Dexfin Litepaper

Abstract

The Dexfin platform provides easy and secure access to onchain protocols, services, and applications. Dexfin is a non-custodial platform, using a novel security architecture centered around onchain smart accounts and passkeys. Dexfin currently supports 7 EVM chains , including Base, and Arbitrum, with support for non-EVM chains Solana and Bitcoin. Dexfin is designed to replace centralized platforms as the primary point of interaction for crypto users.

Ecosystem Overview

Centralized exchanges have dominated the crypto ecosystem for over a decade, beginning with Mt. Gox. There is some irony in a peer-to-peer electronic cash system relying so heavily on centralized platforms for distribution. This situation arose because most users opt for convenience over security. Centralized platforms also enable more efficient speculation; early adoption was much faster because exchanges aggregated liquidity far better than peer-to-peer exchanges. Bitcoin adoption would, therefore, likely have been much slower without these centralized services. While there is nothing inherently wrong with bootstrapping network effects via centralization, the cost to users of these centralized services has been very high due to hacks and fraud.

We no longer need to compromise. We have reached an inflection point where decentralized infrastructure can compete with and exceed centralized services. It is time for a new phase of growth.

Core Philosophy

Dexfin is built to optimize the User Experience. To supplant centralized services, Dexfin must replicate the full user experience of centralized platforms. This contrasts with most decentralized services that start with infrastructure and protocol design and build out to the UX layer. For too long, we have built parts of the experience and expected or hoped adoption would follow. Empirical evidence has completely disabused us of this notion. However, while replicating the UX of centralized services, Dexfin must always remain non-custodial. Within these two constraints, many pragmatic decisions have been and will continue to be made to achieve the outcome of replacing centralized exchanges and other custodial services.

Feature Overview

Centralized services offer many features, which are listed and described below. Many different protocols can deliver these features. The following list is indicative only and represents protocols that have either been discussed by the team and early users. The Dexfin integration process is described later in this paper, but it is open, so anyone can propose integrating a new chain or protocol to deliver new functionality to Dexfin users.

Custody

Storing assets safely is the primary use case of Centralized platforms; however, to do so, they require the user to hand over custody. This can help users avoid losing access to their crypto, but it puts the user at risk of the platform stealing or losing their funds, either through hacks, fraud, or negligence.

The primary custody solution used by the Dexfin platform consists of a combination of passkeys, Lititprotocol, and individual smart accounts deployed to each chain. A proposed extension will use Litprotocol to deploy addresses to legacy chains like Bitcoin and Litecoin, allowing for self-custody while retaining the ability to recover from a lost passkey or other failure modes.

Swaps

Exchanges were created to provide a venue for users to swap or trade between different assets. Initially, this was between fiat and Bitcoin, but many different assets, including stablecoins, were eventually added. The complexity of supporting swaps grew further as new blockchains emerged in the early years of crypto. Today, one of the primary use cases of centralized exchanges is enabling users to trade assets across different blockchains.

Dexfin swap currently supports 6 chains with significant onchain liquidity across many different liquidity venues. The first swap implementation is our Meta Dex Aggregator on EVM chains, which allows swaps between many different assets, leveraging the top DEX aggregators on market. The first swap implementation for Solana will be Jupiter Exchange. Dexfin will be able as well support native swaps between BTC and other chains using Thorchain distributed swaps infrastructure.

Lending

The last cycle saw the rapid emergence and collapse of centralized lending services. The reasons for this growth and collapse are beyond the scope of this paper, but the primary issue was a misalignment of incentives due to the principal-agent problem. CeFi lenders were incentivized to maximize interest return, which led to a race to the bottom, where they lent to the highest-risk counterparties with little regard for preserving collateral. The collapse of platforms like Celsius and Blockfi clearly highlighted the incentive misalignment that can emerge when users give up custody of their assets.

