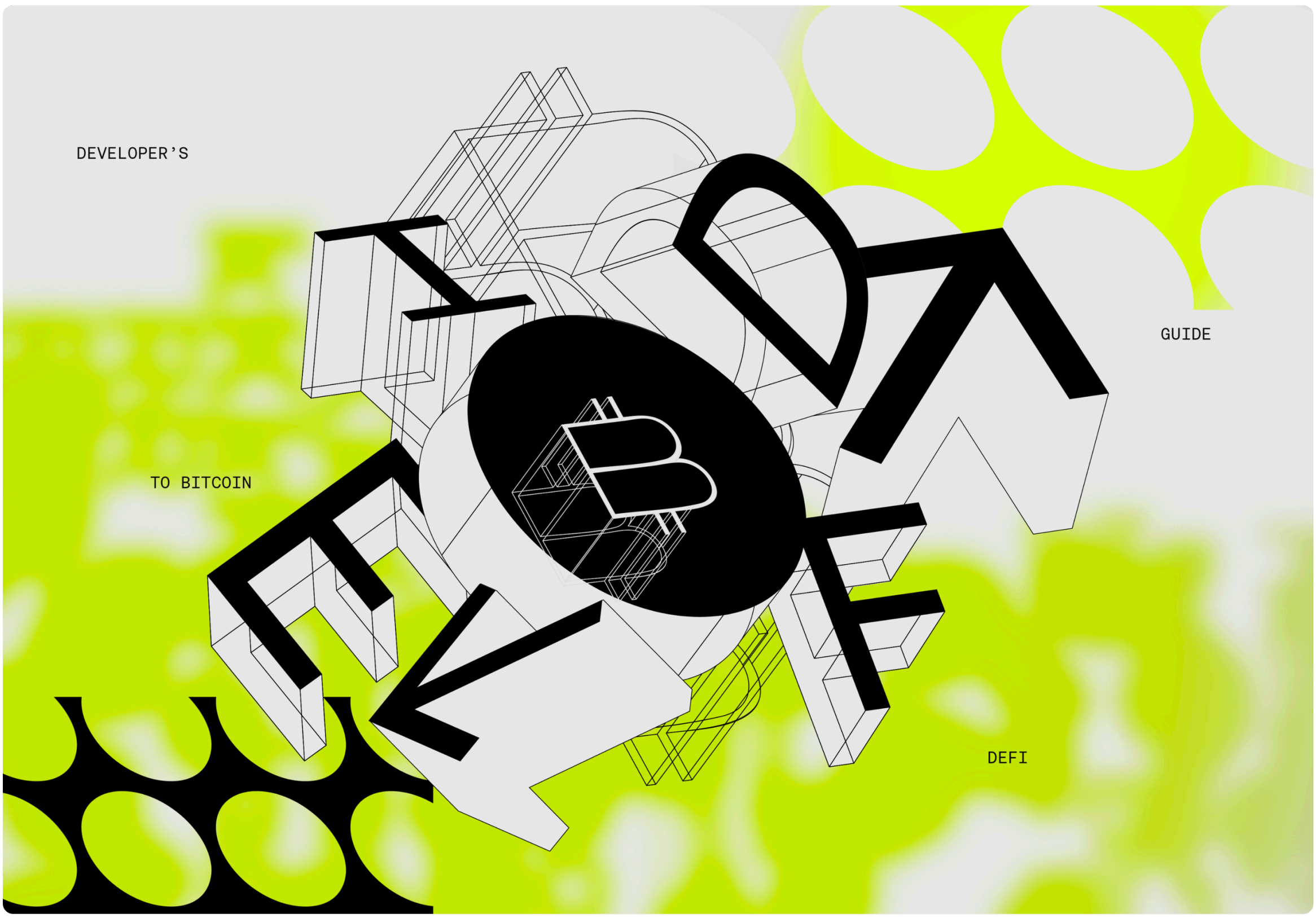
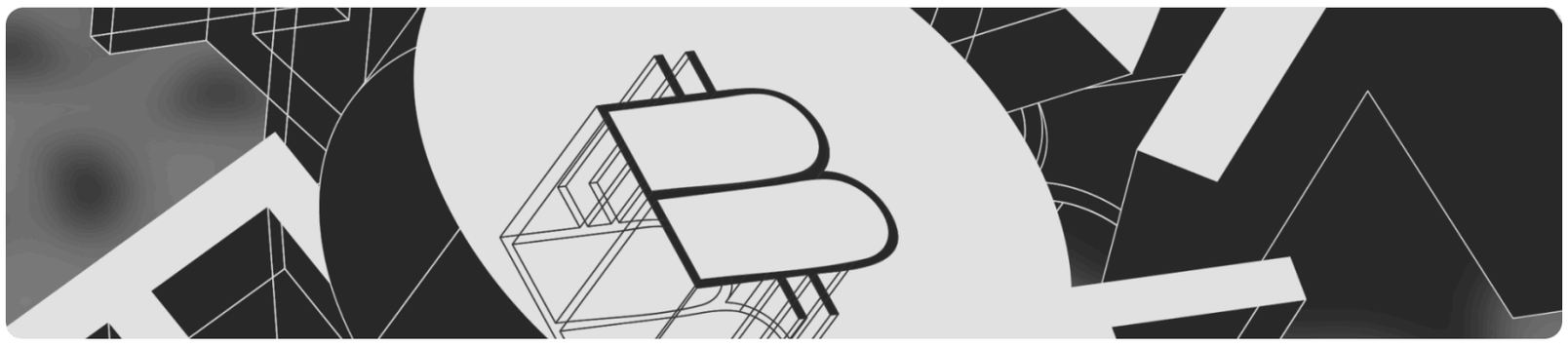
/-/iro : Books

A Developer’s Guide to Bitcoin DeFi





/ Foreword

DeFi is the first breakthrough use case in crypto. This perhaps isn't surprising, since the story of crypto begins with money and Bitcoin's creation of a trustless peer-to-peer digital asset, but that financial thesis took years to play out. It wasn't until 2020, 11 years after Bitcoin's launch, that we saw DeFi take off. Stablecoins, peer-to–peer trading, decentralized lending, derivatives. In just four years, these DeFi categories and more have all become poster children of crypto's success, and indeed, they drove much of the industry growth we've seen today.

Figment launched in 2018 to provide staking services to institutional clients right on the cusp of DeFi's inception, and since then we've witnessed firsthand the market demand for DeFi. Markets want access to crypto assets, and they want to put those assets to work. That manifests in not only the staking space, where liquid staking is one of the biggest categories in DeFi as well as where we provide staking infrastructure to over 250 institutional clients, but also in DeFi as a whole. But one thing that has been missing from DeFi so far is Bitcoin itself, the progenitor crypto asset.

Bitcoin DeFi is something of a white whale within the crypto space. Desired by many, but difficult to catch, or, in this case, build. How do you get the crypto asset with the largest market cap, with the largest number of holders, with the largest amount of latent capital out of cold storage and into DeFi markets? Can you bring some of the learnings from the past few years directly to the oldest blockchain there is?

You'll find those answers and more in this book.

You're in good hands with its author, so I will leave you with this: there's a reason why Bitcoin DeFi is one of the categories we are most excited about in 2024 at Figment, and in our 5 years, we've never seen more builder activity on Bitcoin.

Innovation on Bitcoin is back, and if my intuition can be trusted, it's here to stay.

Lorien Gabel, CEO & Co-Founder of F Figment

/ Table of Contents

01 / What is DeFi on Bitcoin?

Decentralized finance (DeFi) uses blockchain technology to provide a better alternative to traditional finance (TradFi). Whether Wall Street, banks, and exchanges see DeFi as a threat or an opportunity, the fact remains that DeFi is growing in popularity. There is more than $50B locked in various DeFi protocols today, and in November 2021, at the height of the bullet market, DeFi TVL reached as high as $177B.

But why is DeFi so popular and compelling when compared to the traditional financial system? Let's dig into DeFi's four primary traits:

Permissionless

DeFi is permissionless, which means anyone can use it, anywhere in the world, without regard to their social status, political affiliation, or any other factor.

Compared to TradFi where you need to provide a combination of documents (a government-issued ID, utility bills, proof of employment, etc.) to open an account, DeFi has fewer barriers. All a user needs to do is connect their wallet to a DeFi platform, and they can start trading, saving, lending, borrowing, and more. Builders and app developers can freely integrate with different DeFi projects or or even take another project's code altogether to create new financial products and experiences for the end user. That universal access drives DeFi's growing popularity.

> DeFi is permissionless, which means anyone can use it.

Transparency

In DeFi, information is public by default, from contract source code to transaction histories. With this information, anyone can find data and understand how exactly a DeFi protocol works.

> In DeFi, all information is public.

This transparency levels the playing field for all participants. It enables users to conduct due diligence to better avoid projects engaged in unhealthy business practices and identify projects that are promising and worth participating in. This rich, transparent data is updated in real time and allows users to audit the blockchain and trace past events, which can be seen in the ability to track hacked funds.

