I. EXECUTIVE SUMMARY[1]

The increasing use of distributed ledger technology (DLT) in financial services has the potential to generate benefits for many stakeholders but can also pose unique risks. DLT, including blockchains, is used in payments, issuing debt and equity, trade finance, and post-trade processes. Large-scale use of DLT in financial services is currently limited, but use cases are increasing in some jurisdictions.

DLT has the potential to disintermediate markets, reduce costs, increase speed and efficiency, and create secure records of transparent, immutable, and auditable data and activity. DLT can offer greater democratization of data as the data are distributed and control of the data is decentralized. It can improve the provision of financial products and services (including financial inclusion), supply chain management, and record keeping. For supervisors, DLT can provide real-time control and supervision of financial markets; however, some designs can create risks to the natural environment, consumers, market integrity, financial integrity, and financial stability.

Consensus mechanisms underpin the effective operation of blockchains and ensure a single, consistent, and honest ledger. Consensus mechanisms in DLT systems guarantee that a state, value, or piece of information is correct and agreed on by most nodes. Some consensus mechanisms are designed to work best in public networks, while others perform better in private networks. Different consensus mechanisms can also deliver different outcomes, which may require different regulatory considerations. For example, some consensus mechanisms might prioritize speed and efficiency, while others might prioritize security. Quicker methods of forming consensus might be suited for payments, while more secure types of consensus mechanisms might be helpful in areas such as supply chain management.

Within financial services, Proof-of-Work (PoW), Proof-of-Stake (PoS), and Delegated PoS (DPoS) are some of the more popular consensus mechanisms in public blockchains, while practical Byzantine Fault Tolerance (pBFT), Istanbul BFT (iBFT), and federated BFT (fBFT) are popular in private blockchains. Separately, large technology entities (known as BigTechs) have also created consensus mechanisms that have the potential to be used in products and services that could become systemic quickly—for example, DiemBFT.

Supporting the Bitcoin Blockchain, PoW is the most popular consensus mechanism, but it suffers from significant drawbacks. PoW is a secure and resilient method of forming consensus, but it consumes significant energy and can be slow and expensive during times of high network traffic. Although innovations such as the Lightning Network,[2] side chains,[3] and other consensus mechanisms like PoS aim to solve some of PoW's problems, other issues such as probabilistic settlement can create friction with existing regulatory frameworks. pBFT, iBFT, fBFT, and DiemBFT offer immediate settlement; however, they raise new regulatory concerns about areas such as competition, and they run counter to the core "ideals" of decentralized networks.

To ensure they can embrace the promise of fintech while mitigating against any risks, authorities should consider the pros and cons of different consensus mechanisms. The Bali Fintech Agenda (BFA) is a framework that aims to guide authorities in harnessing the benefits of new technologies in financial services, while mitigating any risks, and encourages competition, consumer protection, financial integrity, and financial stability. It can be used as a way to understand the types of characteristics that consensus mechanisms may need if they are to serve the regulated financial sector effectively and compliantly.

[1] This note was prepared by Parma Bains with input from Fabiana Melo (MCM).

[2] The Lightning Network is a second-layer protocol that connects users through off-chain channels. These channels allow connected users to complete multiple transactions off chain, before the transactions are closed out and settled on chain, which makes for faster processing and lower costs—at the expense of reduced transparency and security.

[3] These parallel chains connect to the main blockchain via a two-way peg can store the actual data of transaction, leaving main chains to store just proof of correctness.

Authorities should also consider whether a technology neutral approach can continue delivering mandates when diverse new technologies deliver different outcomes and may consider a more proactive approach to supporting or restricting certain technologies. Authorities should also consider upskilling supervisors to better supervise new technologies. International organizations have a role to play in sharing regulatory best practice, particularly in jurisdictions where there might be a skills gap. Finally, approaches such as TechSprints and regulatory sandboxes, as well as deeper public-private collaboration via formal reviews, can enable authorities to understand the relative strengths and weaknesses of different consensus mechanisms, allowing firms operating in financial services to leverage the benefits of DLT while ensuring that risks are appropriately mitigated.

II. INTRODUCTION[4]

Technology plays an increasingly important role in financial services. With the pace of technological innovation moving ever faster, the role new technology plays in the provision of financial services is becoming increasingly fundamental. New technology can generate efficiencies for firms, lowering costs that can be passed on to end users. It can increase access to financial services and products for consumers, particularly the most vulnerable; however, new technology can also create new risks and unintended consequences that can harm financial stability, consumer protection, and market integrity.

Regulatory authorities' general approach to financial innovation is one of technology neutrality—which is not the same as technology agnosticism, as not all technologies are equal. Authorities are open to the use of new technologies even as they seek to understand and mitigate any unique risks that these technologies might bring. Although regulatory authorities may be technology neutral (the concept of "same business, same activity, same risk"), they might shift to become technology agnostic (as different technologies might generate different risks).[5] Where new technology creates unacceptable risks that could interfere in achieving the mandates and objectives of regulatory authorities, those organizations should take the necessary action to protect financial stability, market integrity, and consumers.

Different types of DLT, like blockchains, can create new opportunities but also bring unique risks and challenges for regulatory authorities, markets, and consumers. (See Box 1.) Their potential for increasing efficiency and resilience in financial markets has been explored and demonstrated across different products and services; however, they can pose risks to consumer protection, market integrity, and financial integrity. When used at scale or in critical infrastructure that is not substitutable, they can also give rise to financial stability risks.

Consensus mechanisms underpin the effective operation of blockchains by ensuring a single consistent and honest ledger—that is, a truthful representation of the transfer of data. DLT relies on rules hardwired into its source codes to operate, and an important rule is determining how nodes on a blockchain can come to agreements on the state of the network. Consensus mechanisms in DLT systems are responsible for ensuring that a state, value, or piece of information is correct and agreed on by most nodes. The design, creation, and implementation of these consensus mechanisms can impede regulatory authorities' ability to achieve objectives and mandates. These mechanisms can, in some instances, inhibit effective competition, create risks to market integrity and consumers, affect the ability of countries to move to a low-carbon economy, and, in larger deployments, potentially affect financial stability.

Aligned with the BFA, this note provides guidance on different types of consensus mechanisms and their regulatory and supervisory implications. The BFA[6] is a framework composed of 12 policy elements designed to help authorities harness the benefits of fintech and mitigate the regulatory risks associated with new technologies and business models. This note uses the BFA as a guide to help authorities understand the types of consensus mechanisms that could usefully be deployed within financial services; it considers the policy and regulatory implications of each approach, without going into substantial technical detail. It follows up on previous advice by the IMF, specifically about BFA developments, regulation of crypto assets, digital money,

[4] Any reference to existing crypto assets, distributed networks, and companies in this paper uses publicly available information and does not mean to endorse or analyze specific features of crypto assets, distributed networks or arrangements.

