Web3 Finace System Hack - DeFI 01

DeFi is an open and global financial system built for the internet age – an alternative to a system that's opaque, tightly controlled, and held together by decades-old infrastructure and processes. It gives you control and visibility over your money. It gives you exposure to global markets and alternatives to your local currency or banking options. DeFi products open up financial services to anyone with an internet connection and they're largely owned and maintained by their users. So far tens of billions of dollars worth of crypto has flowed through DeFi applications and it's growing every day.

What's DeFi?

DeFi is a collective term for financial products and services that are accessible to anyone who can use Ethereum – anyone with an internet connection. With DeFi, the markets are always open and there are no centralized authorities who can block payments or deny you access to anything. Services that were previously slow and at risk of human error are automatic and safer now that they're handled by code that anyone can inspect and scrutinize.

There's a booming crypto economy out there, where you can lend, borrow, long/short, earn interest, and more. Crypto-savvy Argentinians have used DeFi to escape crippling inflation. Companies have started streaming their employees their wages in real time. Some folks have even taken out and paid off loans worth millions of dollars without the need for any personal identification.

A comparison

DeFi	Traditional finance
You hold your money.	Your money is held by companies.
You control where your money goes and how it's spent.	You have to trust companies not to mismanage your money, like lend to risky borrowers.
Transfers of funds happen in minutes.	Payments can take days due to manual processes.
Transaction activity is pseudonymous.	Financial activity is tightly coupled with your identity.
DeFi is open to anyone.	You must apply to use financial services.
The markets are always open.	Markets close because employees need breaks.
It's built on transparency – anyone can look at a product's data and inspect how the system works.	Financial institutions are closed books: you can't ask to see their loan history, a record of their managed assets, and so on.

Bitcoin in many ways was the first DeFi application. Bitcoin lets you really own and control value and send it anywhere around the world. It does this by providing a way for a large number of people, who don't trust each other, to agree on a ledger of accounts without the need for a trusted intermediary. Bitcoin is open to anyone and no one has the authority to change its rules. Bitcoin's rules, like its scarcity and its openness, are written into the technology. It's not like traditional finance where governments can print money which devalues your savings and companies can shut down markets.

Programmable money

This sounds odd... "why would I want to program my money"? However, this is more just a default feature of tokens on Ethereum. Anyone can program logic into payments. So you can get the control and security of Bitcoin mixed with the services provided by financial institutions. This lets you do things with cryptocurrencies that you can't do with Bitcoin like lending and borrowing, scheduling payments, investing in index funds and more.

What can you do with DeFi?

Send money around the globe quickly

As a blockchain, Ethereum is designed for sending transactions in a secure and global way. Like Bitcoin, Ethereum makes sending money around the world as easy as sending an email. Just enter your recipient's ENS name (like bob.eth) or their account address from your wallet and your payment will go directly to them in minutes (usually). To send or receive payments, you will need a wallet.

Stream money around the globe...

You can also stream money over Ethereum. This lets you pay someone their salary by the second, giving them access to their money whenever they need it. Or rent something by the second like a storage locker or electric scooter.

Borrowing

Borrowing money from decentralized providers comes in two main varieties.

- Peer-to-peer, meaning a borrower will borrow directly from a specific lender.
- Pool-based where lenders provide funds (liquidity) to a pool that borrowers can borrow from.

Borrowing with privacy

Today, lending and borrowing money all revolves around the individuals involved. Banks need to know whether you're likely to repay a loan before lending.

Decentralized lending works without either party having to identify themselves. Instead the borrower must put up collateral that the lender will automatically receive if their loan is not repaid. Some lenders even accept NFTs as collateral. NFTs are a deed to a unique asset, like a painting. More on NFTs

This allows you to borrow money without credit checks or handing over private information.

Access to global funds

When you use a decentralized lender you have access to funds deposited from all over the globe, not just the funds in the custody of your chosen bank or institution. This make loans more accessible and improves the interest rates.

Tax-efficiencies

Borrowing can give you access to the funds you need without needing to sell your ETH (a taxable event). Instead you can use ETH as collateral for a stablecoin loan. This gives you the cash-flow you need and lets you keep your ETH. Stablecoins are tokens that are much better for when you need cash as they don't fluctuate in value like ETH. More on stablecoins

Flash loans

Flash loans are a more experimental form of decentralized lending that let you borrow without collateral or providing any personal information.

They're not widely accessible to non-technical folks right now but they hint at what might be possible to everyone in the future.

It works on the basis that the loan is taken out and paid back within the same transaction. If it can't be paid back, the transaction reverts as if nothing ever happened.

The funds that are often used are held in liquidity pools (big pools of funds used for borrowing). If they are not being used at a given moment, this creates an opportunity for someone to borrow these funds, conduct business with them, and repay them in-full quite literally at the same time they're borrowed.

This means a lot of logic must be included in a very bespoke transaction. A simple example might be someone using a flash loan to borrow as much of an asset at one price so they can sell it on a different exchange where the price is higher.

So in a single transaction the following happens:

- You borrow X amount of $asset at $1.00 from exchange A
- You sell X $asset on exchange B for $1.10
- You pay back loan to exchange A
- You keep the profit minus the transaction fee

If exchange B's supply dropped suddenly and the user wasn't able to buy enough to cover the original loan, the transaction would simply fail.

