Genius: CEX On-Chain For The Next Billion Users

A. Kalsi, B. Sundararaman, K. Tora, M. Hussain, R. Myher, S. Kumar, S. Videau,
Written by members of the Shuttle Labs team, who contribute to Genius Bridge Protocol and Genius Terminal

Abstract

This paper presents Genius Bridge Protocol **(GBP,** version 0) and Genius Terminal (www.tradegenius.com), the protocol's associated front-end. GBP is a modular, novel non-custodial cross-chain intent bridge that utilizes Lit Protocol as a global solver to which anyone can contribute liquidity without needing to maintain their own rebalancing infrastructure, minimizing the prevalent centralization risk associated with solvers today. GBP further supports arbitrary call data execution post solving for liquidity allowing for full cross-chain intent execution and abstraction. The Genius Terminal front-end is a trading tool that utilizes GBP to enable entirely chain-invisible cross-chain trading for the end user, rivaling the performance and user experience of a centralized exchange ('CEX') while minimizing counterparty risk. On Genius Terminal, gas management, address management, transaction signing, dApp interactions, and user-facing bridges are entirely eliminated from the user workflow, and are condensed into a single click. This is achieved by leveraging programmable key-pairs, where Genius Terminal is able to programmatically specify the behavior of an Externally Owned Account ('EOA') without taking custody of the EOA's private keys, and uses GBP's liquidity vaults (reserves) within the protocol that live on multiple networks to facilitate cross-chain orders. Unlike traditional solver systems that feature centralized actors competing to fill orders via an off-chain order flow auction, GBP employs decentralized orchestrators. These orchestrators are governed by deterministic JavaScript code, executed and validated on Lit Protocol's secure multi-party compute network. By utilizing native decentralized exchange (DEX) liquidity across networks, GBP enables low-fee swaps for any token on any supported blockchain. GBP's architecture is not constrained by virtual machine type, offering interoperability between EVM, SVM, Movement, Bitcoin, TON, and the Cosmos ecosystem and more. Because Genius Terminal, GBP's front-end, is able to programmatically sign on a user's behalf, the protocol is able to natively call external protocols without the user having to connect to or independently fund accounts on third-party dApps, allowing GBP and Genius Terminal in conjunction to execute on the vision of being the final destination of on-chain finance.

1.0 Motivations

1.1 Counterparty Risk and Opportunity

The collapse of FTX in 2022 exposed significant vulnerabilities in the operation of centralized exchanges, namely counterparty risk. This event precipitated a severe erosion of consumer trust, undermining the industry's claims of transparency relative to traditional financial systems. Nevertheless, FTX attracted a substantial user base, and took a unique place in the cultural zeitgeist as a venue to create real wealth, doing over $21 billion in volume a day in 2021.[1] The exchange was described as the next, obvious movement in the evolution of financial technology toward anti-fragility more broadly. And while this is sincerely true of crypto's effect on financial technology, the irony associated with FTX's collapse only highlights that a *centralized* trading venue cannot deliver on this promise.

[1] BusinessofApps, "FTX Statistics: Revenue, Users & More", March 15, 2024.

Significantly, a lot of true wealth creation happens on-chain. The number of meme-coin millionaires and general liquidity around memes, a trading category in which internet-natives are inherently advantaged in wealth creation, is evidence of latent demand for an open arena for speculation. Members of the ShuttleLabs team have written more extensively about this phenomenon. And yet, this speculation is far out of reach for the average trader; the anecdotal brand awareness of Coinbase vs UniSwap is an obvious example to those in the industry. So why do centralized exchanges win?

1.2 Aggregation, not centralization

Centralized exchanges (CEX) are preferred to their decentralized counterparts because users do not face technical complexities when transacting using their assets on these exchanges. The user does not have to sign transactions, manage gas, or bridge assets within a CEX and has access to peace-of-mind tools like recovery emails, multi-factor logins and passkeys. This is such a meaningful barrier to entry that a net-new user has historically chosen to trade off minimized counterparty risk as well as unfettered access to opportunity (no listing teams) of battle-tested DEXs like UniSwap for the efficiency and ease of use of an exchange like Coinbase. Further, a user on a centralized exchange is most likely unaware of which network an asset lives on when they are making a purchasing decision, and is swayed only by price action. However, it is important to note that CEXs are not inherently better *because* of their centralization, but because everything is in one place, with one unified interface; simply, a CEX's primary advantage comes from a meaningfully more *aggregated and abstracted* alternative to the disparate resources and liquidity pools on DEXs.