[5] *Technology neutral* denotes an unbiased approach to the use of technology in financial services based on input and outcome; *technology agnostic* refers to an unbiased approach to technology, but one where policies are informed by specific risks generated by the outcomes the technology produces. As technologies become more deeply ingrained in financial services, regulatory authorities may not remain neutral and instead become agnostic to the types of technologies used, taking positions of support or concern depending on the risks and benefits of such technologies.

[6] IMF and World Bank (2018). Although the BFA includes many elements, this note will focus only on the consensus-mechanism aspects of the digital architecture.

and anti–money laundering/counter terrorist financing (AML/CFT) aspects of crypto assets (Cuervo, Morozova, and Sugimoto 2020; IMF 2021a, 2021b; IMF and World Bank 2019; Schwarz and others 2021a, 2021b).

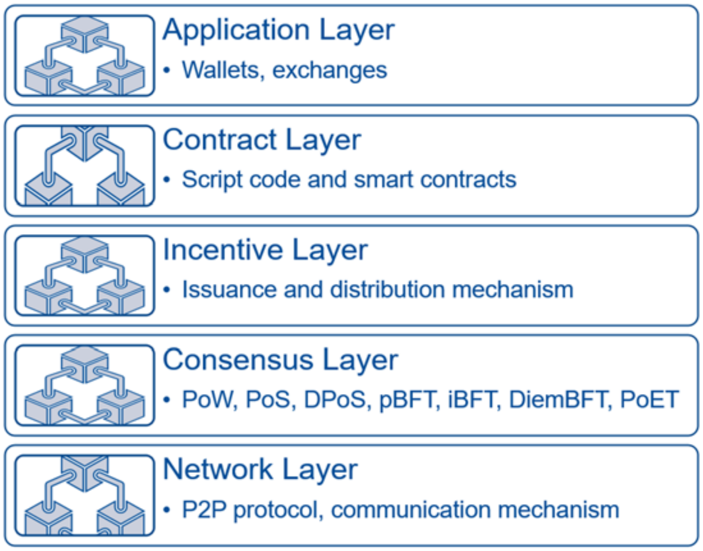
This primer is designed for financial supervisors at central banks, regulatory authorities, and government departments. It adds to existing literature by summarizing key aspects of popular consensus mechanisms at a high level, with a specific focus on how such mechanisms may impact the mandates of supervisors and policymakers when deployed in financial services markets. It could also help inform IMF staff on policy development and technical assistance related to crypto assets, stablecoins, and blockchains.

BOX 1. Definitions

- **Distributed Ledger Technology (DLT):** A set of technological solutions that enables a single, sequenced, standardized, and cryptographically secured record of activity to be safely distributed to, and acted upon by, a network of varied participants. This record can contain transactions, asset holdings, or identity data. Through nodes, DLT is used to maintain and share digital records instantaneously across a network of participants.
- **Blockchain:** DLT in its blockchain form was first used in Bitcoin to facilitate peer-to-peer payments without a central third party. Blockchain is a type of DLT that has a specific set of features, organizing its data in a chain of blocks. Each block contains data that are verified, validated, and then "chained" to the next block. Blockchain is a subset of DLT, and the Bitcoin Blockchain is a specific form of a blockchain.
- **Consensus mechanisms:** Consensus in distributed systems is ensuring that a state, value, or piece of information is correct and agreed on by most nodes. A consensus mechanism guarantees this effort is carried out fairly and independently of any interested party, or in the case of private permissioned networks, to achieve other objectives desired by the network (such as centralized control).
- **51 percent attack:** An attack in which malicious actors gain control over 51 percent of nodes in a network
- **Bali Fintech Agenda:** A framework developed jointly with the World Bank to help authorities balance the benefits and risks of new technologies in financial services
- **Hashrate:** The speed of mining measured as the computational power per second used
- **Mining pool:** The pooling of resources by miners, who share their processing power over a network, to split the rewards
- **Nodes:** A DLT connection and communication point that can create, receive, send, and act on information
- **On/off-ramps:** Usually, centralized points of a crypto-asset ecosystem that allow fiat currencies to be exchanged for crypto assets—for example, trading platforms
- **P2P protocol:** Determines inter-node communication, including how blocks and transactions are exchanged
- **Permissioned/closed networks:** Networks in which only known actors with specific rights can validate existing records and add new ones
- **Permissionless/open networks:** Networks in which anyone is allowed to validate existing records and add new ones
- **Private networks:** Networks in which visibility is restricted to a subset of users
- **Public networks:** Networks in which all users can see records being added or changed
- **Quorum:** The number of nodes required to reach agreement
- **Regulatory Sandbox:** A controlled environment overseen by a regulatory authority that allows firms to test their innovative propositions with real consumers
- **Sybil attack:** An attempt to control a distributed network by creating multiple fake identities
- **TechSprint:** A technology-focused design sprint that brings together diverse participants to collaborate intensively over a short period of time on a software project

III. WHY CONSENSUS MECHANISMS MATTER

BOX 2. How Consensus Fits into Distributed Systems



Application Layer
- Wallets, exchanges

Contract Layer
- Script code and smart contracts

Incentive Layer
- Issuance and distribution mechanism

Consensus Layer
- PoW, PoS, DPoS, pBFT, iBFT, DiemBFT, PoET

Network Layer
- P2P protocol, communication mechanism

The design of blockchains matters, and different consensus mechanisms come with their own advantages and disadvantages. Blockchains can be public or private, permissioned or permissionless. These designs bring with them unique regulatory opportunities and risks, and this note will focus on the most popular consensus mechanisms that underpin blockchain systems in financial services—it is not an exhaustive list of all consensus mechanisms. Regulators must consider trade-offs when looking to understand the regulatory implications of certain blockchains. Some consensus mechanisms provide a greater focus on security and decentralization (good for record keeping), while others encourage greater speed and efficiency—for example, supporting a larger number of payments transactions per second.

There is a fundamental difference in how decisions are made in centralized and decentralized systems. Consensus aims to solve the problem of how to synchronize data across "nodes," which are powerful computers or "pools" of computers. In a centralized single-ledger system, a coordinating actor can make unilateral decisions and ensure a consistent ledger; this actor can read, write, and audit the system unilaterally. In decentralized systems, distributed nodes need to come to agreements, or a consensus, as there is no central authority to assume responsibility.

