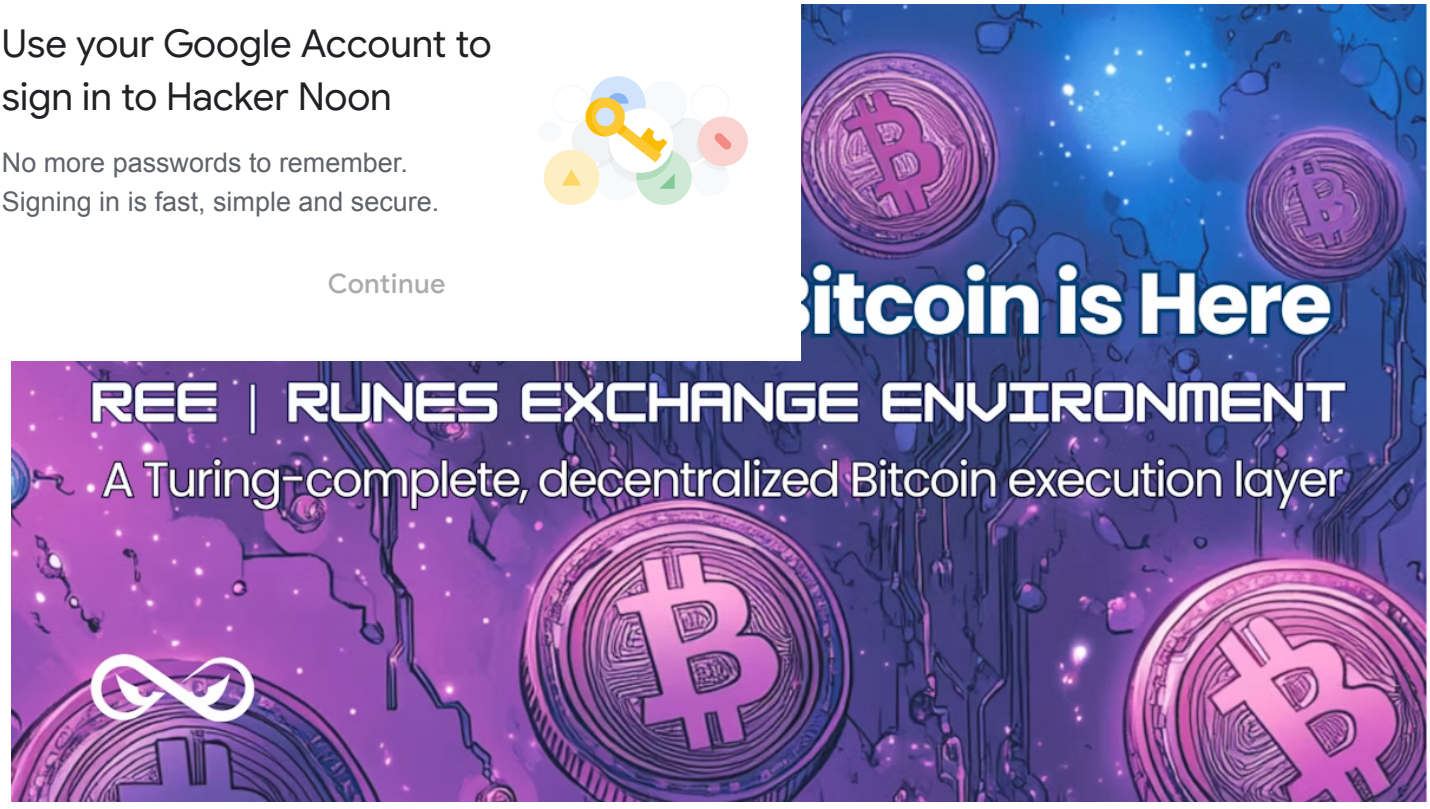
Programmable Bitcoin Is Here: A Turing-complete Bridgeless Bitcoin Execution Layer

by **Omnity Network** December 22nd, 2024



Runes Exchange Environment (REE) Welcomes DeFi Innovators

Web3 on Bitcoin?

Imagine a Uniswap for Bitcoin with no off-chain processes or custody risk and direct settlement on Bitcoin Layer 1. You just connect your Bitcoin wallet and swap away. And what if you could also connect directly to BTCFi DEXs that offered lending, staking, stablecoins, etc. — just like any DeFi Dapp already built on Ethereum or Solana?

We call it *Web3 on Bitcoin* and it's right around the corner.

Brought to you by the developers at Omnity Network.

Omnity Network is excited to share its latest BTCFi supporting infrastructure, Runes Exchange Environment (REE). REE adds a Turing-complete programmability layer to Bitcoin, offering BTCFi developers the tools to replicate EVM & Solana DeFi concepts on REE with native Bitcoin integration.

