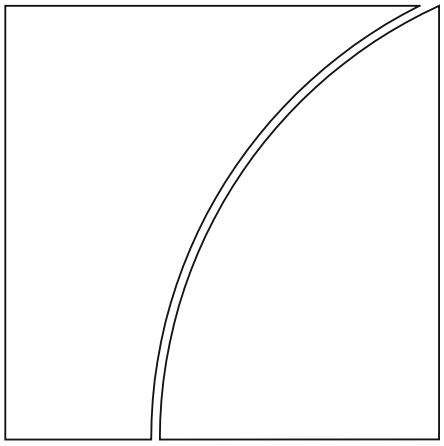
Basel Committee
on Banking Supervision



Working Paper 44

Novel risks, mitigants and uncertainties with permissionless distributed ledger technologies

28 August 2024

BIS

The views expressed in this Working Paper are those of their authors and do not necessarily represent the official views of the Basel Committee, its member institutions or the BIS.

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

Grey underlined text in this publication shows where hyperlinks are available in the electronic version.

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

ISBN 978-92-9259-779-5 (online)

Contents

List of members of the permissionless DLT workstream

Canada	Matthew Gordon	Office of the Superintendent of Financial Institutions
Europe	Christian Moor	European Banking Authority
	Ivan Keller	European Commission
France	Laurent Camus	Bank of France
	Julien Uri	Bank of France
Italy	Paolo Granata	Bank of Italy
Japan	Yoshito Atsumi	Financial Services Agency
	Shun Nakamura	Financial Services Agency
	Taisuke Terada	Financial Services Agency
Singapore	Desmond Kow	Monetary Authority of Singapore
Spain	Rebeca Anguren	Bank of Spain
	Diego Hernandez	Bank of Spain
Switzerland	Christian Capuano	Swiss Financial Market Supervisory Authority
United States	Nathan Palmer	Board of Governors of the Federal Reserve System
	Irina Leonova	Federal Deposit Insurance Corporation
	Thomas Smejkal	Federal Reserve Bank of New York
	Miriam Bazan	Office of the Comptroller of the Currency
Secretariat	Renzo Corrias	Bank for International Settlements
	Monika Spudic	Bank for International Settlements

Novel risks, mitigants and uncertainties with permissionless distributed ledger technologies

Executive summary

Banks that transact on permissionless blockchains or similar distributed ledger technologies (DLTs) face risks related to operations and security, governance, legal, compliance – including money laundering/financing of terrorism (ML/FT) – and settlement finality. Certain risks stem from the blockchains' reliance on unknown third parties, which makes it difficult for banks to conduct due diligence and oversight. These risks require new risk management strategies and safeguards. Current practices for mitigating these risks remain in various stages of development and have not been tested under stress.

Keywords: distributed ledgers, cryptoassets, technology risk

JEL: G21, G28, O30

1. Introduction

Banks that transact on permissionless blockchains or similar distributed ledger technologies may face various risks. This paper considers these risks as well as the development of new risk management strategies and safeguards. While technology-based mitigants are not yet mature and have not been tested under periods of stress, rapid developments may generate new solutions (and risks) which may benefit from further examination.

For the purposes of this paper, permissionless blockchains are defined as networks that do not limit who can participate in the consensus process used to validate transactions and data. They are decentralised across unknown parties. Permissioned blockchains, in contrast, are closed networks in which a previously designated party or parties (sometimes members of a consortium) interact and participate in consensus and data validation.[1]

The remainder of this paper is organised as follows: Section 2 examines novel risks of permissionless blockchains. Section 3 examines potential mitigants to those risks. Section 4 summarises and concludes. Annex 1 includes a survey of international reports relevant to permissionless distributed ledger technologies (DLTs), and Annex 2 surveys definitions of permissionless, permissioned, public and private DLTs.

2. Novel risks posed to banks by activities on permissionless blockchains

2.1 Governance risk

Governance of a permissionless blockchain is decentralised by design. Decentralised governance poses a challenge for regulated entities that must establish clear lines of responsibility and accountability and conduct due diligence on third parties they rely on.

In many permissionless blockchains, nodes must agree on changes and upgrades to the blockchain. This distributed governance may pose challenges in addressing bugs or security vulnerabilities and increase the risk of loss associated with assets that exist on these blockchains. Depending on the degree to which governance is decentralised, banks could struggle to conduct effective due diligence and oversight of third parties. Further, when participants cannot agree on updates to network rules, they may split the blockchain itself, often referred to as a hard fork.[2] If a blockchain splits into two networks, assets that exist on the blockchain may be subject to significant price volatility or loss, potentially causing

[1] Some publications, such as ISO (2024) and MAS & BIS (2023) treat *permissionless/permissioned* as a distinct concept compared to *public/private* for DLTs, such that one could distinguish between *public permissioned* and *public permissionless*. For example, ISO (2024) describes *permissionless* and *permissioned* in terms of restrictions on user and administrator actions and describes *public* and *private* in terms of restrictions on user access. Other publications such as BCBS (2022) do not draw similar distinctions. This paper largely discusses permissionless DLTs. Annex 2 provides a survey of several of these definitions.

[2] Hard forks are protocol updates that occur when nodes add new rules in a way that conflicts with the previous rules. New nodes can only communicate with others that operate the new version. As a result, the blockchain splits, creating two separate networks. When traditional financial assets are tokenised, a hard fork will lead to a situation in which there are two or more tokens running on different DLTs but only one underlying asset. Soft forks may also present governance challenges, since every version of an asset may not be technically identical. Soft forks are changes to the code that are backwards compatible; that is, nodes running old software will still recognise new blocks as valid when they come from nodes running new, soft-fork software (however, *reversing* a soft fork that has already been released could require a hard fork).

problems for activities such as price determination, exposure calculation, and fulfilling capital requirements.

Many of the governance mechanisms of permissionless blockchains occur off-chain. Governance authority may also be concentrated in entities operating a significant portion of nodes, and off-chain governance might obscure conflicts of interest. Off-chain procedures involve various decision-making and coordination mechanisms, both formal (through decision-making and control structures set up by the founders of the initiative), and informal (for example through blogs, social networks, or other fora established among the participants in the network). These decision-making processes, which may concern important aspects such as structural changes to the DLT protocol, can be time-consuming and can give rise to suboptimal results in emergencies in which timely action is necessary.

2.2 Technology risk / vulnerability to various types of attacks

A fundamental feature of blockchains is that consensus is reached on the record of transactions represented on that chain. Permissionless systems might be vulnerable to so-called "51% attacks," in which a coordinated effort is put forward to control greater than 50% of the validation nodes or 50% of the staked native token and thus select which, and how, blocks are added to the blockchain. Several smaller proof of work (PoW) blockchains have experienced 51% attacks, but to date no proof of stake (PoS) blockchain network has experienced a 51% attack.[3]

Banks that participate in permissionless blockchains depend on unknown third parties to process transactions. There may be compelling reasons to expect those third parties to act honestly, given financial incentives created by the consensus mechanism. As a general matter, a 51% attack will be contrary to the attacker's interest, since it would likely devalue any asset that the attacker was able to steal. Malicious actors might have a different set of incentives – causing economic harm, for example and some could bring more resources to bear to carry out an attack. A successful 51% attack could undermine confidence in the accuracy of the ledger, which in turn could affect the value of the assets on it. However, traditional centralised IT infrastructure is also vulnerable to malicious actor attacks.

Permissionless blockchains are subject to a number of other potential attacks, including some unique to permissionless blockchain infrastructure.[4]

2.3 Legal and compliance risk

2.3.1 Money laundering / financing of terrorism

Permissionless blockchains pseudonymise participants, replacing identifying information with an artificial identifier. This can complicate compliance with know your customer (KYC), anti-money laundering (AML) / combatting the financing of terrorism (CFT), and sanctions regulations. For example, transacting with pseudonymised counterparties creates a risk of transacting with illicit counterparties.[5] Additionally,

[3] At the time of writing, Bitcoin is a popular example of a blockchain using a proof of work (PoW) protocol, while Ethereum is a popular example of a blockchain using of a proof of stake (PoS) protocol.

[4] See Hasanova et al (2019) and Li et al (2020) for discussion of other potential attacks.

[5] As reported by the Financial Action Task Force (FATF), cryptoassets can be used for illicit purposes such as money laundering and terrorism financing. This is due to the different levels of anonymity or "pseudo-anonymity" offered by many blockchains. Indeed, while authorities could potentially be able to track transactions on the blockchain, they may not be able to establish the identity of the two parties of a transaction and, therefore, who is the owner of the asset (eg on a permissionless blockchain, only the data relating to the public sender and recipient address of the transaction are recorded, but there is no association between these addresses and the identity of the private key owners). Many permissionless networks also explicitly promote privacy-protecting coins, such as Monero and zCash. Further, permissionless networks generally permit non-custodial wallets, which could allow users to participate without going through KYC.

whenever a transaction is registered on a blockchain, validators often collect transaction fee payments (sometimes referred to as "gas fees"). The transaction fees could be paid to illicit entities conducting validation services pseudo-anonymously ("gas fee risk").