First developed in 1982, the Byzantine Generals Problem is a way of explaining the problem of trust, miscommunication, and misaligned incentives between users of decentralized systems, which equally applies to many blockchains.[7] This risk of miscommunication or purposeful malicious actions can be found in blockchains where distributed nodes need to agree on the validation of information. The decentralized

[7] The problem focuses on an imagined scenario centered in the Byzantium region of the Eastern Roman Empire. In this scenario, three Byzantine generals and their armies are encamped around an enemy city. Each general and their armies are in separate camps on different sides of the city. For the generals to successfully attack the city, they must all act together, and to do this they must agree on a time of attack; however, communication between the generals is only possible through messengers who must cross from one camp to the other through enemy territory. This approach creates several issues, among them: the messengers could get captured or killed on the way from one camp to another, or they could get captured or killed on their return journey. If they are captured, the enemy might read or change the message, compromising the strategy, which means generals can never be sure that the message received is genuine. It's also possible that one or more generals might be traitors and send false messages.

nature of the system means incentives such as double spending[8] can lead to fraudulent transactions or reversing legitimate transactions, which can create competing or inaccurate ledgers. Consensus mechanisms are used to solve these problems and ensure that there is one consistent and honest ledger and that distributed participants can come to agreement. Distributed ledgers are considered Byzantine Fault Tolerant if they can solve such problems and ensure agreement.

Consensus mechanisms primarily aim to seek agreement and ensure that it is carried out fairly and independently of any interested party. A good consensus mechanism should ensure robust network security, which certifies that participants and end users, like consumers, are protected. The BFA emphasizes the importance of integrity in financial systems, and, accordingly, consensus mechanisms should be scalable, efficient, and instrumental in creating an honest network. This, in turn, limits risks to market integrity.

The concept of open competition forms an important element of the BFA; therefore, consensus mechanisms should seek to be collaborative, egalitarian, interoperable, and inclusive. Consensus mechanisms must not favor certain members over others; DLT networks should be open to as many participants as possible while ensuring these participants are "known," to protect financial integrity (through customer due diligence). Such consensus mechanisms should not create unnecessary barriers to entry; they should create open, free, and contestable networks that operate in the interest of all stakeholders.

The BFA stresses the stability of financial systems; therefore, operational resilience is important. Consensus mechanisms should be secure and support blockchains' strong operational resilience. Without resilience, financial stability risks could emerge where the technology is deployed at scale—for example, in a global stablecoin—or where a central bank digital currency (CBDC) is deployed using DLT.[9]

BOX 3. Selected Risks of Some Consensus Mechanisms

Risk Type	How Risks Might Arise
Consumer Protection	Some consensus mechanisms can lead to poor outcomes for consumers if the mechanisms' method of generating consensus leads to slow transactions times or high transaction costs. In cases where consumers are vulnerable or lack technical literacy, such costs can be unexpected and unacceptable.
Market Integrity	Consensus mechanisms that are less secure could result in fraudulent transactions where malicious nodes are able to get access to the network through, for example, a 51 percent attack, or where a leader node has malicious intent. In financial markets, the result of such actions could lead to market manipulation and market abuse.
Financial Integrity[10]	The pseudonymous nature of most DLT transactions can pose risks related to fraud, theft, money laundering, and terrorist financing. Although blockchains provide transparency, auditability, and immutability, end users and many market participants (such as nodes) are often not known, which can make sanctions or enforcement actions difficult to implement.
Financial Stability	A small network of entities (or a single entity) could gain market dominance through private blockchains with consensus mechanisms that rely on permissioned access. This situation could create a network that has high barriers to entry, is nonsubstitutable, and that could become "too big to fail." Separately, where a crypto asset (such as a stablecoin or a CBDC) gains popular and widespread adoption, failure of the underlying consensus mechanisms could generate risks to financial stability.

[8] Double spending refers to the risk that a unit of digital money or crypto assets could be spent twice. This concern is largely a nonissue in a centralized system, where a single entity can determine whether a transaction is valid.

[9] Not all CBDCs are built on DLT.

[10] Financial integrity matters are more fully covered in IMF publications on AML/CFT issues related to crypto assets; see Schwarz and others 2021a, 2021b.

Consensus mechanisms should not harm or interfere with the global aim to transition to a low-carbon economy. A transition to a greener economy supports the goals of the IMF as well as the goals of many regulatory authorities, which seek to ensure sustainable growth in their respective markets while not harming the environment. The use of energy-intensive methods to achieve consensus presents unacceptable risks to financial stability and society, as such methods exacerbate the effects of climate change. Recently, to manage the risks of climate change and mitigate environmental impacts from crypto assets, the Swedish Finansinspektionen called for the European Union to ban PoW mining (Finansinspektionen 2021). A key consideration of authorities should be moving to less environmentally damaging methods of operating blockchains.

Regulators monitoring the development of blockchains should consider how their use interacts with existing regulatory frameworks and whether they meet the aims of the BFA. Certain consensus mechanisms are more likely to fit into existing regulation—for example, where settlement is immediate as opposed to probabilistic.[11] There are trade-offs in achieving these goals; for example, a more open network might limit barriers to entry but could slow down transaction rates or create risks to consumer protection or market integrity.

[11] Many types of consensus mechanisms that underpin public blockchains can only deliver probabilistic settlement due to the possibility of forks in the blockchain which might cancel earlier transactions if they are not included in the longest chain.

IV. PUBLIC AND PRIVATE BLOCKCHAINS: REGULATORY IMPLICATIONS

Public blockchains are considered the "pure" form of blockchain, as envisaged by early developers, and so data are distributed widely and control of that data can be decentralized. Public blockchains are permissionless and decentralized, although there can be public-permissioned blockchains in which certain nodes are given specific rights. Such blockchains can remove reliance on single counterparties and authorities, and they aim to democratize the transfer of data between network participants on the blockchain.

From a regulatory perspective, public blockchains are, in principle, less susceptible to cyberattacks, operational failures, and malicious behavior by individuals or entities, although they bring unique risks. The key advantage of public blockchains—specifically, larger public networks—is the decentralization of information, which, among other things, makes them less susceptible to cyberattacks. But even public blockchains can have centralized points of risk—for example, applications built on those networks like wallets and exchanges. Furthermore, it can be more difficult to supervise participants on a public blockchain because they can be global or unknown, and this challenge can pose risks such as financial crime, or there may be a lack of recourse to end users or no way to fix market errors should any failure or fraud occur.

Private blockchains usually consist of a single or small number of entities and tend to give permissions to known and identifiable participants. In this way, private blockchains run counter to the intended "ideals" of the decentralized community in that they shift risk from one centralized entity or authority to another (the network administrators). Within the payments space, these blockchains are proposed for so-called global stablecoin arrangements as well as proposed CBDCs.