In contrast, information in TradFi is opaque and often in walled or siloed proprietary databases. Users frequently have to make decisions based on incomplete or outdated information.

Self Custody

DeFi enables self-custody of crypto assets, meaning users themselves hold their assets. Self-custody in DeFi contrasts with the custodial nature of TradFi, where users cede control of their assets to centralized intermediaries who then execute transactions on their behalf.

> DeFi users are sovereign and hold their own assets.

These centralized services can provide important functions, such as securing your assets or providing access to credit. However, they also assert control over your assets: they can limit withdrawals or require approval for payments. And sometimes, that control can lead to bad outcomes for users. For instance, Wells Fargo once charged more than 800,000 customers for unneeded auto insurance; making more than 250,000 customers delinquent after the charges piled up.

Government overreach can also impact these centralized services, such as the Lebanese central bank limiting access to cash withdrawals in the wake of a financial crisis in 2019, or when India demonetized certain banknotes in 2016, or in 2022, when the Canadian government froze the bank accounts of hundreds of protesters.

Whether they don't trust custodians, the government, or simply value independence, many people want self-custody.

Global Markets

DeFi is borderless, creating global unified markets for anyone with an internet connection to access. DeFi is always on, meaning it runs 24/7. The lack of opening or closing times in the DeFi market allows for more timely transactions because trades can be executed in real time—no more waiting for market hours to open, which can drive greater liquidity and more efficient price discovery.

> DeFi creates global unified markets.

In TradFi, many developing economies are excluded from financial services, and international policy influences who can access what service. Even those with access to traditional finance, need to wait for market hours to open.

What About Bitcoin?

Why Do You Want Bitcoin in DeFi?

Bitcoin is the most well-known cryptocurrency. There are 172M active addresses that hold Bitcoin. There are nearly 17,000 Bitcoin nodes. Bitcoin is the most decentralized and the most well-known cryptocurrency. In 2021, Bitcoin's adoption jumped more than 880% across disparate countries, from Vietnam to Afghanistan.

You can't have DeFi without assets. Alongside a permissionless, transparent financial system, of course you want a permissionless and transparent store of value. There's already $900B+ of Bitcoin on the sidelines. Is it any wonder that users and devs alike want to tap into that latent capital and put it to work?

> Alongside a permissionless, transparent financial system, of course you want a permissionless and transparent store of value.

What's more, if you are building a decentralized financial system, wouldn't you want the foundation of that system to be the most decentralized and secure blockchain? That's Bitcoin.

The Challenge With Bitcoin DeFi

While Bitcoin DeFi is a no brainer on paper, the reality of building it is much more complex. You can trace this challenge to one simple fact: Bitcoin's scripting language is extremely limited and does not support smart contracts.

To illustrate the challenge of building on Bitcoin, let's take a closer look at the protocol design: the Bitcoin chain does not have a concept of user accounts or wallets. Unlike account-based blockchains (like Ethereum), Bitcoin uses an **unspent transaction output** (UTXO) model, which tracks *who can* spend BTC, and *how much* they can spend. In short, every single transaction in a UTXO model consists of a spent transaction output and an unspent transaction output, and the protocol tracks these individual UTXOs to understand which future transactions are valid or invalid.

> You can't build Bitcoin DeFi on Bitcoin alone.

A UTXO-based model introduces additional computational complexity when compared to an account model. First, building smart contracts and apps with an account-based protocol is more intuitive for developers to build on. Second, all contract logic in a UTXO model would need to track a) which outputs are spent/unspent b) which UTXOs to use when sending a new transaction.

Imagine a common scenario in which there are two smart contracts that interact with each other. In an account-based system, it's easy enough to change the balances between the two contracts in batches, but in a UTXO model, each individual transaction must be broadcast, eating into the throughput in the overall network (which is already quite low at an average of just 7 transactions per second).

You can see how Bitcoin's design complicates the ability to create DeFi contracts. Then consider Bitcoin Script, a programming language so limited in what it can do as to prevent on-chain smart contracts altogether, making the design constraints a moot point.

In short, you can't build Bitcoin DeFi on Bitcoin alone. To do that, you need Bitcoin layers.

What Are Bitcoin Layers?

To extend the possibilities of Bitcoin, a number of different projects are building Bitcoin layers to expand what devs and users alike can do with Bitcoin. The simplest definition of a Bitcoin layer has three parts:

1. Bitcoin Dependence

   Bitcoin layers are dependent on Bitcoin, meaning they cannot function without Bitcoin. By contrast, Bitcoin is a sovereign chain, meaning it is a self-contained system with its own rules, meaning it does not rely on any other chain to function.

2. Bitcoin Settlement

   Bitcoin layers "settle" back to Bitcoin, meaning they store information, whether it's a block hash, state changes or full transaction data, in a Bitcoin block, leveraging the security budget of Bitcoin. This settlement makes Bitcoin layers harder to attack, since in order to change the history of a Bitcoin layer, you would have to change the history of Bitcoin. Bitcoin maintains its security through Proof of Work. In order to attack the network, an attacker has to outspend the majority of honest miners, that threshold is Bitcoin's "security budget"—how much an attacker would have to spend to successfully attack the network.

3. Extended Functionality

   Whether it's scaling solutions, better payments or fully expressive smart contracts, Bitcoin layers offer something that Bitcoin lacks. Bitcoin layers typically extend the functionality of Bitcoin without changing the Bitcoin core protocol.

Today, there are a lot of projects building Bitcoin layers, and they come with a variety of design tradeoffs. Here's an overview of some of the projects building on Bitcoin today:

CHAINS

DEFINITION

Sidechains & independent blockchains use different consensus mechanisms than Bitcoin's Proof of Work but ultimately settle or connect to the main Bitcoin chain.

EXAMPLES

Stacks - Rootstock - Liquid - Internet Computer- Nomic - Mintlayer* - Spiderchains*

OFF-CHAINS NETWORKS

DEFINITION

State channels and networks where data is stored/updated off-chain, then settled back to the Bitcoin main chain.

EXAMPLES

Lightning - Ark* - RGB*

ROLLUPS

DEFINITION

Rollups process transactions off the Bitcoin chain and then port that transaction data in batches back to the Bitcoin chain. All Bitcoin rollups are in active development.

EXAMPLES

BitVM* - Chainway* - Sentinel Chains* - Validity Rollups* - ZeroSync*

PROTOCOLS

DEFINITION

Many Bitcoin projects center on changes to the core protocol itself or innovations on how to use data from the core protocol. These can be popular BIPs as well as metaprotocols.

EXAMPLES

Ordinals - Covenants* - Drivechains* - DLCs* - Fedimint* - Sapio*

*Projects with a * are not yet live on mainnet.*

And these are the projects that make Bitcoin DeFi possible, a topic we'll now be diving into in the rest of this book.

What You'll Learn in This Book

In this book, we'll show you the basics of Bitcoin DeFi including:

- **How do devs put the BTC asset into Bitcoin apps?**
- **What are the primitive building blocks of DeFi** (including decentralized exchanges, stablecoins, and more)?
- **What are some more advanced DeFi protocols** (including lending protocols, derivatives, and more)?

DeFi is complex, and the space is big. In this book, we'll focus more narrowly on **Bitcoin** DeFi, and how the growing ecosystem of DeFi apps on Bitcoin is different from broader Web3. But even within that tighter focus, we won't cover everything in Bitcoin DeFi. For example, we won't be covering peer-to-peer payments like Lightning or yield farming. But this guide will jumpstart your journey and point you in the right direction. Let's get into it.

02 / Putting Bitcoin in DeFi

As we mentioned in the previous section, the Bitcoin blockchain is limited in its capabilities, which means that you can't really build DeFi apps on the Bitcoin blockchain itself. First, you have to move that BTC from the Bitcoin blockchain to another chain, whether that is to a Bitcoin L2 or to another ecosystem altogether.

It's also worth clarifying a distinction between using Bitcoin in *Web3 Defi vs Bitcoin DeFi*. By the former, we mean bridging BTC to another Web3 ecosystem and then using a synthetic BTC asset to transact in DeFI apps. By Bitcoin DeFi, we mean a DeFi system where not only is BTC used in various DeFi apps, but those apps exist on Bitcoin layers and ultimately settle back to the Bitcoin blockchain.

So how do you move BTC to a Bitcoin layer or to another blockchain ecosystem? You need a bridge.

> How do you get Bitcoin into a DeFi app?

Bridges, Pegs, and Synthetic Assets

In order to use BTC in a DeFi app, users must first go through a bridge. A blockchain bridge is a protocol that serves as a connection between different blockchains, allowing for the transfer of tokens and data between them.

In this case, a bridge connects the Bitcoin blockchain to the destination blockchain and allows users to move BTC between those two chains.

The BTC on the new chain is referred to as a tokenized asset, a synthetic asset, or a wrapped asset (and often has a specific name that corresponds to what bridge was used). The bridge itself is sometimes called a "peg" because the design must peg the value of the synthetic asset in a 1:1 ratio with BTC, such that 1 synthetic Bitcoin = 1 BTC.

