

This brief is part of a series produced by the Digital Finance Project Team (DFPT)
of the Bretton Woods Committee's Future of Finance Working Group (FFWG)

DeFi Technology

OPPORTUNITIES AND CHALLENGES

By Greg Johnson, Adam Schneider and Marsha Vande Berg

INTRODUCTION

This brief from the Digital Finance Project Team (DFPT) examines the unique features of the underlying technologies that support the digital finance ecosystem. From blockchains and their consensus protocols to smart contracts and their wide variety of uses, the spectrum of new and repurposed technologies is growing exponentially and has the potential to disrupt many traditional financial service activities. This brief explores how these technologies could reduce costs, mitigate systemic risks, and facilitate innovative business models. It also examines the limitations and shortcomings that need to be addressed for these technologies to achieve their full potential.

For the reader's convenience, a glossary of key digital finance terms used in this brief is included at the end of this paper.

BACKGROUND

Blockchain technology serves as the foundation of digital finance. Blockchain builds upon the ledger system of finance, which began in the ancient world and blossomed with the invention of double-entry bookkeeping in the Italian Renaissance. Blockchain can be viewed as the next evolutionary step in the double-entry ledger system—but one that could only

exist in a world where computer networks are global and ubiquitous.

Arguably, few white papers today have had greater impact than *Bitcoin: A Peer-to-Peer Electronic Cash System*, authored and published by Satoshi Nakamoto in 2008. This document formed the blueprint for much of digital finance as we know it today. While Satoshi is a pseudonym and the author remains anonymous, this white paper outlines the key notions and principles that underpin the development of Bitcoin. These include seminal works by pioneers S. Haber, N. Szabo, W.S. Stornetta, R.C. Merkle and W. Feller, each of whom is credited with prior advances in cryptography, smart contracts, hashing, and game theory.

Also noteworthy is that the timing of Satoshi's white-paper coincided with the Global Financial Crisis which is widely considered purposeful. The launch of Bitcoin and the ensuing decentralized finance (DeFi) technologies represent a direct response to the erosion of confidence in financial and governmental institutions caused by that crisis.

Today, DeFi has become ubiquitous and diverse. Blockchain and related technologies now reach audiences in the public, private, and nonprofit sectors. They have given birth to a new lexicon as well as a range of

businesses and commercial models dedicated to specific segments of the digital finance industry. These include centralized digital exchanges, such as Gemini, Coinbase, FTX, and Binance; decentralized crypto exchanges, or DEXs, such as Uniswap, PancakeSwap, 1inch, and DeFi Swap; crypto miners, such as Riot, Bitfury, and Marathon Digital; cash and investment products that substitute for traditional financial instruments, such as Circle's USDC (a dollar-denominated "stablecoin"); and dedicated research companies, such as Chainalysis, Elliptic, and TRM Labs.

BLOCKCHAIN BASICS

A blockchain is a public digital ledger of transactions maintained and verified by a decentralized network of computers using a consensus mechanism to validate transactions. Every computer within a blockchain network maintains its own copy of a shared ledger, and thus it is virtually impossible to alter completed transactions or manipulate the ledger as long as no group controls more than half of the network. Whereas a traditional ledger is controlled by its sponsor (e.g., a financial institution), the blockchain is decentralized and is only secured by cryptography. While technological advances such as quantum computing may ultimately challenge cryptography in the future, today it is the fundamental pillar supporting the DeFi industry.

Blockchains do not rely on authorities such as banks to enable users to transact in a secure and verifiable fashion. Instead, blockchain technologies rely on consensus mechanisms for their operations; the network of computers must agree before posting a transaction. One type of consensus mechanism is called proof of work (PoW), a model popularized by the Bitcoin blockchain network. At its core, Proof of Work (PoW) relies on a process of computational "mining," in which participating miners utilize computer hardware to solve complex

cryptographic puzzles to confirm and add transactions to the ledger. For this work, they are compensated with distributions of the network's underlying cryptographic token—in this example, a bitcoin—which is stored in a "wallet," a digital address on the blockchain that is not tied to a financial institution.

