INTERNATIONAL MONETARY FUND

Blockchain Consensus Mechanisms

A Primer for Supervisors (2025 Update)

Parma Bains

WP/25/186

2025
SEP

WORKING PAPER

 WP/25/186

IMF Working Paper
Monetary and Capital Markets

Blockchain Consensus Mechanisms: A Primer for Supervisors (2025 Update)

Prepared by Parma Bains

Authorized for distribution by Jay Surti
September 2025

ABSTRACT: Consensus mechanisms underpin the effective operation of blockchains by ensuring a single consistent and honest ledger. The design and implementation of these consensus mechanisms can improve or impede the ability of regulatory and supervisory authorities to achieve their objectives and mandates. This paper provides an update to the Fintech Note *Blockchain Consensus Mechanisms: A Primer for Supervisors (2022)* by reviewing the growth of existing consensus mechanisms, exploring new consensus mechanisms, and the development of layer 2 protocols. It is a non-technical and accessible note to provide supervisors a broad understanding of the technology within their remits.

RECOMMENDED CITATION: Bains, P. (2025). *Blockchain Consensus Mechanisms: A Primer for Supervisors (2025 Update)*. IMF Working Paper, Monetary and Capital Markets.

JEL Classification Numbers:	G18, G21, G23, G28, O16, O32, O33
Keywords:	Distributed ledger technology; dlt; blockchain; consensus; fintech; supervision; layer2; crypto; digital; bitcoin; ethereum; solana
Author's E-Mail Address:	pbains@imf.org

WORKING PAPERS

Blockchain Consensus Mechanisms

A Primer for Supervisors (2025 Update)

Prepared by Parma Bains[1]

[1] The author would like to thank Jay Surti and Nobu Sugimoto for their guidance and Marie-Bernadette Armand de Mendieta for editorial support. The author thanks Ashley Lannquist, Xavier Lavayssiere, Matthias Bauer-Lanngartner, and Philip Hochreiter for their early review and input. The author also thanks Gabriela Conde, Marco Reuter, and Nicholas Zhang for their comments.

Contents

Comparison of Consensus Mechanisms[2]

	Bitcoin	Ethereum	Solana
Consensus Mechanism	Proof-of-Work	Proof-of-Stake	Proof-of-Stake (transactions sequenced using Proof-of-History)
Settlement Finality	Probabilistic (Nakamoto Consensus)	Probabilistic (Nakamoto + BFT)	Probabilistic (BFT)
Layer 1 Transactions Per Second (TPS)	Circa 5 TPS (YTD)	Circa 15 TPS (YTD)	Circa 4000 TPS (YTD) (including validator votes)
Layer 1 Average Transaction Fee (USD)	$1 - $2.5 (YTD)	$0.3 - $6 (YTD)	$0.00025 (estimated)
Operational Resilience (estimated)	~ 99.99%+ lifetime uptime	~ 99.8%+ lifetime uptime (minor protocol-level incidents)	~ 99.6%+ lifetime uptime (frequent short historical outages)
Strengths and Opportunities	• Security • Consistency • Longevity • Largest circulating crypto token by market cap (Bitcoin)	• Security • Longevity and ecosystem maturity • Decentralized developer activity • Most stablecoins deployed • Token standard dominance	• Fast growing network with potential consumer facing applications • Popular network for defi protocols • Quick transaction throughput • Lower fees
Market Integrity Risks	• Mining pool concentration • Selfish mining	• Maximal extractable value • Liquid staking and rehypothecation (including leverage) • Large validator influence	• Relatively centralized validator list • Limited slashing penalties
Other Considerations	• Energy and computational costs • Settlement finality	• Potential locked liquidity and fragmentation across protocols and L2s • Settlement finality	• Some operational downtime • Less well established
Layer 2's explored in this note	• State Channels (Lightning Network)	• Optimistic Rollups • ZK Rollups	

[2] It is important to note that some of these measurements are not directly comparable given these networks may be used for different use cases. As Bitcoin evolves into being used more as an asset class than a peer-to-peer electronic cash network, TPS becomes less important. The data are also dynamic, the theoretical maximum TPS is larger in all networks than the average TPS between January and July 2025, likewise, fees can spike during periods of network congestion (although the use of layer 2's has resulted in reduced fees generally). Data has been generated from on-chain and commercial data providers.

Introduction

The growth of distributed ledger technology (DLT) based products and services has occurred in step with a rapid increase in the number and diversity of blockchain networks. DLT enables a single, sequenced, standardized, and cryptographically secured record of activity to be safely distributed to, and acted on by, a network of participants. More simply, we can say this technology is a way to transfer, store and process data in distributed systems, with the ability to establish and maintain technology-enabled trust between diverse users. This record, or data, can contain transactions, asset holdings, or even identities.

A blockchain is a type of DLT that has a specific set of features, organizing its data in a chain of blocks.[3] Each block contains data that are verified, validated, and then "chained" to the next block. Blockchains constitute a subset of DLT, and the Bitcoin blockchain is a specific form of a blockchain. Blockchains can be public or private, permissioned or permissionless. Public networks allow anyone to view this record of activity, and permissionless networks allow anyone to participate in creating a record of activity. Private networks restrict viewing, and permissioned networks restrict write access.[4] Permissionless networks use crypto tokens as a method to compensate validators, permissioned networks generally do not.

Consensus mechanisms underpin the effective operation of blockchains by ensuring a single, consistent and honest ledger. Their design and implementation can improve or impede the ability of financial sector authorities to achieve their objectives. As blockchain-based products grow in popularity in the financial services industry and are used by regulated financial firms, the ability of financial supervisors to identify where innovation may be beneficial, and where it might cause risks to organizational mandates becomes important. This is particularly so in areas such as operational resilience, governance and risk management, and transaction execution and settlement.