In general, bridges involve trade-offs between performance and trust. Bridges are evaluated based on how well they work (performance) and how they custody the BTC deposited into the bridge (trust). These trade-offs exist on a spectrum, with centralized closed models on one end, and decentralized, open models on the other.

Closed (Centralized) Bridge Model

- These bridges rely on a trusted third party (either a single entity or a federated group) to custody the deposited BTC and process the bridge transactions (deposit and withdrawals). This is why they are also referred to as "trusted" models.
- While this method can be faster and more efficient, it compromises the principle of decentralization and exposes users to counterparty risk, meaning the trusted entity could potentially act maliciously or incompetently (stealing or losing all user funds).

Open (Decentralized) Bridge Model

- These bridges minimize the reliance on intermediaries as much as possible, instead using cryptographic proofs and smart contracts to automate the transfer process. Any trusted third party that this design might use is typically an open-membership model that anyone can join or participate in. This approach upholds the decentralization ethos of blockchain and reduces counterparty risk.
- However, they are technically more complex and regularly face attention from hackers looking to exploit bugs and drain the bridge of funds. While these designs have lower centralization risks than closed models, there's a valid argument that decentralized bridges have higher "smart contract risk".

Regardless of whether the bridge is trusted or trust-minimized, the user flow is similar. First, a user deposits BTC, whether with a custodian or in a smart contract. Then a corresponding amount of synthetic BTC is sent to the user for use on the destination blockchain.

To withdraw their BTC, the user sends the synthetic BTC back to the custodian or smart contract, and a corresponding amount of BTC is sent back to their wallet.

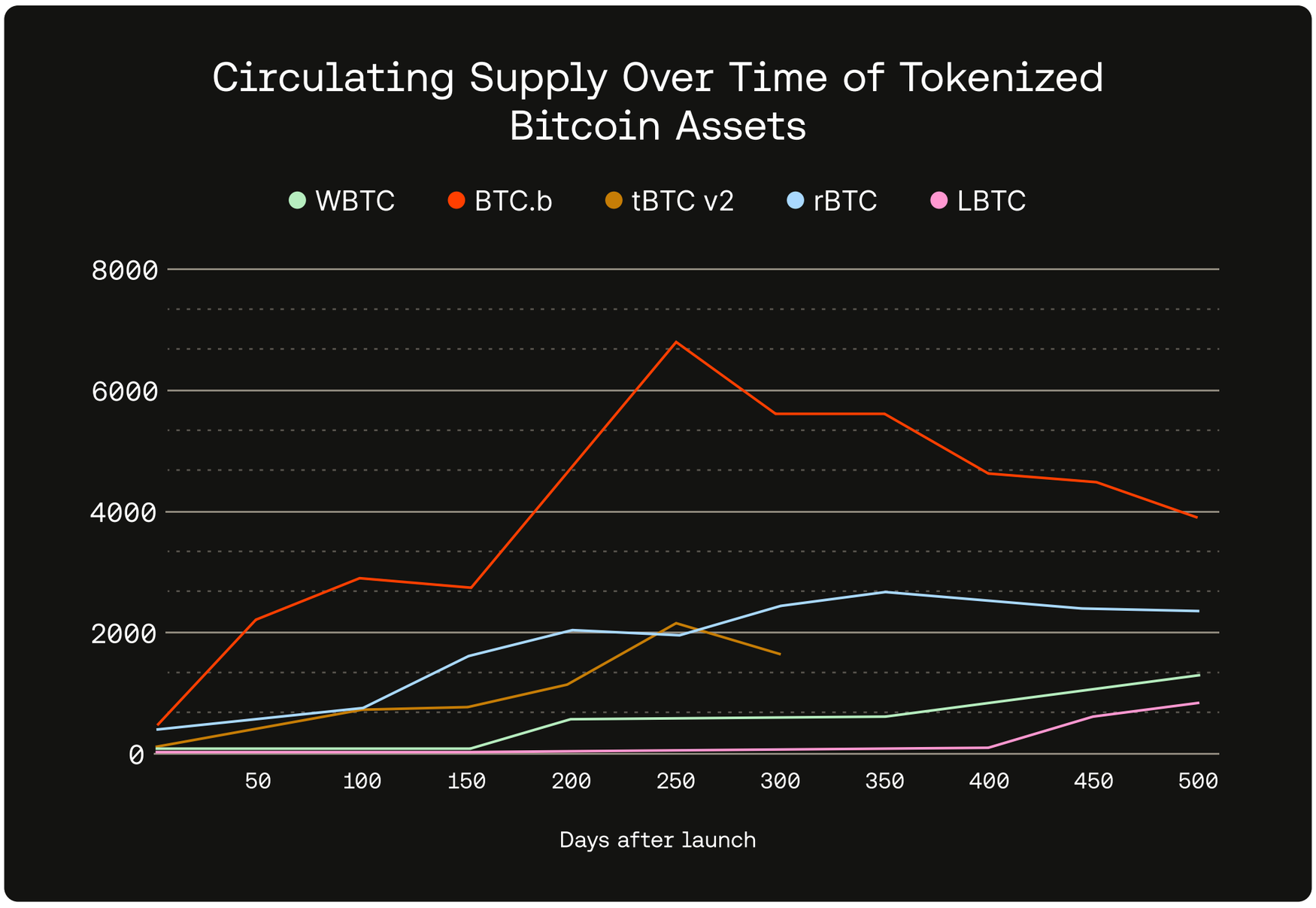
So what does the tokenized BTC landscape look like today?

Tokenized BTC Landscape

Comparison of Products Fully Backed 1:1 to Bitcoin

	WEB3 DEFI BRIDGES			BITCOIN DEFI BRIDGES		
	WBTC	BTC.b	tBTC	RBTC	LBTC	sBTC
Blockchain, token type	Ethereum (ERC-20)	Avalanche (ERC-20)	Threshold (ERC-20)	Rootstock (RBTC)	Liquid	Stacks (SIP 010)
Bridge launched	Jan 2019	June 2022	Jan 2023	Dec 2020	Sept 2018	In development
Circulating supply AS OF JAN 11, 2024	153,962 WBTC	3,797 BTC.b	1,281 tBTC	3,202 RBTC	3,774 LBTC	Est. launch summer 2024
Bridge design	**Closed membership:** 50+ merchants and custodians with keys to the WBTC multi-sig contract on Ethereum	**Closed membership:** eight wardens (relayers) and a private codebase (SGX enclave)	**Open membership:** rotating set of randomly selected nodes manage a threshold wallet	**Closed membership:** 9 organizations supporting the Powpeg, no direct control of Bitcoin multi-sig private keys	**Closed membership:** 50+ members of Liquid Federation manage multi-sig contract	**Open membership:** All wallets participating in Stacking process peg-out requests and manage a multi-sig wallet

To better understand the market traction of these bridges, let's take a look at their adoption and how their circulating supply grew in the days after their launch:



Of the implementations of tokenized Bitcoin in the chart above, it's worth digging a bit deeper into two of them.

WBTC

Wrapped Bitcoin (WBTC) is the first and most popular version of tokenized Bitcoin to date. Over 90% of tokenized Bitcoin assets in circulation are WBTC. WBTC brings BTC to the Ethereum ecosystem and other EVM-compatible chains, with over 153,000 in circulation today, nearly 1% of all BTC in circulation.

Each WBTC is pegged 1:1 with Bitcoin. For every WBTC token in circulation, there is one Bitcoin held in reserve by BitGo and a consortium of custodians. This ensures that WBTC can always be redeemed for an equivalent amount of Bitcoin.

> WBTC is the most popular version of tokenized Bitcoin on the market.

WBTC is an ERC-20 token. ERC-20 is a token standard used for fungible tokens on the Ethereum blockchain. As an ERC-20 token, WBTC can interact with any interface or app on an EVM-compatible chain as well (such as Ethereum, Avalanche, BNB, Ethereum layer 2s, and more).

Unlike decentralized bridges, retail users cannot mint or burn WBTC directly. Minting and burning is handled by a consortium of merchants and custodians. In order to acquire WBTC, retail users purchase WBTC from pre-approved merchants after passing KYC and AML requirements.

Why are people building alternatives to WBTC? While WBTC is the most popular Bitcoin bridge, many Bitcoiners are in search of a Bitcoin bridge that doesn't sacrifice decentralization or self-sovereignty. Let's look at one of the newest designs for Bitcoin DeFi bridges—sBTC.

sBTC

sBTC is an upcoming asset that represents Bitcoin on the Stacks network. This proposed design for a decentralized, 1:1 Bitcoin-backed asset, is described in detail in the sBTC whitepaper. sBTC makes it possible for anyone to move BTC in and out of Bitcoin layers in a secure and decentralized way.

sBTC is distinct from WBTC in several ways:

- It has no centralized custodian since the Bitcoin peg is maintained by smart contracts and an open, decentralized network of validators (also called signers).

- It is more cost efficient since there are zero custodian fees and low transaction fees for users to deposit and withdraw BTC. These additional processing fees are common in other trusted peg solutions like WBTC.