Initially, mining was performed using personal computers, and only a small community of early adopters participated. Over the past decade, as the complexity of computation and the value of the rewards have grown, most mining is now performed by large "mining farm" and "mining pool" entities using sophisticated hardware designed for the sole purpose of mining cryptocurrencies.¹

SMART CONTRACTS

But ledger recordkeeping is not enough—who initiates the transactions themselves? In traditional finance, a bank might receive funds and add them to a customer's account balance. In contrast, in the DeFi ecosystem, smart contracts are the primary mechanism used to generate transactions. In 1994, noted cryptographer and computer engineer Nick Szabo used the term *smart contract* to describe a computer program that executes tasks when a preestablished set of conditions is satisfied without the need for third-party intervention. It is analogous to the programs used by financial institutions to update a balance but instead of being "part of the bank" it is a public set of code and protocols. Today, smart contracts can be used to perform many real-world transactions, and this technology has garnered considerable attention and capital investment. For example, smart contract technologies are at the core of the widely publicized non-fungible token (NFT) industry, have fueled the growth of the Ethereum blockchain, and are used to execute transactions to purchase and sell cryptocurrencies.

¹ Estimated to exceed \$2 billion in 2021. Brandessence Market Research, *Cryptocurrency Mining Market Size* (London: Brandessence Market Research, 2022), <https://brandessenceresearch.com/cryptocurrency/cryptocurrency-mining-market>.

BENEFITS AND CHALLENGES FOR THE FINANCIAL SYSTEM

While the distributed nature of DeFi and the power of its associated concepts creates an opportunity to reduce society's reliance on financial institutions, it is also a capability that can be used by existing financial institutions in select areas to become more efficient. For traditional firms, blockchain technologies can increase coordination across geographies, across institutions and across customers, simplifying the chain of financial intermediaries. There is enormous potential to improve coordination, security and accuracy in tracking transactions.²

For example, Broadridge, a major financial industry processor, has created a blockchain-based capability for the global repurchase agreement market. Through increased efficiency and reuse of collateral, the company expects that platform users will save up to \$1 million for every 100,000 repo trades per year—solely as a result of the new business model enabled by its technology.³ Another example is Celo, which aims to reduce income inequality and support global philanthropy with a payments platform that makes DeFi products available on mobile devices.⁴

For institutions, the technology has a number of attractive features:

- It supports collaboration. Multiple parties have access to identical information and can build processes based on this real-time access. Instead of multiple copies of information and enormous reconciliation work, there is the possibility of improving business processes to rely on a single source of truth even across entities.

- Transactions are processed in real time. Instead of being settled in a daisy chain across multiple firms with their own processing timelines, transactions can be processed to completion immediately. For example, Oliver Wyman and J.P. Morgan estimate that using a multicurrency central bank digital currency network has the potential to reduce the cost of cross-border fund transfers by up to 80 percent, relative to today's system of multiple banks with multiple settlement windows.⁵
- Data are immutable and transparent, allowing organizations to "trust" that shared data are correct, including accurate history and full auditability. This is valuable in providing trading partners with trusted data on transactions and has become an important tool for managing supply chains.
- Data do not need reconciliation. There is only a single version of the facts, rather than disparate databases that must repeatedly be compared and reconciled.

OUTSTANDING CHALLENGES

Despite these favorable attributes, fundamental challenges persist with blockchain technology and its use. Some of the core challenges include the following:

- Blockchain technology is only as good as the coding that drives it, and code is rarely perfect. Smart contracts execute autonomously and must rely on information presented to perform transactions and obtain information, using "oracles." Both oracles and the smart contract code can be exploited; the smart contract code may have a

2 See, for example, Deepika Sharma, Natalya Thakur, Dawn Fitzpatrick, Michael Kruse, and Adam Schneider, *Emerging Digital Financial Ecosystem and Positive Use Cases* (Washington, DC: Bretton Woods Committee, 2022), https://www.brettonwoods.org/sites/default/files/documents/2022-06-19_DFPT_Brief_II_Final.pdf.

3 Broadridge, *2021 Sustainability Report* (Lake Success, NY: Broadridge, 2021), https://www.broadridge.com/_assets/pdf/broadridge-sustainability-report-2021.pdf.