Let's get into it.

Why it's Hard to Build DeFi on Bitcoin

Bitcoin's security is unmatched, and the sheer scope of Bitcoin's adoption gives it

unparalleled liquidity. But Bitcoin's functionality is programmably restrained. Its scripting language is rooted in simplicity and resilience, which intentionally limits its capabilities.

Bitcoin's UTXO (Unspent Transaction Output) model is fundamentally different from the account-based model used by other blockchains like Ethereum and Solana, which can support Turing-complete smart contracts.

In the UTXO model, each transaction output can only be spent once, and transactions must reference specific outputs, making it challenging to manage complex, stateful applications required for DeFi.

Bitcoin simply doesn't have an execution layer -- *until now*.

Introducing REE—A Turing-complete Bitcoin Execution Layer

The Runes Exchange Environment (REE) introduces a decentralized execution layer for Bitcoin, enabling builders to innovate DeFi protocols on Bitcoin without forks, bridges, or any new opcodes.

Any DeFi protocol on Turing complete chains like Ethereum and Solana can be replicated on REE. DeFi builders can employ REE's Exchange-Pool model's programmability and flexibility to build whatever they can imagine.

Last week, Omnity released the REE whitepaper. The REE platform is slated to launch Q1 2025, along with the first DeFi protocol based on REE — a Runes AMM DEX called RichSwap.

How does REE work?

REE is not a Bitcoin Layer 2.

REE smart contracts embrace Bitcoin's UTXO model by interacting with it directly, but also providing advanced programmability and self-custody.

Traders don't need to lock their Bitcoin assets on cross-chain bridges. Instead, they interact with smart contracts by signing a PSBT (Partially Signed Bitcoin Transaction) using their

Bitcoin wallets. Transactions are settled on Bitcoin.

What's a PSBT?

PSBT originated from the need to simplify the process of coordinating multi-party Bitcoin transactions. Multisig transactions on Bitcoin have been fundamental to the Bitcoin ecosystem for years, introduced by BIP-11 in 2011.

PSBT was formalized in Bitcoin Improvement Proposal 174 (BIP-174), authored by Andrew Chow, to improve interoperability between wallets, hardware devices, and other Bitcoin tools. PSBT v2 was later introduced in BIP-370 to align with the structure of Bitcoin transactions defined in BIP-144 and BIP-341 (SegWit and Taproot, respectively.)

Let's look at a simplified depiction of PSBT.

In traditional multisig workflows, human participants sign transactions to meet predefined conditions. Typically, one participant acts as the coordinator who aggregates each party's signatures and then broadcasts the transaction to the Bitcoin network.

Partially Signed Bitcoin Transaction (PSBT)

REE embraces PSBT and extends so that dApps can directly participate in Bitcoin PSBT signing transactions through composable smart contracts. **REE's Decentralized Multisig Coordination (DMC)** synchronizes the PSBT signing of multiple decentralized protocols in a collaborative transaction.

The Decentralized Multisig Coordination (DMC) Process

The general process of DMC involves a trader, multiple BTCFi protocols (A, B, and C), and a coordinator on a public blockchain (which is abstracted from the UX.) REE chose ICP, the Internet Computer Protocol, as the public blockchain for DMC. The Coordinator aggregates signatures and broadcasts the final transaction to the Bitcoin network.

REE's Decentralized Multisig Coordination (DMC)

A DMC process can be viewed in three phases.

1. **Negotiation Phase:** Trader negotiates terms with multiple protocols such as DEX, lending, stablecoins, etc.
2. **Signing Phase:** A PSBT is constructed that reflects the agreed upon terms. The Coordinator summons each protocol (A, B, and C) to sign the PSBT.
3. **Broadcasting Phase:** Once the PSBT is signed, the Coordinator broadcasts the transaction to the Bitcoin network for settlement.

In DeFi, traders usually trade against protocols (smart contracts) as counterparties. But “a trader” doesn’t necessarily have to be a person; it could be an off-chain process or a smart contract. This opens up possibilities for on-chain or off-chain yield aggregators or arbitrage bots.

In REE the role of the “Coordinator” is handled by the **REE Orchestrator** smart contract. The Orchestrator manages the lifecycle of all REE Tx and validates that all PSBT inputs and outputs comply with REE standards. Using Omnity’s on-chain runes indexer, the Orchestrator verifies asset types and quantities. It’s also responsible for informing exchanges with relevant state transition events.

Let’s put this all together and look at workflows in REE Architecture for Builders, Traders, and smart contracts.

REE Architecture and Workflows

REE Architecture

The example above is of a multi-step process for concluding a Bitcoin transaction on REE involving two exchanges, the REE Orchestrator, and a front-end interface. Let's take it step-by-step.