- Lastly, all sBTC transactions settle on Bitcoin, with 100% Bitcoin finality. This means that sBTC benefits from the full security budget of Bitcoin itself.

Similar to WBTC, sBTC is backed 1:1 to Bitcoin. However, from there the designs diverge. In sBTC, a user deposits BTC to a threshold signature wallet controlled by an open, decentralized network of validators, also known as signers. To be a validator in the Stacks network, signers must lock up a dynamic threshold of STX tokens in Stacks' consensus mechanism Proof of Transfer (PoX) and run a software node that processes sBTC withdrawals (deposits are processed automatically by the protocol). In exchange for that work, validators earn BTC rewards generated by PoX.

> sBTC is an upcoming Bitcoin-backed asset that is decentralized, trust-minimized, collateral-backed, and open membership.

This connection to the Bitcoin main chain is a key aspect of the sBTC design. sBTC can have a higher fidelity to Bitcoin's state because Clarity smart contracts have read access to Bitcoin and sBTC forks with Bitcoin. For Ethereum-based tokenized Bitcoin, oracles or intermediaries are needed in order to stay up to date in the event of a Bitcoin fork.

Each time BTC is sent to the sBTC threshold signature wallet (a deposit), an equal number of sBTC are sent to an address of the sender's choosing. This process happens automatically through smart contracts, as opposed to a series of intermediaries (like merchants or custodians). Validators process withdrawal requests (converting sBTC back into BTC) by destroying the requester's sBTC and transferring BTC to the requester's Bitcoin address, and thus maintaining the peg.

The open membership of the sBTC peg is enabled by PoX, a consensus mechanism unique to Stacks. Rather than having a single custodian, sBTC is maintained by a public network that anyone can join.

There's a lot of promise in sBTC's design, and an ecosystem-wide development effort is under way to deploy sBTC to mainnet in H2 2024. You can learn more about the timeline to sBTC's launch here.

Now that you have an understanding of how you can put Bitcoin into Bitcoin DeFi, let's dive into the world of DeFi itself and the various building blocks that play a role in this new financial system.

03 / Basic Building Blocks of DeFi

Now that you have an understanding of what DeFi is, and how you get Bitcoin into DeFi apps, it's time to go deeper. What are the basic concepts in DeFi that you need to understand before you can build more complex DeFi apps on your own?

	WEB3 DEFI	BITCOIN DEFI
WALLETS	• Trust • MetaMask • Rainbow • Zerion • Phantom	• Leather • Xverse • Casa • Alby • Liquality
STABLECOINS	• Tether USDT • Circle USDC • DAI • TrueUSD	• Arkadiko USDA • DOC • L-USDt • Stablesats • Uwu (in development) • Taproot Assets (in development)
DEXS	• Uniswap • Curve • PancakeSwap • THORChain • Sushi • Jupiter	• ALEX • Sovryn • Bisq • Uniswap (via Rootstock) • SideSwap • Velar (in development) • Bitflow (in development)
ORACLES	• Chainlink • Pyth • Band Protocol	• Chainlink • Pyth • Band Protocol

Wallets

Overview

Web3 wallets are software or hardware tools for storing cryptocurrencies, NFTs, and most importantly for this book interacting with DeFi apps.

> DeFi requires hot, non-custodial wallets.

These wallets cryptographically store and manage each user's identity and funds through a single blockchain address, which leverage public-key cryptography. Unlike custodial wallets (for example, a Coinbase account where a user opens an account directly through the app, and the app holds the user's assets), DeFi requires hot, non-custodial wallets:

- **Hot:** meaning the wallet is connected to the internet (and can interact with DeFi apps)
- **Non-custodial:** meaning users hold and control their own assets.

In the context of DeFi, wallets are 1 of 2 places crypto assets are held: the other being smart contracts related to various DeFi apps. As an app builder, you need to integrate and support a range of wallets in order to reduce onboarding friction and meet users where they are, and for wallet builders, you should build with DeFi in mind, meaning that your wallet should support:

- Holding the various token standards in a given ecosystem
- UI that shows whether tokens are liquid or staked
- UI that shows as much information related to DeFI transactions as possible (scams are rampant; the more that you can show users exactly what transaction they are signing, and what it will do, the better)

Market Traction

Wallets are the gateway to DeFi, and there are well over 100 Web3 wallet companies today (here's a non-exhaustive list). In 2022, the wallet market was valued at $8.4B, and that market is expected to grow at a 24% CAGR through 2030. As the crypto tide rises, all currents flow through Web3 wallets.

Example DeFi Wallets

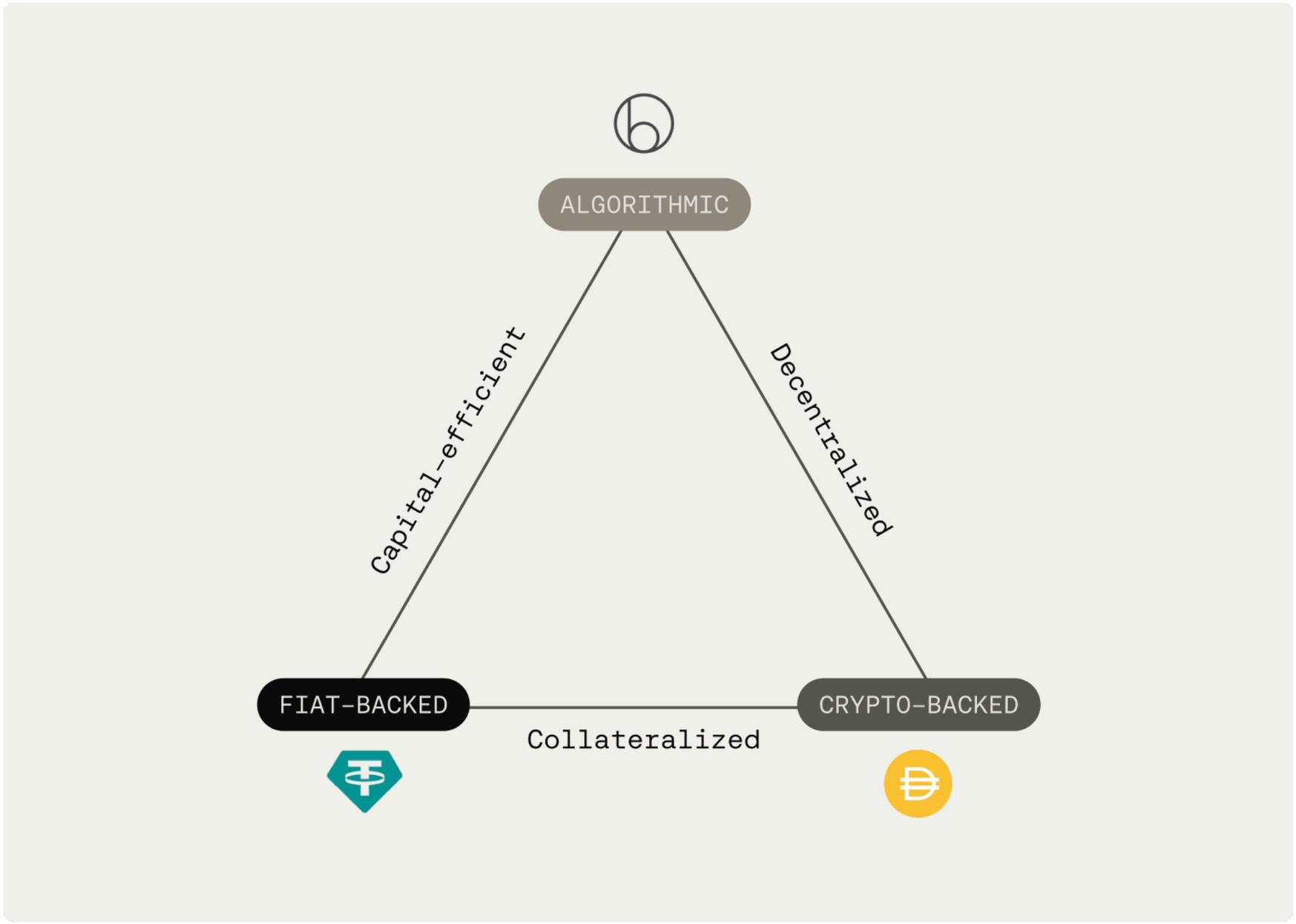
There are hundreds of wallets in Web3. Some of the most popular include Trust and Zerion, both of which support a wide range of ecosystems. However, an early trend has been that each blockchain ecosystem has its own wallet providers, and these local wallets are more popular for DeFi users, so they derisk and don't custody all of their assets in the same place. For example, in Ethereum, you have MetaMask and Rainbow. In Solana, you have Phantom. In Bitcoin DeFi, you have Leather, Xverse, Electrum, Casa, Alby, Liquality, and more.

To inspire your building, view the source code for the Leather wallet here.

