Decentralized Finance—Opportunities, Challenges and Auditing of Smart Contracts

In recent years, the rapid development of blockchain technology and cryptocurrency has influenced the financial industry by creating a new crypto economy. The impact of this has been compounded by next-generation decentralized applications (DApps) that do not involve a trusted third party, which have emerged thanks to the appearance of smart contracts. Smart contracts are designed to facilitate, verify and automatically enforce negotiations and agreements among multiple parties. Despite the opportunities created by smart contracts, several challenges continue to undermine their adoption, such as security threats and execution. The auditing of smart contracts is evolving as the technology is increasingly adopted within the financial industry. Although there are no dedicated guidelines for auditing smart contracts at this time, there are several best practices that auditors can follow.

Despite the opportunities created by smart contracts, several challenges continue to undermine their adoption, such as security threats and execution. The auditing of smart contracts is evolving as the technology is increasingly adopted within the financial industry.

What Is Decentralized Finance?

Decentralized finance (DeFi) is a blockchain-based financial infrastructure that provides a trusted framework upon which computer code can be deployed to execute instructions as written. The term generally refers to a decentralized, open and highly interoperable protocol stack built on smart contract platforms such as Ethereum.

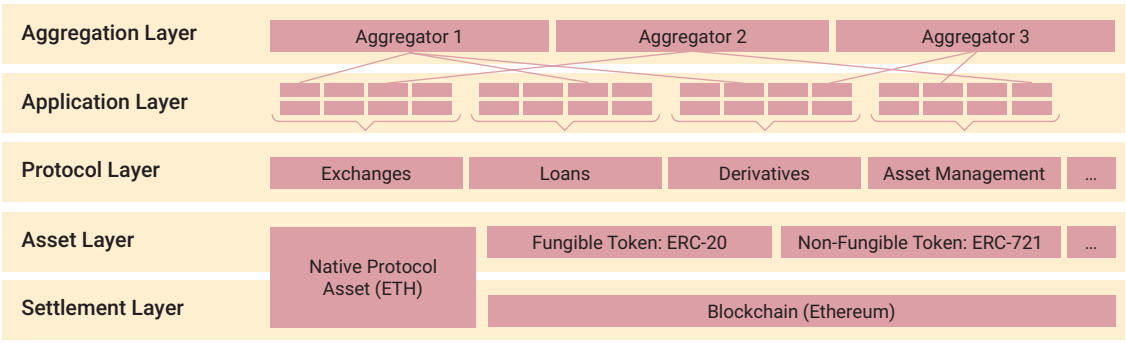
DeFi does not rely on intermediaries or a centralized institution because it is based on open protocols and DApps. Agreements are enforced by code, and transactions executed are verified by stakeholders. This architecture can create an interoperable financial system with transparency and little need for custodians or clearing houses as most of these roles are replaced by smart contracts, which are the backbone of all DeFi protocols and applications. **Figure 1** illustrates the DeFi stack, including the different layers that make up a DeFi network.[1]

PINKAL SHAH | CISA

Is a senior manager in risk assurance at PricewaterhouseCoopers (PwC) and has more than 10 years of experience in auditing various aspects of information systems for various sectors such as banking and financial services, telecommunications, manufacturing and retail, including with new technologies such as cryptocurrency. He has worked across different offices within PwC including India and Mauritius.

FIGURE 1

DeFi Stack



To better understand smart contracts, it is helpful to consider a typical server-based web application. When interacting with such an application, a user does not see the application's internal logic. Moreover, the user is not in control of the execution environment. Both the logic of the application and the user can be manipulated. As a result, the user must trust the application service provider (or in-house IT team's expertise in the case of in-house developed applications). Smart contracts mitigate both problems as they are computer-coded blockchain applications that can be publicly scrutinized. They work within the bounds of preprogrammed terms and conditions, which govern transactions between two or more parties in parallel, ensuring legitimacy. Smart contracts can act as custodians by storing crypto assets and determining how, when and to whom assets can be released, resulting in an ecosystem with a variety of different applications.

The DeFi ecosystem is slowly and steadily gathering momentum. The value of funds that are locked in DeFi-related smart contracts reached more than US$10 billion in 2021 (**figure 2**).[2] However, that sum is still a relatively small portion of the overall financial market. MakerDAO was one of the first decentralized stable coins to garner significant public attention. Subsequently, Aave, PhoenixDAO, Compound and Alchemix built on the ecosystem's growth to deliver financial services without financial intermediaries. They have gained traction by trying to bring existing financial systems into existing blockchain ecosystems.