At the same time, in certain circumstances, distributed ledgers (both permissionless and permissioned) have the potential to enhance AML/CFT compliance, insofar as they provide visibility into the entire universe of transactions (rather than just transactions at one institution), which might help institutions identify suspicious transactions. Also, pseudonymity on permissionless networks is imperfect, meaning it is possible (albeit sometimes difficult) for financial institutions to attribute on-chain activity to individual participants.

2.3.2 Settlement risk and probabilistic settlement

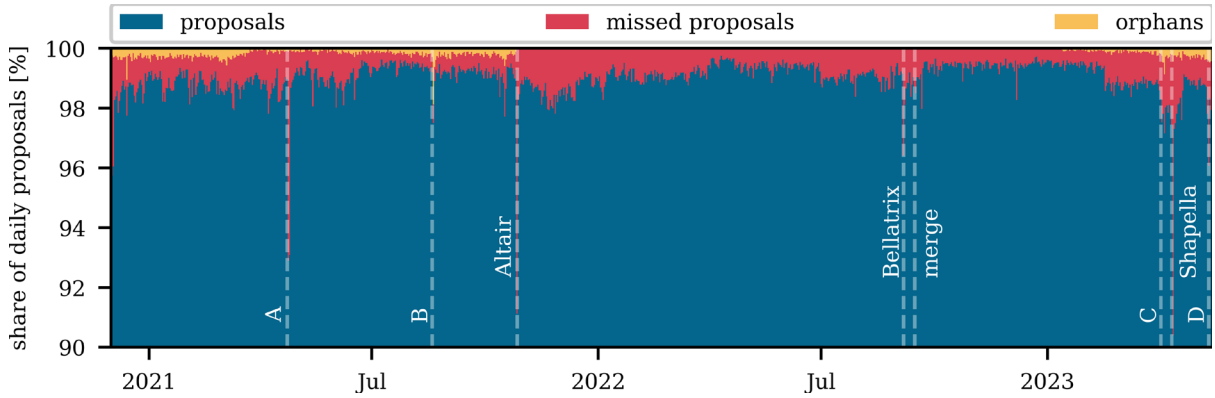
In many permissionless DLTs, settlement remains probabilistic, meaning the probability that a transaction could be revoked converges to, but never reaches, zero with the passage of time. This creates settlement risk in permissionless blockchains.[6] For a variety of reasons, the system may reverse a block containing what participants may have thought was a settled transaction. These may be referred to as "orphaned blocks", which while a small fraction of total blocks, may occur at a daily frequency (see Graph 1).

Well-designed and well-operated payment and settlement systems ensure clear and certain settlement of transactions, giving confidence to their users about when transactions become final and that once final, transactions cannot be revoked or unwound. Legal settlement finality is often defined very precisely in legal frameworks of jurisdictions[7] and rules, procedures, and contracts of existing payment and settlement systems. However, it is often unclear whether and how permissionless blockchains could adapt their rules, procedures, and contracts to ensure they have clear and certain legal foundation for settlement finality; or who would be accountable for enforcing settlement finality provisions on those blockchains. Even if the relevant legal framework and the blockchain's rules, procedures and contracts have defined the point at which final settlement occurs, the use of probabilistic settlement may still cause misalignment between legal finality and technical settlement which can result in uncertainty about the settlement status of transactions for the parties involved.

[6] Settlement risk is the risk that settlement of transactions does not take place as expected. Some blockchain consensus mechanisms are designed such that technical settlement is not probabilistic. See Bains (2022) and Davidson (2023) for a discussion of mechanisms that address finality.

[7] For example, the European Settlement Finality Directive defines three distinct stages of legal settlement finality – the moment of entry of a transfer order into the system, the moment after which the transfer order becomes irrevocable, and the moment at which the order becomes binding and enforceable against third parties. For a more detailed discussion of settlement finality, see CPMI-IOSCO (2022, 2012).

Graph 1: Estimates of the percentage of orphaned blocks



Daily share of successful (shown in blue), missed (shown in red), and orphaned proposals (shown in yellow). Major upgrades/events that had a noticeable impact on the network participation are indicated by white dashed lines. The Altair upgrade heavily reduced the number of orphaned blocks. Also highlighted are incidents A, B, and D. in all three cases bugs in the Prysm and Teku consensus clients resulted in increased numbers of missed/orphaned proposals. Incident C marks an attack on MEV-Boost.

Source: Grandjean et al (2023). Copyright Grandjean, Heimbach and Wattenhofer; reproduced with permission of the authors.

Orphaned blocks occur as part of the technical process of building the blockchain, and the probability of transaction reversal falls as the block containing the transaction sinks further into the blockchain. The transactions of reversed (orphaned) blocks may get executed within other blocks or join the settlement queue again. Businesses that use blockchains, for example crypto exchanges, have conventions around how many blocks deep a transaction must sink before it is considered "processed" for the purpose of crediting funds to a blockchain user.[8]

Less frequently, orphaned blocks can be caused by malicious nodes taking over the network via a 51% attack, rewriting past legitimate transactions and validating (executing) fake ones (eg transferring assets, and then re-transferring the same assets again, also known as double-spending).[9]

2.3.3 Privacy, confidentiality and consumer protection

Some permissionless blockchains provide an open record of transactions that can be viewed by the public. This can raise concerns about privacy and confidentiality depending on the design of the ledger. Those concerns are mitigated, to some extent, by the pseudonymity of blockchain transactions, although the pseudonymity has substantial limits and cannot fully ensure privacy.[10] The ability to view user transactions may also enable cyberattacks.

There is an apparent tension between the difficulty of auditing pseudonymous activity on the blockchain, as described in section 2.3.1, and the potential privacy concerns described in this section. It takes some effort to hide one's activities on a permissionless blockchain; those who wish to hide their activities may make it quite difficult to track their behaviour, while those who are not paying as close

[8] For example, the crypto exchange Kraken lists block depths required for nearly 250 cryptocurrencies, with mean and median transaction processing times of 35 minutes and 14 minutes respectively: Kraken (2024).

[9] The probabilities of such an attack are very much dependent on the size of the blockchain network and the type of consensus mechanism used. They usually require the malicious actors to obtain 51% of the validation power or staked native token on the network. In large, decentralised permissionless networks, such as Bitcoin and Ethereum, the costs of reversing *technical* finality is very expensive and runs in the billions of euros. To note that because of hacking risks and risks of operational failures, technical settlement finality is also probabilistic in permissioned systems or centralised traditional systems – the hacking of the Bangladesh Central Bank in 2016 and illegal transfer of $81 million to designated accounts illustrates the point.

[10] See Mascelli (2023) for an in-depth discussion of privacy and its limits on DLTs.

attention, or less sophisticated users, may take fewer precautions and be much easier to identify and track.[11]

In addition, depending on how cryptoassets are designed on a permissionless blockchain, the ability of nodes to order transactions in a block may run afoul of regulations and consumer protections. Maximal extractable value (MEV) is a particular example of this type of activity.[12]

2.4 Additional risks

2.4.1 Liquidity risk and the "paradox of transparency"

The transparency of permissionless networks could cause or heighten liquidity risks at participating banks. Transaction visibility may spur or exacerbate runs on the cryptoassets on the permissionless blockchain and may also act as a coordination device among users whose incentive to withdraw increases when other users do so. For example, recent research indicates that the transparency of a permissionless system exacerbated the run that occurred in the Terra/Luna crash.[13] Decentralised, non-contracted validators may be unable to coordinate to mitigate liquidity risk during a stress event by, for example, limiting withdrawals on the network.

Some of the most popular permissionless blockchains have low transaction throughput compared to traditional payment clearing and settlement systems. This can be exacerbated in times of system stress when herding behaviour might cause the system to experience congestion. Additionally, many permissionless blockchains have dynamic pricing; as a result, in times of stress, the price of transacting itself may increase, and transactions may not be able to be conducted in a timely manner.[14] This can impose a liquidity risk on tokenised assets that use permissionless blockchains.