This paper provides an update on developments since the publication of the 2022 Fintech Note Blockchain Consensus Mechanisms: A Primer for Supervisors evaluating whether previously highlighted supervisory risks crystalized, and where new supervisory risks, particularly those related to market integrity, might arise.[5] Proof-of-Work (PoW) remains a popular consensus mechanism, but the transition of the Ethereum network to Proof-of-Stake (PoS) since the 2022 paper has led to a growth of PoS based networks. Newer blockchain networks like Solana, Cardano, and Polkadot have grown and so-called payment blockchains focused on stablecoins have been announced. More DLT-based activity has challenged whether blockchain networks are scalable for financial markets therefore scalability solutions have grown, with the introduction of Optimistic and ZK-rollups, and the growth of the Lightning Network.

This paper explores the main developments in blockchain consensus mechanisms since the last publication, as well as the growing use of so-called "layer two protocols", and their impact on supervisors. This paper, which focuses on consensus in public and permissionless networks, is targeted towards supervisors with little previous exposure to distributed ledgers.

[3] There are other types of DLT and distributed computing architectures such as Directed Acyclic Graphs and Holochain
[4] Hybrid networks can combine public and permissioned characteristics at the protocol, token, smart contract, or application level.
[5] Bains (2022).

Consensus Mechanisms

Generating consensus across distributed participants where trust is necessary, miscommunication is possible, and misaligned incentives are a barrier, is challenging. The Byzantine General's Problem (BGP) sets out these problems which are applicable to public blockchain networks where distributed participants (commonly referred to as nodes) need to agree on the common state of distributed ledgers.[6]

There are two broad frameworks for generating consensus in blockchains, both aim to be Byzantine Fault Tolerant (BFT).[7] First is the Nakamoto Consensus in which consensus occurs based on which chain of past transactions blocks is the longest, and second are traditional BFT models where a supermajority votes and agrees on the state of the network. Within these categories sit what are commonly known as consensus mechanisms. Bains (2022) provides background on blockchain infrastructure, private networks, and further information on PoW, PoS, Delegated PoS, and Proof-of-Elapsed-Time.

In this section we focus on consensus mechanisms that cover Nakamoto, BFT, and hybrid frameworks, underpinning three networks: Bitcoin, Ethereum, and Solana. The section first covers how each network generates consensus and then evaluates whether supervisory risks highlighted in Bains (2022) crystallized. These include market integrity risks (including market manipulation and market abuse), consumer protection (in the absence of digital literacy), and potential financial stability risk (if a network scales rapidly or increases connections with wider financial markets). In the second part of the section, emerging supervisory risks are considered, and where relevant, the steps being taken to manage them.

Nakamoto Consensus: PoW in the Bitcoin Network

The Nakamoto Consensus was developed by Satoshi Nakamoto, the pseudonymous creator of the Bitcoin network. It is now used across several blockchain networks. It solves the BGP through PoW and the longest chain rule which states that in the event of competing forks, the chain with the most computational work (in the form of confirmed number of blocks) is the valid chain.[8]

The Bitcoin network consists of distributed participants (called nodes) that have a copy of the Bitcoin blockchain which is a distributed ledger that records all transactions on the network. Conducting a transaction requires several steps. First the sender specifies what they want to send and where they want to send it, which is then converted into a standard byte format.[9] Each time a transaction is broadcast by the sender, it is run through a cryptographic hashing function twice to produce a unique transaction ID. The Bitcoin blockchain uses a cryptographic hashing function called SHA-256 which produces a fixed-length string of alphanumeric characters called a hash for any given input.

[6] It is based on a computer science and cryptography thought experiment that illustrates the challenges of reaching consensus in a system where some participants maybe malicious, unreliable, or dishonest see Lamport and others (1982).

[7] In the context of blockchains, BFT involves maintaining an accurate history of transactions as long as no more than one-third of the nodes are in technical failure or inaccurately voting on new transactions.

[8] Forking is the divergence of transaction history that results in two or more set of blocks on the end of the blockchain which a new block of transactions could cryptographically link. These can be temporary or a more permanent change in protocol rules.

[9] This is a way of representing complex data in a binary, standardized form that can be transmitted easily and securely.

The sender then signs the transaction using their private key as a way of showing control of the bitcoin which is then broadcast to the network.[10] Transactions contain several important metadata including transaction amount, transaction fee amount, input references (transaction ID, digital signature, sender's public key) and output scripts (where the bitcoin in the transaction will go). If a transaction is valid,[11] it enters a memory pool (commonly known as a mempool) which contains recent transactions broadcast to the network but currently unconfirmed on the blockchain. These transactions can be publicly viewed.

Here, network participants known as miners group the transactions together to form a set of validated transactions, called a block. Miners help maintain the network and keep it secure, expending energy costs in return for rewards in the form of transaction fees associated with each transaction and newly minted Bitcoins. There is a limit on how many transactions can be grouped into a block as each block has a capacity of 1MB (which can typically support 2000-4000 transactions) and so the incentive is that miners will pick the transactions with the largest transaction fees per byte first. Recently, a protocol update called Segregated Witness (SegWit) has grown in popularity. By separating some information contained in each bitcoin transaction (the digital signature) and storing it outside the main block structure, it allows for more information to be included in each block, which can potentially double the block capacity depending on the complexity of each transaction (although the base block size remains 1MB).[12]

When the transactions are grouped together, the PoW process begins. Each miner runs the SHA-256 mathematical function on the input data creating a fixed-length string of alphanumeric characters called a hash. The process of hashing produces a completely different output even if the input is changed by only one number or letter (yet the exact same input always produces the same hash output). The input data is the block header, and this includes a reference to the previous block, a timestamp, difficulty target, Merkle root[13], and a nonce.[14] The miner changes the nonce using trial-and-error (done automatically on a computer or, more commonly, specialist mining hardware) until it produces a valid hash – usually an output below a target that starts with a series of leading zeros. If successful, the miner will broadcast the hash (as a proof of work) to the network.

A subset of participants validate the output and if a majority of the network agrees, the miner is rewarded with newly minted bitcoin, as well as the transaction fees, although the reward is locked for 100 blocks to ensure settlement finality.[15] The reward mechanism and transaction fees incentivize miners to be active on the network. In particular, the payment of transaction fees ensure continued incentive provision during periods of network congestion and given the fact that block rewards halve every four years.