From a regulatory perspective, this centralization creates points vulnerable to operational, cyber, and default risk and potential failure—but some important regulatory benefits remain. On the one hand, a private blockchain can be altered by its owner, and it also forms a more centralized "honey pot" for hackers. On the other hand, in blockchains where participants are known, they are more easily captured by existing or new regulatory frameworks, and blockchain developers and crypto-asset issuers can come under the scope of regulation. Regulators might find it easier to have oversight over such systems (although "knowing" participants doesn't always make supervising them easier, particularly if they are located in offshore jurisdictions).

A. Consensus Mechanisms in Public Blockchains

There is a large and growing variety of consensus mechanisms. These are the most common examples in public blockchains within financial services:

- Proof-of-Work
- Proof-of-Stake
- Delegated Proof-of-Stake

Proof-of-Work (PoW)[12]

As the fundamental underpinning of the Bitcoin Blockchain developed by Satoshi Nakamoto, PoW is the most frequently used and well-known consensus mechanism. PoW involves "nodes" solving complicated, asymmetrical mathematical puzzles to produce new blocks in a process known as "mining"—thereby showing proof of work. The Bitcoin protocol adjusts the difficulty of these puzzles to ensure that a new block is

[12] Well-known use cases are Bitcoin, Litecoin, and Dogecoin.

produced every 10 minutes. Although the puzzles are designed to be hard to solve, they are easy for the network to verify. Sometimes, several nodes may solve the puzzle, which can create parallel blocks, more commonly known as "forking."[13] In these instances, the forks are usually only temporary, as all nodes will eventually move to the longest chain while the other chains get discarded by the protocol.

PoW uses two reward mechanisms to incentivize nodes to be active on the network and ensure a large and diverse number of nodes. On the Bitcoin Blockchain, nodes that solve the puzzle get to add their block to the blockchain and are rewarded with new Bitcoins. These rewards are halved every four years and from May 2020, the block reward fell from 12.5 Bitcoins to 6.25 Bitcoins. This concept of rewarding active nodes with crypto assets is replicated in many other consensus mechanisms. The second reward is the transaction fee. When users send Bitcoins, they attach a transaction fee and the higher the fee, the more likely a node will validate the transaction—meaning a faster transaction time. PoW mechanisms allow for large number of nodes to participate in the network, which can make the network scalable. The larger the network of nodes, the higher the hashrate, the less likely it is for a single node to hold power over the network and engage in fraudulent transactions. This approach ensures that the mechanism is sufficiently robust to ensure network security. From a regulatory perspective, nevertheless, the lack of control in terms of who can enter and participate in the system can be a problem.

To solve the mathematical puzzles generated by the Bitcoin protocol, nodes need to use "brute force," which, in turn, consumes considerable energy because brute force requires specialized computing systems to run through all possible solutions until the winning solution is found—an effort that uses significant power. The IMF has set out that the financial sector has an important role to play in the fight against climate change and seeks to support reductions in climate change risk and mitigating the impact of adverse climate events.[14] However, the total energy usage of Bitcoin mining is comparable to Poland at 140 Terrawatt-hour, and so runs counter to this aim.[15] Regulators using or supporting consensus mechanisms that rely on large-scale energy use should pay attention to this energy consumption; most of them will likely find such damaging impacts to the environment unacceptable.

Although PoW guarantees eventual consistency in the blockchain, there may be some instances where there are competing forks, which can impact the network by making it slow, expensive, and inefficient. Forks can lead to slower settlement times, making the usage of PoW inefficient in certain areas of financial services (for example, payments). Currently, the Bitcoin Blockchain can process approximately 7 transactions per second, and although the development of the Lightning Network offers promise in this area (albeit with its own flaws), its transaction rate is currently much lower than that of traditional payment mechanisms like Visa—which averages roughly 1,700 transactions per second.

Inconsistencies can also lead to risks to settlement finality. Transactions between counterparties carry risks—including credit, liquidity, operational, and legal risks—all of which can trigger systemic hazards. Rules around settlement finality aim to mitigate these risks; however, the possibility of forks in a blockchain makes achieving settlement finality difficult. This probabilistic settlement creates challenges around ensuring PoW-based blockchains fit within broader settlement regulation, as well as the impact this has on areas like custody. The proposed European Union DLT Sandbox aims to identify—among other things—where such legal issues could interfere with existing regulatory frameworks.

Further, PoW is seen to be potentially centralizing, which could negate the security that PoW offers. As mathematical puzzles become increasingly complex, more powerful computing power is needed to solve them. Given the large cost involved, such technology is available only to certain individuals or entities, or

[13] Forks can be "soft," which are backward compatible and temporary in nature, or "hard," which create permanent new chains.

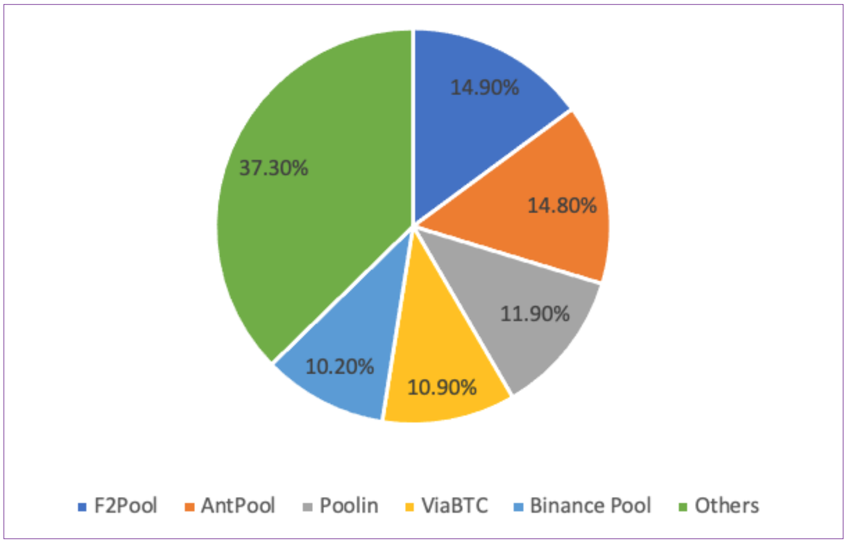
[14] Climate Change Indicators Dashboard (imf.org)

[15] Cambridge Bitcoin Electricity Consumption Index (CBECI)

where mining pools are formed. This scenario can give rise to questions around the powers, tools, and options available for the regulator to fix an eventual market failure (for example, an individual who, or entity that, becomes "too big to fail").

