details (addresses, amount, fees). Validators will then compete to verify the transaction, and whoever finishes first (ie emerges with a valid proof-of-work (PoW)) adds the transaction

[2] Permissionless DLT allows any entrant to serve as a validator or node in the network (without permission), using an address (a type of pseudonym) rather than a verified identity – it is thus "pseudo-anonymous". New "blocks" of transactions are added to the ledger to create a blockchain. Blockchains are often referred to as "layer 1" networks, ie the base networks that can validate, process and finalise transactions on the chain without the need for another network. "Layer 2" solutions build on layer 1 networks, but transactions mostly happen off-chain and are only sporadically reported back to the underlying layer 1 chain.

[3] Even though blockchains offer anonymity in principle, the full transaction history of specific cryptocurrencies is recorded on a public ledger. This means that if a user's address is identified, it is possible to trace the full history of that user's transactions – thus violating user privacy. These same features mean that blockchain analytics companies and law enforcement can make use of auxiliary information (eg posts on an online forum associated with transactions) to identify transacting parties.

to the blockchain. The updated blockchain is then shared among all miners and users, who verify that the transaction does not violate the past history. However, this process is costly, as it requires computing power or, in the case of proof-of-stake (PoS), significant amounts of staked cryptocurrency (ie "skin in the game").[4] Validators need to be compensated through monetary incentives, ie block rewards and fees. Fees are denominated in the cryptocurrency underpinning the specific blockchain network and are usually paid by the parties involved in a transaction. In Ethereum these are called "gas fees". The level of gas fees, which is determined primarily by the demand for transactions, fluctuates widely.

DeFi is a range of financial applications that aim to provide services and products similar to those of traditional finance, but in a decentralised manner built on blockchains (Aramonte et al (2021)). Transactions are executed in cryptocurrencies, often through self-executing code that triggers transactions if specific events occur ("smart contracts"), and they are recorded on the blockchain. Smart contracts were made possible by the development of Ethereum, the first major blockchain that allowed for programmability. This means that transactions or transfers can be made contingent on meeting certain pre-specified conditions. Blockchains with programmability thus underpin decentralised applications (dApps) that offer services such as lending or trading in cryptocurrencies.

Congestion and high fees lead to a fragmentation of the crypto landscape

It is the inherent features of blockchains – first and foremost, the need to incentivise decentralised nodes to validate transactions – that drive the fragmentation of the crypto landscape.

Self-interested validators are responsible for recording transactions on the blockchain. To ensure the integrity of the ledger, validators have to be incentivised through sufficiently high monetary rewards: Due to the pseudo-anonymity of the crypto system, they have no reputation to lose, cannot be fired and often cannot be held accountable in the legal system. Fees also need to be sufficiently high to deprive validators of an incentive to cheat and steal funds. Should fees become too low, the consensus mechanism would fail, undermining the security of the system. This trade-off is at the heart of the "blockchain scalability trilemma" between decentralisation, security and scalability (Buterin (2021)).

Thus, to guarantee sufficient rewards to validators, blockchains limit the number of transactions per block (Hubermann et al (2021)). On Ethereum, this currently implies a limit of about 30 transactions per second.[5] Once requested transactions approach this limit, there is congestion, and the transaction cost increases exponentially (Graph 1, centre panel). The reason is that transactions offering higher fees are more likely to be validated, as they yield higher rewards. To avoid long waiting times, users offer higher fees, thereby bidding up the price during periods of congestion. For example, while transaction fees during times of modest traffic average around $1, they can average more than 75 times higher on days with high congestion. The necessary limit to the number of transactions, which arises from economic incentives to ensure consensus, also means that simply adding validators will not overcome congestion.

The built-in limits to scale and associated high transaction costs lead to fragmentation as gas fees spike and users switch to alternative blockchains ("layer 1 networks") to transact at lower fees. For example, spikes in gas prices on Ethereum are followed by rapid growth in the number of protocols on other blockchains, eg Avalanche, Binance or Solana (Graph 1, right-hand panel). In consequence, as more users enter the DeFi system, more and more competing blockchains are used.

Even though newer blockchains initially share protocols with older ones, they differ in their specific design features. Indeed, the first protocols to run on new blockchains were already available on Ethereum (Graph 2, left-hand panel). This pattern suggests that users switch to other blockchains to perform

[4] In a PoS system validators pledge ("stake") their own cryptocurrency as a type of collateral. If they neglect their duties or make fraudulent decisions, they are punished by losing some of their stake. In that sense, their stake serves as "skin in the game".