[10] For Bitcoin the Elliptic Curve Digital Signature Algorithm is run on specific parts of the hash of the transaction data to create a digital signature.

[11] Nodes confirm that the sender (i) has sufficient Bitcoin, (ii) the signature matches their private key, and (iii) the transaction format is correct.

[12] SegWit adoption has almost doubled since the last publication Segwit Adoption: % Of Transactions Using Segwit (Chart)

[13] The transaction IDs in the block are hashed together in pairs until only a single hash of all the transactions in a block remains called the Merkle root.

[14] Nonce derives from "**n**umber-used-only-**once**", an arbitrary number added to the block by the miners

[15] When a successful PoW is broadcast to the network (i.e., a miner claims to have solved the puzzle) a full validation is performed on the block where certain nodes will check the block header (the hash is correct, the size and structure of the block is correct, the block references the previous block) and then validate transactions within the block.

The difficulty of finding the hash (with the correct number of leading zeros) is automatically adjusted every 2016 blocks (roughly every 2 weeks) to ensure a block is successfully added to the blockchain roughly every 10 minutes. If there are a lot of miners on the network (and so greater computing power or hashrate) the valid hash becomes harder to find (a greater number of leading zeros), and if miners exit the network, then the valid hash becomes easier to generate (a smaller number of leading zeros).

PoW is most commonly associated with Bitcoin, but it is also used by several other networks that follow the same or a similar consensus mechanism with some differences. Litecoin, which is a fork of Bitcoin, was launched in 2011 to ensure faster block times. Dogecoin is a fork of Litecoin and was launched in 2013 as a meme token[16] to poke fun at the speculative behavior around crypto tokens which took it away from its original aspiration to become decentralized electronic cash. Both Litecoin and Dogecoin use a different cryptographic hashing algorithm (Scrypt, instead of SHA-256).

There were two main challenges with PoW explored in the previous note (Bains 2022) where new data are available. First was the possibility of the centralization of mining pools. This could lead to financial stability risks if the network is used at scale or interconnected to wider financial markets as control of the network could lead to manipulated transactions and disrupt settlement finality. Four mining pools (Foundry USA, AntPool, ViaBTC, and F2POOL) currently control roughly 75% of the hashrate of the Bitcoin network.[17] However, centralizing risks have not been pronounced in the Bitcoin network due to the diversity of miners that operate under each mining pool, although it's an area worth monitoring given the possible risks of selfish miner or 51% attacks, or delayed settlements risks.[18] Notably, a PoW network (Ethereum Classic) was subject to a 51% attack, but such attacks become costly with network size. Supervisors can use public information to identify concentration levels and conduct monitoring.[19]

Second, is the issue of how to attenuate significant energy consumption. While this challenge remains, the energy mix has evolved in the direction of renewables more recently, albeit continuation of this trend depends on where mining is cheapest. There are a growing number of public repositories that explore the energy consumption of PoW networks as well as the energy mix (fossil, renewables etc.).[20,21]

Hybrid BFT / Nakamoto: PoS in the Ethereum Network

Following the transition of the Ethereum network to PoS, such consensus mechanisms have grown in popularity and use. The Ethereum network uses a PoS mechanism that is a combination of the Nakamoto Consensus and more traditional BFT consensus where a supermajority votes and agrees on the state of a network for finality. While most associated with Ethereum, variants of PoS are also used in other networks like Cardano and Polkadot.

[16] A meme tokens are a type of crypto token inspired by cultural references that gains popularity through hype
[17] Bitcoin Mining Pool Data | Hashrate Index | HashrateIndex
[18] https://www.nber.org/system/files/working_papers/w25592/w25592.pdf
[19] Cost of a 51% Attack for Different Cryptocurrencies | Crypto51; Mining Pool Stats;
[20] Cambridge Blockchain Network Sustainability Index: Bitcoin GHG Emissions
[21] Digital Currencies and Energy Consumption

Transactions in PoS networks operate broadly similarly to PoW networks, but the way consensus is generated differs. Some PoS networks, like Cardano, use an unspent transaction output (UTXO) model[22] similar to Bitcoin, where transactions consume unspent outputs from previous transactions and create new outputs, allowing for parallel transaction verification. Others, like Ethereum, use an account-based model, where balances are updated directly, simplifying smart contract execution but making transaction validation more sequential.

In the Ethereum implementation of PoS (called Gasper), an algorithm randomly selects validators for block creation based on the value of crypto tokens that a token holder stakes and the length of time they have held a stake. The more native tokens that a validator stakes, the greater their chances of being selected. First a proposer is selected, then a block is proposed, and then validation of the proposed block occurs. Finality is reached if two-thirds of validators confirm the block which makes this BFT-like.

In Bains (2022), there were three risks explored for which there is now more data. First is the concept of a community where 'the rich get richer' given that they would be more able to stake larger amounts of crypto tokens, get chosen more often for block validation, and receive the block reward more frequently – generating risks to consumers and potentially to market integrity.[23] However, following the growth of PoS networks, further work has been done in this space. It is not clear whether wealth accumulation through staking occurs on PoS blockchains, although the potential for certain entities (like exchanges) to exert influence over networks remains. Some evidence suggests that while some PoS networks are dominated by large stakes, they do not lead to wealth accumulation[24] although the way PoS is implemented in different networks can impact outcomes. Some research suggests that the openness of validator sets can impact the how equitable rewards are, while the growth of Delegated PoS offers another alternative with a goal of increasing reward fairness.[25]

Second is the "nothing at stake" problem where validators that are not expending any energy or staking any crypto may be incentivized to vote on conflicting chains (forks) with no penalties which could generate risks to market integrity.[26] Since the publication, the concept of slashing – which had been used at a small scale for many years – is now widely used, including on the Ethereum network. Slashing refers to penalties enacted on validators that try to validate blocks on multiple chains, even if they know some of these blocks include invalid transactions. On the Ethereum network, these penalties are currently a loss of 1/32 of staked ether up to 1 ether, the suspension of the dishonest validator for 36 days incurring an additional penalty of approximately 0.07 ether, and a correlation penalty based on the total ether of all slashed validators in the previous 36 days.