Authorities should note that although PoW consensus mechanisms lay the foundation for secure and resilient blockchain systems, they can be slow, they consume significant energy, and settlement is probabilistic. PoW is one of the most secure validation methods and can be useful in records and supply chain management, but the attendant lack of speed, scalability, and settlement finality—and PoW's considerable energy consumption—are likely to pose regulatory risks that many authorities will be unwilling or unable to accommodate in areas like payments. DLT based on PoW consensus mechanisms might not fit within existing regulatory frameworks focused on settlement finality. Supervisors should also be aware that many blockchains that make use of PoW tend to be decentralized, where not all identities of nodes are known, and so can give rise to supervisory difficulties.

FIGURE 1. Bitcoin Mining Pools Janaury 2021 to January 2022[16]



Source: One-year pool distribution calculated by blocks from BTC.com.

Proof-of-Stake (PoS)[17]

In a PoS consensus mechanism, an algorithm randomly selects validators for block creation based on the amount that token holders stake from their crypto-asset ownership. The first step is selecting a proposer, then a proposed block, and then validation of the proposed block. Holders with larger ownership of the native token have a greater chance of being selected—like playing the lottery. Even though everyone who buys a ticket has a chance of winning and selection is random, those with the most tickets have the greatest odds of winning.

By not requiring energy-intensive mining operations, PoS improves on some of the weaknesses in PoW consensus mechanisms, such as large energy consumption, while preserving network security. This lessened energy consumption also means a lower need to issue many new coins to incentivize nodes to participate in the network. It also limits the risks of a 51 percent attack: although it would be very difficult and expensive

[16] Pool Stats - BTC.com

[17] Well-known use cases are Cardano, Tezos, and Ethereum (announced—as of publication, the Ethereum Network is transitioning from Proof-of-Work consensus to Proof-of-Stake). Ethereum's transition aims to solve issues of environmental impact, transaction throughput, and aims for greater decentralization. Over the long term, Ethereum 2.0 might reduce transaction fees through sharding—a process of splitting the database and creating new chains.

for anyone to carry out a successful 51 percent attack in a large PoW-based blockchain, it is even more expensive to do it in a large PoS-based one.

Given that nodes aren't working to solve complex mathematical problems and there are fewer validating nodes, transaction rates can be increased—but settlement issues remain. A greater transaction throughput makes the PoS model much more useful in certain financial services contexts, like facilitating payments; however, to increase the chances of being selected, validating nodes might vote on multiple blocks—even those whose underlying information might be incorrect, creating risks around broader market integrity. PoS models can do this because, unlike PoW models, validating nodes in PoS don't have to expend anything (like energy). While voting on multiple blocks maximizes the chances of nodes receiving a reward through transaction fees, it also increases the risks of multiple forks, which can create uncertainty with settlement finality; this situation is known as the "Nothing at Stake" problem. Newer models of PoS seek to solve it by creating monetary penalties for the work validators do on blocks that do not get included in the chain. These models, however, are still in their infancy.

Because ownership directly correlates with the chances of being selected, PoS consensus mechanisms can theoretically create a community where richer individuals or entities are more likely to be selected. This means those participants are also more likely to be rewarded, fueling an environment where the rich get richer. This scenario can lead to those participants with smaller holdings exiting the network if they aren't able to generate rewards. In effect, PoS consensus mechanisms could create conditions where the network isn't inclusive, as certain members (that is, those with larger holdings) are more likely be favored over others, increasing the potential for centralization.

Weaknesses within PoS consensus mechanisms might impact stability and integrity, such as centralization in smaller networks and the inefficiency of staking. In the long term, these flaws can lead to centralization-related issues, which can be particularly problematic in smaller networks or networks in their infancy—and can therefore impact market integrity. Authorities could consider elements like sandboxing to help protect nascent networks.[18]

The potential for centralization is similar for PoW, where participants that can afford the most powerful machines are better able to generate rewards; however, PoW-based advantages in terms of centralization are based on the different nature of the capital used for validation and the friction to switch between the currency and the hardware and electricity. Even in larger PoS networks, the potential for validator cartels to form can lead to concerns around centralization, while exchanges and wallet providers could also theoretically exercise disproportionate control given their large holdings. PoS is also inefficient in its use of network-native resources. Given that crypto assets might be locked up for staking purposes, PoS removes the ability to transfer or spend a proportion of the total number of crypto assets in circulation. A liquidity shortage could arise if token holders hoard their tokens to increase their chance of being selected as validators; this act would lower the speed of transaction rates, and the network could suffer from the lack of circulation.

Safeguarding the integrity of financial systems is an important aspect of the BFA, so regulators should think about appropriate network security and fairness. Authorities should consider those frameworks that incorporate appropriate systems and controls to mitigate against cyber and operational risks, such as the Basel Committee on Banking Supervision (BCBS) Principles for Operational Resilience (BCBS 2021). In line with the BFA elements on improving financial inclusion and ensuring open, free, and contestable markets, authorities should also consider how to work with market participants developing these networks to ensure that they are as inclusive and collaborative as possible and that these networks do not work to benefit a small privileged group and lead to areas of financial markets that lack contestability. Finally, due to the Nothing at Stake problem, authorities may want to pay attention to the risks created by competing chains.

[18] In PoS, security improves with scalability; therefore, until they achieve sufficient scale, nascent networks might benefit from proof-of-concept to proof-of-value–style controlled environments, such as certain types of sandboxes.

Delegated Proof-of-Stake (DPoS)[19]

DPoS adds a democratic element to the PoS consensus mechanism by outsourcing the validation process. As with PoS, block validation is randomized, and individuals or entities (stakeholders) who stake the greatest amount of a particular crypto asset are more likely to win the opportunity to validate a block and generate a reward. The DPoS model operates a voting system where the stakeholders chosen to validate a block can outsource their work to a third party. These third parties are known as "witnesses" and are responsible for achieving consensus during the generation and validation of new blocks. Rewards are shared between the witnesses and the stakeholders.

Benefits of DPoS include energy savings, greater decentralization, and positive participant behaviors. DPoS promotes greater democratization: all token holders can play some role in the operationalization of a network. It should be noted that in many models of blockchains that use DPoS, voting is proportional to the amount of stake that participants place. DPoS also aims to promote positive behaviors from participants. Those witnesses that add value to a network and are good network citizens are more likely to be repeatedly voted in; any witness that loses credibility, doesn't participate, or looks to carry out fraudulent activity is likely to be voted out. This process ensures that witnesses work with the network's best interests in mind. DPoS also makes use of "delegates" who are voted on to govern the system and propose any core changes. Like witnesses, delegates are placed into position through voting—and they can be removed through voting if they are seen not to serve the needs of the network.