2.4.2 Political, policy and legal uncertainty

A change in laws, regulations, and/or policies surrounding cryptoassets could change validator behaviour, sometimes suddenly, in a way that makes the blockchains themselves operationally unstable. For example, jurisdictions could ban or discourage cryptoasset mining for a variety of reasons. Such developments could serve to reduce the amount of computing power or staked native tokens available to secure the blockchain, temporarily increasing the risk of a 51% attack.[15] Furthermore, there is continued uncertainty in some jurisdictions as to how various permissionless cryptoassets will be classified and thus what regulatory regimes will apply.

3. Discussion of potential mitigants

This section presents potential mitigants that could be used to mitigate the risks of permissionless blockchains. Table 1 below maps out the potential mitigants to the risk(s) that they are intended to

[11] Importantly, there may be ways to use privacy-preserving technologies to encourage both increased privacy and auditability. For further discussion, see US Department of the Treasury (2023).

[12] The concept of MEV was introduced in Daian et al (2020); see Qin et al (2022) for updated estimates. MEV may include a wide range of activities, such as price arbitrage between exchanges or front-running transactions; see Auer et al (2022) for a discussion of the latter.

[13] Liu et al (2023).

[14] See, for example PYMNTS (2022).

[15] See Griffith and Clancey-Shang (2023) for a discussion of the temporary and permanent effects of the 2017 and 2021 Chinese bans on various cryptoassets.

address; different mitigants may address diverse aspects or sub-risks of similar concerns. These mitigants have varying degrees of real-world deployment. The discussion of each mitigant seeks to address whether the mitigants are conceptual (with minimal real-world implementation), experimental (real-world implementation, but only in pilot or exploratory setting), or implemented with varying degrees of usage. Given the fast-moving developments in DLT, the state of mitigants is dynamic and many mitigants have not been tested under real stress scenarios. Finally, some risks do not have effective mitigants listed, such as risks around settlement finality.

Potential mitigants Table 1

Mitigant	Risk(s) that it is intended to address
A. Business Continuity Planning	Governance risk; technology/attack risk; political, policy, and legal uncertainty
B. Technology-based control over parties and transactions	Legal/compliance risk (money laundering/financing of terrorism)
C. Permissioning a subset of node infrastructure	Legal/compliance risk (money laundering/financing of terrorism); technology/attack risks, consumer protections risk
D. Technology to address privacy/confidentiality/consumer protection risks	Privacy/confidentiality/consumer protection risks
E. Technology to address liquidity risk	Liquidity risk

3.1 Business continuity planning

To manage the risk that a permissionless blockchain fails or experiences a material disruption, perhaps the most effective risk mitigation strategy currently available, particularly for traditional financial assets issued on a blockchain, is business continuity planning (BCP) by the issuer.[16] BCP could involve a registry that can be used to recover ownership after disruption, such as an off-chain database. For example, in the event of a hard fork or an attack on the blockchain that creates uncertainty as to the distributed ledger's accuracy, the off-chain records could be used to identify the rightful owner of the assets or the branch of the fork that should be followed. BCP could also set out all relevant internal processes, including those to ensure that all transactions and participants are traceable, potential lost data can be recovered, and the records on the ownership of the assets can be retrieved within a reasonable timeframe. In addition, BCP could define an alternative blockchain where assets would be created or ported in case of disruption of the primary blockchain ("designation of a contingency chain").

The efficacy of BCP remains an open question. While BCP has been deployed successfully in some experimental instances, it has not been tested under stress. Transitioning an asset from a failed blockchain to either a different permissionless blockchain or a conventional system of records could prove complex and expensive.

Banks could reduce governance and technology/attack risk, to a certain extent, by monitoring permissionless blockchains' governance. This would enable banks to take appropriate actions (such as those in BCP) in case of a disruption. However, BCP would not fully mitigate the lack of clear and direct lines of responsibility and accountability in the permissionless network, which is a component of governance risk.

[16] Business continuity plans are discussed in BCBS (2021).

3.2 Technology-based control over parties and transactions

On certain permissionless blockchains, tokens that parties transact in are created or subject to constraints programmed by smart contracts. Those smart contracts determine the tokens' operational attributes and limitations. Among other things, smart contracts can be used to control and limit access to and ownership of a token and even to reverse transactions that have already been processed. These features, in turn, could be used to mitigate some of the AML/CFT risk associated with permissionless blockchains.

Implementation of permissions can take a number of forms:

1. *Denylisting*: when a crypto-asset has deny-listing functionality, the issuer can use the smart contract to bar specified addresses on the blockchain from holding or accessing the asset. A banking organisation might use this functionality to prevent transactions to or from wallets associated with known terrorists, criminals, or states subject to Office of Foreign Assets Control (OFAC) sanctions. The ability to infinitely create new wallets may limit the effectiveness of this mitigant.

2. *Allowlisting*: the inverse of denylisting. The token in question is programmed to be accessed only by approved addresses on the blockchain. Addresses that are not on the allowlist will not be able to receive or send the asset. The issuer can add or remove participants to the allowlist via the smart contract.

3. *Privacy-preserving identity verification*: technologies such as zero-knowledge proofs may allow identity verification while preserving privacy at the transaction level. Such technologies are nascent in both development and application; see section 3.4 for further discussion.[17]

4. *A controller*: smart contracts can also be used to empower a designated entity (the controller) to control and limit access to the cryptoasset; block and reverse transactions that are fraudulent; and amend the code that implements the cryptoasset functions to address any deficiencies that may emerge. The controller could be the entity that develops and maintains the business continuity plan (discussed above). The controller would not exercise control over the permissionless network itself, but over the specific tokens of a specific issuance. The controller could use its authority to help mitigate legal/compliance risks, in particular money laundering/financing of terrorism and OFAC sanctions risks, through the use of off-chain due diligence and blockchain-related permissioning technology.

These approaches could, to varying degrees, mitigate some of the legal and compliance risks associated with permissionless networks. The extent to which denylisting (3.2.1), allowlisting (3.2.2), and privacy-preserving identity verification (3.2.3) are used in practice is unclear. Varying levels of controller authority via smart contracts (3.2.4) appear to be employed in both experimental settings, and in practical settings.[18]

3.3 Permissioning node infrastructure

Permissioning a subset of nodes might create known validators that are deemed safe for particular users such as banks to interact with.[19] This may help address risks such as legal and compliance risks (including gas fee risks or ML/FT risks), technology/attack risks (including MEV risks), and consumer protection. This

[17] A zero-knowledge proof is a method by which one can prove that a given statement is true without conveying additional information. See Berentsen et al (2023) for a discussion of zero-knowledge proofs, and for an example of a nascent application see Buterin et al (2024).

[18] See, for example: Pereira (2023), De (2020) and European Investment Bank (2021).

[19] Permissioning all nodes would turn a permissionless blockchain into a permissioned one and is unlikely to be feasible.

would likely come at the cost of slowing down transactions for the parties attempting to avoid paying gas fees to nodes operated by criminals or other sanctioned parties.

3.4 Technology to address privacy, confidentiality and consumer protection risks

Technology to address privacy, confidentiality, and consumer protection risks is being developed. Some potential solutions, such as zero-knowledge proofs, may take the form of permissioned chains "one level up" from the primary blockchain. In such a configuration, the primary chain is referred to as a layer 1 chain, while the chain one level up is referred to as a layer 2 chain. Alternatively, a separate blockchain that communicates with the permissionless primary blockchain, called a sidechain, may be employed.[20] In addition to zero knowledge proofs, other methods such as fully homomorphic encryption might be used to protect consumer information.[21]

3.5 Technology to address liquidity risk

Low transaction throughput of popular permissionless blockchains can be exacerbated in times of system stress, imposing liquidity risk on tokenised assets. Several variations on layer 1 consensus mechanisms are intended to speed up the clearance of transactions. In addition, many blockchain projects aim to speed up transaction processing on layer 2 chains and sidechains. However, while these solutions aim to off-load transaction volume from layer 1s, they still depend on the base permissionless blockchain for final settlement and therefore only partly compensate for the layer 1's transaction processing speed. These technologies are all developing rapidly.

4. Summary and conclusions

Permissionless blockchains create risks that fall into existing risk taxonomies – chiefly operational risk and to a lesser extent liquidity risk and market risk. Banks have experience managing these kinds of risks, but permissionless blockchains present some novel challenges that may require new or additional methods to manage risk. Practices for mitigating these risks are in various stages of development and have generally not been tested under stress. While technology-based solutions to these risks are not yet mature, rapid developments may generate new solutions (and risks) which may benefit from further examination.

[20] In these examples, the layer 1 chain is the original blockchain. Layer 2 is software that processes transactions off layer 1. Typically, layer 2 bundles transactions together and then records the net transaction on layer 1. By bundling transactions, layer 2 increases the effective throughput of layer 1.

[21] Fully homomorphic encryption is an emerging cryptographic technology which allows certain mathematical operations to be conducted on encrypted data, without needing to decrypt the data first. For a discussion of fully homomorphic encryption see Brandao and Peralta (2021).