2.0 Intents and Solvers

Chain Abstraction is Not Enough

2.1 The Uninspiring Chain Abstracted Present

The demand for intent-based bridges represents a real appetite for faster solutions to conventional bridges and a unification of the vastly distributed liquidity that exists on decentralized networks today. And intent-based bridges are very useful for this purpose. However, the three core problems with existing intents architecture are the centralization associated with *solving*, the lack of sufficient incentives to change the aforementioned centralization risk, and the apparent inability of infrastructure builders to commit to building a real, application specific use case of their infrastructure.

2.2 Centralization and Trust Assumptions of *Solving*

The intent-solver model, despite its widespread claims of decentralization, introduces severe centralization risks on the solving side. Empirical data from Across, a popular intent-based bridge, reveals that a single agent, operated by Risk Labs (the team behind Across), filled 92.8% of the total order flow on the platform.[2] This is an obvious example of centralized concentration. Similarly, in DLN, another leading intent-based protocol, three agents handle the majority of order flow, with patterns suggesting these agents are likely operated by the DLN team itself.[3] This centralization extends beyond individual protocols; the broader intent-based ecosystem is dominated by a handful of well-capitalized market makers like Wintermute or protocol teams themselves, who run the risk of becoming "rent seeking middlemen".[4] The barrier to entry for new solvers is prohibitively high, with some protocols requiring

[2] LI.FI, "The Untold Trade-Offs in Intent-Based Bridges", March 15, 2024.
[3] Ibid
[4] Q. Kilbourn, G. Konstantopoulos, "Intent-Based Architectures and Their Risks", Paradigm, June 1, 2023.

multi-million dollar investments just to participate. For instance, Synapse Labs proposed taking a $5 million loan from the Synapse DAO merely to deploy an agent in SynapseRFQ.[5] These factors create a system that is functionally centralized and inaccessible to the average liquidity provider.

2.3 Solver Incentives

The economic incentives in the intent-solver model are fundamentally misaligned with user interests. In Across, 98.6% of transactions (104,952 out of 106,442) face no competition among solvers.[6] This lack of competition eliminates any potential benefits of an auction system, leaving users at the mercy of monopolistic pricing. The situation is similarly dire in DLN, where 91.9% of bids are unopposed.[7] This absence of competition is not a temporary state; it is a structural issue arising from the high costs and complexities of running solver infrastructure across multiple chains. Solvers must constantly rebalance to fulfill cross-chain intents, a task that becomes exponentially more complex as the number of supported chains increases.[8] There is a broad analogy to be made here to other industries where centralization leads to maximal efficiency gains that are net beneficial—cloud computing clusters are an apt example—but concentrate pricing power as an unintended byproduct. The incentives simply do not exist for larger players to *want* to more efficiently decentralize risk.

2.4 User Experience

The term "chain abstraction" is not sufficient to capture the real end state of on-chain activity—chain *invisibility*. Chain abstraction protocols in their current implementation still require knowledge of transaction signing, gas management, and multi-chain address management. In practice, a swap from Arbitrum to Solana on DLN still requires knowledge of native gas on two separate virtual machines, and two separate account addresses, as well as the allocation of capital to different chains. While this certainly moves the needle in terms of the speed of cross-chain DeFi, it does not address the other problems with on-chain transactions, offering only a partial solution to the "UX problem" and falls short of realizing the vision of beating a centralized exchange on both centralization risks and usability.

3.0 Genius Part One:
Genius Bridge Protocol (GBP):

The Global Liquidity Orchestration Layer—The Road for The Car

3.1 Goal: Enable the *Chain Invisible* Future

The goal with adopting the following architecture within GBP is two-fold: (1) be meaningfully more decentralized than existing solver architecture, and (2) leverage existing DEX liquidity to facilitate lower fees and create novel incentives for liquidity providers. In this way, the protocol's aim is to be the missing UX layer of crypto. To use an analogy, GBP is to be a multi-purpose road on which any car (chain invisible app) can drive. Genius Terminal (expanded in section 4) is the beautifully designed sports car that was purpose-built to drive on this specific road. To build this infrastructure "road" layer, GBP is partnered deeply with Lit Protocol.