In terms of financial services, and payments in particular, transaction rates are likely to be quicker in DPoS than in both PoW and PoS due to network engagement. This is because witnesses are likely to participate more actively and at greater speed to retain their position in the community. Witnesses are also likely to be limited in number, which increases transaction throughput; however, if there are an excessive number of validators, there is a greater risk that the network will slow down. So, a balance around greater scalability must be struck.

Although DPoS promotes greater decentralization, in some instances, such as where participation in the voting process is low, concerns about centralization can arise. For example, having a limited number of token holders could impact and influence the network. As with PoS, DPoS stakeholders can use their power from larger stakes to form cartels, which can make the network more centralized and less resilient to attacks—resulting in both regulatory authorities without relevant powers or tools to rectify such issues and concerns about market integrity and operational resilience.

DPoS is relatively new, yet it provides opportunities for firms to generate efficiencies through a relatively fast transaction throughput and can be delivered in both permissioned and permissionless networks. If developed and implemented in a compliant manner, DPoS can create positive outcomes for markets and consumers by providing interesting use cases in regulated activities, like payments. This is because it can create a truly decentralized environment with the potential for quicker transaction rates. That said, because the mechanism has not been tested as long as PoW or PoS have been, regulators should consider associated network-security risks, cartel-like behavior, and limited voter participation.

B. Consensus Mechanisms in Private Blockchains

This section covers the most common consensus mechanisms deployed in private blockchains within financial services:

- Practical Byzantine Fault Tolerance
- Federated Byzantine Fault Tolerance
- DiemBFT
- Proof-of-Elapsed-Time

[19] Well-known use cases are EOS, Ark, BitShares, and Tezos.

Practical and Istanbul Byzantine Fault Tolerance (pBFT/iBFT)[20]

The consensus mechanisms explored so far work well when network participants are not trusted—that is, they work well with public or permissionless networks. This next section deals with those consensus mechanisms in which network participants are trusted; pBFT is among the most well-known examples. pBFT works best in cases where network participants are at least partially trusted—that is, in permissioned networks. It predates blockchains in terms of the underlying theory, but it has been applied to blockchain networks with some success. It can be considered a Proof-of-Authority (PoA) type of mechanism where nodes stake their identity and reputation, as opposed to a financial or computational stake such as PoW and PoS. This means identities are known, and therefore networks are likely to be centralized.

Nodes in pBFT are sequentially ordered and constantly communicating to keep network throughput high. There is one main node, also known as the "leader" node, and several backup nodes. pBFT assumes that some of these nodes are likely to be fraudulent and therefore likely to be sending out malicious or false messages. To counter this act, all nodes communicate with each other. The aim is that all the honest nodes come to an agreement on the state of the network through a majority consensus. As more honest nodes are likely to come to agreement on the state of a network than fraudulent nodes coming to agreement on a false decision, incorrect information should be rejected by the majority. Nodes in the system share messages when determining whether to commit a block to the chain. This ensures that a message came from a specific peer node and that it wasn't tampered with during transmission. These messages take the form of four rounds, known as "views," that are proposed by the leader.[21] If a view has gone on too long, nodes can agree on a timeout. Leader nodes can be changed after every view.

Although pBFT is a pre-blockchain proposal for distributed systems, slightly modified for blockchain, iBFT was developed specifically for blockchain. iBFT can be thought of as a type of pBFT consensus mechanism with some modifications. Rather than using leaders and backup nodes, iBFT employs "proposers" who play a role like leaders and validators who play roles like backup nodes, in that they can validate blocks but play no role in the consensus protocol. After each consensus round, the validators can choose a new proposer who is responsible for providing the candidate block for the next interval. The primary modification in iBFT is that validators can be removed or added; in pBFT the set of validators is static. So, validators in iBFT are more invested in the network and likely more honest and engaged. iBFT may create lower barriers to entry depending on how the blockchain is implemented.

Both iBFT and pBFT work where fraudulent or malicious nodes do not exceed a third of the overall nodes in a network. This means that network security increases when the overall number of nodes in the network increases. The main advantage of pBFT and iBFT when deployed in financial services is that there are no forks and there is immediate settlement and so settlement finality. Unlike in PoW, PoS, and DPoS, which require confirmation of a block state, the stream of communication between nodes on a pBFT and iBFT network ensures that there is agreement on the state of a network at a specific time, which means the state of an agreed-upon block is final.

There is little energy consumption when compared to PoW-based networks, as there are no miners working to solve complicated mathematical puzzles and nodes are known to each other. Both pBFT and iBFT can lower the need for and variance of rewards, as decisions are made collectively; every node can be incentivized and rewarded in a similar fashion. Even though more nodes mean more network security, pBFT and iBFT work best when node numbers are limited because of the large number of messages exchanged between the nodes. The more nodes there are, the longer it takes for actions (like transactions) to be

[20] Well-known use cases are Hyperledger Fabric and Consensys Quorum.

[21] These views involve a client sending a request to the leader node; this request being broadcast to backup nodes; the nodes acting on this request, voting between themselves, and then replying to the client; and then finally the client waiting for replies from different nodes, ensuring the result is the same.

completed. Unlike the consensus mechanisms mentioned earlier, pBFT and iBFT work where nodes are known to one another; however, even with known nodes, a pBFT- or iBFT- based network can be susceptible to Sybil attacks in which a single node, like the leader, can manipulate other nodes in the network, therefore compromising security. While this risk can be mitigated with a network of more nodes, such expansion may reduce network speed and efficiency.

pBFT and iBFT can ensure efficient and fast networks and may protect consumers; however, the mechanism may facilitate networks that hamper competition. Within financial services, pBFT and iBFT are likely to work best where organizations represent the different nodes in a network and these organizations work within a single governance system. These organizations may create barriers to entry for new joiners, particularly where there is a closed loop of data sharing, sharing of efficiencies, or a closed ecosystem. This case is completely different from that of PoW, PoS, and DPoS, where almost anyone can become a node within a network, providing open, free, and contestable markets. It also means pBFT requires trust in some central entity or group of entities. This trust in intermediaries runs counter to a core tenet of the original Bitcoin Blockchain and most blockchains developed since. Decentralization and democratizing of actions (like currency transactions) are a key reason for the development of blockchains. Authorities may need to work with broader domestic regulators and competition authorities to mitigate against possible risks to competition.