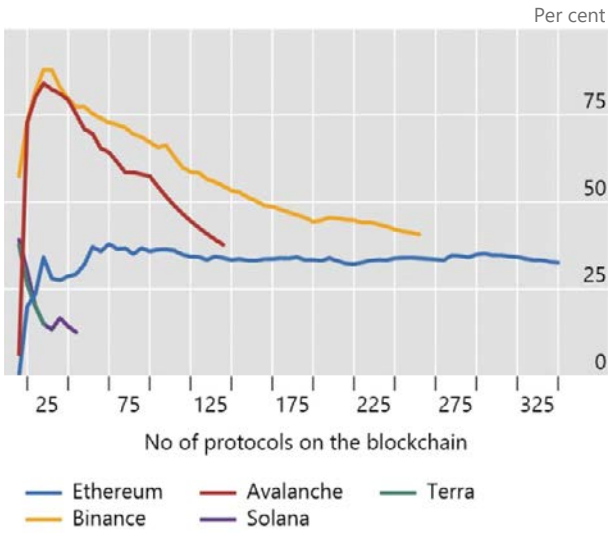
[5] By comparison, Visa processes around 1,700 transactions per second on average.

transactions that became prohibitively expensive on Ethereum. However, newer blockchains often aim for higher transaction limits, even if these come at the cost of greater centralisation and weaker security.[6]

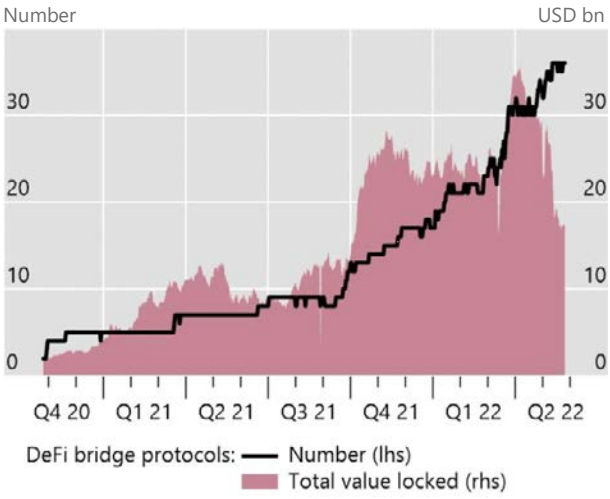
Blockchain fragmentation and the rise of bridges

Graph 2

Blockchains often share common protocols[1]



The number of bridges is increasing[2]



[1] Percentage of protocols running on a given blockchain that are also running on another blockchain (y-axis) as a function of the total number of protocols on the blockchain (x-axis). [2] Based on bridges and cross-chain protocols.

Sources: CoinGecko; Defi Llama; authors' calculations.

More monies, more problems: interoperability, cross-chain bridges and security cracks

The fragmentation of the crypto system introduces additional risks, as different blockchains are not interoperable. Interoperability refers to the ability of protocols and validators to access and share information across different blockchains. In other words, this means that different blockchains can verify each other's transaction history and share the same "truth". However, interoperability is not achievable in practice: as chains feature different validation mechanisms, they cannot reach the same consensus about the validity of transactions on the other blockchain (Buterin (2016)).[7]

To mitigate the problem of interoperability and allow for the transfer of coins across chains, "cross-chain bridges" have emerged. For example, a user can send 100 Ether to a centralised party (the bridge), where the Ether is stored. This transaction would be validated on the Ethereum blockchain. The bridge then mints new currency on another chain of equivalent value to the 100 Ether and transfers it to the user. This second transaction would be recorded on the other blockchain, not on Ethereum. As the number of blockchains has increased, so has the number of bridges (Graph 2, right-hand panel). Not only do bridges not solve the fragmentation of the blockchain landscape, but they imply that the consensus mechanism is highly concentrated, thereby introducing new security risks. Bridges often require the majority of only a limited number of validators to verify transactions. Such consensus mechanisms allow for faster

[6] Ethereum has over 300,000 validators, compared with ~1200 on Avalanche and ~1600 on Solana. In 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 validators, and hence higher required rewards. Such blockchains therefore get more rapidly congested. On blockchains with fewer validators, on the other hand, there is more potential for a group of validators to manipulate the network.

[7] Even if two chains shared the same validation mechanism, interoperability would not be achievable. As Buterin (2016) explains, "*[…] it is impossible for a mechanism inside chain A to fully validate chain B and a mechanism inside chain B to fully validate chain A at the same time, for the same […] reason why two boxes cannot simultaneously contain each other*".

