COMMENT BY

ESWAR PRASAD In their paper, Makarov and Schoar do a very nice job of discussing the exciting new world of cryptocurrencies and decentralized finance in a rigorous but balanced fashion. Here, I attempt to complement their discussion by discussing some aspects of decentralized finance and the regulation of the new financial ecosystem spawned by these new technologies.

COIN OFFERINGS The proliferation of cryptocurrencies has resulted in the creation of new financial instruments. An initial coin offering (ICO) is a fundraising tool that involves the generation and sale of a set of blockchain-based tokens to finance a particular project or initiative that is usually also blockchain-based. The tokens are sold in exchange for one of the prominent cryptocurrencies or for fiat currencies, and they then become linked to the project they helped finance. An important difference relative to an IPO (an initial public offering of stock for a company listed on a stock exchange) is that an ICO usually does not involve the transfer of ownership stakes to investors.

ICOs are, in effect, bets on the future of a particular cryptocurrency. In the United States, ICOs are far easier to implement than IPOs, which require filings with the Securities and Exchange Commission (SEC) and other extensive disclosure requirements. Companies undertaking ICOs simply create white papers explaining the project's business model, the amount of money they plan to raise (usually a maximum amount is specified), the duration of the ICO campaign, and who is eligible to participate in the ICO. Most ICOs have been carried out on the Ethereum platform.

ICOs have become a key source of funding for blockchain start-ups and other firms operating at the frontiers of this technology. ICOs hold the promise of extraordinary returns for believers in the transformative potential of this technology, but they also imply huge risks for investors. Investors usually have little information beyond a white paper describing the ICO with which to evaluate the business model and the earnings potential of the issuer.

Some ICOs take the form of equity token offerings (ETOs). A company conducting an ETO adds shares to its capital. These shares, which are recorded on a blockchain, grant investors a percentage of voting rights as well as titles of ownership within the company. This differentiates ETOs from normal ICOs, which do not involve any transfer of ownership stakes.

Initial exchange offerings (IEOs) are similar to ICOs except that the tokens are issued through a partnering exchange rather than directly to

investors. The exchange does not in any way guarantee the value or legitimacy of the token issued through an IEO. Still, IEOs are seen as safer than ICOs: the exchange has an incentive to carry out due diligence on the issuing company and its business model, since the exchange faces risk to its reputation if the tokens prove worthless or fraudulent.

IEOs conducted by a particular exchange tend to be standardized, unlike ICOs, whose terms and structure are determined at the sole discretion of the issuing company. Another difference is that tokens issued through an IEO are immediately tradable on the issuing exchange; with ICOs that is not necessarily the case, especially where there are private placements.

Recognizing that tokenization could be used to broaden the investor base for their offerings, some governments and financial institutions have used another investment product, security token offerings (STOs), which in some ways bridges the gap between IPOs and their cryptocurrency counterparts. STOs involve selling digital tokens on cryptocurrency exchanges. Security tokens are securities, similar to stocks and bonds, that usually represent ownership stakes in a particular company. The tokens represent ownership information about the investment product, recorded on the blockchain. STO tokens are sometimes backed by and represent ownership shares in particular tangible assets, especially illiquid assets such as real estate and fine art. STOs are generally regulated as securities, offering more protection to investors. In the United States, for instance, the SEC has jurisdiction over STOs.

All of these types of digital coin offerings show how blockchain technology is powered by and, in turn is changing finance. Innovations in digital and financial technologies are feeding off each other, creating more opportunities for direct financing of innovative technologies and giving even retail investors the opportunity to participate in the financial benefits (and risks) that could flow from such innovations.

DECENTRALIZED FINANCE Decentralized finance (DeFi) or open finance is a model for providing a broad range of financial services—including credit, savings, and insurance—in a decentralized manner and making the services and products available to anyone in the world (Harvey, Ramachandran, and Santoro 2021; Prasad 2021).

DeFi is built on decentralized blockchains. There are three elements that characterize such systems. Decentralized blockchains have decentralized architectures (no centralized point of failure), decentralized governance (control rests with the members of a network rather than a central authority), and decentralized trust (trust is achieved through a public

consensus mechanism). But the system is logically centralized—the entire network of nodes that make up such a system is linked and is in a commonly agreed-to state at all times. Bitcoin could be considered the earliest form of DeFi.

DeFi relies on smart contract blockchains, of which Ethereum is by far the most widely used. In principle, decentralization confers many advantages over traditional financial systems. One is fault tolerance—failure is less likely because such a system relies on many separate components. Another is attack resistance—there is no central point, such as a major financial institution or centralized exchange, that is vulnerable to attack. A third advantage is collusion resistance—it is difficult for participants in a large decentralized system to collude; corporations and governments, by contrast, have the power to act in ways that might not necessarily benefit common people. A decentralized system is also permissionless (anyone can use it), censorship resistant (no one can stop it), and open (anyone can verify the execution of a transaction).