Although most regulatory and technical risks are like those of pBFT, a network using iBFT will always produce blocks at regular intervals. This is true even if there are no actions or transactions. So, there might be many blocks with zero actions. Authorities may consider the implications of this type of block creation, as it can take up valuable storage space and create unnecessary energy expenditure. However, with "known" participants, authorities might be better able to regulate and supervise network participants, and, with immediate settlement, propositions built on such networks are more likely to fit into existing regulatory frameworks.

Federated Byzantine Fault Tolerance (fBFT)[22]

fBFT is a Byzantine Fault Tolerant consensus mechanism that aims to solve issues of centralization with greater scalability. In the BFT mechanisms described above, identities of all participants are known; however, in fBFT the identities of all nodes do not have to be known. So, membership is open and control can be decentralized. fBFT can be thought of as semi-trusted as it relies on "quorum slices," or a Unique Node List, which means only a subset of nodes is needed for agreement. In most implementations of fBFT, nodes individually choose the other nodes they trust for information. These nodes are likely to overlap or intersect with other quorum slices. Where this occurs it is known as a "quorum intersection." Quorum intersections allow small quorum slices to build agreements across the network, improving scalability.[23]

Within financial services, BFT consensus mechanisms can generate large efficiencies for retail payments, wholesale settlements, and other back-office functions, but BFT works best where network participants are known. These algorithms are built for speed and have immediate block finality. The latter is particularly operationally flexible, as it allows groups of validators to be modified over time. With increasing scale, speed

[22] Well-known use cases are Ripple and Stellar.

[23] For example, you might trust five individuals known to you, but you do not trust a sixth, unknown individual. The five known individuals would be your quorum slice; however, one of your five trusted individuals might know and trust the sixth individual. This is a quorum intersection, as your quorum slice overlaps with another. The sixth individual might have a further five individuals who are not known to your quorum slice but are known to the sixth individual. This can mean that from a small subset of known individuals, an agreement is reached across the network. This approach can create strong network security, as well-behaved nodes may not want to keep failed nodes in their slices out of concern the failed nodes will affect them negatively.

and trust can become compromised; therefore, these models do have the potential to create barriers to entry. This problem is something that fBFT aims to solve with its approach of a Unique Node List.

Authorities might consider how fBFT consensus mechanisms can balance a decentralized and distributed network with efficiencies, such as a high transaction rate and settlement finality, to generate positive outcomes for markets. With its unique ability to mix known and unknown participants, fBFT could create greater risks to financial integrity than the BFT mechanisms described earlier, and it suffers from additional flaws and weaknesses that must be considered (most notably, in security, with the presence of faulty or malicious nodes). However, given its potential to be both efficient and scalable, authorities may need to collaborate both domestically and across borders to ensure that any risks to financial stability are appropriately mitigated.

DiemBFT[24]

DiemBFT is a Byzantine Fault Tolerant protocol based on the HotStuff protocol, which itself builds on pBFT and aims to increase speed and efficiency. The aim of the protocol is to provide a quicker network by reducing the large number of messages and communication between nodes that are seen in pBFT, while retaining network security and accuracy. The HotStuff protocol achieves this goal through a type of communication that relies more heavily on the leader node, rather than on communication between all nodes, creating a star communication network. Security is also enhanced using the HotStuff approach of unpredictable leader election whereby a new leader is determined randomly. Like pBFT, HotStuff and DiemBFT are based on a leader/follower paradigm. In the DiemBFT Diem Network, members act as nodes and receive transactions from clients, which are communicated with others through a shared mempool.[25] Nodes can rotate and become leaders through a dynamic leadership model that is based on the HotStuff protocol, which allows these rotations to occur within rounds (or "views") with minimum timeouts, and DiemBFT builds on this effort with a pacemaker mechanism to ensure every round has an upper time limit. Leaders propose new blocks of transactions to add to the chain and follower nodes vote to approve them. Once a node block gets a majority vote from the follower nodes, the leader node creates a Quorum Certificate that is broadcast to all nodes. Once the Quorum Certificate is verified, transactions can be committed to storage.

DiemBFT allows for faster transaction throughput. Transactions on the Diem Network have the potential to be relatively quick and low cost. Unlike the Bitcoin Blockchain, which can only process 7 transactions per second, the DiemBFT proposes to process 1,000 at launch. DiemBFT is also planning to support additional resources, such as decentralized applications, rather than just transferring Diem stablecoins.

However, the DiemBFT has several drawbacks that can impact competition as well as create issues around data and privacy. When used as part of the Diem stablecoin proposition, DiemBFT is a centralized network where nodes must commit at least $10 million to join and have access to appropriate computing hardware. And while these sunk costs reduce the incentive for those nodes to then become malicious, they create concerns around barriers to entry and market contestability, which run counter to the BFA's aims. DiemBFT also relies on only a few counterparties (the nodes) as well as the leader node in each "view."

Given the development of the DiemBFT by a "BigTech," authorities have several unique and important challenges to consider. In addition to the high barriers to entry, the potential of the DiemBFT, when utilized by Diem Network members, to become a systemic payment infrastructure due to a potentially large embedded userbase (that is, service users of existing network members) may require extensive collaboration among regulatory authorities worldwide, including both financial services regulators to manage payments related risks, and non-financial regulators including competition authorities for broader risks (Bains, Sugimoto, and Wilson 2022; IMF 2021c).

[24] A well-known use case is Diem.

[25] A mempool is used to store information such as unconfirmed transactions that are waiting to get validated.

Proof-of-Elapsed-Time (PoET)[26]

PoET is a privately developed consensus mechanism that aims to prevent large energy consumption and can be used in both permissioned and permissionless blockchains. It also seeks to limit other forms of resource utilization—for example, locking up amounts of crypto assets as stakes and centralizing rewards. Like fBFT, it has been developed for a permissioned setting but has the potential to be scalable and extend to permissionless networks. Intel created this consensus mechanism and offers a ready-made tool to solve the computing problem of randomly selecting a leader. PoET makes decisions about mining rights and block winners on a network; it aims to spread the chances of winning fairly across the largest number of network participants.

Each node on a PoET network generates a random wait time and is required to wait for their chosen wait time to expire, which can save energy. The first node to complete the wait time—that is, the node with the shortest randomly generated wait time—wins the new block. Importantly, while the node is waiting for its wait time to expire, it goes to sleep, so it can use its processor for other tasks or no tasks at all, therefore limiting energy consumption. Intel's ready-made tool ensures that networks using its mechanism can both generate random wait times and ensure the random wait time is genuinely fulfilled. PoET solves the problems with energy consumption, the potential centralization of rewards, and concerns about random leader selection. Furthermore, it can keep transaction rates fairly high.