To be able to do the above example in the traditional finance world, you'd need an enormous amount of money. These money-making strategies are only accessible to those with existing wealth. Flash loans are an example of a future where having money is not necessarily a prerequisite for making money.

Grow your portfolio

There are fund management products on Ethereum that will try to grow your portfolio based on a strategy of your choice. This is automatic, open to everyone, and doesn't need a human manager taking a cut of your profits.

A good example is the .This is a fund that rebalances automatically to ensure your portfolio always includes.You never have to manage any of the details and you can withdraw from the fund whenever you like.

Fund your ideas

Ethereum is an ideal platform for crowdfunding:

- Potential funders can come from anywhere – Ethereum and its tokens are open to anybody, anywhere in the world.
- It's transparent so fundraisers can prove how much money has been raised. You can even trace how funds are being spent later down the line.
- Fundraisers can set up automatic refunds if, for example, there is a specific deadline and minimum amount that isn't met.

Quadratic funding

Ethereum is open source software and a lot of the work so far has been funded by the community. This has led to the growth of an interesting new fundraising model: quadratic funding. This has the potential to improve the way we fund all types of public goods in the future.

Quadratic funding makes sure that the projects that receive the most funding are those with the most unique demand. In other words, projects that stand to improve the lives of the most people. Here's how it works:

1. There is a matching pool of funds donated.
2. A round of public funding starts.
3. People can signal their demand for a project by donating some money.
4. Once the round is over, the matching pool is distributed to projects. Those with the most unique demand get the highest amount from the matching pool.

This means Project A with its 100 donations of 1 dollar could end up with more funding than Project B with a single donation of 10,000 dollars (dependent on the size of the matching pool).

Insurance

Decentralized insurance aims to make insurance cheaper, faster to pay out, and more transparent. With more automation, coverage is more affordable and pay-outs are a lot quicker. The data used to decide on your claim is completely transparent.

Ethereum products, like any software, can suffer from bugs and exploits. So right now a lot of insurance products in the space focus on protecting their users against loss of funds. However there are projects starting to build out coverage for everything life can throw at us. A good example of this is Etherisc's Crop cover which aims to protect smallholder farmers in Kenya against droughts and flooding(opens in a new tab)↗. Decentralized insurance can provide cheaper cover for farmers who are often priced out of traditional insurance.

Aggregators and portfolio managers

With so much going on, you'll need a way to keep track of all your investments, loans, and trades. There are a host of products that let you coordinate all your DeFi activity from one place. This is the beauty of DeFi's

open architecture. Teams can build out interfaces where you can't just see your balances across products, you can use their features too. You might find this useful as you explore more of DeFi.

How does DeFi work?

DeFi uses cryptocurrencies and smart contracts to provide services that don't need intermediaries. In today's financial world, financial institutions act as guarantors of transactions. This gives these institutions immense power because your money flows through them. Plus billions of people around the world can't even access a bank account.

In DeFi, a smart contract replaces the financial institution in the transaction. A smart contract is a type of Ethereum account that can hold funds and can send/refund them based on certain conditions. No one can alter that smart contract when it's live – it will always run as programmed.

A contract that's designed to hand out an allowance or pocket money could be programmed to send money from Account A to Account B every Friday. And it will only ever do that as long as Account A has the required funds. No one can change the contract and add Account C as a recipient to steal funds.

Contracts are also public for anyone to inspect and audit. This means bad contracts will often come under community scrutiny pretty quickly.

This does mean there's currently a need to trust the more technical members of the Ethereum community who can read code. The open-source based community helps keep developers in check, but this need will diminish over time as smart contracts become easier to read and other ways to prove trustworthiness of code are developed.

Ethereum and DeFi

Ethereum is the perfect foundation for DeFi for a number of reasons:

- No one owns Ethereum or the smart contracts that live on it – this gives everyone an opportunity to use DeFi. This also means no one can change the rules on you.
- DeFi products all speak the same language behind the scenes: Ethereum. This means many of the products work together seamlessly. You can lend tokens on one platform and exchange the interest-bearing token in a different market on an entirely different application. This is like being able to cash loyalty points in at your bank.
- Tokens and cryptocurrency are built into Ethereum, a shared ledger – keeping track of transactions and ownership is kinda Ethereum's thing.
- Ethereum allows complete financial freedom – most products will never take custody of your funds, leaving you in control.

You can think of DeFi in layers:

1. The blockchain – Ethereum contains the transaction history and state of accounts.
2. The assets – ETH and the other tokens (currencies).
3. The protocols – smart contracts that provide the functionality, for example a service that allows for decentralized lending of assets.
4. The applications – the products we use to manage and access the protocols.

Build DeFi

DeFi is an open-source movement. The DeFi protocols and applications are all open for you to inspect, fork, and innovate on. Because of this layered stack (they all share the same base blockchain and assets), protocols can be mixed and matched to unlock unique combo opportunities.

Ethereum enables us to own our own identity and use a decentralized identifier. Our key details are stored in our wallets, and specific information can be shared when needed without revealing other parts of our identity.