PraveenKumar Radhakrishnan

PraveenKumar Radhakrishnan, MSc, MBA, is lead manager, exponential technologies, head of BIP Consulting's blockchain practice. He has designed and developed a variety of blockchain projects including launching tokenised financial instruments on decentralised platforms.

Giorgio Alessandro Motta

Giorgio Alessandro Motta is BIP Consulting's specialist, exponential technologies. He has developed blockchain projects involving private and public blockchain to track and trace assets and develop new business models for diverse markets..

Decentralised finance

The new financial revolution

PraveenKumar Radhakrishnan and Giorgio Alessandro Motta

Blockchain technology, born in 2008 in the wake of the global economic crisis triggered by subprime mortgages, enabled a revolutionary new form of peer-to-peer exchange of monetary value—bitcoin. The philosophy of blockchain is disintermediating third parties from value chains by moving from a scenario where a central entity places users in an ambience of manufactured trust (think banks) to a 'trustless' system where the network is governed algorithmically.

This is not a standalone, monolithic technology, but rather an ensemble of technologies and concepts such as cryptography, digital cash, peer-to-peer networks, smart contracts, distributed ledgers, consensus mechanisms, economic networks and game theory.[1,2,3,4] However, the now-famous cryptocurrency—bitcoin—which started it all is not the be-all and end-all of the underlying blockchain technology, but merely an application.

Cryptocurrencies were the first application of blockchain technology. The year 2015 saw the advent of preconditioned transactions governed by *smart contracts*, a capability introduced by the blockchain network called Ethereum. Then came the wave of blockchain-based 'decentralised applications' or *dApps*, and *interoperability* [meaning two or more different systems can communicate and exchange value] between the various blockchain networks.

Today, the technology is going through another evolution-spurt, effectively cementing the evolution of the internet from being one of information to one of value through Decentralised finance (DeFi) as discussed by Swan et al in *Blockchain: Blueprint for a new economy*. The goal of this paper is to provide an overview of DeFi.

What is DeFi?

Staying true to the philosophy behind the conception of blockchain technology, DeFi disintermediates traditional, centralised financial models, enabling anyone with an active internet connection to participate. Typically built upon public blockchains, DeFi systems effectively cut out intermediaries such as banks, brokerages or other middlepersons who may introduce inefficiencies. Thus, DeFi blockchains algorithmically govern interactions between peers, permitting them to buy, sell, lend and borrow more efficiently and economically.

DeFi applications typically have three macro layers:

i) ***The application layer:*** this is where the user-interface to the application resides, permitting peers to buy, sell, lend or borrow while covering the complexities of the underlying layers

ii) ***The protocol layer:*** this layer contains the set of agreed-upon rules and standards that govern the transactions in a particular industry, in this case, financial services

iii) ***The settlement layer:*** This is the layer where all transactions are settled. In the case of DeFi, this layer is typically a public blockchain layer. The 'currency' used to settle these trades/transactions is typically the cryptocurrency native to the blockchain network in question, for instance, [the cryptocurrency Ether (ETH)] ETH is used in Ethereum. In addition, certain blockchain networks also

enable the tokenisation of real-world assets, for example, a piece of real estate, and the creation of alternative currencies called *Altcoins*, that can be used as the medium of settlement. Today, DeFi applications also deal with digital representations of fiat currencies [that is, currencies issued and backed by a government, but without intrinsic value] known as *stable coins*, to counteract the volatility of the cryptocurrencies' value stemming from rampant speculation. These concepts are explored by Schär in *On Blockchain and Smart Contract-based Financial Markets*.

Smart contracts

Smart contracts are pieces of code that encapsulate and execute the terms and activities necessary for the functioning of these decentralised financial services. These play multiple roles in the DeFi context; that of custodians, escrow agents, and central counterparty clearing (CCP).

In real-world finance, transactions between banks are settled by CCP. Instead, in DeFi, CCP is disintermediated, and transactions are settled *atomically* [an *atomic* settlement uses technology that enables the exchange of one cryptocurrency for another without using centralised intermediaries]. This ensures that value is either exchanged between the two parties simultaneously and instantaneously or, the transaction results in an error.

For example, a token that represents a piece of real estate is sent to the buyer and the tokenised cash to close the purchase is sent to the seller simultaneously. This atomic swap reduces the mistrust, time and effort in the value chain that is typically capitalised on by third parties and governing institutions.

