



**EMERALD**  
*DRIVEN BY RESEARCH*

White Paper

April 2021

## **“Decentralized Finance, the Category Killer?”**

Decentralized Finance is Reshaping the Financial Services Industry

By: Steven E. Russell, Esq.  
Vice President & Portfolio Manager  
Emerald Advisers, LLC

---

3175 Oregon Pike, Leola, Pennsylvania 17540  
Tel: 717-396-1116 • Fax: 717-556-8895  
[www.teamemerald.com](http://www.teamemerald.com)

# **Decentralized Finance, the Category Killer?**

## **Decentralized Finance is Reshaping the Financial Services Industry**

Decentralized Finance (DeFi) refers to the movement from traditional, centralized financial systems to a financial system driven by distributed ledger technology and a financial system built on “smart contracts” built on distributed ledger technology. Distributed ledger technology, sometimes incorrectly referred to as blockchain, is a database that is consensually shared, replicated, and synchronized. From lending and borrowing platforms to stablecoins and other digital tokens, the DeFi ecosystem has launched an expansive network of integrated protocols and financial instruments. As of April 25, 2021, the total value locked into the smart contracts of DeFi applications and protocols stood at more than \$54 billion. DeFi has emerged as the most active sector in the distributed ledger technology ecosystem with a wide range of use cases for individuals, developers, and institutions.

Traditional financial systems today run on centralized infrastructure that is managed by central authorities, institutions, and intermediaries. Distributed ledger technology provides for the application of smart contracts to be used to drive financial transactions on infrastructure such as the Ethereum blockchain. By deploying immutable smart contracts on decentralized ledger technology, DeFi developers can launch financial protocols and platforms that create an alternative financial system that can be more decentralized, innovative, interoperable, borderless, and transparent.

Smart contracts are essential to how distributed ledger technology will be used for financial services. A smart contract is a contract that has been translated into the software language of the distributed ledger, stored on the distributed ledger, and can be autonomously executed by a triggering event. The smart contract is essentially a series of if/then statements programmed and saved on the distributed ledger. Once the requirements of the smart contract are met, the contract will automatically be executed and the resulting action will be stored and shared across the distributed ledger. For example, a songwriter can sell a digital song at a certain price in an online music app. This agreement could be programmed into a distributed ledger as a smart contract. The smart contract will automatically distribute payment to the songwriter when a fan buys the digital song and capture the transaction in the distributed ledger.

We believe, to understand the technical aspects of distributed ledger technology (DLT) or blockchain, which is one type of DLT; it is helpful to explain the concept through an example. When an individual deposits a sum of money into a banking institution, the individual trusts that the sum will be there until they decide to exchange it for goods or services. The individual trusts the bank will have an accurate record of the transaction, such as the amount, depositor, date, and time of the deposit. More broadly, society relies on central repositories, such as banks or governments, to collect, maintain, and protect the recorded actions of individuals or institutions. Distributed ledger technology differs from centralized repositories in that it

decentralizes the source of trust. An individual deposits funds into a digital wallet and the value is captured on the DLT. If this individual purchases a digital song, the transaction is captured in the DLT along with the change in fund level in the digital account. The bank is not required as a trusted third party. The trustworthy record is recorded in the DLT shared by all the parties on the network.

During the development of distributed ledger platforms, system developers have the ability to program smart contracts that will render transactional data, or records, cryptographically inaccessible. This means the records are not deleted from the ledger, but are cryptographically redacted to block the data from general view.

Distributed ledger technology, while similar to databases, are not used for general data storage, but rather hold information about transactions. Sometimes the distributed ledger technology will contain the transactions themselves or may include the proof that the transaction is valid. The replication and storage of transactional data by each party, or node, in distributed ledger technology enables conflicts, or inaccuracies within the database, to be automatically resolved with predefined ledger rules.

We will now take a closer look at blockchain technology as an example of how distributed ledger technology works. Blockchain technology contains three core parts, the block, the chain, and the network.

The “Block” is a list of recorded transactions that remain on the chain forever. Transactions can represent virtually any type of activity from registering a land deed to a single purchase. Any rules relating to the block itself are established when the network is first created. For example, the maximum number of transactions in a block or the size of each block can be limited.

The “Chain” is created when the block reaches its maximum size of transactions; it is chained or linked to the preceding block through a “hash”. A hash is an algorithm that takes a variable string of data and generates a fixed length value. The hash value of one block is inserted into the next block. This makes a link between the new block and the previous block. Repeating a hash function on an unaltered block of data will always generate the same fixed-length value. If a block of data is altered, the resulting hash output will be different. A user can then see the hashes are different and will know the original block has been altered and may no longer be trustworthy.

The “Network” is a cluster of servers or “nodes” running a blockchain. Each node contains the complete record of all transactions on a blockchain. No centralized "official" copy exists and no node is "trusted" more than another is. The data integrity is maintained by the blockchain being replicated on all of the nodes. Each blockchain has its own rules or algorithms governing how nodes validate transactions intended for entry into the blockchain. These rules are called a consensus mechanism and are established when the blockchain is created. By embedding a consensus mechanism, blockchains create a way for parties who do not know if they can trust

each other to agree an entry should be added to the blockchain. This addresses the so-called Byzantine Generals Problem. The Byzantine Generals Problem describes a situation in which, in order to avoid catastrophic failure of a system, the system's actors must agree on a concerted strategy, but some of the actors are unreliable. Each blockchain has its own consensus mechanism depending on the type of transaction it is capturing. Some consensus mechanisms are known as "proof of work", "proof of space" or "proof of stake". The mechanisms facilitate authenticity, or the immutability of transaction records.