Third is the possibility of staking leading to locked network liquidity which could impact investors looking to trade crypto tokens which, at scale, could reduce market responsiveness and be impactful during

[22] This refers to crypto tokens remaining after a transaction that can be used as input for future transactions.

[23] Bains (2022) discusses the development of "Delegated PoS" as a potential alternative to solve this particular problem.

[24] Coin concentration of Proof-of-Stake blockchains - ScienceDirect

[25] Reward Distribution in Proof-of-Stake Protocols: A Trade-Off Between Inclusion and Fairness | IEEE Journals & Magazine

[26] Conflicting chains (forks) can arise for many reasons and validators could vote on all these chains without additional cost as they have already been chosen for block validation. Without disincentives, this would present a rational option.

stressed events. In some networks, like Cardano, almost two-thirds of tokens are staked.[27] However, the growth of liquid staking in the interim is one method to potentially solve this problem. This refers to generating a tokenized representation of the staked asset (called liquid tokens) which can be freely used, although this creates new risks. Some estimates suggest that roughly a third of all staked ether is locked in liquid staking protocols,[28] although liquid tokens can be rehypothecated to create leveraged positions (explored later). Liquid staking protocols have often used a small number of professional validators which creates concentration of validators as well as liquid staking protocols.[29]

BFT Consensus: Proof-of-History (PoH) and Tower BFT in the Solana Network

PoH is a way of ordering transactions rather than a consensus mechanism used by networks like Solana. Network security and economic incentives are provided through PoS while consensus is generated through a variant of Practical BFT (PBFT) called Tower BFT (TBFT). In PoW and PoS, transactions are timestamped when a block is proposed and accepted by the network. Timestamping is important because it ensures there is no double spending and that transactions are valid. Validators check that this timestamp is greater than the previous block's timestamp but not in the future. This requires communication and waiting period between blocks, and this can slow the network down.

PoH solves this by creating an internal clock in the network so that timestamps are being continuously generated. It does so by using sequential hashes (based on SHA-256) that take a set amount of time to compute, and the output is an immutable pre-ordering of transactions that can be verified later. This means that the network doesn't have to wait for validators to determine which transactions comes first.

In PBFT consensus mechanisms, network participants come to agreement quickly through constant communication by sending multiple rounds of communication between market participants that results in a high communication overhead which might work in small private networks but is inefficient in broader public networks. TBFT aims to remedy this by leveraging PoH pre-ordered transactions to enable network participants to more quickly reach consensus without high communication overheads.

In Solana, validators stake their native tokens (SOL) just as they do on the Ethereum network with ether to participate in block production, but in the Solana network, these validators are known and the network is more centralized.[30] A validator schedule is also known in advance and this schedule is determined by the amount of SOL that they stake, changing over time as amounts staked change. During the turn of a validator (known as slots) the validator collects transactions and records them in the PoH sequence.

To achieve this, validators repeatedly create a hash using a modified SHA-256 in a sequential way. Each hash depends on the output of the previous hash which creates an irreversible chain that acts as a clock allowing network participants to know the order of transactions. Hashing occurs regularly and repeatedly

[27] Popular Crypto Projects and their Average Staking Rewards

[28] SoK: Liquid Staking Tokens (LSTs) and Emerging Trends in Restaking

[29] There is growing experimentation toward larger validator sets in protocols such as Rocket Pool and Tenderize.

[30] Known by their public key, but the pseudonymity a public key affords provides for privacy.

whether there are transactions or not which creates a verifiable passage of time, but ultimately blocks are placed within slots of these hashes.[31] A transaction can be inserted at any point in this sequence and the position of the transaction in the sequence acts as a cryptographic timestamp. As with the Bitcoin blockchain, anyone can verify that the sequence was run correctly by running the same function.

The state of the network is then voted on by a supermajority for finality allowing for consensus even in the presence of faulty or malicious participants which acts as BFT. Voting is time locked and as more votes accumulate over time it becomes increasingly difficult for validators to reverse past posts which increases the level of confidence in a particular chain. The chain with the most accumulated votes creates a "tower" of votes pushing it closer to economic and legal finality. The PoS element ensures validator participation while Tower BFT provides long-term finality which may be closer to economic and legal finality.[32]

Supervisory Considerations for Consensus Mechanisms

Understanding consensus mechanisms can guide supervisors to develop risk-based supervision where the technology might be meaningfully deployed at scale or generate unique risks, and where it might only be used for niche purposes or where outcomes might not challenge regulatory mandates. Blockchain technology presents the opportunity for data that are distributed, immutable, auditable, and transparent, depending on the network rules. While some networks have suffered outages and attacks, the largest ones have demonstrated impressive operational resilience with little to no downtime since their respective launches. These elements have the potential to generate new and interesting use cases in markets.

It has also become clearer that generating distributed consensus means some networks cannot support large scale financial services where volumes are high and values are low given scalability challenges.[33] Use cases and technology have, therefore, evolved. Some developers are sacrificing decentralization for scalability, which is commercially attractive but removes the technology from the goal of decentralized operation. It might also impact regulatory treatment in some markets. For example, one legislative proposal in the United States uses the term "mature blockchain" to reflect blockchain systems that are not subject to control by a person or group of persons under common control. Crypto tokens issued on these networks are proposed to be supervised by the Commodity Futures Trading Commission.[34]

Furthermore, the increasing complexity and interconnectedness of some networks could present future financial stability risks, particularly where links are strengthened with wider financial markets.[35] These potential risks have led to the Basel Committee on Banking Supervision (BCBS) categorizing crypto tokens, including stablecoins, deployed on public permissionless networks as riskier when compared to those on permissioned networks and subject to greater prudential requirements.

[31] Shinobi Systems' Solana Proof of Stake + Proof of History Primer

[32] Tower BFT: Solana's High Performance Implementation of PBFT | by Anatoly Yakovenko | Solana | Medium

[33] Some firms are developing more centralized so-called payment blockchains focused on stablecoins to remedy this.