DeFi vs. CeFi

Traditional centralized finance (CeFi) ecosystems are made up of centralized organizations that store funds in their custodial wallets and abide by local laws and regulations. Cryptocurrency trading is currently one of the most common activities enabled by centralized finance. In addition to cryptocurrency trading, services that fall under CeFi include borrowing, lending and margin trading. They may appear complex to consumers who are often unaware of the underlying rules or agreements that govern financial assets.[3]

> Cryptocurrency trading is currently one of the most common activities enabled by centralized finance.

DeFi is establishing a reputation as an ecosystem with the ability to provide transparency and interoperability due to its underlying integrity-protected blockchain.

Figure 3 illustrates the advantages of DeFi compared to CeFi.

Benefits of Smart Contracts in DeFi

There are many benefits of using smart contracts in banking and finance processes, including:

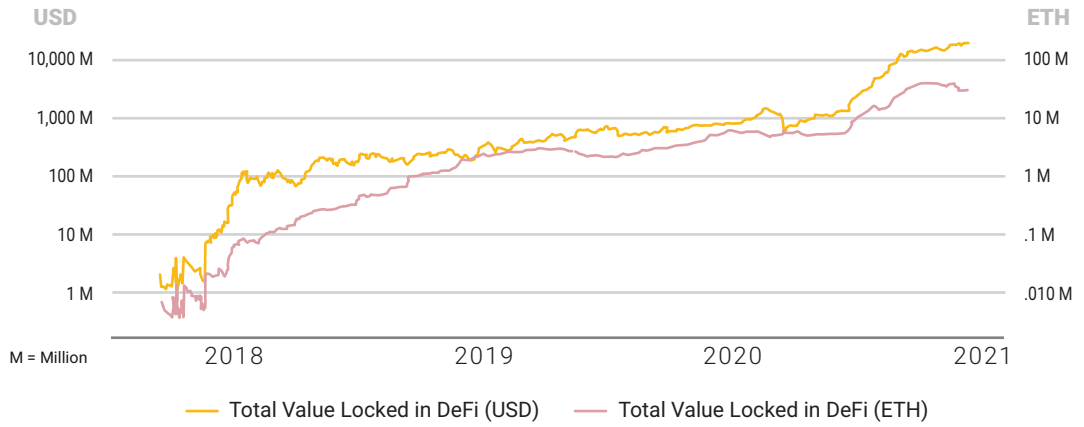
- **Lower transaction costs**—Transactions governed by smart contracts are self-regulated and reduce manual intervention resulting in lower transaction costs related to record keeping.
- **Transparency in auditing**—Smart contracts support advanced bookkeeping tools rather than using traditional manual bookkeeping, which involves a high volume of paperwork. They are based on distributed codes in blockchain and are incorruptible.

LOOKING FOR MORE?

- Read *Opportunities, Challenges and Auditing of Smart Contracts. www.isaca.org/blockchain-framework-audit-program*
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

FIGURE 2

Total Value Locked in DeFi Contracts (US$ and Ethereum [ETH])



Source: DeFi Pulse, *https://www.defipulse.com/*. Reprinted with permission.

- **Increased speed**—Because they execute automatically, smart contracts speed up banking operations by cutting down on unnecessary manual processes.
- **Accurate contracts**—Because there is no human intervention, chances of error are low, which can result in increased trust among the parties involved.
- **Streamlined know your customer (KYC) processes**—Banks or other financial institutions can verify customers' credit scores based on blockchain records and use that information to decide if they want to enter into a transaction with them.

Blockchain-powered smart contracts offer banks the ability to streamline trade clearing and settlement activities, which are labor-intensive and highly prone to errors.

- **Easy insurance claim processing**—Smart contracts facilitate easy claim processes and automatic validation through distributed ledgers on the blockchain network.
- **Peer-to-peer transactions**—Smart contracts offer convenience and reliability by enabling cross-border payments without the involvement of a third party or any intermediaries.