4 Versions of this technology also can be implemented in more traditional ways. For example, a bank may prefer a private, permissioned chain so that only its customers can use it to process transactions. This may enable institutions to perform basic functions more efficiently, such as Know Your Customer.

5 Jason Ekberg, Tek Yew Chia, Michael Ho, and Laura Liu, "Unlocking \$120 Billion Value in Cross-Border Payments," Insights, Oliver Wyman, <https://www.oliverwyman.com/our-expertise/insights/2021/nov/unlocking-120-billion-value-in-cross-border-payments.html>.

flaw, or the data it receives may be incorrect. And as smart contracts are public, it is relatively easy for malicious actors to study their code and look for weaknesses.

- DeFi implication: There have been many such attacks, which serve as a reminder that DeFi is in its infancy, that digital technologies are not a panacea, and that the skill and integrity of the coders and testing processes are of critical importance.
- Traditional finance implication: Traditional methods of evaluating and securing systems may remain a competitive advantage, for example, using Model Risk Management techniques in this domain.
- Another challenge is the lack of adequate safeguards and legal recourse. A Bitcoin wallet is a string of text; lose this text and your assets are inaccessible. The technology inherently allows the ownership of addressees used in a wallet to remain unregistered, so there is potential for abuse by criminals or for money laundering. And many products that use blockchain to record ownership trumpet the fact that the record is immutable—but in fact that immutable record simply “points” to an asset, instead of instilling legal ownership.
 - DeFi implication: A much more robust governance and ownership structure will need to be created.
 - Traditional finance implication: Governance and ownership structures are well defined, and there is a set of “safety nets” using a well-defined legal framework; this may be a source of competitive advantage.
- A related challenge is the state of regulation. DeFi is not easily made compatible with many

of the regulatory requirements of the traditional financial system, such as Know Your Customer rules and defining title of ownership, because in its most straightforward form it operates outside these requirements.

- DeFi implication: Significant activity may be pushed outside the regulatory perimeter—which might lead to greater fraud and loss or loss of trust in the efficacy of the new technology and its way of doing business. Alternatively, DeFi firms will need to work with regulators to establish appropriate guardrails and safeguards that are compatible with the new decentralized ecosystem.
- Traditional finance implication: Coherent regulatory frameworks that support trust and reliability may be a persistent source of advantage.
- Another challenge is the vast amount of electricity that some of the consensus mechanisms consume. For example, industry watchdogs have concluded that Bitcoin mining accounts for more than 140 terawatt-hours (TWh) per year, or roughly the equivalent of the annual electrical consumption of Argentina or Norway.⁶
- Another challenge has been difficulty in scaling. The original bitcoin blockchain has very limited throughput compared to traditional technologies, requiring software firms to build additional capabilities to speed the blockchain or change its structure and use new blockchains to achieve volume goals.
- Yet another challenge is systemic governance. Who is in charge in a decentralized environment? Is your record and asset really defined by

⁶ See Jeremy Hinsdale, “Cryptocurrency’s Dirty Secret: Energy Consumption,” *State of the Planet*, Columbia Climate School, May 4, 2022, [https://news.climate.columbia.edu/2022/05/04/cryptocurrency-energy/#:~:text=How%20much%20energy%3F,of%20Argentina%2C%20population%2045%20million](https://news.climate.columbia.edu/2022/05/04/cryptocurrency-energy/#:~:text=How%20much%20energy%3F,of%20Argentina%2C%20population%2045%20million;); and John Schamidt and Farran Powell, “Why Does Bitcoin Use So Much Energy?” *Forbes*, May 18, 2022, [https://www.forbes.com/advisor/investing/cryptocurrency/bitcoins-energy-usage-explained/#:~:text=It's%20estimated%20that%20Bitcoin%20consumes,terawatt%2Dhours%20\(TWh](https://www.forbes.com/advisor/investing/cryptocurrency/bitcoins-energy-usage-explained/#:~:text=It's%20estimated%20that%20Bitcoin%20consumes,terawatt%2Dhours%20(TWh).

code? Should coders, for example, have fiduciary responsibility?⁷

- DeFi implication: “In code we trust” may not be a long-term business model.
- Traditional finance implication: Sound governance may be a source of competitive advantage.
- And finally, DeFi has an insufficiently tested model for data ownership. While the blockchain attributes of openness and full transparency are appealing, financial institutions today store data privately with permissioned and limited access. Moving all data to public view is a significant change in the established operating model and has privacy and societal implications.