Stablecoins

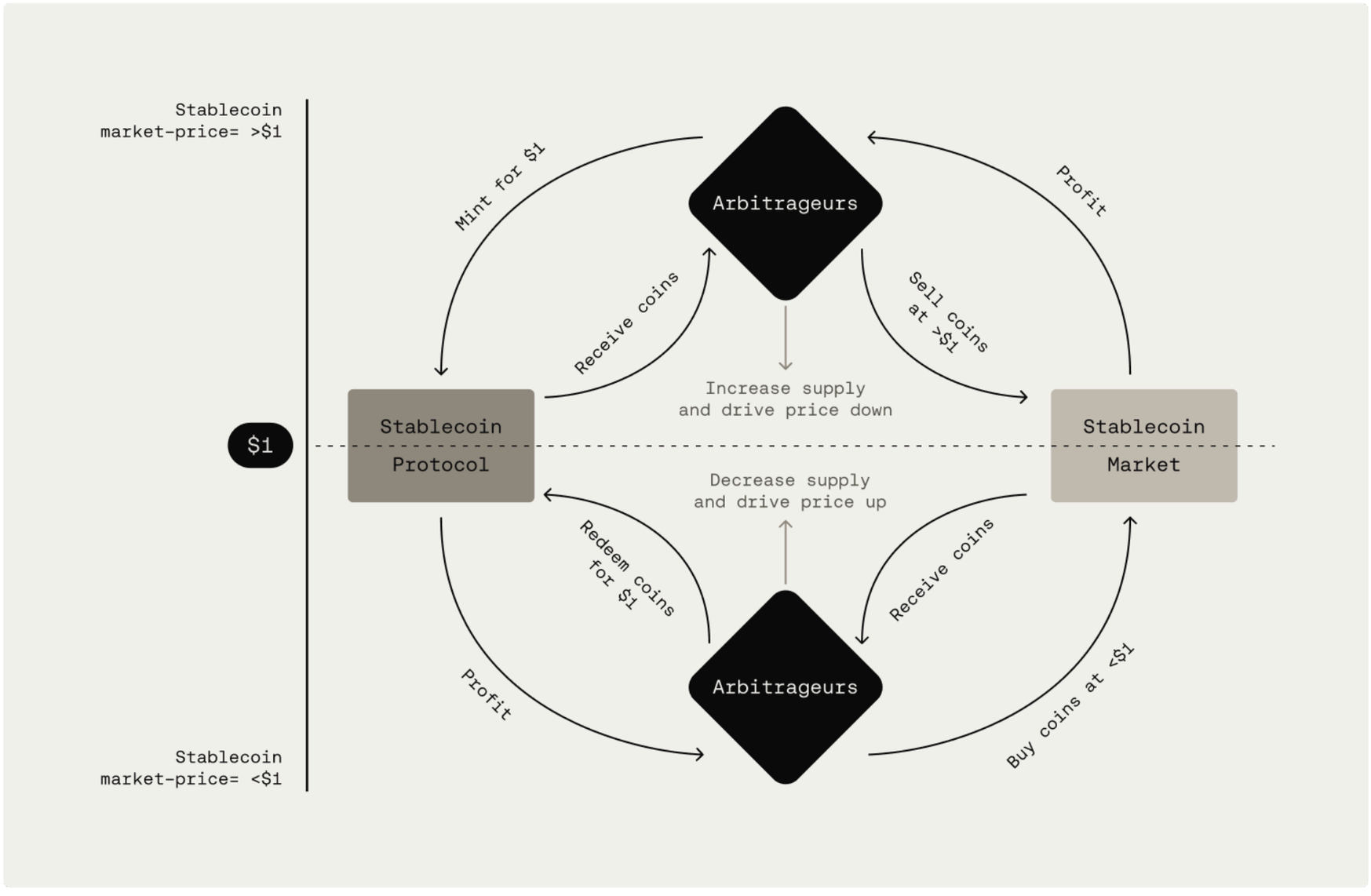
Overview

Stablecoins are fungible tokens (they are interchangeable like a dollar bill) that are pegged 1:1 to a specific asset or basket of assets, such as a traditional fiat currency, often the US dollar. At a high level, there are 3 kinds of stablecoins:



Stablecoins are designed to maintain their stability despite market volatility and use different mechanisms to maintain that stability. Users deposit an asset to mint a stablecoin, and part of what makes stablecoins, well, stable, is that they can always be redeemed for the underlying collateral. For example, deposit $1, get 1 stablecoin; burn 1 stablecoin, withdraw $1.

If the 1:1 peg ever deviates, market arbitrage will recover the peg:



Stablecoins are valuable in crypto because they offer a stable unit of exchange, which helps create more liquidity in the ecosystem. Users may not want to sell or borrow an asset whose value may be very different tomorrow, but they may be willing to sell or borrow an asset whose value is fixed.

Market Traction

Stablecoins are one of the first major crypto use cases to break through to the mainstream. The market cap for stablecoins is well over $130B, and 2 of the top 10 biggest cryptocurrencies by market cap are stablecoins. More than 100,000 people transact with stablecoins every single day.

Example Apps

STABLECOINS

WEB3

- Tether USDT
- Circle USDC
- DAI
- TrueUSD

BITCOIN

- Arkadiko USDA
- DOC
- L-USDt
- Stablesats
- Uwu (in development)
- Taproot Assets (in development)

The most popular stablecoins in Web3 are Tether's USDT, Circle's USDC, Maker's DAI, and TrueUSD.In the world of Bitcoin DeFi, you can use stablecoins from other ecosystems, and you also have projects built natively on Bitcoin like Arkadiko's USDA, which is pegged to the US dollar. Other examples include Rootstock's DOC stablecoin, and Liquid's Liquid-based Tether (USDt). Stablesats enables USD payments on Lightning. Uwu is another recent market entrant that is currently in beta, and Lightning released Taproot Assets, which enables devs to issue new assets.

To inspire your building, check out the source code of Arkadiko.

Market Traction

Stablecoins are one of the first major crypto use cases to break through to the mainstream. The market cap for stablecoins is well over $130B, and 2 of the top 10 biggest cryptocurrencies by market cap are stablecoins. More than 100,000 people transact with stablecoins every single day.

DEXs

Overview

Decentralized exchanges (DEXs) are platforms that enable the non-custodial peer-to-peer (P2P) trading of crypto assets. Think Coinbase, a centralized exchange (CEX), but without a central company holding your assets and managing the order book. On DEXs, users retain control over their assets in their wallets, and smart contracts manage the order book and trades.

DEXs come in various types, including order book DEXs and automated market makers (AMMs).

- **Order book exchanges** enable users to place buy and sell orders, placing a desired price and quantity of the asset they want to trade. The exchange then matches buy and sell orders and executes trades based on those submitted prices.
- **AMMs** use liquidity pools and algorithms to enable users to trade immediately with the protocol itself; there is no need to wait for a buyer or seller on the other side of the trade. Users can separately deposit assets into an AMM to provide liquidity and earn fees from executed trades in the AMM, and prices on the AMM are determined based on the asset ratio of that submitted liquidity in the protocol.

DEXs are a game changer in enabling access to financial instruments because their permissionless nature eliminates the geographical restrictions of traditional trading platforms.

Traction

DEXs have grown in popularity within the broader DeFi industry—the spot volume in DEXs currently stands at about $84B spread across 21 DEXs in December 2023. To put that number into context, the global equity markets were worth $105.07 trillion as of June 2022—there's a lot of room for growth.

Decentralized exchanges are growing in popularity as a non-custodial way to trade assets without the need for a middleman. The DEX to CEX spot trade volume has grown from about 0.94% in May 2020 to 12.63% in May 2022 (meaning DEX volume is gaining on CEX volume).

Example Apps

In the world of Web3, there are a number of popular DEXs, including Uniswap, Curve, PancakeSwap, THORChain, Sushi, Jupiter, and more. For every popular Web3 ecosystem, there is at least one corresponding DEX, and sometimes several.

In Bitcoin DeFi, popular DEXs include ALEX, Sovryn, Bisq, Velar, Bitflow, SideSwap, and popular DEX Uniswap was even ported to Rootstock too.

To inspire your building, check out the source code for ALEX.

Oracles

Overview

Blockchain oracles are third-party services that connect DeFi apps to external data sources, including on-chain data from other blockchains as well as off-chain data from other applications and services.

Using data from an oracle, an app can display that information to its users or leverage that data to affect the outcome of smart contracts and actions within the app. For example, one very common type of oracle in DeFi is a price oracle: an oracle that makes the price of an asset in 1 ecosystem available in another.