References

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

Bains, P (2022): "Blockchain consensus mechanisms: A primer for supervisors", *IMF Fintech Notes,* no 3, January.

Berentsen, A, J Lenzi and R Nyffenegger (2023): "An Introduction to Zero-Knowledge Proofs in Blockchains and Economics", Federal Reserve Bank of St. Louis, *Review*, vol 105, no 4.

Bank for International Settlements (BIS) Committee on Payments and Market Infrastructures (CPMI) and International Organization of Securities Commissions (IOSCO) (2012): *Principles for financial market infrastructures,* April.

——— (2022): *Guidance on the Applications of the Principles for Financial Market Infrastructures to stablecoin arrangements*, July.

Basel Committee on Banking Supervision (BCBS) (2021): *Principles for operational resilience*, March.

——— (2022): *Prudential treatment of cryptoassets*, December.

Brandao, LT and R Peralta (2021): "Privacy-enhancing cryptography to complement differential privacy", *NIST Cybersecurity Insights*, 3 November.

Buterin, V, J Illum, M Nadler, F Schär and A Soleimani (2024): "Blockchain privacy and regulatory compliance: Towards a practical equilibrium", *Blockchain: Research and Applications*, vol 5, no 1.

Davidson, M (2023): "State Machine Replication and Consensus with Byzantine Adversaries", *NIST Internal Report,* NIST IR 8460 ipd, April.

Daian, P, S Goldfeder, T Kell, Y Li, X Zhao, I Bentov, L Breidenbach and A Juels (2020): "Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability", in *2020 IEEE symposium on security and privacy,* May, pp 910-927.

De, N (2020): "Circle confirms freezing $100k in USDC at law enforcement's request", *CoinDesk*, 9 July.

European Investment Bank (2021): "EIB issues its first ever digital bond on a public blockchain", 28 April.

Financial Stability Board (FSB) (2020): "Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements", October.

——— (2022a): "Assessment of risks to financial stability from cryptoassets", February.

——— (2022b): "Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative report", October.

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

Global Financial Markets Association (GFMA) (2023): *Impact of distributed ledger technology in global capital markets*.

Grandjean, D, L Heimbach and R Wattenhofer (2023): "Ethereum Proof-of-Stake Consensus Layer: Participation and Decentralization", *ETH Zurich Working Paper*.

Griffith, T and D Clancey-Shang (2023): "Cryptocurrency regulation and market quality", *Journal of International Financial Markets, Institutions and Money*, vol 84.

Hasanova, H, UJ Baek, MG Shin, K Cho, and MS Kim (2019): "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures", *International Journal of Network Management*, vol 29(2).

Heimbach, L, L Kiffer, C Torres, R Wattenhofer (2023): "Ethereum's proposer-builder separation: promises and realities", in *Proceedings of the 2023 ACM on Internet Measurement Conference*, October, pp 406-420.

International Organisation for Standardisation (ISO) (2024): *Blockchain and distributed ledger technologies – vocabulary*, ISO 22739:2024.

International Organization of Securities Commissions (IOSCO) (2022): "IOSCO decentralized finance report", March.

Kraken (2024): "Cryptocurrency deposit processing times", www.support.kraken.com/hc/en-us/articles/203325283-Cryptocurrency-deposit-processing-times

Li, X, P Jiang, T Chen, X Luo and Q Wen (2020): "A survey on the security of blockchain systems", *Future generation computer systems*, vol 107.

Liu, J, I Makarov and A Schoar (2023): "Anatomy of a Run: The Terra Luna Crash", *National Bureau of Economic Research Working Paper*, no 31160, April.

Mascelli, J (2023): "Data Privacy for Digital Asset Systems", Federal Reserve Board, *Finance and Economics Discussion Series*, no 2023-059.

Monetary Authority of Singapore (MAS) and Bank for International Settlements (BIS) (2023): *Project Guardian: enabling open and interoperable networks*, June.

Pereira, A (2023): "Circle, Tether freezes over $65m in assets transferred from multichain", *Cointelegraph*, 8 July.

PYMNTS (2022): "Bored apes NFT rampage spikes transaction fees to $200m for 55,000 sales", 2 May.

Qin, K, L Zhou and A Gervais (2022): "Quantifying blockchain extractable value: How dark is the forest?" in *2022 IEEE Symposium on Security and Privacy*, May, pp 198-214.

US Department of the Treasury (2023): "Illicit Finance Risk Assessment of Decentralized Finance" April.

Yaga, D, P Mell, N Roby and K Scarfone (2018): "Blockchain technology overview", NIST IR 8202, October.

Annex 1: Reports from international bodies

This Annex provides a non-exhaustive outline of relevant reports from other international bodies. Views are first organised by topic and then by document.

Views by topic

In related work, international bodies have noted challenges that may have an impact on how features of particular activities performed on DLT observe certain risk management standards and principles. Although permissionless blockchains were not the specific focus of these reports,[22] the noted challenges could be relevant to activities performed on permissionless blockchains.

Governance

Activities performed on or related to permissionless blockchains may not have clear and direct lines of responsibility and accountability.

- *CPMI-IOSCO (2022)* "an [Stablecoin Arrangement]'s governance may be partially or fully decentralised and there may be no legal entities and persons in control of the FMI function. In particular, the transfer function can be set up as a smart contract on a permissionless public ledger. These smart contracts could specify the validation mechanisms on which transfer functions rely to effect settlement. For these SA models, governance of the transfer function may be performed solely by software (while human interaction with the smart contract may be part of the SA's coding) and there may be no identifiable legal entities or persons that assume responsibility and accountability for the transfer function".
- *FSB (2020)* "Fully permissionless ledgers or similar mechanisms could pose particular challenges to accountability and governance and authorities therefore need to ensure that appropriate regulatory, supervisory, and oversight requirements can be effectively applied to such arrangements."
- *FSB (2022a)* "The technology and distributed nature of DeFi poses a number of regulatory challenges and threats. DeFi platforms aim to provide a decentralised governance structure by issuing the governance tokens, making it challenging for public authorities and regulators to identify an entity or individual accountable for meeting regulatory obligations (eg if they maintain control of a DeFi application).

  In an extreme case, where a DeFi platform is completely decentralised, there may be no single person or entity that could be held responsible for the functioning of the protocol (even though this may not be the case in the current generation of decentralised governance arrangements). Instead, the DeFi developers' claims of no responsibility or disclaimers of liability would be that responsibility would lie with its entire (pseudonymous) user base. Furthermore, given DeFi's global nature, the applicable legal jurisdictions may not always be clear or well-defined."
- *FSB (2022b)* "Where crypto-asset activities are conducted in ways that may frustrate the identification of the responsible entity, such as through DeFi protocols or setting up other complex corporate structures, such conduct of activities must not undermine robust governance and accountability arrangements."

[22] For example, the CPMI-IOSCO work contemplates decentralisation across a range of activities, not specifically the use of blockchains.

- *IOSCO (2022)* "Recognising the existing risk of the potential for intermediary failures in traditional finance, unlike in traditional finance where, for example, information systems and processes are governed by an intermediary, in blockchain, this responsibility lies with validators, who typically are economically incentivised to participate in a non-malicious manner. If the incentive structure does not sufficiently motivate a validator to participate or does not deter malicious behaviour, the network could be compromised."

  "A set of unique risks arise relating to governance over DeFi protocols and smart contracts. Two primary areas where these risks arise is in the control of administrative keys and the functioning of protocol governance structures. If there is no disclosure of material information about these governance arrangements to potential investors, they are deprived of information that could have a substantial impact on the performance of the product or system."

Risk management

Comprehensively managing the risks of activities performed on or related to permissionless blockchains may be a challenge.