[34] Text - H.R.3633 - 119th Congress (2025-2026): Digital Asset Market Clarity Act of 2025 | Congress.gov | Library of Congress

[35] New Evidence on Spillovers Between Crypto Assets and Financial Markets

Settlement finality is a challenge for supervisors. In wider financial markets, settlement finality creates trust in the financial system by delivering legal certainty to parties when transacting. However, settlement is probabilistic at the point of block validation in both PoW and PoS networks. Moreover, the time it takes for a transaction to be considered final differs across these networks. For example, settlement is often considered final by market participants after 6 block confirmations on PoW networks, but block times differ across PoW networks.[36] This means that settlement finality occurs after roughly 1 hour on the Bitcoin blockchain, about 15 minutes on Litecoin, and about 6 minutes on Dogecoin. However, the point where it is economically infeasible to reverse transactions is up to 100 block confirmations (the point at which a coinbase reward is paid). On PoS networks, settlement is considered technically final after 2 epochs, which is about 13 minutes on the Ethereum network, but technical finality could be as little as a second on Solana. Furthermore, there are challenges around technical and economic finality, and legal finality which considers factors beyond on-chain settlement.

Some financial sector authorities are looking to tackle the challenges of settlement generated by the use of different consensus mechanisms through policy sandboxes. Both the UK Digital Securities Sandbox and the EU DLT Pilot Regime have been developed to try and solve frictions that arise in capital markets when emerging technologies like blockchain are used and there is a specific focus on the challenges of settlement. It is still too early to determine their efficacy, but these are promising developments.

The issue of staking in PoS networks when delivered through a third-party (so called staking-as-a-service) could meet the definition of a security in some jurisdictions and therefore be subject to securities markets regulation. While some regulatory authorities have moved to provide clarity, in others it remains an open question.[37] Additionally, the growth of liquid staking has the potential to generate new supervisory risks around market integrity, which could evolve to broader financial stability risks if the market grows.

While a leveraged portfolio created by re-staking multiple times does not seem to generate enough profitable returns to meet the capital required in the current market environment, such returns may become attractive if and when interest rates are lower in the future. This can be exacerbated where the staked tokens are rehypothecated, which allows leverage to build up within the network.[38] Some studies indicate the estimated level of leverage of positions identified in the Ethereum network over the last few years to be under 4 times.[39] If such leveraged re-staking becomes popular during a period of market growth, any periods of market stress following this market expansion would require such leveraged positions to be unwound rapidly. Staking protocols, which are often concentrated, would face significant redemption pressure. Investors would be subject to additional margin pressures or liquidation of their collateral held by the lending platforms. This may create contagion pressures on other networks through protocols and platforms that operate across multiple networks.

[36] It is generally argued that this is the point where it is not feasible for a malicious actor to have enough computational power to manipulate the transactions unnoticed, i.e., re-calculate all six blocks faster than the rest of the network.

[37] For example, the UK and the US have provided exemptions for staking from existing securities regulations.

[38] For example, when Lido, the largest liquid staking protocol on Ethereum, faced large selling pressure for staked Ether following the collapse of FTX, the value dropped to 0.94 staked Ether per Ether resulting in losses for anyone wanting to quickly sell their staked tokens.

[39] See the performance analysis on leverage staking with liquid staking derivatives conducted by X. Xiong and others. They analyzed 442 positions of leveraged staking positions identified in Ethereum network for 963 days from Dec 2020 to Aug 2023.

An issue for PoW networks that could generate market integrity risks is selfish mining where dishonest miners hide the generation of new blocks. Rather than broadcasting the successful mining of a block, the miners keep this information private and secretly work on the next block while the rest of the network is working on an outdated chain. Once the dishonest chain is longer, they broadcast their newly mined blocks to the network, generate rewards, and force the rest of the network to move to this longer chain.[40] Likewise, on PoS networks validators can re-order transactions to generate profit, called Maximal Extractable Value.[41] This could include front-running, back-running, or sandwiching transactions to exploit profit, particularly where some transactions could be market moving. This behavior also happens in wider capital markets. For supervisors, it is important to understand and monitor such behaviors as they could undermine market fairness, distort price discovery, and impact consumer protection in areas like tokenized securities or if blockchain-based products become more integrated in wider financial markets.

Approaches such as embedded supervision have been proposed to tackle some on-chain supervisory challenges.[42] Although novel, it is unclear whether such approaches are necessary, proportionate, and cost effective at present. Emerging research suggests that a fragmented ecosystem, need for specialist and technical expertise, limited on-chain data, and the pseudonymity of wallets are significant challenges that would need to be addressed first. [43] Combining on-chain and off-chain data from several public and private repositories is increasingly being considered good practice.

Financial regulatory authorities take a technology neutral approach to the use of emerging technology in financial services. For blockchain this means that the focus is on the end product or service being offered rather than the underlying technology itself. It is important to note that while regulation might be technology neutral, supervisors should understand the unique benefits and risks of different technologies and focus their offsite monitoring and onsite inspections accordingly. Increasingly, the notion of tech neutrality is being challenged. BCBS distinguishes between crypto tokens deployed on permissioned and permissionless networks which can then influence prudential requirements. The United States is considering distinguishing between truly decentralized blockchain networks (so-called mature blockchain systems) and more centralized networks. Therefore, a proactive approach to understanding the opportunities and risks of emerging technology is sensible.

However, in line with global recommendations, regulators should not be moving toward trying to regulate or supervise blockchain networks themselves but firms providing services on these networks (banks, BigTech, crypto exchanges, custodians, etc.) Proposals like embedded supervision and regulators-as-a-node may be unnecessary unless decentralized networks grow sufficiently large, but the use of policy sandboxes could be promising to help develop regulation that allows innovation while ensuring consumers and markets are protected.[44]

[40] [1311.0243] Majority is not Enough: Bitcoin Mining is Vulnerable

[41] [1904.05234] Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges

[42] Embedded supervision: how to build regulation into blockchain finance

[43] Embedded supervision of decentralized finance - Publications Office of the EU

[44] Institutional Arrangements for Fintech Regulation: Supervisory Monitoring

Scalability Solutions

While blockchain-based distributed ledgers solve for the BGP, the scalability trilemma that arises has been a significant inhibitor to larger scale adoption. The trilemma refers to the tradeoffs of achieving security, decentralization, and scalability at the same time. For example, the Bitcoin blockchain is secure and decentralized but as volumes on the network increase, so do transaction costs while the number of pending transactions in the mempool increases. The Bitcoin blockchain can handle about 7 transactions per second, although the growing adoption of SegWit since publication allows for a potential doubling of this number. Conversely, permissioned blockchains (model dependent) can be quick, cheap, relatively secure, but are not always decentralized.