That said, settlement remains probabilistic. Issues can arise with existing regulatory regimes when a PoET-based blockchain network is used in certain financial services capacities. Probabilistic settlement raises concerns about the ability of such blockchains to meet existing regulatory requirements on settlement finality as well as their use in certain financial service propositions (for example, payments). There are concerns about the network's vulnerability to Sybil attacks, and giving centralization of the consensus mechanism to a third party (that is, Intel) runs counter to the goal of removing trust in intermediaries. Authorities should consider whether security concerns are likely to impact the provision of financial products and services based on PoET; they should develop relevant systems and controls for greater operational and cyber resilience. Although a single entity (such as Intel) is theoretically easier to regulate than unknown or distributed entities, regulatory authorities may find it difficult to draw an effective financial regulatory perimeter.

[26] A well-known use case is Hyperledger Sawtooth.

V. CONCLUSION

Consensus mechanisms are deployed depending on the type of operation a particular blockchain network is likely to carry out. Mechanisms used in permissionless networks tend to focus to a greater extent on security and ensuring that consensus is achieved among untrusted nodes. Mechanisms used in permissioned networks sacrifice decentralization for settlement finality and quicker transaction rates.

PoW is too energy intensive to be considered a viable consensus mechanism involving many regulated financial services activities. It runs counter to several of the IMF's aims, particularly those that involve transitioning to a greener economy. Although the mechanism is secure, resilient, and offers true democratization of data within distributed systems, significant energy consumption, the nature of forking, and the attendant issues around probabilistic settlement are likely to create friction with many regulatory frameworks, regulatory mandates, and the BFA. Some of these issues are also apparent in other consensus mechanisms where settlement is likely to be probabilistic—like PoS, DPoS, and PoET.

TABLE 1. Comparison of Different Consensus Mechanisms

	PoW	PoS/DPoS	PoET	pBFT/iBFT	fBFT	DiemBFT
Blockchain Type	Permissionless	Permissionless	Both	Permissioned	Both	Both
Settlement Finality	Probabilistic	Probabilistic	Probabilistic	Immediate	Immediate	Immediate
Transaction Rate	Low	High	Medium	High	High	High
Scalability	High[27]	High	High	Low	High	High
Contestability	High	High	High	Low	Medium	Low
Environmental Impact	High	Medium	Low	Low	Low	Low
Security	High	High	Medium	Medium	Medium	Medium

These issues are generally solved by closed network consensus mechanisms, but they introduce new risks and run counter to blockchain principles of disintermediation and decentralization. Mechanisms such as pBFT, iBFT, DiemBFT, and PoET are designed to be quick and energy efficient, although some of them suffer from scalability and access problems. These (and similar) mechanisms are more likely to be deployed in financial services where participants are known and are likely to be used in global stablecoins and potential CBDCs, which can create risks to financial stability. These mechanisms can give rise to risks around competition and contestability where networks are closed and barriers to entry are high, and if such networks deploy widely used products (like global stablecoins), a lack of competition and substitutability could lead to networks that are "too big to fail."

Public-private collaboration might better allow authorities to monitor developments in the market and ensure the development of compliant business models in financial services. Where development of DLT is small or nonsystemic, authorities might decide to take a "wait and see" approach. Where development of DLT operates at a larger scale, authorities might take a "test and learn" approach through outreach and

[27] While the PoW can be expandable and so scalable, it does not necessarily mean that increased volumes will reduce the cost of each transaction.

engagement, to better understand the risks and benefits as well as additional variables. Such variables include interoperability with other financial systems, emerging standards across financial institutions, or support by major industry leaders, all of which have regulatory implications.

Engagement between authorities and industry can happen through short-term engagements, using "business as usual" supervision, or through longer term engagement, via innovation hubs. Short-term public-private collaboration can happen through joint events or commissioned surveys focused on consensus mechanisms; longer term collaboration can be through joint research, experiments, and testing. Partnership between regulators, technologists, security experts, and other relevant stakeholders (for example, academia and industry bodies) can help supervisors fully understand the implications of different consensus mechanisms.

Regulatory authorities should consider the implications of different consensus mechanisms in terms of regulation and supervision and consider a technology agnostic approach. They should determine whether the consensus mechanisms are appropriate in relation to the desired outcomes of a specific proposition. By taking a technology agnostic approach, authorities can work with market participants to better understand the strengths and weaknesses of different consensus mechanisms and where comparative advantages in the provision of different financial products and services (for example, payments, issuing debt/equity, supply chain management, record of activity) might exist. Through shifting to a technology agnostic approach, authorities remain unbiased to the use of different technologies but recognize that different technologies bring different risks and authorities are not "neutral" to these risks. Authorities can then make determinations on specific technologies. Utilizing the BFA as a framework, regulators with a deeper understanding of these consensus mechanisms can better contextualize whether they are likely to encourage competition and increase efficiency—or create risks to market integrity, consumer protection, and financial stability.

Supervisors should be upskilled and, where possible, trained experts should be hired to better help authorities understand consensus mechanisms so that supervisors can ask firms pertinent questions and make accurate judgments on the risk and efficiency of different consensus mechanisms. Although many regulatory authorities are beginning to make the shift toward becoming more data-driven digital regulators resources, budgets, and the availability of skilled supervisors remain a challenge for many of them. Here, international organizations like the IMF have a role to play in providing technical assistance and sharing best practices. Furthermore, standard-setting bodies can help by developing global recommendations that can provide minimum requirements for consensus mechanisms when utilized in regulated financial entities.

Authorities could also consider utilizing tools such as TechSprints to better understand the strengths and weaknesses of different types of consensus mechanisms. TechSprints are short collaborative programs that bring together participants to develop technology-based ideas or proof of concepts to address specific industry challenges. Participants can be within financial services, but they can also come from academia, government, and nonprofit organizations, among others. Programs like TechSprints can help move authorities from being technology neutral to technology agnostic; they can give authorities a better understanding, at a high level, of how different types of consensus mechanisms are likely to impact the development and delivery of certain financial products or services.

Where a proposition based on a certain type of DLT is ready to enter the market, regulatory sandboxes and digital sandboxes can better allow authorities to understand specific benefits and risks, thereby fostering innovation while mitigating dangers to financial stability, market integrity, and consumer protection. In many cases, the choice of consensus mechanisms used either by regulated entities or by the regulator itself in a SupTech[28] capacity is a long-term decision: once you select it, you're stuck with it. This choice requires more formal reviews and collaboration involving many actors of the ecosystem.

[28] SupTech refers to Supervisory Technology, or the use of new technology to support the objectives of authorities.