DeFi has spawned new and creative financial products. For instance, a flash loan is a type of smart contract that typically involves borrowing without collateral, using that money for a transaction, and then returning the borrowed amount, all for a fee that is usually very small. A flash loan is initiated, executed, and completed essentially instantaneously. The key element of a flash loan is that all elements of the contract are executed serially in a batch operation on Ethereum. This eliminates default risk—if the loan is not repaid, the entire set of transactions is nullified. Since it is instantaneous, a flash loan also involves no liquidity risk—if any of the parties in a transaction could not meet their commitments, the flash loan would simply disintegrate, rolling back all of the operations.

A flash loan can be used to arbitrage among assets or across markets without having the principal needed to execute the arbitrage. Such arbitrage behavior can actually make markets more efficient by eliminating price differentials, so flash loans might serve a useful purpose. Flash loans can also be used to refinance loans and other operations that involve swapping various kinds of assets and liabilities.

One of the broader attractions of DeFi is a feature referred to as permissionless composability. This means that a developer can easily, and without having to seek permissions, connect multiple DeFi applications built on open-source technology to create new financial products and services. For example, a user can deposit cryptocurrency into a loan contract, withdraw some stablecoins collateralized by that deposit, and put those stablecoins in a yield-bearing contract. Multiple users pooling their stablecoins could

even build a savings game on top of that structure—all of the interest earned on the pooled stablecoins is awarded to a lucky winner, with everyone else getting their initial deposits back. In principle, compliance tools can also be plugged into such a structure to ensure regulatory compliance in each relevant jurisdiction.

DeFi certainly has the potential to expand the frontier of finance and democratize it. However, while DeFi protocols are already dealing in large amounts of money, there are many questions about whether DeFi operations can be scaled up to rival traditional financial institutions in any serious way.

DeFi diminishes some risks while creating new ones. Since flash loans are instantaneous, default and liquidity risks are minimized. Moreover, computer tools can perform rigorous economic risk assessments of smart contracts and specific DeFi products. Despite the open-source nature of DeFi applications, which should help expose and eliminate security and other weaknesses, there are many residual risks. Sophisticated hackers have been able to take advantage of technical and design vulnerabilities in DeFi products. Malevolent agents can exploit the larger "attack surface" created when combining multiple applications. Other risks that could undermine confidence include software bugs and users who do not fully understand the risks of such products.

Blockchains are self-contained but need information about prices and ownership of assets to execute certain transactions. Computer programs called oracles obtain such off-chain information and also pass on-chain information back to the real world. Oracles are vulnerable to technical risks, including hacks, and to problems with external data providers.

Certain hacks are difficult to thwart because decentralization implies the absence of a central authority to police such behavior or put in place safeguards. DeFi relies on idealistic libertarian norms, such as its own rule of law, with the community creating and enforcing rules that are in the broad interests of stakeholders. In reality, nascent blockchain systems are vulnerable to governance capture by small groups of stakeholders who could twist rules in their favor.

FINANCIAL REGULATION The approaches of governments and central banks to permitting and regulating cryptocurrencies span a wide spectrum. One question for financial regulators is whether there are implications for institutions that fall within their regulatory ambit or if there are any other systemic implications that merit their intervention. Another set of concerns arises regarding whether cryptocurrencies can be used for money laundering, tax evasion, and illicit commerce.

The regulatory responses can be classified into three broad categories. First, a number of countries do not limit the trading or use of cryptocurrencies but are endeavoring to create a framework in which to regulate them and related financial products. The United States regards Bitcoin and other cryptocurrencies as financial assets that are subject to tax laws as well as anti–money laundering (AML) regulations and regulations designed to combat the financing of terrorism (CFT). Canada and Japan have explicit laws concerning the trading and use of cryptocurrencies.

Second, a number of countries have either limited or banned the use of cryptocurrencies altogether. China banned domestic Bitcoin exchanges when it was trying to restrict speculative capital outflows in 2017 and subsequently blocked access to cryptocurrency exchanges. China also banned domestic ICOs, along with prohibiting individuals and institutions from participating in them. In April 2018, India's central bank, the Reserve Bank of India, prohibited banks, financial institutions, and other regulated entities from dealing in virtual currencies, although this was overturned by the country's supreme court in 2020.

A third approach, adopted by the majority of countries, is passive tolerance. This involves not banning cryptocurrencies but discouraging their use by financial institutions and, in many cases, not clarifying the legal status of such currencies even as means of payment. The lack of regulatory clarity often serves as an effective deterrent to the wider use of cryptocurrencies. It stifles innovation as entrepreneurs fear running afoul of the law and discourages investors who lack protection and fear being taken advantage of by unscrupulous operators. Indeed, government oversight can be a powerful tonic in building confidence that cryptocurrencies and related financial products will at least not easily become scams.