---

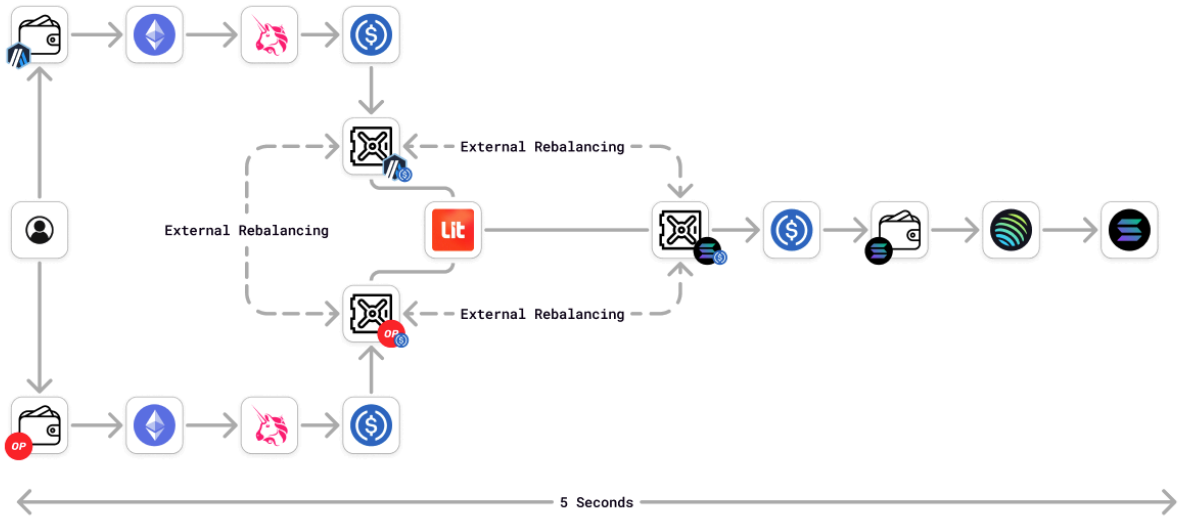
[5] LI.FI, "The Untold Trade-Offs in Intent-Based Bridges", March 15, 2024.
[6] Ibid
[7] Ibid
[8] Ibid

3.2 Overview of Lit Protocol and Lit Actions

Lit Protocol is a decentralized key management network enabling programmable signing and encryption. It operates through sealed encrypted virtual machines (Trusted Execution Environments) on independently operated servers, ensuring processor interiors remain inaccessible; that is, the code that the processors are running remains inaccessible to the processors themselves.[9] Lit employs distributed key generation, where key pairs are shared among operators, with no single party holding the entire key. Operations require two-thirds network consensus, enhancing security. Lit nodes use AMD's SEV-SNP for hardware-level isolation.[10] Each node contains a JavaScript environment for executing immutable Lit Actions governing signing and encryption operations. Lit Actions are extremely composable logic that can be used to orchestrate wallet behavior cross-chain and automate web3 functions. Given that these Lit Actions are stored on an IPFS CID, the action is immutable and persistent. The protocol supports multiple cryptographic curves, enabling wide interoperability. Lit Actions are used to create Genius Protocol's decentralized bridge solving model, which is expanded below.

3.3 Overview of GBP's functional mechanism

A high level overview of Genius Bridge Protocol architecture is pictured here:



1. **Source Chain Operations:**
   The user initiates an order by calling the Genius Router (see section 3.4). Their funds are swapped from the source token to USDC using native DEX liquidity. This USDC is subsequently deposited into the Genius Vault on the source chain. To ensure the best rates, the protocol queries multiple DEX aggregators. The Genius Vault contract then emits a successful deposit event. Using a Lit action, the protocol coordinates with the target chain to ensure any target chain operations are only taken once this source chain action/swap is confirmed. Genius often achieves positive slippage, directly benefiting the user.
2. **Target Chain Operations:**