- *CPMI-IOSCO (2022)* Issues with comprehensive risk management could emerge if the arrangement relies "for their transfer function on other entities (such as other FMIs, settlement banks, liquidity providers, validating node operators and other node operators, or service providers) that could pose material risks to the function"…. "the entities that perform other SA functions may be independent from the entity performing the transfer function and/or may not qualify as either participants or service providers to the FMI. Yet, other SA functions and the entities that perform them can have risk implications (legal, credit, liquidity, business, operational, and other risks) on the transfer function, and vice versa. These factors may complicate the SA's task to comprehensively manage risks…"
- *FSB (2020)* "Risk management measures and technical standards should cover relevant activities performed by providers of activities in the GSC arrangements, paying particular attention to compliance by permissionless or anonymous networks."
- *FSB (2022a)* "The sector has already seen numerous operational and cybersecurity incidents, and failures of governance. DeFi related hacks made up over 75% of the $481 million known total hack and theft volume of cryptoassets through September 2021."
- *FSB (2023)* "the pseudonymous nature of information on public ledgers inhibits the ability to ascertain the types of investors in the crypto-asset ecosystem. While some transaction data at the wallet level are accessible, the lack of data about the identity of wallet owners makes the assessment of vulnerabilities much more challenging."
- *IOSCO (2022)* "Smart contracts are software that exist for the most part on public permissionless blockchains. While this open access can facilitate financial innovation, there are no technological restrictions on developers, including no required professional or licensing qualifications that govern who may deploy, manage, or engage with smart contracts. While participants do engage in efforts to test and vet code (eg through "bug bounty" programs), there are no formal code auditing requirements. Thus, anyone can develop, deploy and engage with new smart contracts that could subject DeFi participants to code vulnerabilities, fraud, theft and other significant risks. Many projects launch through copying another developer's code. While open sourcing of good code has certain advantages and efficiencies, the propagation of bad code can have adverse consequences. Further, since DeFi products and systems generally must be upgraded, there will be continuing risk of coding error.

  Smart contracts are what determine a crypto-assets' technological features and any vulnerability or bug in the smart contract code that controls or engages with a crypto-asset, if it

surfaces or is exploited, could adversely impact any crypto-asset issued, tracked or held by the smart contract, and could permanently impair the crypto-asset's function and value.

In addition to risks to assets and protocols impacted by smart contracts, there are additional vulnerabilities that arise due to the composability feature of many smart contracts. Smart contracts typically are designed to be composible, ie they may interact with other smart contracts in that they may essentially be "daisy chained" together to compose new products and systems. It is difficult to anticipate all potential issues that may arise through this daisy chaining.

Further, the ability to modify or upgrade a smart contract, once deployed, may be limited, unless and to the extent that the smart contracts was created with the ability to delete or alter the contract after creation. Thus, a smart contract can essentially operate in perpetuity on a blockchain, regardless of administrator or user behaviour. Some will exist even if administrators or users wish to disable them. For other smart contracts, administrators may have retained an "administrative key" allowing them to delete or alter the contract after creation."

"Perhaps due to the nascent and permissionless nature of DeFi, protocols and smart contracts have been susceptible to cybersecurity attack, and particularly hacking. As of the end of 2021, the total amount of money lost due to smart contract, software and crypto wallet hacking was reported at more than $10 billion, with more than $2 billion stolen in 2021 from DeFi alone, representing an increase in loss value of over 1300% from 2020. Hacks can result in the leak of sensitive information and the loss of funds, often with no recourse. An industry has started to form around smart contract "auditing," but standards and in some cases legal accountabilities are not yet established. DeFi projects regularly use bug bounties and appeals to open-source software principles (such as using template code and technical standards such as ERC-20) to further mitigate cybersecurity risk, but hacks remain common."

Legal basis

Inadequate, uncertain or opaque legal basis may exist for activities performed on permissionless blockchains.

- *CPMI-IOSCO (2022)* With probabilistic settlement (a common feature of public blockchains), a misalignment between the state of the ledger and what is considered legally final/settled may occur: "With probabilistic settlement, even if the relevant legal framework and the SA's rules and procedures have defined the point at which final settlement occurs, the possibility remains that the validation of a transaction on the ledger (technical settlement) can never be achieved with absolute certainty or forks emerge that could lead to a revocation of transactions validated on competing (and later discarded) forked ledger(s)." This situation "may be exacerbated in the absence of a legal entity responsible for the SA's transfer function…". "Without a responsible legal entity, there may be no way to enforce the legal finality of a transaction or the resulting legal claim if it conflicts with the settlement status on the ledger." "Moreover, settlement finality aims at ensuring protection against revocation in case of insolvency of one or more participant(s) or the settlement operator(s), ie ensuring that transactions of an insolvent entity settled with finality is honoured as final, and is not considered void or voidable by liquidators and relevant authorities. While a fork may not constitute a revocation in this sense, it may have similar adverse consequences for acquired positions of transferees as well as subsequent onwards transfers."
- *FSB (2022a)* "In an extreme case, where a DeFi platform is completely decentralised, there may be no single person or entity that could be held responsible for the functioning of the protocol (even though this may not be the case in the current generation of decentralised governance arrangements). Instead, the DeFi developers' claims of no responsibility or disclaimers of liability would be that responsibility would lie with its entire (pseudonymous) user base. Furthermore,

given DeFi's global nature, the applicable legal jurisdictions may not always be clear or well-defined."

- *FSB (2022b)* "Authorities should require crypto-asset service providers to have a well-founded, clear, transparent and enforceable legal basis for each material aspect of their activities in all relevant jurisdictions."

Regulation, supervision and oversight

Activities performed on permissionless blockchains may fall outside of, or be in non-compliance with, the existing regulatory perimeter.

- *FSB (2020)* "Authorities should have and utilise the necessary powers and tools, and adequate resources, to comprehensively regulate, supervise, and oversee a GSC arrangement and its associated functions and activities, and enforce relevant laws and regulations effectively" and "Authorities should apply comprehensive regulatory, supervisory and oversight requirements and relevant international standards to GSC arrangements on a functional basis and proportionately to their risks".
- *FSB (2022a)* "The technology and distributed nature of DeFi poses a number of regulatory challenges and threats. DeFi platforms aim to provide a decentralised governance structure by issuing the governance tokens, making it challenging for public authorities and regulators to identify an entity or individual accountable for meeting regulatory obligations (eg if they maintain control of a DeFi application)."
- *FSB (2022b)* "Authorities should have the powers and capabilities to enforce applicable regulatory, supervisory and oversight requirements, including authorisation and licensing requirements, the ability to undertake inspections or examinations, and, when crypto-asset issuers or service providers are not complying with applicable laws or regulations, to require corrective actions and take enforcement actions as appropriate, for example, by imposing restrictions on the access by domestic users to foreign crypto-asset activities and markets where they do not comply with applicable domestic regulations."

  "Regardless of whether crypto-asset activities are conducted in decentralised structures or other ways that frustrate the identification of a responsible entity or an issuer of the crypto-assets, authorities should adopt or have in place a regulatory approach that aims at adequate protection for all relevant parties, including consumers and investors, and aims at achieving the same regulatory outcome".
- *FSB (2023)* "the lack of reporting producing consistent and reliable data because parts of the crypto-asset ecosystem fall outside of, or are in non-compliance with, the regulatory perimeter at present. This means that crypto-asset market participants typically do not comply with common disclosure, recordkeeping and reporting rules covering entities in traditional finance, hampering data quality and comparability."

Views by document

Survey of relevant international reports — Table 2

CPMI-IOSCO (2022)	Pg 7: "Where an SA performs a transfer function and is determined by authorities to be systemically important, the SA as a whole would be expected to observe all relevant principles of the PFMI." Pg 8: "The guidance in this report does not create additional standards for SAs beyond those set out in the PFMI, but rather aims to provide increased clarity and granularity on how systemically important SAs should approach observing certain aspects of the PFMI."