Use Cases for Smart Contracts in Financial Institutions

Uses of smart contracts in DeFi include:[4]

- **Improving KYC**—Obtaining customer credit histories under legacy systems is tedious and costly, but it is a necessary step to avoid financial fraud. A smart contract system can help banks streamline know your customer (KYC) operations. They can easily verify customer identity through records maintained on the blockchain and trace down an individual's credit history.
- **Monitoring lending with well-defined terms and conditions**—Many borrowers cannot meet the stringent criteria of traditional lending institutions. Deploying a smart contract system helps monitor the loans of such borrowers. Using distributed ledger technology (DLT), borrowers who do not qualify for a loan from a bank can borrow directly from investors, thus shortening the time frame for procuring loans. BlockFi, a crypto trading platform, even facilitates lending against cryptocurrency collateral with well-defined terms for interest payments.
- **Trade clearing and settlement**—Blockchain-powered smart contracts offer banks the ability to streamline trade clearing and settlement activities,

FIGURE 3

DeFi vs. CeFi

ADVANTAGES	DeFi	CeFi
Interoperability	DeFi applications can run on several blockchains, and applications can be built by combining DeFi applications.	There are several applications to manage day-to-day operations and some applications cannot be integrated, which can lead to major operational costs, which is often required for various reasons, from business to audit.
Transparency	DApps code is publicly available to view or to audit. All transactions on DApps are public and viewable by anyone. Most of the time the senders and receivers are anonymous on a blockchain.	Not all users can observe and verify the transactions because access is restricted to the people executing them.
Availability	DeFi applications are available 24/7 and the only requirement is an Internet connection for performing transactions.	CeFi is available during market hours when stocks or goods can be traded.
Autonomy	Everything for DeFi applications is done via smart contracts and no institution or central authority governs them. Once a smart contract is deployed on a blockchain, the application can self-execute. Customers can easily switch to another application if they do not like the existing DeFi application. This gives customers more power and responsibility.	Intermediary custodians keep the assets and monitor them on behalf of customers.
Disintermediation	No third-party intermediary is involved if the user's crypto wallet can interact directly with the smart contract.	

which are labor-intensive and highly prone to errors due to the number of parties involved in approval and reconciliation. Smart contracts help to avoid discrepancies and save costs by providing an efficient equity settlement system. The US financial industry is testing smart contract-based clearing and settlement systems with 40 global banks within the R3 consortium, which designs and delivers distributed ledger technologies to the global financial markets. R3 was founded in 2014 by nine banks including Goldman Sachs, Credit Suisse and JP Morgan. Similarly, the Australian Securities Exchange and the Depository Trust and Clearing Corporation (DTCC) are also working on a smart contracts-based post-trade platform.[5]

Key Challenges of Using Smart Contracts

Though smart contracts have many advantages, the new and still evolving technology also introduces unique risk and challenges. Key challenges encountered include:

- **Execution**—There is risk that something may go wrong during execution. For example, if there are coding errors, they may create vulnerabilities that allow an attacker to cause chaos. The average user will not be able to read the contract code. While audits and formal verification are partial solutions to this problem, a degree of uncertainty remains.
- **Operational security**—Many decentralized protocols use administrative (admin) keys, which allow a certain predefined group of individuals to upgrade the contracts or to perform an emergency shutdown. If the keyholders do not create or store their keys securely, there is a risk that the key will be compromised, which can compromise the smart contract. There is also a risk of corrupt employees performing malicious activities incentivized by potential monetary gain.
- **External data**—Many smart contracts are reliant on external data. Whenever a smart contract depends on data that are not natively available, the data must be provided by external sources. This can lead to centralized contract execution since the data are owned (and hence controlled) by the external party.[6]
- **Illicit activity**—A common concern among regulators is that individuals who want to avoid being monitored may take advantage of crypto assets. Although the network's pseudonym may provide some privacy, it can be abused by users with fraudulent intentions. On the other hand,

privacy may be a desirable attribute of some legitimate financial applications. Currently, central banks and regulators are not able to intervene or regulate because there is not wide scale use of DeFi commercially. There is debate about how regulators can find a reasonable solution that allows them to intervene when required.

- **Scalability**—Ethereum blockchain is regarded as relatively decentralized and secure; however, it struggles to keep up with the demand for storage. Increasing transaction fees and long confirmation times adversely affect the DeFi ecosystem. It is unclear if decentralized blockchain can keep up with the demand and provide a foundation for a transparent and unchangeable financial institution.
- **Hacking**—A major challenge of using smart contracts is their vulnerability to hacking due to poor coding. A bug in the smart contract code can create a unique emergency. In traditional software, bugs can be fixed with a patch, but it is not that simple for blockchain because transactions on the blockchain cannot be reversed. It is estimated that hackers have stolen a total of US$2 billion since 2017 due to hacking on Ethereum networks.[7] One way to counter hacking is through use of artificial intelligence (AI), which can monitor suspicious activity or known issues. Auditing tools are being developed to identify bugs before a smart contract is released. However, the risk of hacking will persist. Therefore, the goal is to reduce it to an acceptable level.