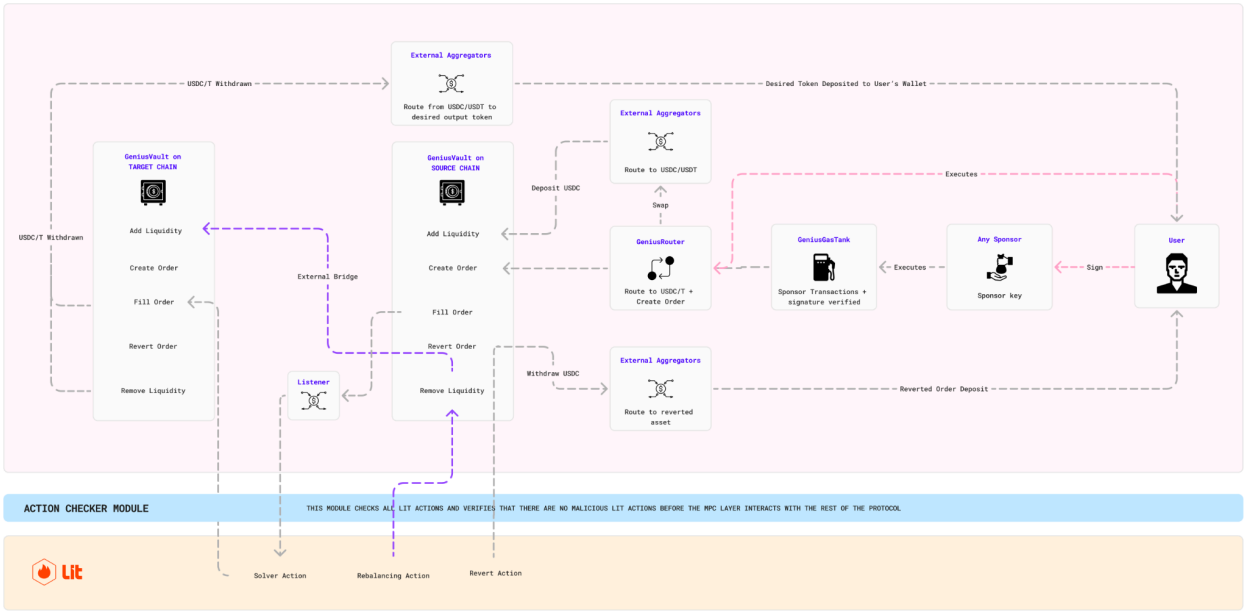
[9] Lit Protocol, "Access Control Overview", March 15, 2024.
[10] Lit Protocol, "What is Lit Protocol?"March 15, 2024.

USDC is swapped from the Genius Vault liquidity reserves that the protocol owns and manages, and to which anyone can contribute, into the desired target token, leveraging native DEX liquidity once again. The best available rate is again secure through querying various DEX aggregators. A withdrawal event is emitted only if a successful withdrawal, swap, and transfer to the user have occurred, programmatically via a Lit Action.

3. **Liquidity Sourcing:**
   The unique proposition of Genius Solving is that anyone can provide USD denominated liquidity and earn yield on it by taking advantage of Genius Protocol's rebalancing infrastructure, without themselves having to create complex multi-chain rebalancing infrastructure. This goes a long distance in democratizing who can be a solver and challenges the conventional tacit understanding that solvers are sophisticated market markers.
4. **Liquidity Rebalancing:**
   The protocol periodically rebalances USD liquidity between supported networks.The smart contracts operate at a specified minimum liquidity level of 25% (current value) to ensure immediate liquidity withdrawals. The protocol utilizes liquidity depending on demand on the target chain, and rebalances to prevent excessive skewing of deficits and surpluses across chains. This rebalancing between vaults occurs by the best available cheapest external bridge (eg., Wormhole, LayerZero etc.), which is amortized to all users and is absorbed in the Genius Protocol fee. The protocol's liquidity reserves facilitate instant trades, mimicking the efficiency of centralized exchanges while maintaining a decentralized structure. This is carried out via Orchestrator wallets, which is returned to in 3.4.

3.3 Modules

Genius Protocol is modular and extensible. This section details the key modules and their functions within the protocol.