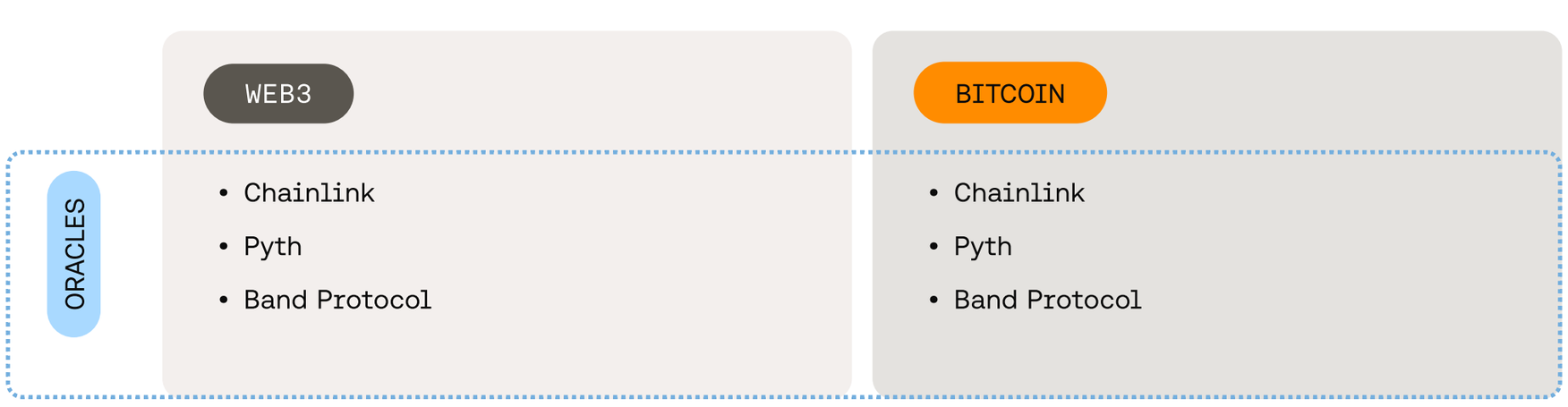
This is a critical function for DeFi apps that want to enable swaps between assets on various blockchains: developers need to ensure that the swap price is fair, and that users are getting market value (minus fees) for whatever asset they are swapping for.

The challenge with building oracles is around trust—how can you trust the data you get from an oracle? To combat that challenge, there are a number of oracle designs on the market today, including trusted-centralized solutions, federated oracle networks with reputation systems, and more.

Market Traction

Today, oracles have a market cap of $10.5B, which equates to 14% of the total DeFi marketcap, showing just how critical oracle infrastructure is to a functioning DeFi ecosystem. Without a way to accurately and reliably price assets, DeFi apps cannot go cross-chain.

Example Apps



Given their function, most oracles are cross-chain and support numerous ecosystems. Some of the most popular oracle solutions includ Chainlink, Pyth, and Band Protocol.

For inspiration, view Pyth's source code.

04 / More Complex Financial Protocols

With a better understanding of how to get BTC into a DeFi app and an overview of various DeFi primitives, it's time to dig a bit deeper. What are more complicated use cases that you can build in Bitcoin DeFi?

The world of finance is complex, and there are so many apps and services out there serving billions of people all over the world. This chapter will barely scratch the surface of what's possible, but hopefully the ideas included here can inspire you as you continue to explore the world of decentralized finance.

	APPS IN WEB3 DEFI	APPS IN BITCOIN DEFI
MONEY MARKETS (Lending/Borrowing)	• Maker • Compound • Aave • Maple Finance	• Zest • Arkadiko • Sovryn • Lend at Hodl Hodl • Tropykus
LIQUIDITY AGGREGATORS	• Yearn Finance • Beefy • Origin • Flamingo • Sommelier	• You?
DERIVATIVES	• GMX • dYdX • Drift • ApeX	• Hermetica Finance
AUTOMATED PORTFOLIO MANAGERS	• Enzyme Finance • Sets • Index Coop • dHedge	• Enzyme Finance • Sets • Index Coop • dHedge
LIQUID STAKING PROTOCOLS	• Lido • Rocket Pool • Marinade • Jito • Benqi	• StackingDAO
INSURANCE PROVIDERS	• Nexus Mutual • InsurAce • Unslashed	• Bitsure • Evertas

Money Markets (Lending + Borrowing)

Overview

One of the primary roles of banking institutions is financing loans and creating greater liquidity in the economy. The same is true in DeFi: money markets (lending and borrowing platforms) are a critical part of its infrastructure.

These platforms let users deposit crypto assets as collateral and withdraw loans denominated in stablecoins, enabling users to:

1. Earn interest on their assets, and/or
2. Take out loans against assets they don't want to sell

Market demand for these solutions is particularly pointed when it comes to Bitcoin: when the vast majority of Bitcoin's $800B market cap is sitting in cold storage. Users want to earn interest on their assets. Businesses want to take out loans to accelerate their growth.The pitch is simple, but the execution is more complicated. Money markets have complex designs to ensure the health of the protocol. This comes in two forms: 1) safely price loan:collateral ratio to make sure the protocol remains solvent and 2) offer some kind of credit score to ensure that users who regularly default on loans can't continue using the platform. This is a particularly challenging problem when crypto can be so volatile (which means that the collateral under-writing the loan is volatile too).

There's a lot of nuance in how to design a money market. Some of those parameters include:

- **Picking a lending asset:** Often money market protocols will use stablecoins (deposit a crypto asset and mint stablecoins against them. Some protocols like Maker and Arkadiko have their own stablecoin (DAI and USDA respectively). Others use an existing stablecoin, such as Compound using USDC. Some money markets don't use stablecoins at all and instead let users borrow a range of crypto assets directly, such as BTC loans with Zest.

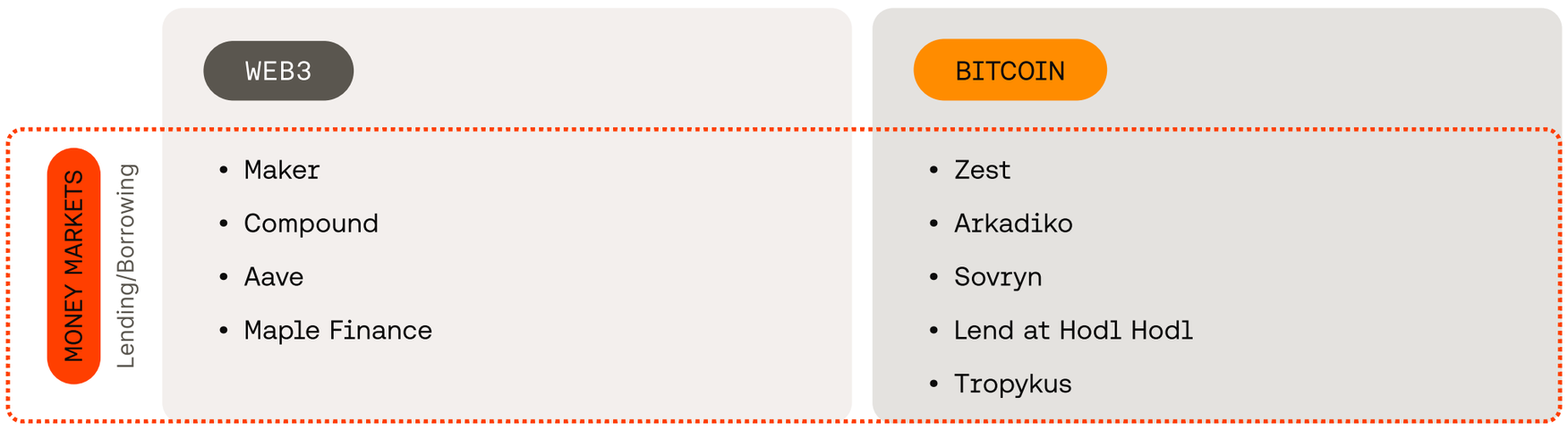
- **Setting a collateralization ratio:** at a high level, there are two types of protocols: collateralized debt and undercollateralized debt. Collateralized debt protocols are overcollateralized, meaning the total value of deposited collateral is always higher than outstanding loans (e.g. a user deposits $150 of BTC to mint $100 of a stablecoin), so in the event of a default, the collateral can always cover the loan. Undercollateralized loans are the opposite: a user can borrow more than they deposit, which is more capital efficient and encourages growth, but comes at higher risk.

There's a lot of ways to set these parameters and build a successful protocol—different designs cater to different users, whether individual lenders, small businesses, large institutions, and everything in between—and we will see all kinds of money markets succeed in Bitcoin DeFi.

Market Traction

The global crowdlending industry is expected to have a transactional value of $278B by the end of 2022, but in the world of DeFi, lending apps have a TVL of just $21B. Bitcoin DeFi might be the key to increasing the adoption of P2P lending in crypto markets if Bitcoin lives up to its expectations as 21st-century digital gold.

Example Apps



There are a number of high profile money markets in Web3, including Maker, Compound, Aave, and Maple Finance.

If you'd like to build lending applications for Bitcoin, you're in good company too. Arkadiko lets users take out loans against BTC and STX tokens. Zest Protocol is another Bitcoin DeFi project through which users will be able to put their BTC to work to earn Bitcoin yield through loans to institutional borrowers.

Other players include Sovryn for fixed interest loans and zero lines of credit, Lend at Hodl Hodl for global P2P lending, Tropykus for lending in Latin America.

To inspire your building, check out the source code of Zest.