The DeFi industry is hard at work addressing many of these shortcomings. For example, the Ethereum network transitioned to a new operating model in September 2022, from “proof of work” to “proof of stake,” which dramatically lowered energy use and facilitated much greater scale and throughput. Given that Ethereum is the world’s second-largest blockchain network, this is a significant advance.

But building robust safety nets will continue to be a concern. It should be noted that in the traditional financial sector the institution itself—its balance sheet, business model, and required regulatory safety net—clearly help mitigate the impact of flaws in code or attacks by malicious entities. It is required that systems are audited, models are validated, and many types of customer accounts are insured. In DeFi, these safety nets are less prevalent or nonexistent, and DeFi users are much more exposed to risk. One recent example is Terra’s Luna stablecoin, a product in principle similar

to a bank deposit. But it imploded in a few days, wiping out billions of dollars of owners’ investment.

CONCLUSION

It is still unclear whether the future will belong to DeFi or whether traditional financial institutions will successfully adopt blockchain technology to their own advantage. Will customers flock to crypto wallets and DeFi? Will the technologies enable incumbent firms to reengineer their capabilities in ways that allow them to expand their product offerings and reduce costs? Will standards develop that provide a level of consistency and quality for smart contracts?

Recent signs of collaboration between traditional institutions and blockchain innovators suggest that may be a robust path forward. For example, in February, Fidelity Investments, the third-largest manager of 401(k) assets, announced its intention to include bitcoin in its retirement plan platform. And in August, BlackRock, the world’s largest asset manager, announced a joint venture with the crypto exchange Coinbase to offer Bitcoin to BlackRock’s clients. Indeed, these types of decisions are likely to trigger increased investment in the infrastructure that digital technology needs to succeed—including greater investment in compliance, risk management, and governance.⁸

If such a transition occurs, will it unfold in a slow, evolutionary way or will it be destabilizing?

This question underscores the need for global regulators to address the regulatory and supervisory challenges that blockchain technology has created. The global regulatory environment for DeFi is still being developed and is currently incomplete and inconsistent. While President Biden’s recent executive order and focus by

7 For opposing viewpoints on whether protocol developers should be held accountable as fiduciaries, see Raina S. Haque, Rodrigo Seira Silva-Herzog, Brent A. Plummer, and Nelson M. Rosario, “Blockchain Development and Fiduciary Duty,” *Stanford Journal of Blockchain Law and Policy*, June 28, 2019, <https://stanford-jblp.pubpub.org/pub/blockchain-dev-fiduciary-duty/release/1>; and Angela Walch, “In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains,” in *Regulating Blockchain: Techno-Social and Legal Challenges*, edited by Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos, and Stefan Eich (Oxford, UK: Oxford University Press, 2019), 58–82, <https://doi.org/10.1093/oso/9780198842187.003.0004>.

8 Wayne Duggan, “Bitcoin Is Coming to Your 401(K),” *Forbes*, May 2, 2022, <https://www.forbes.com/advisor/investing/cryptocurrency/bitcoin-401k/>; Q.ai, “Coinbase and BlackRock Cozy Up on Bitcoin Bandwagon,” *Forbes*, August 5, 2022, <https://www.forbes.com/sites/qai/2022/08/05/coinbase-and-blackrock-cozy-up-on-bitcoin-bandwagon/?sh=5699b7fc3cba>.

the major US regulatory organizations are positive steps forward, there is still no well-defined and consistent set of regulations for DeFi, digital assets, or consumer protection, or even with respect to who will have regulatory authority and jurisdiction.

With this lack of regulatory clarity in mind, the DFPT has also recently examined what needs to be done in terms of regulation and supervision to protect customers and investors and to ensure robust market function and financial stability.⁹

GLOSSARY OF KEY DIGITAL FINANCE TERMS

Application-Specific Integrated Circuit (ASIC)

A device designed for the sole purpose of mining cryptocurrencies.