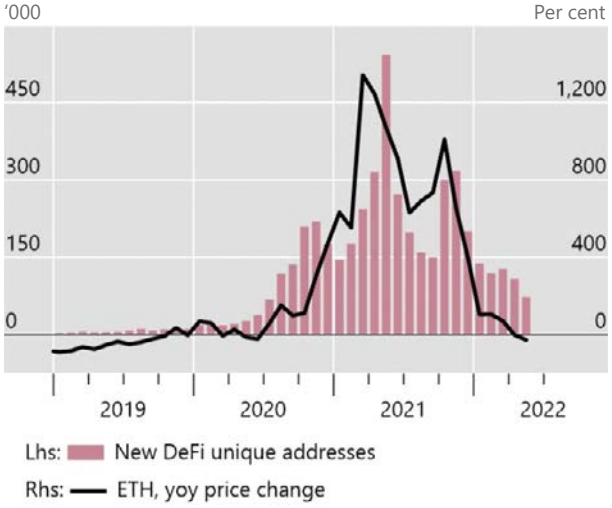
transactions, but they generally rest on the trustworthiness of just a few validators, thus jeopardising security by increasing the risk of an attack. Indeed, cross-chain bridges have been at the centre of several recent high-profile hacks such as that recently affecting Axie Infinity – highlighting the vulnerability to security breaches.[8]

Another attempt at achieving scalability are so-called "layer 2" solutions. Blockchains such as Ethereum, Avalanche, Binance or Solana, are commonly referred to as "layer 1" networks. Any transaction on a layer 1 blockchain is validated and recorded on the respective public ledger, ie "on-chain". In contrast, the bulk of transactions on layer 2 solutions (eg the Bitcoin Lightning Network) happen off-chain, and transactions are only sporadically reported back to the underlying layer 1 chain in bundles. Layer 2 blockchains thereby allow for higher transaction limits and lower fees, but at the cost of giving up decentralisation, posing risks similar to those of bridges.[9]

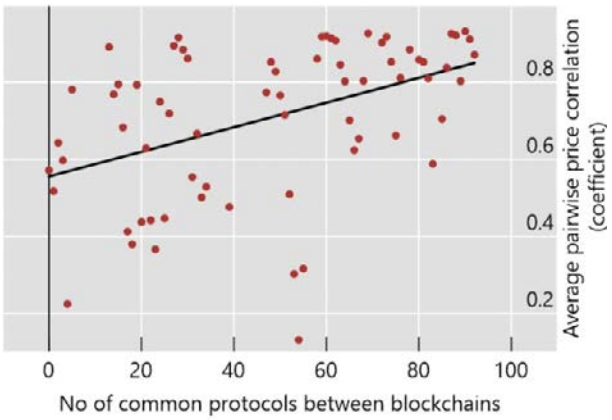
Fragmentation without interoperability implies that cryptocurrencies cannot fulfil the role of money as a coordination device. Fundamentally, money is a social construct, as people accept money in the expectation that others will do so in the future. Money thereby exhibits positive network externalities: the more people use it, the more people are willing to do so. Ultimately, these network effects lead society to coordinate on one unique money, reducing transaction costs. Blockchains, on the other hand, feature negative network externalities. The more a given user transacts on one blockchain, the more they congest the system, and the higher the transaction fees for everybody else. Even if everyone wanted to transact in the same cryptocurrency, congestion would lead to new monies proliferating.

The system is sustained by an influx of new users, driving co-movement in prices — Graph 3

Attracted by rising prices: Ether price and users



Cryptocurrency prices are more correlated when blockchains share more protocols[1]



[1] Based on five blockchains: Avalanche, Binance, Ethereum, Solana, Terra and, therefore, on 10 pairwise correlations of the blockchains' native coin prices over 2019–22. Correlations calculated over a 40-day rolling window.

Sources: @rchen8 via https://dune.com/queries/2972/5739; CoinGecko; CryptoCompare; Defi Llama; authors' calculations.

Despite the proliferation of monies, the system – driven by inflows of speculative users – exhibits strong co-movement in prices across cryptocurrencies. Periods of rising prices are usually followed by a

[8] The Axie Infinity hack is a good example of an attack on a bridge. Axie Infinity is a popular play-to-earn video game that runs on the Ronin layer 2 blockchain. A bridge allows users to transfer cryptocurrencies from Ronin to Ethereum, provided that a majority of the nine validators agree with the transaction. On 23 March 2022, hackers obtained the private keys of five validators, forged withdrawals from Ronin wallets and credited their own Ethereum wallet with $625 million worth of Ether.