Transparency

DeFi is also inherently transparent because all transactions are auditable via blockchain browsers, as blockchain technologies render immutable the data written within them. This could potentially allow for the mitigation of unwelcome events before they arise.

From another perspective, DeFi can be considered a further step in the evolution of the financial system that started with the inclusion of the internet

Centralised finance

Centralised finance (CeFi) is a sub-branch of the financial industry. In CeFi, people earn interest by using cryptocurrency as a form of collateral. Corporations, like Binance or Coinbase, act as lenders and have custody of the assets or funds while lending them out.

Since 2020, DeFi applications and services like *Uniswap* [a protocol that facilitates automated transactions between cryptocurrency tokens on the Ethereum blockchain] have gained a foothold. They have promoted a new way to trade cryptocurrency and financial assets by creating a new financial services stack, and are now presenting alternatives and direct investments through DeFi products.

DeFi services and applications replicate existing offerings on a new technology rail—the blockchain, and allow for the creation of customised, innovative services. They offer a substitute to the current, old-finance world by creating its counterpart in the crypto world with services including exchanges, funds management, insurance, payments, derivatives and asset management.

Although still in its early stages, due to blockchain technology, the level of new product spawning and investment in DeFi is growing exponentially. As of March 2021, US$41.6 billion has been locked into over 83 projects, according to data collected and published by DeFi Pulse.

DeFi: the new opportunities

DeFi has become one of the more discussed topics inside and outside blockchain communities due to:

i) the continuous release of new projects

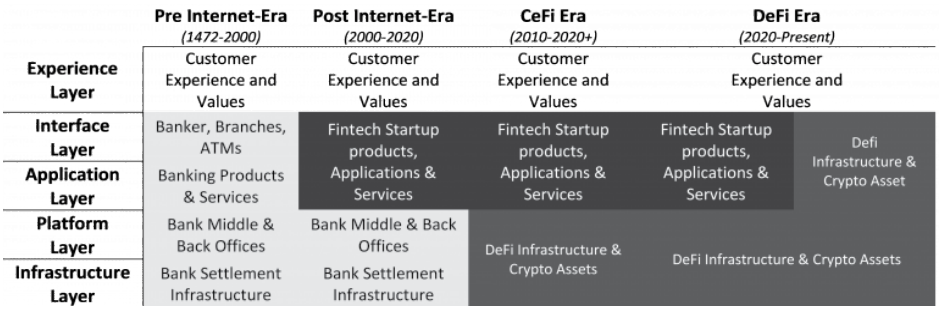
ii) the amount of cryptocurrency locked into the various projects, and the benefits the phenomenon has to offer, such as:

- a much leaner and more efficient financial system
- financial inclusion by being 'permissionless'
- attractive interest rates for investors
- control over one's own finances, as all wealth in DeFi is held in the user's wallet
- heightened transparency, where anyone can view any transactions; the fact that the governing smart contracts reside on the blockchain ensures that any-

The quote

DeFi applications disintermediate traditional, centralised financial models, enabling anyone with an active internet connection to participate.

Figure 1. The evolution of finance



Source: Ian Lee, The Defiant (2020)

one interested and with the right programming knowledge can analyse the governing logic.[5,6]

To appreciate the exponential growth of the DeFi phenomenon, the following discussion highlights some interesting projects and initiatives.

Stable coins

Rampant financial speculation has rendered the value of most cryptocurrencies highly volatile. An answer to this problem has arisen in the form of *stable coins*. Their value is rendered 'stable' (relatively much less volatile) by linking them to price-stable assets, like gold or the US dollar, or crypto [that is, digital as opposed to physical] assets. There are two types of stable coins; custodial stable coins and algorithmic or decentralised stable coins. The first is usually pegged to a real-world asset such as the US dollar; the latter is pegged to crypto assets.

1. ***Custodial stable coins*** store reserves of a fiat counterpart to guarantee the peg (e.g. the cryptocurrency Tether (USDT) is backed 1:1 with the US dollar). The economic principle is similar to the fiat counterpart, in that it is based on trust that the USD reserves are real and fully collateralised.
2. ***Algorithmic or decentralised stable coins*** differ by using as collateral a relatively stable cryptocurrency or a basket of them. In cases where the underlying cryptocurrency itself suffers from volatility, the stable coin is over-collateralised (e.g. the DAI stable coin is backed by Ethereum and provides an economic incentive for arbitrageurs to maintain its peg).