Lending protocols like Aave are extremely robust and secure and have many years and billions of dollars worth of assets secured across numerous chains. For EVM, this will likely be the starting point for borrowing and lending. However, several new protocols offer different mechanisms and trade-offs that should also be explored, including Ammalgam and Morpho. For Solana, Kamino is likely the first lending integration, although other novel projects are being developed that leverage the faster block times of Solana.

Staking

While staking has existed for almost as long as crypto, the transition to PoS for Ethereum significantly accelerated this trend. Most centralized exchanges have some form of custodial staking service available for several different assets and blockchains, including Solana and Ethereum.

The two largest staking ecosystems are Solana and Ethereum. The primary mechanism for enabling staking is from LSTs (Liquid staking tokens). Dexfin will support many LRT tokens, including jitoSOL and wstETH. Eventually, the ability to stake SOL and ETH on the platform into liquid staking protocols will likely be added.

..

Yield Farming

One of the directions that launchpads have gone in is to offer staking to earn tokens in new projects; this is an attempt to replicate airdrop and yield farming that is more commonly executed onchain. One of the key advantages of a platform that uses onchain infrastructure is to be able to directly access these kinds of bootstrapping initiatives, whether they be offered by blockchain protocols or other projects.

Every new network and platform uses growth incentives to drive awareness and usage. While centralized exchanges attempt to replicate this process, it is highly inefficient and less effective in driving user behavior. Dexfin can provide significant user value and differentiation by connecting users directly to these incentives.

Defi AI Agent

An AI DeFi Agent is a sophisticated, system that leverages machine learning and natural language processing (NLP) to perform real-time market and sentiment analysis. It can interpret text or voice commands to execute crypto operations such as trading, staking, lending, or interacting with decentralized finance (DeFi) protocols. By analyzing vast amounts of data from various sources, the AI identifies trends, assesses market conditions, and makes informed decisions, optimizing returns while mitigating risk. Users can easily interact with the AI agent, either through typed commands or voice instructions, to manage their crypto assets and investments seamlessly across DeFi platforms.

Built-in Group chat

A group chat based on Push Protocol enables secure, decentralized, and real-time communication for community engagement, particularly within the Web3 ecosystem. It allows users to connect, share information, and collaborate through encrypted messages while maintaining full control over their data. Push Protocol leverages blockchain technology to ensure that messages and notifications are decentralized, transparent, and tamper-proof. Community members can engage in discussions, share updates, and receive notifications about events, airdrops, or token changes, all within a secure, censorship-resistant environment. By using wallet-based authentication, Push Protocol ensures that only verified participants can join the conversation, fostering trust and authenticity within the community. We will primarily create token/NFT gated chat for Dexfin community, but will be able to extend this to build group chats for other communities.

Fiiat on/off-ramp

A fiat-to-crypto on-ramp and off-ramp aggregator is a platform that connects users with multiple payment gateways, enabling them to easily convert traditional fiat currencies (like USD, EUR, etc.) to cryptocurrencies (like Bitcoin, Ethereum, etc.) and vice versa. This aggregator integrates various payment providers, such as credit card processors, bank transfers, and mobile payment solutions, allowing users to seamlessly access the best rates and options for buying or selling crypto across different platforms. It ensures a smooth and user-friendly experience by consolidating various on-ramp and off-ramp services into one interface, offering competitive fees, fast transaction processing, and a variety of payment methods to cater to diverse user preferences and geographic regions

Market Data Dashboard

The Dexfin Market Data Dashboard provides a comprehensive market overview designed to empower users with real-time insights and analytical tools essential for informed trading and investment decisions. It features detailed tracking of global market capitalization, enabling users to monitor market health at a glance, alongside dynamic highlights of trending tokens to quickly identify promising opportunities. The integrated Dex Explorer simplifies navigating decentralized exchanges, providing transparent transaction data and liquidity metrics. Users stay continuously informed through curated market news, a customizable alert system that notifies them of significant price movements or critical market events, and a dedicated calendar for upcoming crypto events, including launches, updates, and community engagements. Additionally, the dashboard includes a live feed aggregating essential market updates, ensuring users never miss important developments in the fast-paced crypto landscape.