Liquidity Aggregators

Overview

DeFi liquidity is broken up across numerous Web3 ecosystems as well as across various apps within each ecosystem. That can be a problem. Access to deep liquidity is critical for fair pricing and for user discovery: there's a lot going on in DeFi, and it can be hard to find the best protocols, the best pools, and the best individual financial strategy. Users are busy: it's hard to find time to do the research.

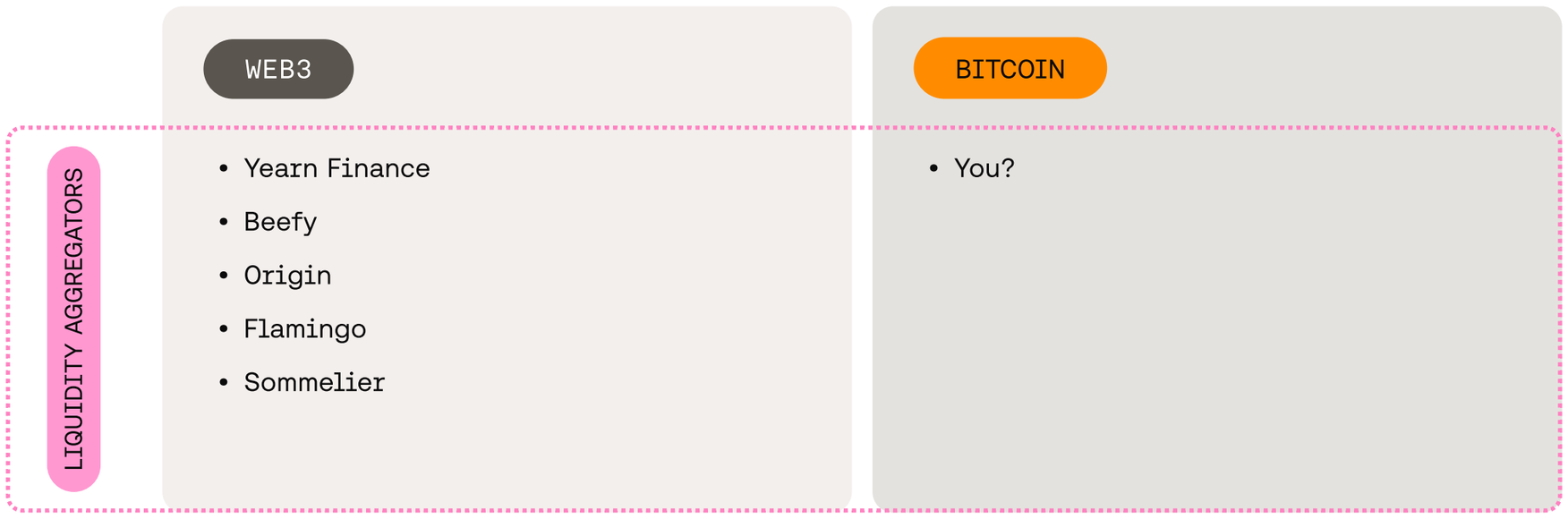
A number of players in DeFi have found success by offering a simple solution to users: aggregating various DeFi strategies under one roof and making the user experience easy, offering them the best strategies to earn the most yield in a simple to use interface. No more researching various projects, reading through white papers, and going through several onboarding flows.

Instead, these aggregators handle that research, handle the integrations, and provide a simple UX for users to discover and use various DeFi apps in one place, making it easy for them to compare the yields of various lending pools, swap assets from different apps, and more.

Market Traction

There are a few players in the yield aggregation space, and today, they have a TVL of $1.1B, about 2% of the total capital locked in DeFi.

Example Apps



There are numerous popular aggregators in Web3, including Yearn Finance, Beefy, Origin, Flamingo, Sommelier, and more.

Given the relative newness of Bitcoin DeFi, there are no aggregators specific to Bitcoin DeFi apps (yet)...a possible fruitful building ground for inspired builders.

To inspire your building, check out the source code of Yearn Finance.

Derivatives Protocols

Overview

As DeFi continues to speed run the history of finance, we are seeing the emergence of more complicated financial instruments. Enter the world of DeFi derivatives. Derivatives are popular instruments in TradFi that allow traders to get exposure to an asset without actually owning that asset. In DeFi, it's the same.

Derivatives include instruments like futures, options, swaps, prediction markets, collateralized loans, and more. These assets are ways to manage a portfolio and hedge price risk. For example, two parties could agree on an option contract that allows user A to buy an asset from user B at a set strike price at some point in the future, with User A paying User B a fee to have that option. This example is a way for both parties to hedge on the future price of the asset, mitigating both the upside and downside of that price movement.

As we've discussed in an earlier chapter, wrapped tokens are a popular way of migrating tokens from one ecosystem to another (as one might migrate Bitcoin to Bitcoin DeFi), and at a high level, you can think of any Bitcoin-backed asset as a derivative too.

Market Traction

The derivatives market is absolutely massive. In 2021, the gross market value of all derivatives in TradFi was $12.4 trillion, with a notional value estimated as highly as $600T for just half the year.

The DeFi derivatives market is much smaller, showing just how much room there is to grow. Today, derivatives have a TVL of $1.6B, roughly 4% of all of DeFi.

Example Apps

Some of the most popular derivatives protocols include GMX, dYdX, Drift, and ApeX. These exchanges offer perpetuals trading, spot trading, margin trading, leverage and more.

In the world of Bitcoin DeFi, you have apps like Hermetica Finance, which is building an exotic option strategy called the European Reverse Knock-out (ERKO).

For inspiration, check out the source code of GMX.

Automated Portfolio Manager

Overview

It's no secret that a lot of the attention in crypto to date has been around financial speculation. Despite that interest, crypto indexes, which basket a number of crypto assets into a single investment, haven't really taken off. Instead, users have to navigate multiple blockchains and multiple apps and self-custody each asset they want to hold, often across multiple wallets. It's a lot of work, particularly if you want a balanced portfolio, given that prices are so volatile.

An automated portfolio manager would enable users to invest across Web3 from a single interface, with a single investment, and help onboard hundreds of millions of new investors to Bitcoin and the world of Web3 at large.

Market Traction

Users want simple investing strategies. Look at TradFi, where indexes have over $4 trillion in net assets in the US alone across 5,000 different indexes. To put that in perspective, the total US stock market is valued at $46 trillion. ETFs were the 3rd most popular investment product in the US in 2020-2022.

Despite the popularity of indexes in TradFi, to date only $488M is locked in crypto indexes, which represents just 0.8% of the TVL of DeFi as a whole locked in indexes. Compare that to TradFi, where 8.6% of the market is held by index funds, and you can see the growth opportunity on the table.

Example Apps

AUTOMATED PORTFOLIO MANAGERS

WEB3	BITCOIN
• Enzyme Finance • Sets • Index Coop • dHedge	• Enzyme Finance • Sets • Index Coop • dHedge

Popular examples of indexes in Web3 include Enzyme Finance, Sets, Index Coop, dHedge, and more. Since the nature of an index is to invest across ecosystems and assets, we don't have examples unique to Bitcoin DeFi to share here because Bitcoin DeFi as a category is too new. There aren't enough sophisticated protocols and a wide enough variety of assets to have a Bitcoin-specific index.

However, as more and more Bitcoin DeFi innovations come to market, so will the demand for a Bitcoin DeFi index of sorts. You could imagine an index for all Bitcoin-native stables, or Bitcoin-based metaprotocols like ordinals.

To inspire your building, check out the source code of Enzyme.

Liquid Staking Protocols

Overview

Staking refers to participating in the consensus process of Proof of Stake (PoS) blockchains to maintain its security and process new transactions. At a high level, this requires users to "stake" an asset (lock it up for a period of time) in exchange for block rewards.

However, staking an asset means that the asset isn't liquid—it can't be used in DeFi. That's changed recently with the creation of liquid staking protocols, in which users can stake their assets (and earn yield via proof-of-stake in the process), and these protocols in turn mint a new token representing the staked asset in a 1:1 ratio. Users can then use these staked tokens in DeFi, leverage them as collateral, trade them with other users, and later redeem them for the corresponding staked asset.