	"A stablecoin arrangement that performs a transfer function should be considered an FMI for the purpose of applying the PFMI." Pg 9: "Although SAs are considered FMIs based on the functional approach, they may present some novel features as compared with other FMIs. The CPMI and IOSCO believe that guidance with respect to these features is useful for SAs and relevant authorities in applying the PFMI to systemically important SAs." The following summarises issues discussed in the guidance report that the current authors consider relevant to public permissionless blockchain. Since the guidance report only covers a subset of PFMI principles, it may not be a complete list of potential issues relevant to observing the PFMI. **Clear and direct lines of responsibility and accountability** Pg 13 Governance issue: "an [Stablecoin Arrangement]'s governance may be partially or fully decentralised and there may be no legal entities and persons in control of the FMI function. In particular, the transfer function can be set up as a smart contract on a permissionless public ledger. These smart contracts could specify the validation mechanisms on which transfer functions rely to effect settlement. For these SA models, governance of the transfer function may be performed solely by software (while human interaction with the smart contract may be part of the SA's coding) and there may be no identifiable legal entities or persons that assume responsibility and accountability for the transfer function". **Comprehensive risk-management frameworks** Pg 15 Issues with comprehensive risk management could emerge if the arrangement relies "for their transfer function on other entities (such as other FMIs, settlement banks, liquidity providers, validating node operators and other node operators, or service providers) that could pose material risks to the function"…. "the entities that perform other SA functions may be independent from the entity performing the transfer function and/or may not qualify as either participants or service providers to the FMI. Yet, other SA functions and the entities that perform them can have risk implications (legal, credit, liquidity, business, operational, and other risks) on the transfer function, and vice versa. These factors may complicate the SA's task to comprehensively manage risks…" **Clear and certain final settlement of transfers** Pg 16 Issues with probabilistic settlement (a common feature of public blockchains) where a misalignment between the state of the ledger and what is considered legally final/settled may occur. "With probabilistic settlement, even if the relevant legal framework and the SA's rules and procedures have defined the point at which final settlement occurs, the possibility remains that the validation of a transaction on the ledger (technical settlement) can never be achieved with absolute certainty or forks emerge that could lead to a revocation of transactions validated on competing (and later discarded) forked ledger(s)." This situation "may be exacerbated in the absence of a legal entity responsible for the SA's transfer function". "Without a responsible legal entity, there may be no way to enforce the legal finality of a transaction or the resulting legal claim if it conflicts with the settlement status on the ledger." "Moreover, settlement finality aims at ensuring protection against revocation in case of insolvency of one or more participant(s) or the settlement operator(s), ie ensuring that transactions of an insolvent entity settled with finality is honoured as final, and is not considered void or voidable by liquidators and relevant authorities. While a fork may not constitute a revocation in this sense, it may have similar adverse consequences for acquired positions of transferees as well as subsequent onwards transfers."
FSB (2020)	Sets out high-level recommendations for the regulation, supervision and oversight of "global stablecoin" (GSC) arrangements. Per the report, "Authorities should: 1. …have and utilise the necessary powers and tools, and adequate resources, to comprehensively regulate, supervise, and oversee a GSC arrangement and its associated functions and activities, and enforce relevant laws and regulations effectively. 2. …apply comprehensive regulatory, supervisory and oversight requirements and relevant international standards to GSC arrangements on a functional basis and proportionately to their risks. 3. …cooperate and coordinate with each other, both domestically and internationally, to foster efficient and effective communication and consultation in order to support each other in fulfilling their respective mandates and to ensure comprehensive regulation, supervision, and oversight of a GSC arrangement across borders and sectors. 4. …ensure that GSC arrangements have in place a comprehensive governance framework with a clear allocation of accountability for the functions and activities within the GSC arrangement."

	Pg 32: "Fully permissionless ledgers or similar mechanisms could pose particular challenges to accountability and governance and authorities therefore need to ensure that appropriate regulatory, supervisory, and oversight requirements can be effectively applied to such arrangements." 5. "Authorities should ensure that GSC arrangements have effective risk management frameworks in place especially with regard to reserve management, operational resilience, cyber security safeguards and AML/CFT measures, as well as "fit and proper" requirements." Pg 33: "Risk management measures and technical standards should cover relevant activities performed by providers of activities in the GSC arrangements, paying particular attention to compliance by permissionless or anonymous networks." 6. "Authorities should ensure that GSC arrangements have in place robust systems for collecting, storing and safeguarding data." 7. "Authorities should ensure that GSC arrangements have appropriate recovery and resolution plans." 8. "Authorities should ensure that GSC arrangements provide users and relevant stakeholders with comprehensive and transparent information necessary to understand the functioning of the GSC arrangement, including with respect to its stabilisation mechanism." 9. "Authorities should ensure that GSC arrangements provide legal clarity to users on the nature and enforceability of any redemption rights and the process for redemption, where applicable." 10. "Authorities should ensure that GSC arrangements meet all applicable regulatory, supervisory and oversight requirements of a particular jurisdiction before commencing any operations in that jurisdiction, and adapt to new regulatory requirements as necessary."
FSB (2022a)	Related to DeFi (which typically leverages public and permissionless blockchains): Pg 17: "The technology and distributed nature of DeFi poses a number of regulatory challenges and threats. DeFi platforms aim to provide a decentralised governance structure by issuing the governance tokens, making it challenging for public authorities and regulators to identify an entity or individual accountable for meeting regulatory obligations (eg if they maintain control of a DeFi application). In an extreme case, where a DeFi platform is completely decentralised, there may be no single person or entity that could be held responsible for the functioning of the protocol (even though this may not be the case in the current generation of decentralised governance arrangements). Instead, the DeFi developers' claims of no responsibility or disclaimers of liability would be that responsibility would lie with its entire (pseudonymous) user base. Furthermore, given DeFi's global nature, the applicable legal jurisdictions may not always be clear or well-defined." Pg 18 "The sector has already seen numerous operational and cybersecurity incidents, and failures of governance. DeFi related hacks made up over 75% of the $481 million known total hack and theft volume of cryptoassets through September 2021."
FSB (2022b)	The report highlights recommendations for effective regulatory and supervisory frameworks and takes an activities-based approach to address the interconnectedness of crypto-asset risks. In order to address the financial stability risks of crypto-asset activities, FSB recommends that "authorities should have the appropriate powers and tools, and adequate resources, to regulate, supervise, and oversee crypto-asset activities and markets, including crypto-asset issuers and service providers, as appropriate." (pg 1) *Recommendation 1 Regulatory powers and tools*: "Authorities should have the powers and capabilities to enforce applicable regulatory, supervisory and oversight requirements, including authorisation and licensing requirements, the ability to undertake inspections or examinations, and, when crypto-asset issuers or service providers are not complying with applicable laws or regulations, to require corrective actions and take enforcement actions as appropriate, for example, by imposing restrictions on the access by domestic users to foreign crypto-asset activities and markets where they do not comply with applicable domestic regulations. Authorities should require crypto-asset service providers to have a well-founded, clear, transparent and enforceable legal basis for each material aspect of their activities in all relevant jurisdictions." *Recommendation 2 General regulatory framework*: "Regardless of whether crypto-asset activities are conducted in decentralised structures or other ways that frustrate the identification of a responsible entity or an issuer of the crypto-assets, authorities should adopt or have in place a regulatory approach that aims at adequate protection for all relevant parties, including consumers and investors, and aims at achieving the same regulatory outcome." *Recommendation 3 Cross-border cooperation, coordination and information sharing*: "Authorities should

	cooperate and coordinate with each other, both domestically and internationally, to foster efficient and effective communication, information sharing and consultation in order to support each other as appropriate in fulfilling their respective mandates and to encourage consistency of regulatory and supervisory outcomes." *Recommendation 4 Governance:* "Authorities, as appropriate, should require that crypto-asset issuers and service providers have in place and disclose a comprehensive governance framework." "Where crypto-asset activities are conducted in ways that may frustrate the identification of the responsible entity, such as through DeFi protocols or setting up other complex corporate structures, such conduct of activities must not undermine robust governance and accountability arrangements." *Recommendation 5 Risk management:* "Authorities, as appropriate, should require crypto-asset service providers to have an effective risk management framework that comprehensively addresses all material risks associated with their activities." *Recommendation 6 Data collection, recording and reporting:* "Authorities, as appropriate, should require that crypto-asset issuers and service providers to have in place robust frameworks for collecting, storing, safeguarding, and the timely and accurate reporting of data, including relevant policies, procedures and infrastructures needed, in each case proportionate to their risk, size, complexity and systemic importance. Authorities should have access to the data as necessary and appropriate to fulfil their regulatory, supervisory and oversight mandates." *Recommendation 7 Disclosures*: "Authorities should require that crypto-asset issuers and service providers disclose to users and relevant stakeholders comprehensive, clear and transparent information regarding their operations, risk profiles and financial conditions, as well as the products they provide and activities they conduct." *Recommendation 8 Addressing financial stability risks arising from interconnections and interdependencies:* "Authorities should identify and monitor the relevant interconnections, both within the crypto-asset ecosystem, as well as between the crypto-asset ecosystem and the wider financial system. Authorities should address financial stability risks that arise from these interconnections and interdependencies." *Recommendation 9 Comprehensive regulation of crypto-asset service providers with multiple functions:* "Authorities should ensure that crypto-asset service providers that combine multiple functions and activities, for example crypto-asset trading platforms, are subject to appropriate regulation, supervision and oversight that comprehensively address the risks associated with individual functions and the risks arising from the combination of functions, including requirements regarding separation of certain functions and activities, as appropriate."
FSB (2023)	Pg 22: "…there is heavy concentration of activity on the Ethereum blockchain (about 60% of DeFi TVL). Hence, any disruptions from malicious activity or from infrastructure maintenance or upgrades affecting the Ethereum blockchain may impact the DeFi ecosystem as a whole." Pg 31: "…the difficulty in aggregating and analysing the vast amount of data available on distributed ledgers. Data available from public blockchains may be transparent and immutable in some respects, but they are generally difficult to collect and analyse." Pg 32: "…the pseudonymous nature of information on public ledgers inhibits the ability to ascertain the types of investors in the crypto-asset ecosystem. While some transaction data at the wallet level are accessible, the lack of data about the identity of wallet owners makes the assessment of vulnerabilities much more challenging." "…the lack of reporting producing consistent and reliable data because parts of the crypto-asset ecosystem fall outside of, or are in non-compliance with, the regulatory perimeter at present. This means that crypto-asset market participants typically do not comply with common disclosure, recordkeeping and reporting rules covering entities in traditional finance, hampering data quality and comparability."
IOSCO (2022)	Related to DeFi: Pg 39: "Recognising the existing risk of the potential for intermediary failures in traditional finance, unlike in traditional finance where, for example, information systems and processes are governed by an intermediary, in blockchain, this responsibility lies with validators, who typically are economically incentivised to participate in a non-malicious manner. If the incentive structure does not sufficiently motivate a validator to participate or does not deter malicious behavior, the network could be compromised. As DeFi is blockchain-based, any disruption or manipulation of a blockchain that underpins a particular DeFi product or service -- including any forks, attacks or nefarious activity -- likely will directly impact the operation of a DeFi product or service."