Launchpad - planned feature

Binance initiated the IEO following the collapse of the ICO boom in 2018. The concept was to launch new projects directly with an exchange listing. While these platforms have pivoted away from direct token launches over the years, there is a significant opportunity for a decentralized solution.

The rise of platforms like pump.fun has been significant over the last year. However, these platforms have high barriers to entry for centralized exchange users. By enabling easier and safer onboarding, allowing users to access earlier-stage tokens and memecoins will drive significant adoption.

User Acquisition

Crypto adoption tends to follow a cyclical pattern, with each peak bringing a surge of new users into the ecosystem. With every cycle, the number of participants grows significantly, often by at least an order of magnitude. This presents a prime opportunity for any emerging platform to challenge the dominant players from the previous cycle. A look at the top platforms from each wave of adoption reveals this pattern; analyzing data across cycles, we observe clear trends of market share dominance among these platforms, even with some variability in regional exchange data. For simplicity, our focus here is on exchanges serving a global audience.

Cycle	ATH (BTC)	ATH Date	Dominant CEX
2009 - 2011	$29.58	09-06-2011	Mt. Gox
2012 - 2015	$1242	29-11-2013	Mt. Gox (pre-collapse), Bitstamp
2015 - 2018	$19783	18-12-2017	Binance, BitMEX (Perps)
2019 - 2022	$67566	11-08-2021	FTX, Binance
2023 - TBC	$73700	13-03-2024	Binance

This pattern of new platforms displacing incumbents is driven by two main factors: the influx of users with limited brand loyalty and the shift in product focus across cycles. Over five crypto cycles, new user acquisition has been fueled by different catalysts, from early Bitcoin demand and altcoins to ICOs, perpetual futures with high leverage, and the rise of the Solana ecosystem. While the NFT boom primarily took place on decentralized platforms, it also played a role in driving recent adoption waves. The factors driving user demand in the current cycle remain to be seen, but **Dexfin** is strategically positioned to leverage on-chain applications and services for growth. On-chain growth strategies, mainly through token and points incentives, will be a key acquisition method, making Dexfin a leading platform to provide secure and user-friendly access to these opportunities.

Distribution

Distribution is essential for capturing and directing user attention. Centralized platforms have historically controlled crypto distribution, with the exception of the brief NFT adoption period. This has created challenges, primarily because centralized services do little to support blockchain security. For example, when Bitcoin custody is dominated by centralized services, fewer transactions settle directly on the blockchain, reducing peer-to-peer activity. This, in turn, weakens Bitcoin's security, as blockchain security is closely tied to demand for block space—an issue that becomes more pressing with each halving as block rewards decline. Additionally, exchanges often drive price-centric distribution, distorting markets and compromising the integrity of network evaluations.

The current market structure is imbalanced, but adopting a platform driven by the underlying technology offers a promising solution. Such a platform creates a feedback loop where the most efficient protocols and applications capture greater market share and awareness, fostering healthy competition and efficiency across the ecosystem.

A platform like Dexfin, which relies on the infrastructure developed by on-chain projects, contributes positively to the ecosystem. At scale, Dexfin will encourage the fundamental use of protocols and on-chain services, rather than focusing solely on asset prices. This alignment fosters a healthier ecosystem where platforms and applications can be directly compared based on utility and efficiency, thanks to an integrated and aggregated single platform.

Technical Architecture

Crypto protocols have traditionally been deployed on one or more chains, with users accessing them via front-end web clients connected through RPC and using browser wallets. This setup, which relies on storing all state on-chain, limits user experience (UX) and can be fragile. As protocols have grown more complex, integrating them into interfaces has become challenging, highlighting the limitations of this architecture.