This trilemma has given rise to layer 2 and other scalability solutions (including layer 1 adjustments) which have become popular. The first layer is the main blockchain, while protocols are built on this layer allowing certain operations to be run off the main chain, with settlement occurring periodically on the main blockchain. There are various scalability solutions that are currently being used across blockchain networks, and many more that are being developed. In general, we can group the most popular scalability solutions into three main buckets: state channels, rollups, and side chains.

State channels

State channels are the oldest layer 2 solution that aim to remedy issues with scalability that arises from network congestion. They allow participants to conduct multiple transactions between themselves off-chain without recording each transaction on the blockchain and settling only the final “state” on-chain.

A state channel is opened when two participants (or more in the case of multi-party channels) lock up some of their crypto tokens in a multi signature smart contract. The locked crypto tokens are the balance available for making transactions off-chain between the participants. When opened, the participants send crypto tokens between themselves with the change in balance recorded within the state channel through digital signatures. Once all transactions are completed, the final balance is then settled on-chain with the crypto tokens locked in the smart contract being distributed to the participants based on that final balance.

While fees are lower than transacting multiple times on layer 1, they are not zero. Opening and closing the channel involves transactions on layer 1 and so require network fees. In some instances, there might be routing fees where a direct peer-to-peer connection between the sender and receiver doesn’t exist, and so payments go through intermediary participants. In this case, participants must ensure that intermediaries are online and have enough liquidity in their state channel to process the transaction. In practice, some state channels will find a route that has the lowest fees and highest liquidity,

The Lightning Network is the best-known state channel, launching to the public in 2018 on the Bitcoin blockchain. It operates as a payment channel allowing bitcoin transactions to happen off-chain before being settled on-chain once the payment channels are closed. While data are not readily available, some estimates suggest that as of late 2024, almost 15% of bitcoin payments are made using the Lightning

Network.[45] The Raiden Network is a state channel based layer 2 protocol that is available on the Ethereum network working along similar principles as the Lightning Network supporting ERC-20 tokens.

Rollups

While the Raiden Network provides a state channel based layer 2 option for the Ethereum network, rollups are the most popular layer 2 protocol on Ethereum. They work by bundling (or rolling up) multiple transactions into a single batch off-chain, before submitting only the proof of those transactions (a form of summary) to the layer 1 Ethereum network for settlement. There are two main types of rollups: optimistic rollups and zero-knowledge rollups.

Optimistic rollups work on the assumption that all transactions are valid unless proven otherwise. Like state channels, a smart contract locks the crypto tokens deposited by a user which allows the rollup account to be funded. Unlike state channels, there are no dedicated private channels, but rather transactions occur on the shared rollup chain. Participants transact on the layer 2 rollup with transactions sent to the rollup operator[46] and recorded in the rollup's internal state which ensures balances off-chain are updated. Operators bundle transactions into batches and compute a new state root which is a cryptographic hash representing the updated state of the rollup chain. The batch submission includes the new state root, a reference to the previous state root, and compressed transaction data.

Given that optimistic rollups assume transactions are valid, it is important that checks and balances are in place. Optimistic rollups allow for a challenge period which is a period of time when network participants can challenge the validity of the transactions in the batch. Where invalid transactions are noticed, network participants can submit a fraud proof to contest the rolled-up batch of transactions. In the course of the dispute resolution process the disputed transaction is re-executed on layer 1 to verify its validity – if it is not valid, the entire batch is rejected and the operator is penalized.[47] Following the end of the challenge period (which can be several days) the batch of transactions is finalized, and users can withdraw their funds if they wish. While this allows for the state of the network to be honest and valid, it can create long periods without settlement where users cannot withdraw their funds.[48]

Zero-knowledge rollups make use of zero-knowledge proofs to generate cryptographic proofs of validity off-chain before transactions are submitted back to layer 1.[49] Like optimistic rollups, participants first lock up their crypto tokens in a smart contract that allows for the rollup account to be funded, however with zero-knowledge rollups the operator generates a zero-knowledge proof to show that the deposit is valid. Participants can then begin to transact off-chain which impacts their off-chain balances and these transactions are bundled together into a batch. Rather than assuming that all transactions are valid, the operator generates a cryptographic zero-knowledge proof to prove that the transactions comply with the

[45] Year-over-Year Data Shows Rising Lightning Network Adoption | CoinGate

[46] Also known as a sequencer, an operator is a node that processes transactions, maintains the rollups state, and batches transactions.

[47] A fraud proof is evidence that a transaction in a batch is incorrect.

[48] An option is to use a liquidity provider that assumes ownership of the pending withdrawal in exchange for fees.

[49] For full discussion on privacy tech see Bains and Gaidosch (2025) Privacy Technologies & The Digital Economy

rollup's rules without revealing the full details of the transactions.[50] The zero-knowledge proof and the state root are then submitted to the layer 1 network and if the proof is valid, the batched transactions are accepted and recorded on the blockchain. Zero-knowledge proof validation means that there is no need for a challenge period and users can withdraw their funds almost immediately, although users must assume or verify that the zero-knowledge proof works soundly.

Optimistic rollups are currently the most popular rollup method as they have been available longer, are currently faster (in the absence of challenges), and are also easier to develop than zero-knowledge rollups. Between January 2022 and June 2024, total value locked and bridged between optimistic rollups and the Ethereum network was approximately $186bn, while for zero-knowledge rollups the figure was around $20bn.[51] Optimism was one of the first large scale rollup chains launching in 2021, and together with Base and Arbitrum are the most popular optimistic rollups on the Ethereum network.

