Bringing Bitcoin to DeFi: A Complete Beginners Deep Dive Into RenVM

By

Michael Burgess

Published on:
September 19, 2020

Opinion: For those that are interested in DeFi but only hold Bitcoin, a protocol like RenVM allows you to use your digital assets in the DeFi space.

Table of Contents

Bringing Bitcoin to DeFi: How It Works

If you own Bitcoin or other digital assets, it might not be obvious that you can use them in DeFi. However, even though different blockchains don't typically speak to one another, there are ways to bridge that gap. With protocols that provide blockchain interoperability, you are able to move digital assets from

blockchain to blockchain — this means that your Bitcoin can actually be used for something like **yield farming** in DeFi, for example.

What Exactly Is RenVM?

RenVM is a protocol that brings interoperability to decentralized finance (**DeFi**).

The easiest way to imagine RenVM is to first think of it as a custodian that holds your digital assets as they move between blockchains. You give BTC to RenVM, it holds that BTC, and then mints that BTC as an ERC20 (a.k.a. renBTC) on Ethereum with 1:1 ratio to ensure your renBTC is always backed by the same amount of BTC.

This approach applies to almost any digital asset and smart contracting platform (for example, RenVM can hold native **Dogecoin** and mint it on the **Polkadot** blockchain).

RenVM achieves interoperability and removes these barriers because it serves as a “universal translator,” or an adapter of sorts. It takes the blockchain’s native format, and converts it to the format needed by its destination chain. (E.G. RenVM takes BTC in its native form and converts it to an **ERC-20**, Ethereum token standard).

How Does RenVM Actually Work?

RenVM uses secure multi-party computation (**sMPC**), which is a subfield of cryptography that allows parties (nodes) to jointly compute a function over their inputs while keeping those inputs private. The inputs are kept hidden from everyone, including the nodes that power them. This means that private key pieces are split up within each node, so that not even the nodes know which pieces they have.

Ren's network — since it is able to manage private keys on multiple blockchains — is able to freely move cryptocurrencies across these blockchains. This ultimately allows RenVM (a network of nodes) to securely manage (ECDSA) private keys on different blockchains, making it an autonomous agent that can move digital assets between these blockchains in a permissionless and decentralized way. Technically speaking, RenVM is a byzantine fault-tolerant protocol that does ECDSA threshold key generation and signing via sMPC.

If you'd like to know more about how RenVM works and understand RenVM's usage of sMPC, check out this *Technical in-Depth Guide.*

What Is the Role of the REN Token?

The REN token is used as a bond to run a node (aka Darknodes, since they are in the "dark" about which information they are processing), which powers the sMPC network (RenVM).

The decentralized network of Darknodes is **permissionless**, but to prevent the forging of a large number of identities, a good behavior bond of 100,000 REN

tokens is required in order to register and run a Darknode. This prevents malicious adversaries from running an unbounded number of Darknodes and overwhelming the network with misbehaving Darknodes.

This requirement is similar to the way that **proof-of-work** uses computational work to restrict block production, or the way that **proof-of-stake** uses staked tokens to restrict block production. For every Darknode that you register, you will need to acquire 100,000 REN and be prepared to bond it into an Ethereum smart contract. This bond will be returned after the Darknode is deregistered.

Every time RenVM moves an asset from one blockchain to another, it takes a small fee. Darknodes (and those who run them) earn these rewards (in BTC, ETH, ZEC, etc.) for contributing to the network. For more info on REN's role in the ecosystem, check out this **wiki** page.

Running a Darknode

Anyone can run a Darknode. All you need is a personal computer, an internet connection and some technical know how.

RenVM is powered by a decentralized network of machines (i.e. nodes), called Darknodes. They contribute their compute power and storage space to the network in exchange for fees.

1. Requirements for running a Darknode is 100,000 REN staked as collateral + running the Darknode software via VPS.

2. The total number of Darknodes is bound by an upper limit of 10,000 determined by the finite supply of 1,000,000,000 REN and the 100,000 REN bond per Darknode.
3. Darknodes earn fees in BTC, ZEC, ETH, etc. for powering the network.