Router Module

The Router Module handles order creation within Genius vaults. It manages the conversion of specified assets into the protocol's stable asset (USDC on most supported networks, USDT on BNB Chain) on the

source chain, determines optimal swap paths, and deposits the resulting stable coin into the appropriate vault.

Vault Module

The Vault Module manages liquidity addition and removal across chains for cross-chain orders and liquidity rebalancing. For cross-chain orders, the vault on each network is responsible for accepting and removing liquidity as determined by user intent. The order payload is sufficiently robust to handle order creations, reversions on failure, limit order support, and arbitrary calldata execution. This means that using the vault module, users can execute complex actions cross-chain, such as taking out a perpetual position in a single order.

Order processing involves generating a unique hash from the order information and a seed, crucial for fulfillment on the target chain. This seed is verified by a Lit Action. Post-execution, the transaction is verified through a Lit Action.

For liquidity rebalancing, a Lit Action takes into account the total amount of liquidity available on the Genius vaults across all supported networks and determines which chains are at risk of running out of liquidity, and which chains have a potential surplus. The action subsequently calls an external bridge via an Orchestrator to rebalance liquidity to ensure a dynamic equilibrium.

Note: The Solana vault contract operates similarly to the EVM-based vault. For swap actions where Solana is the target chain, Genius utilizes Jito bundles to ensure atomicity and efficiency. The bundled transactions include transferring USDC from the Solana Virtual Machine (SVM) vault to the SVM orchestrator, swapping USDC for the desired token, and performing post-swap checks on the Genius Solana smart contract to validate token transfer amounts. Jito bundles guarantee that these transactions either succeed together or fail as a unit, ensuring order integrity.

Gas Tank Module

The Gas Tank enables transaction sponsorship on EVM, eliminating user management of gas fees. It allows third parties to sponsor transactions. The architecture uses Uniswap's permit2 smart contract for transaction execution by user-authorized entities. The Gas Tank includes error handling to ensure only designated sponsors can execute transactions. It further verifies user intent via a signature hash of their order parameters.

Actions Safety Module

The Actions Safety Module secures Lit Action execution within Genius Protocol. Implemented as a singleton contract (on a single chain), it serves as the central authority for Lit Action permissions. Each Lit Action must verify its permission status with this contract before execution. The Genius Foundation DAO (a separate and entirely sovereign entity from Shuttle Labs Inc) governs this module and can designate "Guardians"—individual and DAO-selected EOAs with specific security powers. Guardians can disable Lit Actions in response to vulnerabilities or threats, preventing large-scale security breaches. The pause mechanism allows Guardians to initiate a pause, but only a designated multisig wallet can unpause the contract, ensuring a balanced approach to emergency responses and recovery.

3.4 Account for GBP's use of Lit Protocol:

Orchestrator Wallets: these are Programmable Key Pairs (PKPs) whose authentication scope is limited to approved DAO Lit Actions. In other words, these wallets can only ever execute a transaction when called by an approved Lit Action. Orchestrator PKPs can be created on demand as transaction volume and demand grows. A PKP has one wallet per chain attached to it. For example, one Orchestrator PKP

operates on all networks the protocol is live on. To begin with, Genius Protocol will have 10 Orchestrator PKPs to fill user orders and rebalance liquidity across the protocol.
Rebalancing: Lit Actions are employed to perform automated calculations and rebalancing operations for the protocol. These actions utilize orchestrator keys to execute complex rebalancing tasks across multiple chains, ensuring optimal liquidity distribution without manual intervention.
Intent Solving: The protocol utilizes Lit Actions to solve intents within the Genius ecosystem. This approach allows for decentralized and efficient processing of user intents, enhancing the protocol's ability to execute cross-chain transactions and complex DeFi operations.
Fee Distribution: Lit Actions will play a crucial role in the fair and efficient distribution of fees to liquidity stakers. More details about this will be released when liquidity staking is live.
Order Reversion: In scenarios where an order cannot be solved within the specified time frame and subsequently expires, Genius Protocol employs Lit Actions for order reversion. An orchestrator can trigger the reversion transaction using Lit Actions. A dedicated Lit Action is regularly executed to identify and revert failed orders, ensuring that users' funds are not indefinitely locked in expired orders.