Dexfin takes a different approach, prioritizing censorship resistance at the protocol layer while assuming the rest of the stack will remain accessible. Though this diverges from a strict cypherpunk ethos, it enables the platform to offer an accessible UX crucial for mass adoption. The poor UX of thin clients has led many users to centralized platforms, but by bridging this gap and deprioritizing censorship resistance as the primary design goal, Dexfin provides an experience that encourages migration away from centralized exchanges.

The **Dexfin Platform** is a vertically integrated application consisting of:

Frontend App

The **Dexfin Web Interface** is a modern React Single Page Application (SPA) built with TypeScript, Vite, and Tailwind CSS, utilizing popular tools from the React ecosystem for a responsive and robust user experience. For secure user authentication, it uses WebAuthn APIs to create and manage Passkeys directly within the browser. The app leverages tRPC as the client to communicate with the Dexfin Backend, ensuring type-safe, seamless integration across the entire stack.

Backend Services

The backend is developed in TypeScript and deployed on Cloudflare Workers, providing a scalable, secure environment for managing user sessions, processing core backend logic, handling database interactions, reading and caching blockchain data, and orchestrating onchain transactions. Persistent state is maintained through Cloudflare Durable Objects and a MySQL database hosted on PlanetScale for reliable data storage.

Onchain Infrastructure

Dexfin Accounts are designed to operate across EVM-compatible chains as well as Solana, with Smart Contracts written in Solidity for EVM and Programs written in Rust for Solana. Dexfin's onchain design is leveraging ERC-4337 (Account Abstraction) standard and will leverage chain abstraction in order to offer seamless interaction with various blockchains united under one unified account.

To handle gas and relay transactions on EVM chains, Dexfin uses Zerodev, while Solana transactions are routed through Dexfin's RPC providers, Triton and Helius.

Protocol Integrations

Integrating with onchain programs, contracts, or protocols involves inherent risks, which Dexfin mitigates through a specially designed, modular architecture. Integrations are isolated to safeguard the primary Dexfin Account, allowing users to opt-in to each onchain protocol individually. This approach also minimizes the complexity and frequency of updates to the main Dexfin Account contracts and programs.

Dexfin integrations operate through dedicated programs and contracts that the main Account interacts with via a restricted interface, providing a layer of separation from the Account's private keys. These integrations are fully onchain, with Dexfin managing the backend and user interfaces for a smooth user experience. This modular setup allows Dexfin to expand its functionality beyond centralized exchanges, leveraging onchain composability while controlling complexity. The core Account implementation remains stable with infrequent updates, while individual integrations can be updated regularly, each explicitly opted into by users.

Security Overview

Dexfin simplifies onboarding by enabling users to effortlessly create secure crypto wallets using familiar social logins, such as Google, Apple, Facebook, or Twitter. This streamlined approach eliminates the complexity typically associated with wallet setup, removing technical hurdles and reducing the friction of entering the crypto ecosystem. Users can sign up in seconds, instantly gaining access to powerful decentralized finance tools without needing to remember complex seed phrases or private keys. Enhanced by robust security measures, Dexfin ensures assets remain protected, combining convenience with strong encryption and seamless user experience.

Passkeys

Passkeys are another mechanism securing Dexfin Accounts and authorizing onchain transactions. When users create an Dexfin Account, a passkey (a public-private key pair) is generated by their operating system or password manager and securely stored on their device. The private key remains inaccessible to both the browser and Dexfin. Signing a challenge requires an on-device biometric or password verification, depending on the user's system or password manager.

Passkeys offer robust security by being (a) phishing-resistant, (b) inherently strong, and (c) free from shared secrets. Unlike usernames and passwords or traditional crypto wallets, passkeys cannot be written down, forgotten, or used on non-Dexfin domains, making them a superior choice for account security.

When users log into the Dexfin App, the backend service validates the passkey signature and creates a secure session for the user.

Since passkey signatures currently cannot be verified directly onchain, Lit protocol is used to translate passkey signatures into chain-compatible formats (ECDSA for EVM chains and Ed25519 for Solana).