	Pg 39-40: "Smart contracts are software that exist for the most part on public permissionless blockchains. While this open access can facilitate financial innovation, there are no technological restrictions on developers, including no required professional or licensing qualifications that govern who may deploy, manage, or engage with smart contracts. While participants do engage in efforts to test and vet code (eg through "bug bounty" programs), there are no formal code auditing requirements. Thus, anyone can develop, deploy and engage with new smart contracts that could subject DeFi participants to code vulnerabilities, fraud, theft and other significant risks. Many projects launch through copying another developer's code. While open sourcing of good code has certain advantages and efficiencies, the propagation of bad code can have adverse consequences. Further, since DeFi products and systems generally must be upgraded, there will be continuing risk of coding error. Smart contracts are what determine a crypto-assets' technological features and any vulnerability or bug in the smart contract code that controls or engages with a crypto-asset, if it surfaces or is exploited, could adversely impact any crypto-asset issued, tracked or held by the smart contract, and could permanently impair the crypto-asset's function and value. In addition to risks to assets and protocols impacted by smart contracts, there are additional vulnerabilities that arise due to the composability feature of many smart contracts. Smart contracts typically are designed to be composible, ie they may interact with other smart contracts in that they may essentially be "daisy chained" together to compose new products and systems. It is difficult to anticipate all potential issues that may arise through this daisy chaining. Further, the ability to modify or upgrade a smart contract, once deployed, may be limited, unless and to the extent that the smart contracts was created with the ability to delete or alter the contract after creation. Thus, a smart contract can essentially operate in perpetuity on a blockchain, regardless of administrator or user behavior. Some will exist even if administrators or users wish to disable them. For other smart contracts, administrators may have retained an "administrative key" allowing them to delete or alter the contract after creation." Pg 40 "Perhaps due to the nascent and permissionless nature of DeFi, protocols and smart contracts have been susceptible to cybersecurity attack, and particularly hacking. As of the end of 2021, the total amount of money lost due to smart contract, software and crypto wallet hacking was reported at more than $10 billion, with more than $2 billion stolen in 2021 from DeFi alone, representing an increase in loss value of over 1300% from 2020. Hacks can result in the leak of sensitive information and the loss of funds, often with no recourse. An industry has started to form around smart contract "auditing," but standards and in some cases legal accountabilities are not yet established. DeFi projects regularly use bug bounties and appeals to open source software principles (such as using template code and technical standards such as ERC-20) to further mitigate cybersecurity risk, but hacks remain common." Pg 41 "A set of unique risks arise relating to governance over DeFi protocols and smart contracts. Two primary areas where these risks arise is in the control of administrative keys and the functioning of protocol governance structures. If there is no disclosure of material information about these governance arrangements to potential investors, they are deprived of information that could have a substantial impact on the performance of the product or system."

Annex 2: Permissionless/permissioned and public/private blockchains

This Annex offers a non-exhaustive survey of several definitions of permissionless/permissioned and public/private blockchains. It draws from several sources: ISO definitions, a MAS and BIS joint publication definition, a GFMA definition, a BCBS definition, and two NIST definitions.[23] Of those six sources, three define "public/private" as distinct from "permissionless/permissioned": the ISO, the MAS and BIS, and the GFMA. Thus, it is only under those definitions that the terms "private permissionless" or "public permissioned" are applicable.

The following subsections explore these three definitions, and the final subsection summarises and compares the ISO definition to the BCBS definition, and two NIST definitions.

ISO definitions summary

ISO 22739:2024 defines vocabulary for blockchain and distributed ledger technologies. This section summarises the relevant terminology for public/private, permissioned/permissionless blockchains.

The standard defines public vs private categories as applying to *entities that use services provided by a DLT system*, which we will call **users** as a shorthand.

The standard also defines *permissioned vs permissionless* categories in terms of both **users** (as defined above) as well as in terms of *entities that administer or operate the DLT system*, which we will call **administrators** as a shorthand.[24] The ISO standard does not clarify whether these **administrators** are validators only, or something like the full set of on-chain operators[25] plus those with the off-chain authority to update popular open-source codebases saved in places like github.[26] For our purposes, we consider a wider definition of **administrator** that includes off-chain administrative activities.

To summarise:

- Private and public DLTs:
  - Private: the DLT system is accessible for use only to a limited group of DLT users (3.75)
  - Public: the DLT system is accessible to the public for use (3.78)
- Permissioned and permissionless DLTs:
  - Permissioned: the DLT system requires permissions or authorisation to perform a particular activity or activities; this applies to both the DLT users and administrators (3.72, 3.71, note 1 on 3.75)

[23] The source papers can be found in the References, respectively, as: ISO (2024), MAS and BIS (2023), GFMA (2023), BCBS (2022), Yaga et al (2018) and Davidson (2023).

[24] See Note 1 for entry 3.75 in ISO 22739:2024: ISO (2024)

[25] An expanded set of on-chain operators could include, for example: searchers, block builders, relays, validators, and proposers, as described in Heimbach et al (2023) for adding blocks to the Ethereum blockchain.

[26] Thorough examination of the operation of an open-source code base may be a topic for further work. In particular, how this approach to governance functions under periods of stress. The Ethereum Foundation's official github repository for the go-language implementation of Ethereum can be found here: https://github.com/ethereum/go-ethereum. This code-base is open and anyone can copy the code by "forking" it. At the time of writing, there are 19,800 forks of this repository. Developers can then modify the forked code and either use their modified version, or request that their modifications are re-integrated into the official Ethereum codebase via a pull request. Some developers have administration rights to the official github repository and can accept or reject pull requests for the official codebase. The developers with administration rights could be considered something like off-chain administrators, different from on-chain operators such as validators.

– Permissionless: the DLT system does not require authorisation to perform any particular activity; this applies to both the DLT users and administrators (3.74, 3.73, note 1 on 3.75)

From these, one may form the following definitions:

1. Private permissioned DLT system:
    a. the DLT system is accessible for use only to a limited group of DLT users
    b. the DLT system requires permissions or authorisation to perform a particular activity or activities; this applies to both the DLT users and administrators
2. Private permissionless DLT system:
    a. the DLT system is accessible for use only to a limited group of DLT users
    b. the DLT system does not require authorisation to perform any particular activity; this applies to both the DLT users and administrators
3. Public permissioned DLT system:
    a. the DLT system is accessible to the public for use
    b. the DLT system requires permissions or authorisation to perform a particular activity or activities; this applies to both the DLT users and administrators
4. Public permissionless DLT system:
    a. the DLT system is accessible to the public for use
    b. the DLT system does not require authorisation to perform any particular activity; this applies to both the DLT users and administrators

At first pass there may appear to be contradictions in definitions (2) private permissionless and (3) public permissioned DLTs, and these could both benefit from further discussion.

As indicated by (2.a), the set of users, or *entities that use services provided by a DLT system*, is itself limited. However, for the select users who have access to this DLT, there are no further restrictions on the activities in which they can partake, and likewise there are no restrictions on the activities that the administrators may take. It is not clear that there exists a version of this DLT in practice, but if it existed it might look like a blockchain where anyone could provide validation services, but only a select set of users could actually use services provided by the chain.

The DLT described in (3) is the inverse: as indicated by (3.a), the set of users, or *entities that use services provided by a DLT system*, is the general public, while at the same time the system requires permissions to perform a particular activity or activities, and these restrictions apply to both users and administrators. This definition admits a lot of flexibility. It may be the case that this description can be applied, for example, to some proof-of-authority-based blockchain: while the general public may show up and use the chain, the validators may themselves require being granted authority to validate. Other designs which allow the general public to access the chain but restrict actions on the chain, or restrict actions of validators or administrators, may also fall into this category.