Examples of stable coins are as follows.

Binance USD

Binance USD is a custodial, [fiat-backed] stable coin arising from the centralised crypto-exchange Binance. The stable coin is pegged 1:1 to the US dollar. This varies from decentralised stable coins such as DAI, which are artificially pegged.

Maker

Maker was one of the first to launch decentralised stable coins. It is a smart contract platform constructed on Ethereum in 2017. It has several types of stable coins and a governance token:

- SAI stands for single collateral DAI and is backed only by Ether (ETH) as collateral.
- DAI stands for multi-collateral Dai and is currently backed by Ether (ETH) and Basic Attention Token (BAT)
- Maker (MKR) is a governance token and is used for governance purposes [e.g. holders of MKR have governance rights over the 'terms' of Maker smart contracts].

Lending

Lending is a key aspect of the traditional financial system and is strictly regulated by governments and banks. The current lending system is exclusionary and has evolved in such a fashion that it is unable to cater for a large segment of the world's population.

Decentralised lending allows any user to collateralise their digital assets and use them to obtain loans. Due to this decentralisation, neither the borrower nor the lender needs to identify themselves, and everyone has access to cryptocurrency.

There are various types of lending protocols, some of which are examined in the following discussion.

Compound

Launched in 2017, Compound uses an innovative pool-based lending system, where users who deposit an amount in any of the supported cryptocurrencies are given a number of *cTokens*. These are synthetic tokens that are used to emulate the deposit, on top of which they can accumulate interest. These cTokens also work as collateral to determine the maximum amount a user can borrow at a specific moment. The users earn an annual percentage yield (APY). Compound derives the interest rates for different assets through algorithms that are based on the asset's supply and demand.

Aave

Aave was launched in 2020. It is an open-source, non-custodial protocol for borrowing and lending. Users can borrow tokens that are minted with compliant ERC20 tokens on a ratio of 1:1 of the supplied asset. This creates *aTokens*, synthetic tokens that are used to emulate the deposit. Therefore, a user can lock an amount of the ERC20 token into the smart contract and earn interest from the number of aTokens lent. The interest earned depends on the supply and demand of the asset. A user can opt-in or out anytime, as the protocol has a reserve to ensure withdrawals. Aave is one of the first platforms to offer *flash loans*.

Flash Loans

Flash loans are 'trustless' and uncollateralised loans where the payback needs to occur within the same transaction. With regular loans, a lender advances money to a borrower to be eventually paid back in full. The lender receives a payout from the borrower for temporarily parting with its money. Flash loans differ in the following ways:

- ***Smart contracts:*** flash loans are built on smart contracts which regulate the money flow. If the borrower cannot pay back the loan before the end of the transaction, the smart contract will reverse the transaction, so the loan is called off.
- ***Unsecured:*** flash loans lack collateral. The borrower needs to repay the borrowing almost immediately.
- ***Instantaneous:*** obtaining a traditional loan is a long process. Flash loans assure an instantaneous amount, but need to be repaid within the same transaction. This means that the borrower must execute other smart contracts to perform instant trades with the borrowed capital before the end of the transaction.

Flash loans can be used for the following applications.

Arbitrage: traders use flash loans to profit from the price discrepancy between different exchanges. For example, suppose [the digital currency] pastacoin is $1 at exchange A and $4 at exchange B. In that case, the user can call a flash loan to buy 100 pasta tokens from A and sell them to B and then repay the loan with the profit made.

Collateral swaps: entails instantly swapping the collateral backed by the user's loan for another type of collateral.

Derivatives

Decentralised derivatives are similar to the classic financial product, except that they are tokens that derive their intrinsic value from other crypto assets instead of other real-world assets.

Asset-based derivative tokens

Asset-based derivative tokens are similar to stable coins, but instead of being pegged to fiat currencies, they are pegged to synthetic tokens or price movements of multiple assets.

Event-based derivative tokens

Event-based derivative tokens are usually linked to a possible event outcome with a specific timeframe and resolution. When the market resolves based on the outcome of the event in a particular timeframe, the smart contract, where the tokens are locked, will split the 'winnings' among the users who locked the token for that specific outcome.