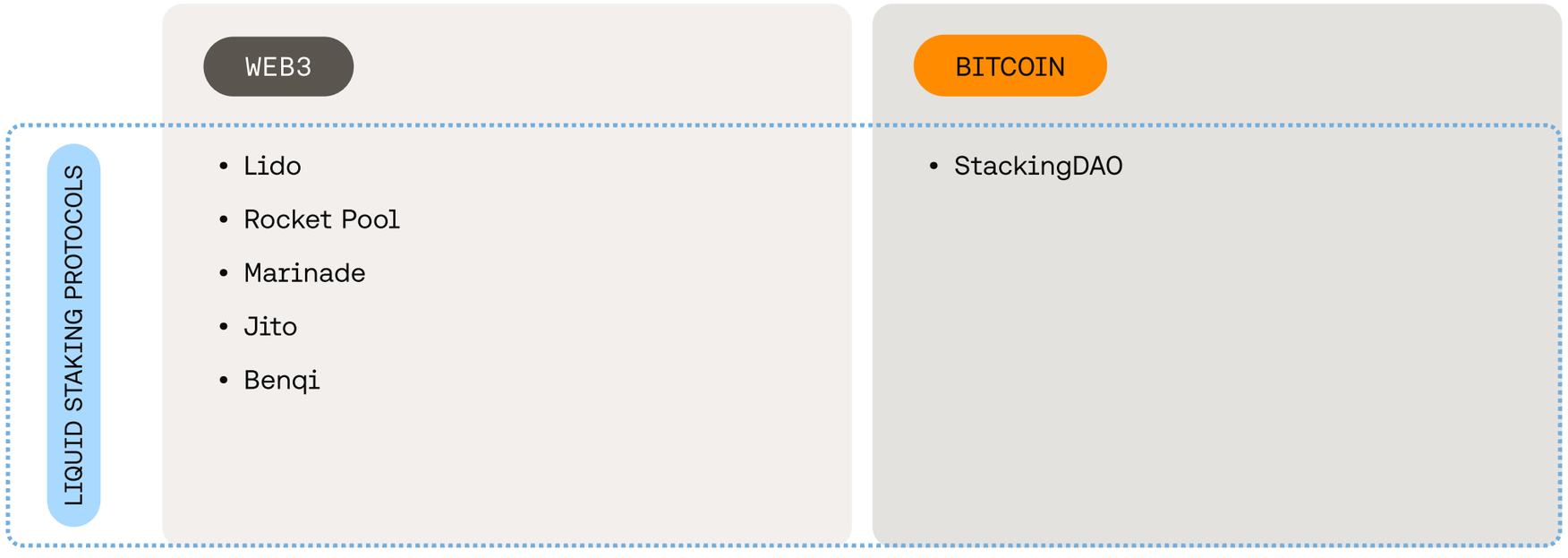
While Bitcoin doesn't use a PoS consensus mechanism, some Bitcoin layers employ a similar mechanism, so these liquid staking protocols will play a role in the Bitcoin ecosystem. For example, Stacks' Proof of Transfer (PoX) consensus mechanism enables users to earn BTC rewards through a process similar to staking called stacking, in which users lock up their STX tokens to help secure the network in exchange for Bitcoin.

Liquid staking protocols would enable Stacks (and other Bitcoin layers using PoS systems) to offer more liquidity and optionality to users in the ecosystem.

Market Traction

While relatively new, liquid staking protocols have become the most popular DeFi category, with a total TVL of $36.B—that's 62% of DeFi's total TVL as a whole.

Example Apps



The most popular liquid staking protocol is Lido, the Ethereum protocol that accounts for $20B in TVL on its own. Other popular options include Rocket Pool (also on Ethereum), Marinade (Solana), Jito (Solana), and Benqi (Avalanche).

In the world of Bitcoin DeFi, you have Stacking DAO for Stacks, which went live on mainnet in December 2023, and as of Jan 11th, already has $13.7M locked in the protocol.

To inspire your building, check out the source code of Lido.

Insurance Providers

Overview

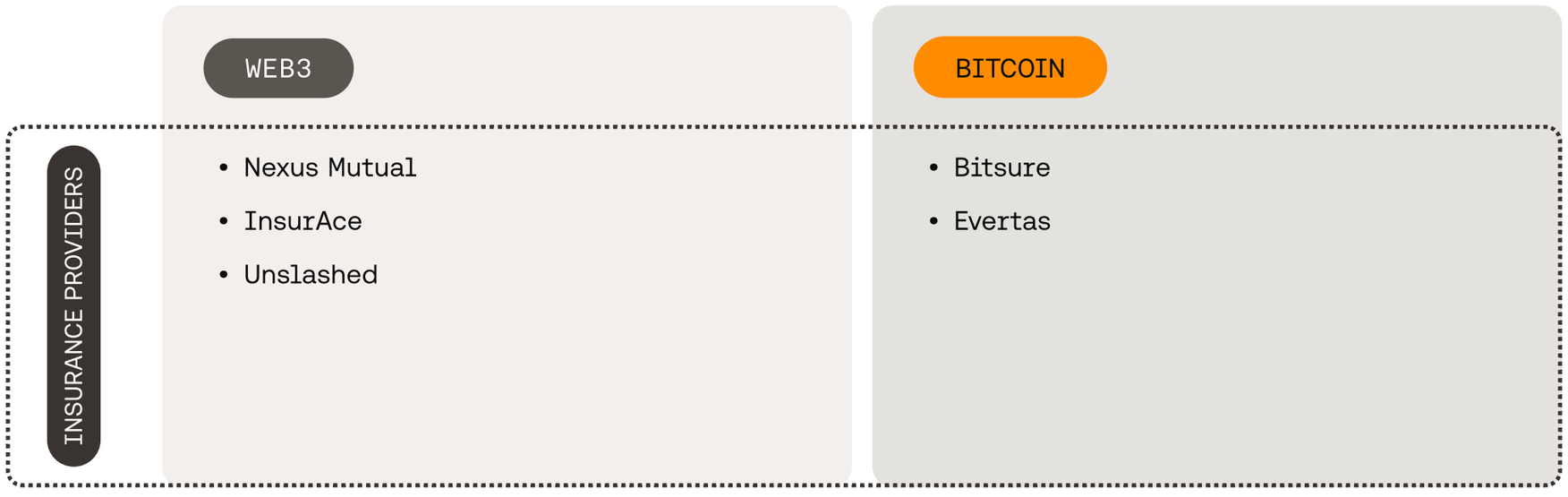
Risk management and loss mitigation through insurance is a core finance function that is appearing more recently in DeFi. These providers can protect users against loss from hacking, private key compromise or rug pulls. They also protect users from unique crypto-native events that don't occur in TradFi, such as protocol failure, stablecoin depegging, smart contract failure, and more.

These providers work similarly to how insurance works today: users buy insurance to protect their assets. The difference comes in who provides the cover. In TradFi, you'll choose and work with a single insurance company with their own underwriting team. In DeFi, protocols enable risk to be shared by a network of users. Users can deposit assets into various pools in the protocol, which underwrite different risks. In return, they can earn a % of fees from the premium fees paid by the users buying insurance.

Market Traction

Today DeFi insurance is much smaller than lending, with a TVL of about $319M compared to lending's $24.5B. However, you can expect the insurance market in DeFi to grow as more institutional and retail players enter the market. Looking at the world more broadly, the global insurance market is expected to hit $6.39T by 2025

Example Apps



Popular examples of insurance companies in the DeFi space include Nexus Mutual, InsurAce, and Unslashed. On the Bitcoin side, while not directly related to DeFi, you have Bitcoin mining insurance companies like Bitsure and Evertas. Over time, as the Bitcoin ecosystem continues to mature, we expect to see new insurance companies launch across different verticals, DeFi included.

To inspire your building, check out the source code of Nexus Mutual.

05 / Start Building Apps in Bitcoin DeFi

With your newfound understanding of DeFi, it's time to start building. Here are some tips on how you can get started:

1. Explore Successful DeFi Apps

   If you need inspiration on what to build, study the masters. In the previous chapters, we link to successful projects building a variety of DeFi apps in different ecosystems. Read their whitepapers and their designs. See what users are saying to understand why those particular projects got traction. Look through their source code to see how the team built it.

   Many devs have launched successful projects by simply recreating what worked in another ecosystem somewhere else. If you're in need of a Bitcoin DeFi idea that will gain traction, you don't need to look farther than other Web3 ecosystems to see what's gained traction there.

2. Get Ready for sBTC

   sBTC stands to be a major unlock for Bitcoin DeFi by creating a programmable, decentralized, Bitcoin-backed asset that can be used in apps across the Stacks ecosystem. Unlike other Bitcoin-backed assets, sBTC is **decentralized**, **trust-minimized**, **collateral-backed**, and powered by an **open membership** network that anyone can join.

   The hard-fork that enables sBTC is coming next year. You can start building a DeFi app on Stacks today to be ready when this asset hits mainnet in 2024. Be a part of the new wave of Bitcoin DeFi.

3. Start Building

   Now that you've finished our book on Bitcoin DeFi, it's time to begin the next stage of your journey: start experimenting. Start building. Below are some resources to get you started.

Bitcoin Primer

New to Bitcoin and Bitcoin layers and need a primer on how to build in the ecosystem? Check out this primer course which will teach you the basics.

Learn more

Community Tutorials

As you continue your journey, check out a number of community tutorials to teach you more fundamentals.

Learn more

Hiro Hacks

Once you get up to speed, sharpen your skills with a series of coding challenges that will familiarize you with our developer tools.

Learn more

sBTC Developer Release

You can view the sBTC developer release here, and via this guide, you can build a basic lending app.

Start building

The future is bright for Bitcoin DeFi. Welcome to the community. We can't wait to see what you build.

A Developer’s Guide to Bitcoin DeFi

/-/iro

hiro.so