0.1 Deploy: Builder deploys the Exchange canister.
0.2 Register: Builder registers the Exchange with the **REE Orchestrator**.

1.1 Inquiry: Trader makes an inquiry from **Exchange A**.
1.2 Inquiry: Trader makes an inquiry from **Exchange B**.
2. Construct PSBT: The **BTCFi front end** constructs a PSBT with assistance from **REE TS SDK** (Typescript SDK).
3. Trader signs PSBT: Trader signs PSBT with Bitcoin wallet.

4. Invoke: The signed PSBT invokes the **REE Orchestrator**.
5. Check Inputs: The Orchestrator, relying on the **Ord Indexer**, checks validates inputs.
6.1 Sign: Exchange A signs PSBT.
6.2 Sign: Exchange B signs PSBT.
7. Broadcast Tx: REE Orchestrator broadcasts the fully signed Tx to the Bitcoin Network.

REE's Exchange-Pool Model

REE is a general-purpose coordinator, and to coordinate the execution of various DeFi protocols, the protocols need to conform to a specific standard. REE's standard is the **Exchange-Pool model.**

As mentioned, Bitcoin's UTXO model isn't compatible with the state model of smart contract

platforms. So, Omnity developed the Exchange-Pool model for REE which adapts to Bitcoin's UTXO state management and can be implemented on account-based public chains like ICP.

The Exchange-Pool model is composed of three simple concepts:

1. **Coin:** A unit of UTXO-based Bitcoin assets. (BTC and runes are accepted as coins in REE.)
2. **Exchange:** A BTCFi protocol that operates on the REE platform.
3. **Pool:** A public key (Chain Key) an exchange uses to hold coins and sign Bitcoin transactions.

An exchange can manage multiple pools, each with its coin holding and state. According to exchange-pool logic, traders throw a bag of coins in one pool and get another bag of coins out of the other. Thus, all DeFi protocols must be implemented in the form of *a bag of coins in and another bag of coins out* (i.e., coin exchange) to participate in REE's Decentralized Multisig Coordination (DMC).

Why Runes?

Runes allow developers to issue stablecoins, utility tokens, governance tokens, meme coins and other community-driven projects directly on Bitcoin. Runes can even represent NFTs through the allocation of unique metadata to specific UTXOs. Because runes are etched directly onto Bitcoin using the OP_RETURN opcode, arbitrary data can be written on-chain without impacting Bitcoin's UTXO set to create an immutable, secure, tamper-resistant record for each rune which defines and authenticates the rune's properties. Whether sh*tcoins or stablecoins, Casey Rodarmor's design has the potential to unlock Bitcoin's next major evolution as a programmable, multi-asset blockchain.

RichSwap

AMM DEX

RichSwap, an AMM DEX built by Omnity, will be launched simultaneously with the REE mainnet. As the first exchange on REE, RichSwap serves the following purposes:

1. RichSwap validates the functionality and performance of the REE platform.
2. RichSwap is open-source, providing a full-scale example for BTCFi builders.
3. Upcoming BTCFi protocols may leverage RichSwap to accelerate liquidity bootstrap.
4. RichSwap presents a token value capture mechanism, which other BTCFi protocols may adopt.

**Although RichSwap is the first exchange, it does not enjoy any privileges. After its launch, REE will quickly transition into an open platform where BTCFi protocols that meet its technical specifications, including AMM DEXs, can be deployed without permission.*

How to Build an Exchange on REE?

We built this cool thing and we want builders to take advantage of it.
The steps to build an exchange on REE are relatively simple.

- **Deployment**: The Builder deploys the exchange canister onto the same subnet as the REE Orchestrator on ICP. (Canisters can call each other cross-subnet, but it adds unnecessary latency.)
- **Registration:** The Builder registers the exchange to the REE Orchestrator.
- **Fund:** Fund the Exchange-Pools.

Exchange builders are responsible for maintenance, upgrades, costs (ICP canisters are recharged with cycles) to keep the exchanges alive. Omnity will provide common facilities to exchange builders for convenience, but they are optional and replaceable.

System Properties

Programmability

REE exchanges operate as independent ICP smart contracts that fully utilize the underlying blockchain's capabilities. ICP smart contracts (canisters) are full-stack, scalable contracts with robust storage and web-serving capabilities that can directly read from and write to the Bitcoin network without external bridges.

ICP canisters are incredibly powerful and have the ability to run intensive computations (e.g.,

face recognition) and host large-scale solutions like ICP's Bitcoin Canister, which stores 500GB of on-chain data at an annual cost of $2,500. (Builders are encouraged to visit ICP's Docs for more information on ICP smart contract development.)