3.5 On Decentralization, Incentives, and Invisibility

Decentralization: Decentralized orchestrator wallets, governed by deterministic JavaScript on a secure multi-party compute network, replace centralized solver models. This, combined with protocol-owned and user-staked liquidity, mitigates centralization risks and reduces liquidity provision barriers.
Incentives: Dynamic fee structures based on slippage and volume optimize transaction costs. Direct positive slippage pass-through to traders. The protocol's liquidity model facilitates competitive rates and flexible swap sizes. Traders can provide liquidity to the protocol in USDC. The same traders then have an incentive to trade on Genius because their trades contribute to fees that their own liquidity accrues. The protocol also has sizably lower fees than competitors like DLN because GBP utilizes native DEX liquidity without external solvers, as a direct result of the security of Lit Orchestrators filling orders.

4.0 Genius Part Two
Genius Terminal: The CEX experience on-chain

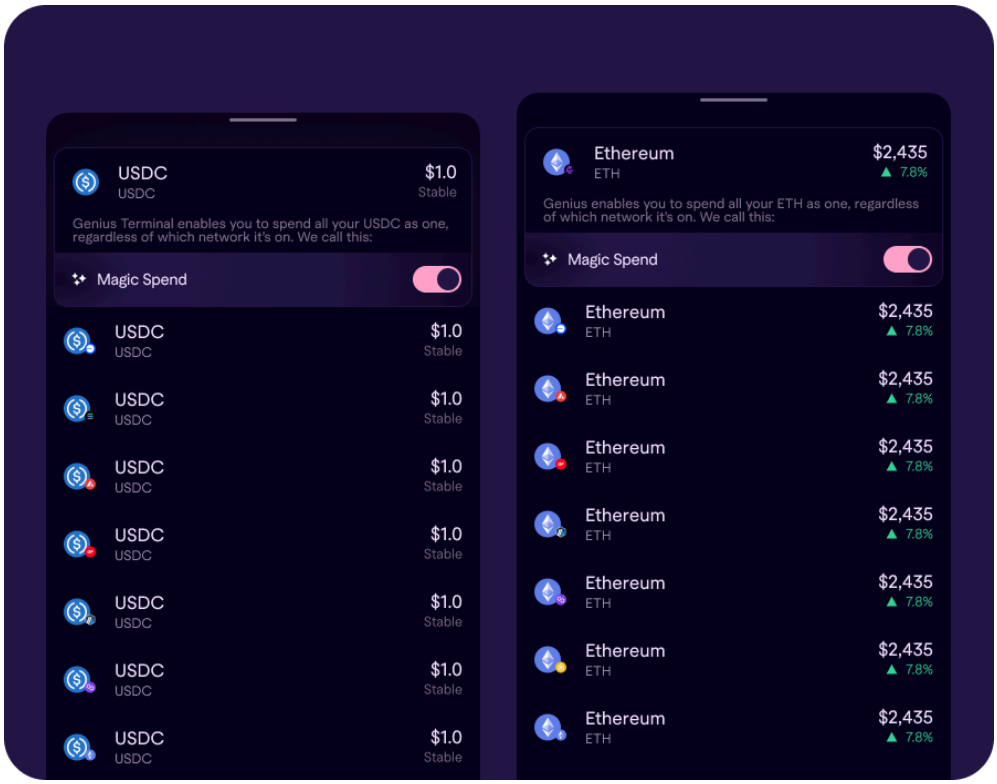
The Car The Road Was Built For

Genius Terminal is the end state of DeFi that GBP was designed to enable. As this paper mentioned earlier, the current prevailing narrative of “chain abstraction” is not nearly extreme enough to capture the real end goal of the Genius Terminal; a signature-free, address-free, gas-free, asset discovery and execution engine designed so that the net-new user does not *need* to know they are on-chain, but with all the optionality for the same user to discover the benefits of being on-chain.
To that end, there are four key features of the Genius Terminal, built as a trading-first front-end for GBP, that will enable the realization of a true centralized exchange experience on-chain.