Lit Protocol

Lit Protocol enables decentralized key management by using a distributed network of nodes to share and manage cryptographic keys without relying on a single point of control. This approach allows users to securely encrypt, access, and authorize data or actions across blockchain and Web3 applications while maintaining privacy and control over their keys.

Secure by Design

Dexfin combines the best of centralized exchange security features (like account recovery, two-factor authentication, and session elevation) with onchain benefits such as transparency, censorship resistance, and decentralization. Recognizing that security needs vary based on user experience, Dexfin's system is designed to provide a balance between security and usability, ensuring that protection mechanisms align with typical usage patterns.

Fund Recovery

A standout feature of Dexfin's security design is fund recovery. If a user loses access to their passkey, they retain a secure way to recover funds.

This process raises two key questions:

1. **How can a user authenticate without their passkey?**
2. **Where should recovered funds be sent?**

For users familiar with onchain security, Dexfin allows recovery via signing a transaction with their own wallet (EOA). For others, social sign-on through Apple or Google accounts provides a secure recovery option. Dexfin acts as a trusted signer to translate off-chain account verification to onchain fund recovery.

Users can link all three recovery methods to maximize recovery options. Since passkey recovery is considered more secure than both EOA and social sign-on (due to the risks of private key theft, phishing, or social account resets), Dexfin requires users to designate a recovery address before displaying their Dexfin Account deposit address, adding an extra layer of security.

By aligning account security with user experience, Dexfin ensures a resilient recovery mechanism.

Censorship Resistance

Funds recovery also supports censorship resistance. If access to a user's Dexfin Account is disabled or if Dexfin were to go offline, users can recover funds by signing a transaction with their recovery EOA directly on the blockchain.

Certain aspects of funds recovery (such as bridging and cross-chain syncing of recovery addresses) currently rely on the Dexfin backend. To increase resilience, Dexfin plans to develop an open-source recovery app hosted on GitHub and expand onchain functionalities for guaranteed fund recovery under any circumstance.

Governance

Dexfin is committed to a neutral, community-driven governance framework, crucial for shifting from centralized to onchain ecosystems. Crypto's history is marked by tribalism, yet Dexfin offers a chance to unite diverse groups around the shared goal of onboarding millions of users to a decentralized platform built on onchain infrastructure.

Dexfin's governance structure includes a Dexfin token, representing governance power. A gated sale will ensure broad token distribution, accessible only to users who created an account and deposited funds during the launch campaigns.

Conclusion

The Dexfin platform is the culmination of a decade of advancements in onchain technology, combining security, usability, and governance into a cohesive ecosystem. This progress reflects the relentless efforts of engineers, developers, and investors who believe in crypto's transformative potential. Dexfin embodies this vision, marking a pivotal step in redefining finance through onchain infrastructure. With Dexfin leading by example, the crypto industry is poised to demonstrate its capability to disrupt traditional finance and revolutionize global coordination.

Business Model & Revenue Streams

1. Transaction Fees
Small fees on token swaps and fiat on/off ramp transactions.
2. Premium AI Analytics Subscription
Advanced market insights
3. Revenue from Third-Party Integrations
Staking, lending, and liquidity partnerships.

Roadmap

Q1 2025

- Dexfin Web App Beta Launch
- Dexfin AI Beta Release
- Seed Sale of DXF Tokens

Q2 2025

- UI/UX Overhaul based on user feedback
- Centralized Exchange (CEX) Listing
- Feature extensions - Fiat On/Off ramp, Social feed, AI Agent automizations, DCA, yield.
- DEX Listing
- Public Sale of DXF Tokens

Q3 2025

- Integration of More Third-Party DeFi Services
- Mobile app development
- Premium Analytics Subscription Launch

Q4 2025

- Premium Analytics Subscription Launch
- Ecosystem Expansion & Partnerships
- More features - Launchpad