These tokens greatly depend on the resolution source's trustworthiness, also known as the *oracle* [third-party services that provide external information to the blockchain], so they can create external dependencies.

Examples of derivative-based protocols are provided in the following section.

Synthetix

Synthetix is a protocol that tracks real-world assets via tokens. It is implemented in such a way that all participants' total debt pool can increase or decrease the aggregate price of the unique synthetic assets. The token can remain fungible [that is, interchangeable with something of the same type], as the redemption does not depend on the issuer but on the pool, as the user assumes the risk when acquiring a token linked to a specific asset. An example of a synthetic asset is Synthetic Gold (sXAU). This tracks the price performance of gold by using the services of Chainlink, a smart contract *oracle* that obtains price feeds from multiple, trusted third-party sources to prevent tampering.[7]

Hegic

Hegic differs from Synthetix as it offers options with any strike price and staking for a defined period utilising its liquidity pools. Users can opt-in and opt-out immediately, as the liquidity of every user is covered. This works the same as in the real financial world, and it differs only by the fact that the tokens are locked into a smart contract.

Insurance

Insurance against losses or other types of financial protection is nothing new to the financial world. In DeFi, a smart contract is used to guarantee the insurance payout. All pertinent funds are locked in the smart contract. Some examples of insurance protocols are as follows.

Nexus mutual

Nexus Mutual is a decentralised insurance protocol built on Ethereum that offers insurance for DeFi products. The system works similar to the fiat-based insurance system. The user chooses a cover period and a cover amount. The user will be automatically refunded upon a specific condition if a claim assessment is done and evaluated by a claim assessor. Once approved, the funds will be paid.

Armor protocol

Armor is the first derivative DeFi insurance product. Armor is an insurance aggregator like Nexus Mutual, as it offers the same type of insurance but differs as it also insures products from Yearn Finance. The products are:

- arNXM: the token that allows an investor to have exposure to NXM, the token of nexus mutual, without undergoing know your client (KYC) protocols. It has also been used for staking, claim assessments, and governance.
- arNFT: used to buy insurance cover on Nexus Mutual.
- arCore: 'pay as you go' insurance, where Armor protocol keeps track of users' funds and moves them across various protocols using a streamed payment system.

Payments

Decentralised payments can already be made via ETH or other tokens, but they are not cheap, as the price of ETH has been rising. DeFi offers faster and cheaper solutions using *Layer 2 solutions* [these are projects that allow timed or conditional transfers]. Some examples of payments protocols are as follows.

Tornado cash

Tornado Cash is one of the first *sidechains* [a separate blockchain which runs in parallel and operates independently to the Ethereum mainnet] to implement *zk-Snarks* to achieve privacy. Transaction privacy is improved by breaking the on-chain link between the recipient and the receiver's addresses. Zk-snarks allow the user to be verified without the need to reveal the exact details of deposits and transfers to a blockchain wallet address. [While the blockchain does not reveal a user's name, transactions are linked to the user's wallet address, this is why Ethereum is considered to be *pseudonymous*]. Tornado cash addresses this so that to the external observer, it becomes impossible to determine which account the transactions relate to.

Xdai

Launched in 2018, xDAI provides a way to conduct small to medium payment transactions easily and quickly. This sidechain can conduct five transactions per second at a low price paid via the xDAI. The xDAI has a 1:1 representation with the DAI stable coin.

DeFi: current drawbacks

Despite its exponential growth, the DeFi phenomenon needs to address some setbacks. Well-established protocols can significantly reduce these risks:

1. ***Infrastructural mishaps and hacks***: A number of scams have already been perpetrated in the rapidly evolving DeFi infrastructure. Hackers have managed to drain a protocol of funds and leave investors unable to trade. In some cases, funds have been recovered.
2. ***Regulation:*** Ironically, the open and distributed nature of the DeFi ecosystem also faces problems when it comes to existing financial regulation. Current laws were crafted based on the idea of separate financial jurisdictions, each with its own set of laws and rules. DeFi's borderless transaction span presents important questions for this type of regulation (e.g. who is culpable in a financial crime that occurs across borders, with DeFi protocols and applications?).
3. ***Smart contracts:*** Smart Contracts are the backbone of DeFi protocol. They are transparent and open-source so that users who participate in the protocol can make an informed decision. Typically, developers who build protocols ensure that their smart contracts go through multiple audit rounds by security firms. However, it is not without precedent that human auditors miss flaws that could potentially be exploited in the future. DeFi, at the end of the day, comprises software systems, and these can suffer malfunctions stemming from various factors.
4. ***The oracle problem***: Blockchains inherently do not have access to off-chain data. This is where oracles or external data-feeds come into the picture. These oracles feed the blockchain (specifically the smart contract residing on the blockchain) with external information, serving as a bridge to the outside world. Such a solution tends to create a central point of trust in an otherwise trustless, decentralised setup. If an oracle broadcasts the wrong information, the consequences could be dire.
5. ***Liquidity risks:*** Another non-technical risk is that protocols could run out of liquidity.
6. ***Rising costs:*** Most DeFi protocols today operate on the Ethereum blockchain. This has led to a congestion of the network and consequently caused the costs of transactions to rise exponentially. However, this is only a systemic risk, and many protocols are plan-

ning an exodus to other public blockchains such as Algorand that are faster, more scalable, and less expensive. Nevertheless, with Layer 2 solutions, DeFi projects are becoming more scalable.

7. ***Governance risk:*** Most DeFi projects can be impacted by their governance structure, as it can negatively affect the platform. Applications that do not have a proper open governance structure will create risks for the platform protocol, liquidity and trustability. [An example was the 'SushiSwap' incident in September 2020 when the founder of SushiSwap, a decentralised exchange, suddenly sold US$13 million worth of SushiSwap tokens causing a significant selloff and drop in the value of the tokens. After pressure from the crypto community however, the founder returned all the coins he had cashed out].

Conclusion

DeFi is a phenomenon built on the tenets of financial inclusion, disintermediation, and accessibility. Most DeFi protocols are accessible by anyone anywhere—all that is needed is internet connectivity.

[Liquidity aggregator Totle uses the following analogy to illustrate this concept] DeFi can be compared to Lego pieces, in that it can be used to build complex or simple structures that are integrated. The essence of DeFi is to build for interoperability. Like Lego, an individual starts with a large bin of pieces that can be combined together and eventually snowballs into a new creation.

For example, a user starts building on Dai, and decides to create a smart contract for MakerDao. The smart contract accepts ETH as collateral for DAI. On that, a new piece is added, a custom Compound smart contract. The Compound uses the MakerDao smart contract for borrowing capabilities and as infrastructure for its lending markets. This will allow any user to collateralise the loan with any cryptocurrency supported by Compound. Lenders will supply the pool with funds and earn interest for their contributions until their funds are withdrawn.

There is no doubt that blockchain technology and DeFi are empowering financial services to be more trustworthy, interoperable, borderless, and transparent. But before we see mass adoption of DeFi protocols from mainstream finance, there will be a medium to long transition period. The future of DeFi will ultimately depend on whether it manages to keep its promises and create value for its users. **FS**

About BIP

BIP Consulting is a primary multinational consulting firm employing more than 3,500 people worldwide. BIP's professionals offer management consulting services and business integration services, helping companies in the research and adoption of disruptive technological innovation.

Notes

1 Antonopoulos, AM. Mastering Bitcoin: Programming the Open Blockchain (2 ed.). O'Reilly Media, 2017.
2 Chaum, D. Blind signatures for untraceable payments. Boston: Springer, 1983.
3 Yaga DMP. Blockchain technology overview. National Institute of Standards and Technology, 2018, pp 2-4
4 Yuan, Y. Blockchain: The state of the art and future trends, 2016.
5 Murray A, Kuban S, Jesfy M & Anderson J. 'Contracting in the Smart Era: The Implications of Blockchain and Decentralized Autonomous Organizations for Contracting and Corporate Governance', Academy of Management Perspectives, 2019.
6 Chen YBC. 'The rise of decentralized business models'. Journal of Business Venturing Insights, 2019.
7 Brooks S, Jurisevic A, Sapn M & Warwick K. A decentralised payment network and stablecoin. Haven, 2018.

For the full bibliography accompanying this paper, refer to https://www.bipconsulting.com/insights/defi-the-new-financial-revolution/