Sidechains

Sidechains are independent blockchains that operate in parallel to a larger main chain with which they are interoperable using two-way pegs. They are not usually considered a traditional layer 2 and can grow to become fully fledged blockchain networks in their own right. Much like layer 2 protocols, they allow certain transactions or tasks to be moved away from the main chain which can reduce congestion on the main chain, but unlike other layer 2 protocols, transactions do not occur off-chain but rather on a parallel blockchain. Sidechains can be public or private, permissioned or permissionless and they operate using their own tokens, consensus mechanisms, as well as miners / validators distinct from the main chain.

To use sidechains, crypto tokens are first locked on the main chain in a smart contract (a bridge) which is verified and validated by the consensus mechanism of the main chain. Corresponding versions of the tokens are then issued on the side chain known as wrapped tokens (for example wBTC, wETH, etc.) These tokens can then be transacted with other wrapped tokens or network native tokens on the side chain. When the user wants to withdraw funds from the sidechain back to the main chain, the wrapped tokens are burned on the side chain, and the remaining balance is unlocked and settled in the main chain. Depending on the type of side chain, fees are lower than transactions on the main chain but not zero as fees are still needed to cash out of the sidechain and support transactions within the side chain.

The concept of sidechains is an old one (in crypto terms) with the first proposal shared in 2014 to improve scalability and utility.[52] Bitcoin has its own sidechains such as Rootstock which allows a 30-second transaction confirmation time and also has the functionality to integrate smart contracts that are compatible with the Ethereum network. One of the most popular side chains is the Polygon PoS sidechain that supports transactions on the Ethereum network. Polygon PoS has its own token (POL), its own set of validators, and produces and settles blocks on two different layers to increase transaction throughput.

[50] This occurs through a computational circuit that describes the rules of the system (transfer of tokens, balance updates etc.) The operator generates a zero-knowledge proof (SNARK or STARKs are most popular) which proves the batched transactions meet the rules of the system.

[51] Zero Knowledge Rollups & Optimistic Rollups: An Overview

[52] sidechains.pdf

The growing popularity of sidechains has also seen a growth in the volume and value of cyber-attacks that target the bridging protocol between main chains and sidechains. The Ronin Bridge which connected a blockchain-based video game publisher's sidechain to the Ethereum network, was hacked in March 2022 resulting in the loss of over $600mn worth of crypto tokens.

Supervisory Considerations of Scalability Solutions

As public permissionless networks grow in size and run into scalability issues, the popularity of scalability solutions has increased. For example, Deutsche Bank is building a permissioned zero-knowledge rollup on the Ethereum network to address challenges faced by banks when using public blockchains as part of the broader Project Guardian.[53] Supervisors need to understand approaches that networks might take to improve scalability, through layer 2 protocols, sidechains, and layer 1 adjustments like sharding.[54] Scalability solutions improve speed and scalability, and many also reduce the cost of transactions. This may make public permissionless blockchains more viable for real world financial services applications.

However, scalability solutions also add an additional layer of complexity on top of blockchain networks. Rather than dealing with just the architecture of the blockchain network, supervisors need to understand the additional steps of conducting transactions through these protocols. In many implementations, these protocols do not benefit from the inherent security of the large blockchain networks like Bitcoin and Ethereum. In some scalability solutions such as sidechains, users are dealing with a completely different set of network participants and potentially completely different ways of generating consensus. This may generate risks to operational resilience and cyber security.

As more regulated financial institutions interact with blockchain-based infrastructure and deploy products or services on these networks, there is a risk they might get caught on less efficient networks, or networks with less users. In a worst-case scenario, a diminishing network might create cybersecurity risks such as the increased likelihood of 51% attacks. A more immediate problem might be having products or services stuck on a network that is no longer popular amongst users or developers if the network is used for tokenizing securities. Relatedly, if a firm or a product is listed across multiple networks or shifts from one to another, liquidity might become shallower as it is split between many networks.

Security risks might also be a factor in some scalability solutions. In the case of sidechains, the use of smart contract bridges provides a central point of failure, and this vulnerability has been a consistent target for cyberattacks. Additionally, the potential centralizing features of some layer 2 protocols might create more opportunities for cyber-attacks.

Finally, market integrity risks may be amplified in certain layer 2 protocols, particularly given the centralizing role of operators in rollups who could front-run user transactions or use information asymmetries (given they can see the full order flow) to their advantage and extract rents.

[53] Project Guardian

[54] This is where the main chain is divided into smaller parts (shards) which has its own nodes, transactions, smart contracts etc.

Conclusion

The growth of blockchain-based products and services, both in crypto and wider financial markets, requires supervisors to take a more active role in understanding blockchain networks. Complex products, growing interlinkages, and the entrance of firms with novel business models are likely to challenge the ability of supervisors to identify where innovation may be beneficial, and where it might cause risks to consumer protection, market integrity, and financial stability.

It is imperative that supervisors understand the key components and tradeoffs of blockchain networks. Only then can they ensure that market participants have effective risk management frameworks in place and financial authorities more broadly have confidence that they can develop robust regulatory frameworks and conduct effective supervision.

Understanding how blockchain networks generate consensus is an important requirement to improving knowledge of the products and services delivered on this technology. Since the last publication, some risks have remained, others have not been realized, while new risks have also emerged. It is the job of a supervisor to continue effective horizon scanning, reflect on emerging risks, and ensure an environment is created that allows innovation to occur but where consumers and markets are protected.

To understand the impact of consensus mechanisms, several supervisory approaches have been proposed to improve horizon scanning capabilities. Embedded supervision experiments are growing but its feasibility is currently unclear and may not be appropriate for most supervisors unless the market grows considerably. Some regulatory authorities have used regulatory (product testing) sandboxes to improve knowledge which has fed into the development of domestic guidance and rules, but generally such tests have provided mixed outcomes.

More recently, the development of policy sandboxes that aim to support new regulation tailored for DLT (rather than testing against existing rules) has shown promise and could provide solutions around settlement finality and recording ownership of products and services deployed on blockchain-based infrastructure. Using a combination of on-chain and off-chain data provided by commercial and public bodies (including regulatory reporting) is considered good practice to improve risk monitoring.