The US experience is a useful illustration of the range of financial activities facilitated by cryptocurrencies and the potential for gaps in regulatory oversight to remain as regulators sort through jurisdictional issues.

US law does not yet provide for direct, comprehensive federal oversight of Bitcoin and other cryptocurrencies or the exchanges on which they are traded. State banking regulators oversee certain US and foreign virtual currency spot exchanges largely through state money transfer laws. The Internal Revenue Service treats virtual currencies as property, which means that cryptocurrency holdings have to be reported on income tax filings and they are subject to capital gains taxes. The Treasury's Financial Crimes Enforcement Network (FinCEN) monitors Bitcoin and other virtual currency transfers, focusing on AML/CFT and know your customer requirements.

The SEC has ruled that Bitcoin and Ether are not securities and therefore do not fall under its regulatory purview. If these cryptocurrencies were to be bundled into investment vehicles such as exchange-traded funds, however, they would become traded securities subject to SEC regulation. The SEC also has the authority to oversee ICOs because they typically involve the offer and sale of securities.

The Commodity Futures Trading Commission (CFTC) has declared virtual currencies to be commodities subject to oversight under its authority under the Commodity Exchange Act. Cryptocurrency futures and options fall within its regulatory ambit, but the agency has only limited jurisdiction over spot markets for cryptocurrency trading; it is entitled to act only against fraud, market manipulation, and failure to deliver the commodity.

As Bitcoin and other cryptocurrencies, along with the technologies underpinning them, start playing a bigger role in financial markets, issues of regulatory jurisdiction and the potential for regulatory gaps take on greater significance. One example that illustrates this problem is that the CFTC seems to regulate spot markets for cryptocurrencies and cryptocurrency-related assets mainly through aggressive enforcement. It appears that the agency does not have the power to proactively set standards for spot markets or require dealers to comply with the CFTC's requirements. This is a consistent theme as many of the efforts of regulatory agencies seem to involve interpreting existing statutes and legislation to bring cryptocurrency-related activities into their regulatory ambit rather than developing new standards and statutes that address some of the novel aspects of cryptocurrencies and the financial products they are spawning.

The president's executive order on digital assets, which was issued in March 2022, sets out an ambitious agenda for regulating cryptocurrencies, stablecoins, and blockchain-based finance, potentially giving the United States a key role in defining global standards in these areas. By design, this is a document that provides a comprehensive overview of a path to regulating new financial technologies and products in a manner that allows potential benefits to be realized while mitigating risks to consumers, businesses, and overall financial stability. This still leaves open the difficult challenges of assigning responsibility across agencies for regulating particular products and technologies while also developing specific regulatory policies that balance the needs of facilitating innovation while reducing risks.

Cryptocurrencies may also require greater coordination and harmonization of regulatory efforts across national regulators. While some cryptocurrency exchanges are nominally domiciled in specific countries, the nature

of these virtual currencies makes it difficult to subject them to national rules and regulations, especially with respect to investor protection.

REFERENCES FOR THE PRASAD COMMENT

Harvey, Campbell R., Ashwin Ramachandran, and Joey Santoro. 2021. *DeFi and the Future of Finance*. Hoboken, N.J.: John Wiley and Sons.

Prasad, Eswar S. 2021. *The Future of Money: How the Digital Revolution Is Transforming Currencies and Finance*. Cambridge, Mass.: Harvard University Press.

GENERAL DISCUSSION Robert Hall said that the complexity of decentralized finance (DeFi) will make it difficult to implement clear regulations, and that DeFi practitioners are likely to find workarounds to any regulations that are imposed. He also discussed the similarities between DeFi and existing technologies. For example, he noted that the concept of smart contracts already exists, since lawyers can create legally binding agreements via word processing software. Hall also pointed out that stablecoins are almost identical in their function to money market mutual funds. He explained that runs on money market funds occurred during the global financial crisis because they ignored provisions of the Investment Company Act of 1940, and that stablecoins do not provide any additional benefits compared to well-regulated money market funds. Hall described DeFi as a dead end.

Antoinette Schoar replied that crypto technologies are still in their early development. She mentioned that smart contract platforms have the potential to facilitate new types of transactions and offer increased openness, scale, and simplicity compared to current payment systems. However, she noted that many types of transactions do not need the permissionless and anonymous features of the Bitcoin blockchain, and that the benefits of these technologies could be obtained via a regulated system that addresses their externalities. With regard to smart contracts, Schoar explained that their self-executing nature requires them to be complete contracts ex ante, since there is no method for obtaining ex post remediation via the legal system. She remarked that this offers potential benefits—including as a self-commitment mechanism or to reduce legal costs—but does not allow disadvantaged parties to lodge legal complaints or be made whole if they were defrauded.

Donald Kohn agreed with Hall that the regulation of stablecoins could be dealt with similar to money market funds. Kohn wondered about other potential financial stability issues related to DeFi applications. He asked