Auditing Smart Contracts

Auditing smart contracts involves conducting in-depth evaluations of smart contracts within blockchain applications. Audits focus on identifying and rectifying security vulnerabilities, design issues and code error. There are best practices for creating an ideal workflow for a smart contract audit, including:

- Understanding the specifications of the smart contract
- Testing
- Analyzing the output
- Reporting

Understanding the Specifications of Smart Contracts

The auditor and the organization first must agree on the specifications of the smart contract. The smart contract documentation should provide a clear explanation of the architecture, build process and design of the project/contracts. The auditor should look for the time of the code freeze,[8] which implies the finalization of the code. By then, auditors can expect that developers have identified and rectified any abnormalities in the source code.

The specifications should include commit hash cryptography and ensure that the auditor and developers have agreed on the code being audited. Developers need to provide assurance that any code changes after the code freeze will not affect the audit. If changes are complete, they should be logged, approved, monitored and reviewed by the organization.

Testing

Once the code freeze has been agreed on with the developers, the auditor can begin testing to assess the logic of the code and determine whether the code works effectively and without any major issues.

Testing offers a straightforward and simple approach to bug detection. A targeted code section can undergo unit testing. Integration testing is available for larger pieces of code.

There is also the option to run a test suite. If the code passes the test, then the auditor is less likely to find an issue. If there are issues in the code, the auditor should discuss them with developers and assess the impact on the business process's efficiency, cost and timing.

The line coverage in the code should also be tested. The auditor should conduct a review of the line coverage by checking the amount of code subject to evaluation. Many audit professionals will look for 100 percent line coverage; however, coverage between 85 percent and 90 percent[9] may be sufficient, depending on the auditor's judgment and the nature of the specific smart contract.

Analyzing the Output: Automated and Manual

When testing is completed, the auditor can begin analysis using automated tools (e.g., Solidity smart contracts) to streamline the audit process and improve the ease of identifying issues in the source code. Automated analysis helps the auditor focus on new and complex vulnerabilities.

With automated processes, there is an inherent risk of not understanding the intentions of the developers of the smart contract.

However, with automated processes, there is an inherent risk of not understanding the intentions of the developers of the smart contract. Therefore, manual inspection is necessary so that the auditor can perform various vouching activities by tracing the transactional document to the source or verifying against the source code to ensure that transactions are happening as per the rules defined in the smart contract.

Reporting

The final step is to create an audit report based on all steps performed. The auditor should discuss the report's findings with members of the product team so that they understand the key vulnerabilities and issues identified and the impact on the organization's reputational, financial and security risk. The auditor should also provide recommendations for overcoming the risk with appropriate procedures or controls.

Conclusion

DeFi offers exciting opportunities and has unleashed a wave of innovation. It consists of numerous applications and protocols wherein data are readily available, and individuals can verify every transaction. Developers are using smart contracts and decentralized layers to create trustless (i.e., one does not have to rely on a third party) versions of traditional financial instruments.

The auditing of smart contracts is in the early stages, but there is value in understanding how smart contracts operate, how to test the code used to develop a smart contract, how to use tools and technologies to identify error in the code, and how to provide detailed audit reports to management that include recommendations for how to rectify errors and overcome risk using appropriate controls.

However, with great potential comes certain risk. Smart contracts can contain security vulnerabilities that may allow malicious access, and scalability issues limit the number of users. Many protocols and applications require use of external data sources and special admin keys to manage the system. However, if these issues can be solved, DeFi may contribute to a robust and transparent financial infrastructure.

Endnotes

1 Shär, F.; "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets," *Economic Research: Federal Reserve Bank of St. Louis*, vol. 103, iss. 2, 2 May 2021, *https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets*

2 *Ibid.*

3 PricewaterhouseCoopers (PwC), *DeFi: Defining the Future of Finance*, China, June 2021, *https://www.pwc.ch/en/publications/2021/defi-defining-the-future-of-finance-may-2021.pdf*

4 Rupareliya, K.; "How Smart Contracts Are Transforming Banks and Financial Institutions," Business of Apps, 8 July 2021, *https://www.businessofapps.com/insights/how-smart-contracts-are-transforming--banks-and-financial-institutions/*

5 *Op cit* Shär

6 *Ibid.*

7 Orcutt, M.; "Once Hailed as Unhackable, Blockchains Are Now Getting Hacked," *MIT Technology Review*, 19 February 2019, *https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/*

8 Iredale, G.; "What Is a Smart Contract Audit?" 101 Blockchains, *https://101blockchains.com/smart-contract-audit/*

9 *Ibid.*