DEFI'S PROMISE AND PITFALLS

Decentralized finance could support a new financial infrastructure if challenges are overcome

Fabian Schär

Digital innovation has brought major improvements to the financial system. But the system's architecture remains essentially the same. It's still centralized.

Decentralized finance (DeFi) offers an alternative. It uses public blockchain networks to conduct transactions without having to rely on centralized service providers such as custodians, central clearinghouses, or escrow agents. Instead, these roles are assumed by so-called smart contracts.

Smart contracts are instructions in the form of computer code. The code is stored on public blockchains and executed as part of the system's consensus rules. DeFi protocols can be designed in a way that prohibits intervention and manipulation. All participants can observe the rules before they engage and verify that everything is executed accordingly. State changes (for example, updates to account balances) are reflected on the blockchain and can be verified by anyone.

In the context of DeFi, smart contracts are used mainly to ensure the atomic (simultaneous and inseparable) transfer of two assets or to hold collateral in an

PHOTO: ISTOCK / ANNA BLIOKH

escrow account. In both cases, the assets are subject to the smart contract's rules and can be released only if the predefined conditions are met.

Making use of these properties, DeFi can mitigate counterparty risk and replicate numerous financial services without the need for intermediaries and centralized platform operators. This can reduce costs and the potential for errors. Lending markets, exchange protocols, financial derivatives, and asset management protocols are just a few examples.

Smart contracts can reference other smart contracts and make use of the services they provide. If, for example, an asset management protocol uses a decentralized exchange, incoming assets can be swapped as part of the same transaction. This concept, of actions across multiple smart contracts that can take place within a single transaction, is referred to as "intra-transaction composability" and can effectively mitigate counterparty risk (the likelihood that other parties will not fulfill their end of the deal).

Benefits of decentralization

Many advantages usually attributed to DeFi—or blockchains in general—can also be achieved via centralized infrastructure. Smart contracts are not limited to decentralized systems. In fact, the same standards and execution environments can be used on centralized ledgers. There are countless examples of the Ethereum virtual machine (a virtual machine that runs on all computers in the blockchain network and executes smart contracts) being employed alongside heavily centralized consensus protocols. Similarly, the same token standards and financial protocols can be used on centralized platforms. Even composability can work on such systems.

Moreover, well-managed centralized systems are much more efficient than public blockchains. That could lead to the conclusion that public blockchains and DeFi are inferior to centralized systems.

However, centralized systems rest on a very strong assumption: trust in intermediaries and institutions that are largely opaque. But such trust should not be taken for granted. History provides countless examples of corruption and errors within institutions. Yet, when economists discuss financial infrastructure and compare the properties of public blockchains with those of centralized ledgers, they usually assume centralized entities are benevolent, making it hard to see the benefits of decentralization.

Public blockchains are transparent. Because they are not controlled by a single entity, they can provide a neutral, independent, and immutable infrastructure for financial transactions. The code is stored and executed on an open system. All data are available and verifiable. This allows researchers and policymakers to analyze transactions, run empirical studies, and compute risk metrics in real time.

Most important, access is not restricted. This has two implications.

First, the absence of access restrictions provides a neutral foundation that cannot discriminate between use cases nor stakeholders. This is in sharp contrast to permissioned ledgers, whose rules are set by a centralized entity. Because it's so centralized, universally accepted standards may be hard to achieve, and the rights to access and use the infrastructure could easily be politicized. In anticipation of such problems, participants who feel that this may be to their disadvantage will not use the centralized infrastructure in the first place. Decentralized systems can mitigate these holdups, potentially preventing the problem of no, or minimal, cooperation.

Second, DeFi is built on a layered infrastructure (see Schär 2021). A decentralized ledger does not mean that everything deployed on top of it must be equally decentralized. There may be good reasons for access to certain tokens or financial protocols to be restricted or subject to intervention. These restrictions can be implemented at the smart contract level without compromising the general neutrality of the base infrastructure. However, if the ledger itself (settlement layer) were already centralized, it would be impossible to credibly decentralize anything built on top of it.

It is very likely that we will see a move toward ledgers that combine payments, tokenized assets, and financial protocols, such as exchanges and lending markets. DeFi is the first example of this development, but there will be similar developments in centralized infrastructure. The rationale is that intra-transaction composability works only if the assets and financial protocols are on the

Centralized systems rest on a very strong assumption: trust in intermediaries and institutions.

same ledger. There are strong network effects, and neither crypto assets nor central bank digital currencies would be particularly compelling if deployed on a ledger with no other assets or financial protocols. It is possible to create composable centralized infrastructure with additional assets and financial protocols, but it would be risky and difficult to govern given the challenges associated with permissioned ledgers. This makes a strong case for decentralization.

Challenges and risks

There are many advantages to be gained from DeFi, but there are challenges and trade-offs to be considered.

First, there is the risk of deception, or "decentralization theater." What is generally referred to as DeFi is, in fact, often heavily centralized. In many cases, DeFi protocols are subject to centralized data feeds and can be shaped or influenced by people with "admin keys," or a highly concentrated governance token allocation (voting rights). While partial centralization is not necessarily a bad thing, it is important to strictly differentiate between true decentralization and companies that claim to be DeFi when in fact they provide centralized infrastructure.

Second, immutability can introduce new risks. It might be harder to enforce investor protection, and smart contract programming errors can have devastating consequences. Composability and complex token wrapping schemes (Nadler and Schär, forthcoming) that resemble the rehypothecation of collateral contribute to shock propagation in the system and may affect the real economy.

Third, the transparent nature of the blockchain and decentralized block creation can be problematic from a privacy perspective. Moreover, it allows for the extraction of rents through generalized front-running—a phenomenon known as miner/maximal extractable value (MEV). Those who observe a transaction that contains an order to swap assets on a decentralized exchange can try to front-run (or sandwich) this action by issuing a transaction of their own. The front-runner thereby profits at the expense of the issuer of the original transaction. There are potential solutions that may at least partially mitigate this problem, but they involve trade-offs.

Finally, the scaling of public blockchains cannot be done easily without compromising some of their unique properties. Decentralized block creation inflicts severe costs. Hardware requirements to run a node can't be arbitrarily high, as this would price out many stakeholders and compromise decentralization. This limits on-chain scalability, pushing up transaction fees. This trade-off between security, decentralization, and scalability is usually portrayed as a trilemma. A potential solution is so-called Layer 2s. These are designed to move some of the burden away from the blockchain while allowing participants to enforce their rights on the blockchain in case anything goes wrong. This is a promising approach but, in many cases, still requires trust and various forms of centralized infrastructure.

DeFi still faces many challenges. However, it can also create an independent infrastructure, mitigate some risks of traditional finance, and provide an alternative to excessive centralization. The open-source nature of DeFi encourages innovation, and there are many talented people—academics and practitioners alike—working on these challenges. If they can find solutions without undermining the unique properties at the core of DeFi, it could become an important building block for the future of finance.

FABIAN SCHÄR is a professor of distributed ledger technology and fintech at the University of Basel and managing director of the Center for Innovative Finance.

References:

Schär, Fabian. 2021. "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets." *Federal Reserve Bank of St. Louis Review* 103 (2): 153–74. https://doi.org/10.20955/r.103.153-74.

Nadler, Matthias, and Fabian Schär. Forthcoming. "Decentralized Finance, Centralized Ownership? An Iterative Mapping Process to Measure Protocol Token Distribution." *Journal of Blockchain Research*. https://arxiv.org/abs/2012.09306.