Blockchain

A distributed ledger system. A sequence of blocks, or units of digital information, stored consecutively in a public database. The basis for cryptocurrencies.

Byzantine Generals' Problem

A situation in which communication that requires consensus on a single strategy from all members within a group or party cannot be trusted or verified.

Central Bank Digital Currency (CBDC)

A CBDC is a digital currency issued by a central bank whose status as legal tender depends on government regulation or law. Can be retail or wholesale.

Consensus

Consensus is achieved when all participants in the network agree on the order and content of the blocks in the blockchain.

Cryptocurrency

Cryptocurrencies are digital assets that use cryptographic technologies to secure their operation. They can provide various financial services (e.g., security, commodity, payments instrument).

Decentralized Finance (DeFi)

A movement encouraging decentralized alternatives to traditional, centralized forms of financial services.

Distributed Ledger Technology

A database that is shared by multiple participants in multiple places. The basis for blockchains.

Exploit

A situation in which code or a computer program does not operate by design because it has been taken over by a bad actor.

Fork

A fork, or chain split, creates an alternate version of the blockchain, leaving two blockchains to run simultaneously.

Governance

In the world of cryptocurrencies, governance is defined as the people or organizations that have decision-making powers regarding the project.

Hash

A hash is the output result of a hashing algorithm, which creates a unique, fixed-length string to encrypt and secure a certain selection of arbitrary data.

Merkle Tree

A tree structure in cryptography, in which every leaf node is labeled with the hash of a data block and every nonleaf node is labeled with the cryptographic hash of the labels of its child nodes.

Miner

A contributor to a blockchain taking part in the process of mining. Miners can be professional miners or organizations with large-scale operations, or hobbyists who have set up mining rigs at home.

Node

A node is the most basic unit and a critical part of blockchain infrastructure, storing its data and allowing all communication/transaction flow to pass through it.

⁹ Richard Berner, Douglas Elliott, Mahesh Kotecha, *Investor Protection, Market Integrity, and Financial Stability in Digital Finance* (Washington, DC: Bretton Woods Committee, 2022), <https://www.brettonwoods.org/>

Peer-to-Peer (P2P)

A P2P network is a distributed network in which computer systems communicate with each other to share data or tasks. This means that two or more parties that agree to deal with each other are sufficient for the whole process to occur.

Proof of Stake (PoS)

PoS involves miners validating additional blocks based upon their share of the cryptocurrency locked up in the system. PoS is emerging as one of the most widely used and important blockchain consensus mechanisms. PoS networks incentivize their participants to stake native coins to help drive network functions. Although they are a relatively newer model, PoS networks are proving that they can be not only faster and more scalable than proof of work (PoW) blockchains but also far more energy-efficient.

Proof of Work (PoW)

A blockchain consensus mechanism involving the solving of computationally intensive puzzles to validate transactions and create new blocks.

Smart Contract

A computer protocol intended to facilitate, verify, or enforce a contract on the blockchain without third parties.

Zero-Knowledge Proof

In cryptography, a zero-knowledge proof enables one party to provide evidence that a transaction or event happened without revealing private details of that transaction or event.



Future of Finance Working Group

CO-CHAIRS: William C. Dudley and Afsaneh Beschloss

Digital Finance Project Team

CO-LEADS: William C. Dudley and Carolyn Wilkins

Daniela Bassan, Richard Berner, Bill Coen, Larissa Delima, Douglas Elliott, Jonathan Everhart, Diana Farrell, Dawn Fitzpatrick, Daniel Gleizer, Daniel Goldman, Michael Greenwald, Sarah Hirsch, Greg Johnson, Mahesh Kotecha, Teresa Kong, Michael Kruse, Kay Lazidis, Caitlin Long, Sultan Meghji, Marsha Vande Berg, Jonathan Padilla, William Papp, Franco Passacantando, Daniel Runde, Jason Schenker, Adam Schneider, Deepika Sharma, Andrew Slack, Heather Smith, Lynn Thoman, Kunal Thakur, Natalya Thakur, Tomicah Tillemann, Peter Tomozawa, Antonio Weiss, and Benjamin Weiss



THE BRETTON WOODS COMMITTEE
1701 K St NW #950, Washington, DC 20006
www.brettonwoods.org