[9] Another proposed solution is sharding, which involves dividing up the work of validation among different groups of validators.

further influx of users attracted by the potential of quick gains (Graph 3, left-hand panel). As the same user often also buys several cryptocurrencies (Shams (2020)), there is strong price co-movement. The pairwise correlation in cryptocurrency prices across different blockchains averaged 0.6 in Q1 2022, ranging from a low of 0.25 between Ethereum and Terra to a high of 0.91 between Ethereum and Bitcoin (right-hand panel). The price correlation of cryptocurrencies across two blockchains is especially high when the blockchains offer similar services (ie share common protocols, on the x-axis), suggesting that investors use comparable protocols to carry out similar transactions on different blockchains (eg borrow a stablecoin to speculate on another cryptocurrency). The crypto landscape hence offers little room for portfolio diversification.

When the influx of new users stops, the market can quickly unravel. The Terra blockchain, which collapsed spectacularly in May 2022, is one example. It relied on a coin, Luna, and an algorithmic stablecoin called TerraUSD. As the latter lost its peg, users rapidly lost confidence that the price of Luna would further increase. As a consequence, both TerraUSD and Luna experienced a classic run, causing their prices to collapse. This also led to security risks for the blockchain, itself. The Terra blockchain allowed for 10,000 transactions per second, but its delegated PoS mechanism meant that only about 130 delegators were responsible for validation. As the value of validators' Luna stakes fell to almost zero, anybody could have acquired a large amount of Luna to stake at almost no cost and become the dominant validator, thereby drastically increasing the risk of governance attacks. As a result, Terra had to halt its blockchain.

Conclusion

Building on permissionless blockchains, crypto and DeFi seek to create a radically different monetary system, but they suffer from inherent limitations. A system sustained by rewarding a set of decentralised but self-interested validators through fees means that network effects cannot unfold. Instead, the system is prone to fragmentation and costly to use.

Fragmentation means that crypto cannot fulfil the social role of money. Ultimately, money is a coordination device that facilitates economic exchange. It can only do so if there are network effects: as more users use one type of money, it becomes more attractive for others to use it. Looking to the future, there is more promise in innovations that build on trust in sovereign currencies.

References

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

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

Bank for International Settlements (2021): *Annual Economic Report*, Chapter 3, "Central bank digital currencies: an opportunity for the monetary system", June.

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

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

Duarte, A, J Frost, L Gambacorta, P Koo, H S Shin (2022): "Central banks, the monetary system and public payment infrastructures: lessons from Brazil's Pix", *BIS Bulletin*, no 52, March.

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.

Shams, A (2020): "The structure of cryptocurrency returns", *mimeo*.

Previous issues in this series

No 55 19 May 2022	Rising household inflation expectations: what are the communication challenges for central banks?	Fiorella De Fiore, Tirupam Goel, Deniz Igan and Richhild Moessner
No 54 18 May 2022	Commodity market disruptions, growth and inflation	Deniz Igan, Emanuel Kohlscheen, Gabriela Nodari and Daniel Rees
No 53 04 May 2022	Are major advanced economies on the verge of a wage-price spiral?	Frederic Boissay, Fiorella De Fiore, Deniz Igan, Albert Pierres-Tejada and Daniel Rees
No 52 23 March 2022	Central banks, the monetary system and public payment infrastructures: lessons from Brazil's Pix	Angelo Duarte, Jon Frost, Leonardo Gambacorta, Priscilla Koo Wilkens and Hyun Song Shin
No 51 17 March 2022	Anchoring of inflation expectations: has past progress paid off?	Tirupam Goel and Kostas Tsatsaronis
No 50 10 March 2022	Housing market risks in the wake of the pandemic	Deniz Igan, Emanuel Kohlscheen and Phurichai Rungcharoenkitkul
No 49 10 December 2021	Interoperability between payment systems across borders	Codruta Boar, Stijn Claessens, Anneke Kosse, Ross Leckow and Tara Rice
No 48 11 November 2021	Bottlenecks: Causes and macroeconomic implications	Daniel Rees and Phurichai Rungcharoenkitkul
No 47 27 October 2021	Labour markets and inflation in the wake of the pandemic	Frederic Boissay, Emanuel Kohlscheen, Richhild Moessner and Daniel Rees
No 46 18 August 2021	Could corporate credit losses turn out higher than expected?	Mikael Juselius and Nikola Tarashev
No 45 02 August 2021	Regulating big techs in finance	Agustín Carstens, Stijn Claessens, Fernando Restoy and Hyun Song Shin
No 44 22 July 2021	Covid-19 and bank resilience: where do we stand?	Yuuki Ikeda, Will Kerry, Ulf Lewrick and Christian Schmieder
No 43 15 July 2021	Global reflation?	Flora Budianto, Giovanni Lombardo, Benoit Mojon and Daniel Rees

All issues are available on our website www.bis.org.