For more info on running a **Darknode**, check out this **instruction manual**.

Technical In-Depth Guide to RenVM

For those that are more interested in the technical side of this protocol, and how it can help you bridge the gap from your Bitcoin into the DeFi space, we've created this very in-depth technical guide to RenVM. The most important component of Ren is the multi-party computation (sMPC) algorithms, which allow RenVM to move digital assets back and forth between multiple blockchains.

How Does RenVM Work?

RenVM is a **Byzantine fault tolerant** (BFT)-based protocol that enables universal interoperability between blockchains. By combining a consensus mechanism with shamir secret sharing and secure multi-party computation (sMPC) algorithms, RenVM is able to instantiate a decentralized, **permissionless**, and trust-less custodian; capable of locking assets on one chain, and minting one-to-one pegged representations of them on other chains.

TL;DR: RenVM is a decentralized crypto asset custodian that:

- Enables universal interoperability between blockchains: anyone can use RenVM to send any asset to any application on any chain in any quantity.
- Has robust security: large bonds, large shard sizes and continuous shuffling make RenVM extremely difficult to attack, even for irrational adversaries. In the unlikely event of a successful attack, RenVM can restore lost funds.
- Is scalable: as more assets are locked into the custody of RenVM, the algorithmic adjustment of fees allows RenVM to automatically scale its capacity to meet demand.
- Provides an optimal user experience: users can interact with multiple assets, applications and chains with only one transaction.

A more in-depth technical guide to all that is RenVM, can be found here: **https://github.com/renproject/ren/wiki**

What sMPC Algorithm Does RenVM Use?

The Ren team has pioneered an sMPC algorithm that allows RenVM to manage private keys in a way that remains safe and lively in a decentralized setting (its formal name is the RZL sMPC Specification).

White Paper: **https://github.com/renproject/rzl-mpc-specification**
Audits: **Trail of Bits Audits & ConsenSys Diligence**
Code: **https://github.com/renproject/mpc/wiki**

What Consensus Engine Does RenVM Use?

RenVM Hyperdrive is an implementation of a Byzantine fault tolerant consensus algorithm designed for secure multi-party computations. It is based on the **Tendermint consensus engine** described in "**the latest gossip on BFT**

consensus" by Buchman et al. with modifications for interactive execution and sharding.
Hyperdrive assumes the existence of a peer-to-peer networking that can broadcast messages to all peers, and a storage device that can persist data-to-disk, but it does not specify how these functionalities are implemented. In practice, RenVM uses **airwave** for peer-to-peer networking, and **kv** is used for cached persistent storage.

RenVM's Safety and Liveness

Every Byzantine fault tolerant system needs to understand the conditions under which it can be attacked, and the limitations of its security. In this **wiki**, we discuss the safety and liveness properties of RenVM, the conditions under which these properties can be broken and how RenVM prevents these conditions from being realized.

Digital Assets RenVM Currently Supports

RenVM can support any ECDSA based blockchain. Information on what chains are currently supported can be found **here.**

Track RenVM's usage

The main place to track RenVM's usage is via the **RenVM Command Center**.

This article contains links to third-party websites or other content for information purposes only ("Third-Party Sites"). The Third-Party Sites are not

under the control of CoinMarketCap, and CoinMarketCap is not responsible for the content of any Third-Party Site, including without limitation any link contained in a Third-Party Site, or any changes or updates to a Third-Party Site. CoinMarketCap is providing these links to you only as a convenience, and the inclusion of any link does not imply endorsement, approval or recommendation by CoinMarketCap of the site or any association with its operators.

This article is intended to be used and must be used for informational purposes only. It is important to do your own research and analysis before making any material decisions related to any of the products or services described. This article is not intended as, and shall not be construed as, financial advice.

The views and opinions expressed in this article are the author's [company's] own and do not necessarily reflect those of CoinMarketCap.