Table 3 places *access restrictions for users* in the rows, and *action restrictions for users and administrators* in the columns, and then fills in which type of the four combinations of blockchain fall into which category.

ISO DLT Categorisation

Table 3

Administrators and users Users	Actions not restricted	Actions restricted
Access not restricted	Public permissionless	Public permissioned
Access restricted	Private permissionless	Private permissioned

Sources: ISO (2024)

MAS and BIS summary

The relevant definitions can be found in section 5 of the report: MAS and BIS (2023). The section uses participation and control as two primary dimensions of definition, and defines them as follows:

- Participation: Public (open) vs Private (closed): "the level of participation that a platform allows rather than whether data is publicly visible to everyone."
  - Public (open): "public platforms, just like the public internet are open to participation by any entity. Any entity may join a public platform."
  - Private (closed): "closed to a selected group of members only and operate on an invite-only basis, where invitations are extended to participants for entry into these platforms."
- Control: Permissionless vs Permissioned
  - Permissionless: "all participants may view, edit and conduct activities, including deploying smart contracts on the platform."
  - Permissioned: "the governing body is tasked to decide and permit the type of activities that each participant can conduct. For instance, only designated service providers may be permitted to deploy smart contracts, while financial regulators may be allowed to view transactions within the platform, based on their authorisations."

The report contains the following table that summarises the public permissionless, private permissioned, and public permissioned categories.

Illustrative platform models

Table 4

	Model P1	**Model P2**	**Model P3**
Category	Public and permissionless	Private and permissioned	Public and permissioned
Access	Anyone may join	Requires approval from consortium members	Anyone may join (subject to identification and acceptance of terms)
Validators	Anonymous	Known entities	Known entities
Fees	Paid in native crypto tokens	Paid in fiat	Paid in fiat
Consensus algorithm	Probabilistic settlement	Deterministic settlement	Deterministic settlement
Governance	Decentralised Governance	Consortium Governance	Consortium Governance
Example	Ethereum	Partior	LACChain

Sources: MAS and BIS (2023)

A similar two-dimensional table for the MAS and BIS, using the two dimensions noted above, is as follows.

MAS and BIS Categorisation — Table 5

Control of activities User access	All participants may view, edit and conduct activities, including deploying smart contracts on the platform	Governing body…permit[s] the type of activities that each participant can conduct
Any entity may join	Public permissionless (P1)	Public permissioned (P3)
Closed to a selected group of members only; invite-only basis	Private permissionless (NA)	Private permissioned (P2)

Sources: MAS and BIS (2023)

Note that table 5 has been constructed such that the results (public permissionless, public permissioned, …) are in the same locations in the table here as in table 3 above, and then the categories are filled in for user access and control of activities. The mapping is not a perfect fit. Note that "private permissionless" is not explicitly named and described under this definition.

GFMA definitions of private-permissioned, public-permissioned and public-permissionless

The GFMA (2023) report categorises DLTs in the following summary table:

Comparison of defining characteristics across distributed ledger network archetypes — Table 6

Defining characteristics	**Private-permissioned**	**Public-permissioned**	**Public-permissionless**
Governance	Centralised	Centralised (for the relevant application)	Decentralised
Accessibility to users	Closed	Closed (for the relevant application)	Open
Control over privileges	Can be defined as required	Users authenticated for specific roles	All users can perform all roles
Identification requirements	All users known	All users known (for the relevant application)	Pseudonymous
User base	Very limited (by design)	Limited (for the relevant application)	Broad
Interoperability	Can be developed as required but lower ease of implementation	Can be designed as required (for the relevant application)	Higher interoperability given existing DLT-based ecosystem

Sources: GFMA (2023)

A similar exercise can be conducted as above, organising blockchains in terms of user access and control of activities. As above, this has been constructed such that the results (public permissionless, public permissioned, etc) are in the same locations as in tables 3 and 5, and then the categories are filled in for user access and control of activities. The first four rows of table 6 above are used to fill out the description of the categories. For the public-permissioned category, the parenthetical "for the relevant application" is taken to imply that there exist other applications for which, respectively, governance is decentralised,

accessibility is open, and identity may be pseudonymous. As above there is no discussion of private-permissionless blockchains.

GFMA Categorisation — Table 7

Control of activities User access	**Governance:** decentralised or centralised for some applications **Privileges:** all users perform all roles, or authenticated for specific roles **Identification:** pseudonymous, or all users known for some applications	**Governance:** centralised for some or all applications **Privileges:** authenticated for some or all roles **Identification:** all users known for some or all applications
Open, or closed for relevant activities	Public-permissionless	Public-permissioned
Closed	Private-permissionless (not discussed)	Private-permissioned

Sources: GFMA (2023)

BCBS, ISO and NIST definitions compared

This section draws definitions from each of the source documents of the BCBS (2022), ISO (2024), and NIST (2018, 2023) definitions, and compares them using the "user participation" and "administration" categories that are implied by the ISO definition. These categories are indicated in the first and second columns, respectively, and for each the definition is indicated to be "open" or "closed" to the general public. The definitions from the source and key points are described in the third column.

Workstream literature — Table 8

User participation	**Administration**	**Source and key points**
BCBS (2022): Prudential treatment of cryptoasset exposures		
Open	Open	"Cryptoassets may rely on a public ('permissionless') ledger, whereby the validation of transactions can be done by any participating agent, or distributed among several agents or intermediaries, which could be unknown to the users. On a permissionless ledger, there may be less control of technology."
Closed	Closed	"A private (**permissioned**) ledger restricts and pre-defines the scope of validators, with the validating entities known to the users. On a permissioned ledger there may be a small group of validators with greater control."
ISO (2024): Blockchain and distributed ledger technologies		
-	Closed	"DLT system (3.35) in which **permissions** are required (3.71)"
-	Open	"DLT system (3.35) that is **permissionless** (3.73)" "**Permissionless** (3.73) not requiring authorisation to perform any particular activity."
Closed	-	"3.75. **Private** DLT system (3.35) that is accessible for use only to a limited group of DLT users (3.36)"[27]
Open	-	"3.78. **Public** DLT system (3.35) which is accessible to the public for use"

[27] Note 1 to entry: Public and private categories apply to DLT users (3.36), and permissioned (3.71) and permissionless (3.73) categories apply to DLT users (3.36) and those entities (3.38) that administer or operate the DLT system (3.35)."

NIST: Yaga et al (2018): Blockchain technology overview		
Open	Open	"In a **permissionless** blockchain network anyone can read and write to the blockchain without authorisation. **Permissionless** blockchain networks are decentralised ledger platforms open to anyone publishing blocks, without needing permission from any authority. Anyone has the right to publish blocks, this results in the property that anyone can read the blockchain as well as issue transactions on the blockchain. **Permissionless** blockchain networks often utilise a multiparty agreement or 'consensus' system (see section 4) that requires users to expend or maintain resources when attempting to publish blocks." S. 1
Closed	Closed	"**Permissioned** blockchain networks limit participation to specific people or organisations and allow finer-grained controls. **Permissioned** blockchain networks are ones where users publishing blocks must be authorised by some authority (be it centralised or decentralised). Since only authorised users are maintaining the blockchain, it is possible to restrict read access and to restrict who can issue transactions. Permissioned blockchain networks may thus allow anyone to read the blockchain or they may restrict read access to authorised individuals. They also may allow anyone to submit transactions to be included in the blockchain or, again, they may restrict this access only to authorised individuals." S. 5f
NIST: Davidson (2023): State machine replication and consensus with byzantine adversaries		
Open	Open	**Permissionless** systems: "Permissionless systems differ from classical ones in four key ways, according to Pass and Shi [31]: (1) There is no access control mechanism that determines which nodes can join the system, and nodes can freely join or leave the system at any time. (2) Nodes are not aware of the other protocol participants a priori. In particular, communication is not over authenticated channels, so message senders are not authenticated. (3) The protocol itself may be unaware of how many nodes are participating in its execution. (4) The number of nodes involved in the system can grow or shrink over time." pp 13ff "In permissionless networks, the intention is to allow anyone to participate anonymously." pp 34
Closed	Closed	A **permissioned** system require a fixed set of identifiable participants known in advance. "In the permissioned model of consensus, there are replicas, which may be under the control of the adversary … the identity of the replicas are known to every participant. Communication between participants typically takes place over authenticated channels, in which case the existence of a public key infrastructure (PKI) is generally assumed. At a minimum, every replica needs to agree with every other replica about the set of public keys used in the system" "In any distributed system, processes are required to communicate over a network. In the majority of **permissioned** systems, **every node will have direct, point-to-point communication channels with every other node** (see section 8 for some examples of exceptions). **Permissionless** networks, on the other hand, have a **more complex design space**." pp 13ff, 245