4.1 Chain invisibility and Magic spend

Chain invisibility is the idea that the end user does not ever have to know which networks their tokens live on. All they have to know is that they own the token. Let us assume, as is the case with many major tokens like USDC, ETH, USDT, UNI, LINK, etc. that the tokens are deployed on multiple networks. Being able to spend these multi-chain tokens as though they were a single token balance is what Genius

Terminal terms “Magic Spend.” For example, if a user has USDC on Base, Optimism, Arbitrum, and Polygon, the Genius Terminal frontend simply displays the combined USDC value as spendable cash available to the user as buying power. If the user decides to trade the multi-chain USDC, GBP will allow the end user to simultaneously swap into the desired asset on multiple source networks at once.



4.2 The Elimination of Gas

Genius Terminal uses GBP’s GasTank module to sponsor gas for users for cross-chain trades. This means that users never have to think about minimum gas spend for transaction success. Net-new users also do not have to learn about gas as a concept. Crucially, this means that a cross-chain user experience is frictionless, and users have access to more liquidity, asset variety, and exchange depth without a technical learning curve and management of multiple gas assets.

4.3 Trading workflow: no addresses, signing, permissions

On Genius Terminal, users do not need to sign individual transactions, set permissions for token spends, or manage different addresses for cross-chain trades. See section 3 for an explanation of how Lit’s programmable signature and encryption network works. Once a user creates an account, Genius Terminal’s logic ties multi-chain addresses to a single authentication method, and has the ability to programmatically sign on the user’s behalf. Combined with the elimination of gas considerations, a net-new user can perform a swap on Genius Terminal by (1) depositing capital with their debit card—eg. USDC on Base, (2) finding an asset they want to trade—eg. MooDeng on Solana, (3) and simply hitting

“submit order.” This is the vision the crypto industry has been dreaming of since the inception of decentralized exchanges.

4.4 The Unification of DeFi

Programmable key-pairs enable transaction signing on users' behalf, allowing seamless third-party protocol integration without independent connection or funding of external accounts. This abstracts complex multi-protocol interactions, providing a unified interface for DeFi to compete with CeFi. Genius Terminal plans to integrate perpetual trading protocols in an aggregated view. That is, showing traders multiple perpetual markets as single markets with unified depth, liquidity and averaged funding rates. For example, if Genius Terminal integrates Avantis, GMX, Drift Protocol, Zeta Markets, and BlueFin, and each of these venues offers a Bitcoin perpetual contract, users will have the ability to trade across them simultaneously, or specify where they would like to trade, spending their Genius Terminal balance as one balance, regardless of which chain their preferred protocol lives on. Similarly, if Genius Terminal integrates Aave, Morpho, Kamino, Ethena, etc. users will be given the ability to “earn yield” directly from their Genius Terminal portfolio page, bypassing the need to connect to external protocols and navigate cluttered and often complicated user interfaces.

Conclusion

GBP and Genius Terminal are building toward the anti-fragile future. At scale, Genius will reinvent the average consumer’s relationship with non-custodial finance. As crypto evolves and more of the world’s value is tokenized on consumer rails, Genius Terminal has the opportunity to become the largest facilitator of liquidity and value globally in a way that is decentralized, secure, and performant. It has the capacity to be the first point of contact for consumer crypto, and connect to all manner of specialized individual apps. Individual protocols can become specific, point solutions and invest resources into becoming more efficient, while delegating the consumer front-end experience entirely to Genius. Simultaneously, noting the vast and rapid uptick in institutional interest in crypto, GBP has the opportunity to become the default liquidity orchestration layer between institutional networks that operate privately, as GBP becomes more composable and decentralized. Genius, both the bridge protocol and the front-end represent the idea that open, programmable systems will eventually outcompete their brittle, centralized counterparts when adjusted for risk and speed, on the basis of efficiency.

Disclaimers:

1. Genius Terminal V0 does not use the GBP to settle cross-chain trades but instead relies on third party intents bridges. This is to protect consumers because GBP is still being audited.
2. The Actions smart contract will go into effect at the direction of the GeniusDAO, which will be set up by the Genius Foundation.

References

LI.FI, "The Untold Trade-Offs in Intent-Based Bridges", March 15, 2024.

Q. Kilbourn, G. Konstantopoulos, "Intent-Based Architectures and Their Risks", Paradigm, June 1, 2023.

BusinessofApps, "FTX Statistics: Revenue, Users & More", March 15, 2024.

Lit Protocol, "Access Control Overview", March 15, 2024.

Lit Protocol, "What is Lit Protocol?", March 15, 2024.