Composability

REE smart contracts support Bitcoin-style composability: Exchanges focus solely on their inputs and outputs. Multisig transactions are orchestrated atomically and are either completed in full or revert entirely which is crucial for DeFi applications. Transactions are processed sequentially, with PSBT signing following a logical pipeline where entities—whether a trader, off-chain process, or ICP smart contract—can provide inputs independently of order. With ICP's powerful and secure Chain Fusion stack, REE exchanges can interact with other blockchains. For instance, a state change on Ethereum or Solana triggers a REE transaction, and vice versa.

Performance

REE improves Bitcoin performance by 100X. Serial REE transactions are settled on the Bitcoin chain in batches. Since one memory pool transaction can have a maximum of 25 descendants, each Bitcoin block settles up to 25 transactions for a single REE exchange pool. Therefore, 25 can be considered the throughput limit for an individual REE exchange pool.

When price competition is unnecessary, exchange builders may want to add redundancy pools to enhance concurrency. For example, distributing tokens across ten pools for an airdrop with 100,000 recipients would significantly reduce the likelihood of transaction failures caused by multiple users claiming simultaneously.

Cost

Builders bear exchange operating costs (cycles) on ICP. REE minimizes settlement transaction sizes using P2TR (Pay-to-Taproot) introduced by BIP 341. P2TR shifts operating costs to ICP.

MEV

REE eliminates slippage, as PSBT inputs and outputs are locked upon signing. If front-running occurs, the transaction fails, leaving the front-runner exposed to price risk without affecting

the trader. (Although theoretically possible, ICP subnet nodes extracting MEV by reordering transactions is unheard of.)

Join Omnity in Bringing Web3 to Bitcoin

REE introduces secure, Turing-complete smart contracts for Bitcoin without relying on asset bridging or protocol forks. This bridgeless execution model unlocks new possibilities for a trustless and permissionless BTCFi ecosystem, built on Bitcoin's unmatched liquidity and security.

REE will be launching in Q1 of 2024 with its showcase AMM DEX RichSwap. Development on REE will then open in stages to developers interested in BTCFi.

Interested developers and builders are invited to read the REE Whitepaper and feel free to reach out to the Omnity team for more information. *Let's build Web3 on Bitcoin!*

About Omnity

REE is built by the developers of the Omnity Hub a 100% on-chain, cross-chain architecture connecting various chains to Bitcoin without off-chain processes or centralized components.

- Omnity Hub currently supports the three primary assets in the Bitcoin ecosystem: BTC, Runes, and BRC20.

- Omnity Hub is connected to more than a dozen EVM-compatible chains, Solana, Osmosis, and ICP, all with native Bitcoin integration.

The Hub is being adopted quickly and has gained the trust of multiple partners and communities.

Suzanne Leigh is the Editor of *Omnity Network.*

L O A D I N G

. . . comments & *more!*

About Author

Omnity Network @omnity

Omnity Hub is a fully on-chain hub that connects any Layer 1, Layer 2, or appchain to the Bitcoin network.

Read My Stories About @Omnity

TOPICS

WEB3 #bitcoin #runes #programmable-bitcoin #bitcoin-interoperability #btcfi #defi-on-bitcoin #omnity-network #hackernoon-top-story

THIS ARTICLE WAS FEATURED IN...

RELATED STORIES

Automation & Colony Sim Game That Programmers Love!

visit **Forklift** **#Sponsored**

Gaming Network Effects And Their Paradoxes

by **oct_network** Jun 03, 2022 **#blockchain**

06/09/2018: Biggest Stories in the Cryptosphere

by **BlockEx** Sep 06, 2018 **#bitcoin**

06/02/2018: Biggest Stories in the Cryptosphere

by **BlockEx** Feb 06, 2018 **#bitcoin**

05/02/2018: Biggest Stories in the Cryptosphere

by **BlockEx** Feb 05, 2018 **#bitcoin**

0 to Pro Crypto Trader: Your Ultimate Guide to Bitcoin and Altcoin Investing

by **kennymuli** Jan 13, 2018 **#bitcoin**

Join HackerNoon

Latest technology trends. Customized Experience. Curated Stories. Publish Your Ideas

ABOUT

- Careers
- Contact
- Cookies
- Emails
- Help
- Privacy
- Sitemap
- Shareholders
- Startups 2023
- Terms
- Testimonials
- Updates
- Startups 2024

READ

- Archive
- Categories
- Image Gallery
- Leaderboard
- Learn Repo
- Noonification
- Signup
- Tech Beat
- Tech Brief
- Tech Tags
- Terminal Reader
- Top Stories
- Newsletters

WRITE

- Distribution
- Editing Protocol
- Editor Tips
- Guidelines

BUSINESS

- Billboard
- Book Demo Meeting
- Business Blogging
- Case Studies