While the use of DeFi is still in the "early innings" and some would say the game has not even started, there have been some good examples of how the technology may be used moving forward. Exodus Movement, Inc., a Delaware corporation that has developed a leading non-custodial cryptocurrency software platform, received notice that the Securities and Exchange Commission has qualified its offering of Class A common stock under Regulation A. The company began offering shares in the Exodus Wallet at 9:00 pm ET on April 8 2021. The shares were listed for \$27.42 apiece, with a maximum investment of 2,733,229 shares. According to Exodus, the offering will close once the maximum offering amount of \$75 million has been reached. The crypto wallet company is already 96% toward reaching that target, with participation from over 4,000 investors. The most important aspect of the offering is that it has been done solely within a digital wallet rather than through a centralized investment-banking firm. Exodus will be the largest capital raise via a digital wallet, to date, but it was not the first. Blockchain project Stacks was the first crypto company to get permission from the SEC to conduct a token sale, raising \$23 million. Trading platform INX is in the middle of what it hopes is a \$117 million registered token offering.

Other commonly used distributed ledger technology applications include clearance and settlement systems as well as buying and selling assets. We believe distributed ledger technology like blockchain enable bank transactions to be settled directly and permanently recorded better than existing protocols such as the Society for Worldwide Interbank Financial Communications (SWIFT). An average bank transfer takes a few days to settle because it is limited by the way the financial infrastructure was built.

Moving money around the world is a logistical challenge to many banks. A simple bank transfer needs to bypass a complicated system of intermediaries such as custodial services before it reaches its destination. Moreover, the bank balances need to be reconciled across the global financial system, which comprises a broad network of funds, asset managers, traders, and more.

For example, if you would like to send money from an account in a German bank to one in the United States, that transfer will be executed through SWIFT. However, the centralized SWIFT protocol processes only the payment orders. The actual money is processed through a system of intermediaries. Each of them comes at an additional cost, creates additional friction, and extends the amount of time necessary to complete the transaction.

A decentralized ledger of transactions like blockchain enables banks to keep track of all the transactions publicly and transparently. Banks using blockchain do not need to rely on a network of custodial services and regulatory bodies like SWIFT. Using decentralized ledger technology, the banks simply settle transactions directly on a public blockchain.

Buying and selling assets like stocks, commodities, or debts are based on keeping track of who owns what. In a centralized financial system (CeFi), financial markets accomplish this through a complex network of exchanges, brokers, clearinghouses, central security depositories, and custodian banks. All of these different parties have been constructed around an outdated system of paper ownership. As a result, CeFi is not only slow but also riddled with errors and prone to deception. By removing the intermediary and asset rights transfer, we believe blockchain lowers the asset exchange fees and reduces the instability of the traditional securities market.

Executing such transactions electronically is complicated because most of the time, buyers and sellers do not rely on the same custodian banks, and these do not always rely on trusted third parties to hold onto all the paper certificates. Instead, when buying or selling an asset, the order will be relayed through numerous third parties and each party maintains its own version of the truth in a separate ledger. We believe the system is not only inefficient but also imprecise.

We believe blockchain will revolutionize financial markets by creating a decentralized database of digital assets. A distributed ledger allows transferring the rights of an asset through cryptographic tokens that can represent such assets off-chain. We believe that cutting out the intermediary will lower the asset exchange fees and accelerate the process significantly.

We believe that DeFi will significantly change the banking and financial services industry. Whether that happens in a year, five years, twenty years or beyond is yet to be determined. We do believe that to remain “relevant” and a part of the ecosystem, banks need first to develop the infrastructure required to operate a global network using matching solutions via distributed ledger technology. We believe banks must develop a working knowledge of DLT and commit to making the necessary investments today that we believe will eventually come with significant returns. Once fully adopted, we believe decentralized ledger technology will enable banking institutions to process payments faster and more accurately, all the while reducing transaction-processing costs. Overall, we believe decentralized ledger technology enabled banking applications will deliver a better customer experience and help traditional banking institutions to compete with fintech startups.

**Important Disclosure**

This report is furnished for the use of Emerald Advisers, LLC, its affiliates and its clients and does not constitute the provision of investment, legal or tax advice to any person. It is not prepared with respect to the specific investment objectives, financial situation or particular needs of any specific person. The information contained in this report was obtained from sources deemed reliable. Such information is not guaranteed as to its accuracy, timeliness or completeness by Emerald. Any opinions contained in this report represent the judgment of the authors as of the publication date. The information contained in this report and the opinions expressed herein are subject to change without notice. Past performance is no guarantee of future results. Neither the information in this report nor any opinion expressed herein constitutes an offer nor recommendation to buy or sell any security or financial instrument. Accounts managed by Emerald's affiliated advisory firms may take positions from time to time in securities discussed in its reports.