The growth of layer 2 protocols generates new supervisory complexities and may alter the balance of some of the benefits provided by large public networks like transparency and auditability while making the technology more commercially viable and scalable. Supervisors should be aware of the various tradeoffs of layer 2s to understand their potential market impact while also allowing for the development.

It is not clear whether DLT is the future of financial services or whether it will remain a technology that supports some functions rather than replacing the financial plumbing as we know. As supervisors, it is important to actively monitor developments, but to let the private sector drive that development. However, to avoid a repeat of the Global Financial Crisis, supervisors must have a broad understanding of the technology which can then better allow supervisors to analyze the products, services, and firms operating on this technology and take the appropriate steps to protect markets and consumers.

References

Agur, I., and others (2022) Digital currencies and energy consumption. International Monetary Fund. Available at: https://www.imf.org/en/Publications/fintech-notes/Issues/2022/06/07/Digital-Currencies-and-Energy-Consumption-517866

Auer, R. (2019), Embedded supervision: how to build regulation into blockchain finance. available at: https://ssrn.com/abstract=3463885

Bains, P. (2022) Blockchain consensus mechanisms. International Monetary Fund. Available at: https://www.imf.org/en/Publications/fintech-notes/Issues/2022/01/25/Blockchain-Consensus-Mechanisms-511769

Bains, P., and Gaidosch, T. (2025) Privacy technologies and the digital economy. Available at: https://www.imf.org/en/Publications/WP/Issues/2025/03/28/Privacy-Technologies-The-Digital-Economy-565415

Bains, P., and Wu, C. (2023) Institutional arrangements for fintech regulation: supervisory monitoring. International Monetary Fund. Available at: https://www.imf.org/en/Publications/fintech-notes/Issues/2023/06/23/Institutional-Arrangements-for-Fintech-Regulation-Supervisory-Monitoring-534291

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J. and Wuille, P. (2014) Enabling blockchain innovations with pegged sidechains. Blockstream. Available at: https://blockstream.com/sidechains.pdf

Buterin, V. (2014) Ethereum: A next generation smart contract and decentralized platform. Available at: Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.

Chainalysis (2023) 'Zero-knowledge rollups vs. optimistic rollups: An overview'. Available at: https://www.chainalysis.com/blog/zero-knowledge-rollups-optimistic-rollups-overview/#zk-rollups-defined

Cong, L., He, Z., and Li, J. (2019) Decentralized mining in centralized pools. Available at: https://www.nber.org/system/files/working_papers/w25592/w25592.pdf

Daian, P. and others (2019). Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. Available at: https://arxiv.org/abs/1904.05234

Ethereum Foundation (n.d.) 'Optimistic rollups'. Available at: https://ethereum.org/en/developers/docs/scaling/optimistic-rollups/#data-availability

Ethereum Foundation (n.d.) 'ZK-rollups'. Available at: https://ethereum.org/en/developers/docs/scaling/zk-rollups/

European Commission (2024) Proposal for a regulation of the European Parliament and of the Council on a framework for financial data access. Available at: https://op.europa.eu/en/publication-detail/-/publication/772103b9-e829-11ef-b5e9-01aa75ed71a1/language-en

Eyal, I., and Sirer, E (2013). Majority is not enough: Bitcoin mining is vulnerable. Available at: https://arxiv.org/abs/1311.0243

Gudgeon, L., Moreno-Sanchez, P., Roos, S. and Grossklags, J. (2023) 'Economic and environmental analysis of blockchain energy consumption', Finance Research Letters, 58, p. 104065. Available at: https://www.sciencedirect.com/science/article/pii/S0165176523002446

Irresberger, F. and Yang, R. (2023) 'Coin concentration of proof-of-work blockchains', Finance Research Letters, 58, p. 104065. Available at: https://www.sciencedirect.com/science/article/pii/S0165176523002446

Iyer, R, and Popescu, A. (2023). New Evidence on Spillovers Between Crypto Assets and Financial Markets. Available at: https://www.imf.org/en/Publications/WP/Issues/2023/09/30/New-Evidence-on-Spillovers-Between-Crypto-Assets-and-Financial-Markets-539476

Lamport, L., Shostak, R, and Pease, M. (1982). The Byzantine Generals Problem. SRI International. Available at https://lamport.azurewebsites.net/pubs/byz.pdf

Li, S.-N., Spychiger, F. and Tessone, C.J. (2023) 'Reward distribution in proof-of-stake protocols: A trade-off between inclusion and fairness', IEEE Access, 11, pp. 134136–134145. Available at: https://ieeexplore.ieee.org/document/10328590

Nakamoto, S. (2008) A peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf

Shinobi Systems (n.d.) Solana Proof of Stake + Proof of History Primer. Available at: https://www.shinobi-systems.com/primer.html

Tortola and others (2024) Tethering Layer 2 solutions to the blockchains: a survey on proving schemes. Available at Tethering Layer 2 solutions to the blockchain: A survey on proving schemes - ScienceDirect

U.S. House of Representatives. (2025). Digital Asset Market Clarity Act of 2025, H.R. 3633, 119th Cong. Available at Text - H.R.3633 - 119th Congress (2025-2026): Digital Asset Market Clarity Act of 2025 | Congress.gov | Library of Congress

X. Xiong, Z. Wang, X. Chen, W. Knottenbelt, and M. Huth, "Leverage staking with liquid staking derivatives (lsds): Opportunities and risks," Imperial College London and University of Sussex, 2024, Leverage Staking with Liquid Staking Derivatives (LSDs): Opportunities and Risks

Yakovenko, A. (2017) Solana: A new architecture for a high performance blockchain. Available at Solana: A new architecture for a high performance blockchain

Yakovenko, A. (2018) 'Proof of history: A clock for blockchain', Solana Labs Medium Blog. Available at: https://medium.com/solana-labs/proof-of-history-a-clock-for-blockchain-cf47a61a9274

PUBLICATIONS