# Sifchain: The Omni-Chain Decentralized Cryptocurrency Exchange Lite Paper

Version 0.3

October 2020

Note: The contents of this document are subject to change.

# Background

In 2019, $8.5 billion in cryptocurrency derivatives trading occurred per day for a total of $3 trillion in the year[1]. Most of this trading occured on centralized exchanges even though cryptocurrency investors prefer decentralized exchanges because they can maintain standards of security, availability, reliability, and censorship resistance on a publicly verifiable blockchain.

A primary constraint for existing decentralized exchanges is that they limit investors to a small subset of blockchain ecosystems. Another constraint is that they are slow and charge high fees due to performance limitations of their underlying blockchain. To capture the full market, an omni-chain solution on a more performant blockchain is needed.

Sifchain is that solution. Built with the Cosmos SDK, Sifchain processes substantially more transactions per second than Ethereum, making it 100x more efficient than the current leading DEXes. Sifchain uses Thorchain as a reference implementation and uses pegged tokens to support a wide array of blockchains. Sifchain will support cross-chain transactions for 20-25 of the top blockchains such as Bitcoin, BinanceChain, Polkadot, and EOS. These blockchains represent the overwhelming majority of all cryptocurrency trading volume. In addition, Sifchain will support an on-chain governance process for developing additional pegged tokens for new blockchains as needed.

# Hybrid Orderbook and CLP

Sifchain uses both an order book and a CLP for trade completion. Orders are placed with a commit-reveal scheme[2] to circumvent front-running from validators. Committing a limit order will

[1] TI-2019Cryptocurrency Derivatives Exchange Industry Annual Research Report-20200117

[2] Commitment Scheme Generally speaking, this scheme is still vulnerable by either: (i) committing multiple transactions and selectively revealing only the profitable ones, or (ii) committing multiple transactions and selectively invalidating the unprofitable ones (not enough collateral, or proxy contract

require traders to actually transfer the value posted, regardless of whether or not it is revealed. Sifchain derives its internal asset price from its CLPs. One CLP is used for trades directly involving Rowan, two CLPs are used for all other trades. For example, the USDC:BTC internal price is calculated using the USDC:ROWAN and ROWAN:BTC CLPs.

Traders execute market orders (swaps) directly against CLPs immediately after placing them. Traders place limit orders by posting an on-chain transaction depositing their capital in whichever currency they prefer, along with the name of the currency they'd like to purchase and their requested price. When Sifchain's internal asset price moves to a favorable range for a limit order, a CLP swap is executed so that the limit order is filled with an average price that does not exceed the trader's requested price. This means limit orders may be partially filled.

The key benefit of the CLP is the fee structure, which is responsive to the demand for liquidity by market-takers. Prices inherit an inertia since large fast changes cause high fee revenue. As demand subsides, the fee paid decreases. This liquidity-sensitive fee penalises traders for being impatient. This is an important quality in markets, since it allows time for market-changing information to be propagated to all market participants, rather than a narrow few having an edge.

Sifchain supports conditional market and limit orders, including stop loss and take profit orders. It also supports amending limit orders that have been placed but not executed to enable trailing orders.

Sifchain prioritizes limit order execution based on the yet-fulfilled quantity of purchased tokens, not the time the orders are placed or the requested price. This allows CLP liquidity providers to maximize revenue and encourages traders to post trades that accurately reflect their market view. CLPs are expected to maintain accurate asset prices because any inaccurate asset price presents an opportunity for market makers to profit through arbitrage[3]. However, traders are able to request oracle verification if they believe the internal asset price may temporarily deviate substantially from its external asset price. In such a case, orders will only be executed to the extent that the average price is within a specified range of the oracle price.

Sifchain enables liquidity providers to add liquidity into Sifchain's liquidity pools where they can earn income without the constraints that other exchanges put on them. Liquidity providers are able to deposit any token Sifchain supports to the appropriate pool. They can add liquidity asymmetrically, meaning they can add only Rowan or only TKN for any token. Liquidity providers can add or remove liquidity whenever they choose.

---

exception). However, we considered a transaction valid only if it was revealed within n blocks of being committed. If n is sufficiently small, traders will have nearly no time to selectively reveal.

[3] Converging to Reference Prices

# Margin

Traders are able to borrow liquidity from a CLP. This allows them to long cryptocurrency on margin, leveraging the value of the cryptocurrency they already own and increase their investment size. This enables traders to potentially magnify returns, assuming the value of the investment rises. Traders borrow the currency they're using as collateral (for example, if a trader is using USDC as collateral, they will borrow USDC). Interest is set based on market demand and CLP supply. The borrow occurs when the trade is executed, not when it is placed.

After a trade with no margin occurs, the purchased tokens are released to the trader. However, after a trade with margin, the purchased tokens are held by the protocol. A trader can manage the position by placing and updating orders. To exit a position, they must sell all of the assets they purchased. At this point, their collateral is returned with adjustments for gains or losses.

A position can be liquidated if the price of an asset falls below a liquidation threshold. This liquidation threshold is a function of both the purchase price and the amount of margin used. Positions with less margin will have more favorable liquidation thresholds, all else being equal. As with spot traders, margin traders can decide whether to use Sifchain' internal asset price or an oracle's external asset price for liquidation or orders related to their position.

Both borrowing and returning capital unbalances the CLP, making it profitable for arbitrageurs to fix. Thus, margin trading both provides a new revenue source for liquidity providers (lending) and increases the revenue from trading fees.

# Rowan

Rowan is the governance token for Sifchain. Post-mainnet, all protocol changes will be voted on by Rowan-holders, with voting weight being proportionate to tokens held. SifDAO (Sifchain's Decentralized Autonomous Organization) will be deployed with Rowan as the governance token.

Rowan is provided to validators from protocol emissions, also known as block rewards. Validators must stake Rowan to participate in network consensus.

Finally, Rowan is the settlement token for Sifchain. Traders must directly or indirectly purchase Rowan to execute trades against CLPs, ensuring demand for the token.

# Underlying Architecture

As a Cosmos SDK blockchain, it uses the Tendermint consensus algorithm[4] and will support the Cosmos Networks' Inter-blockchain Communication Protocol (IBC)[5].

In many blockchain orderbook systems, cancellations and order updates are sensitive to suppression attacks such as intentional mempool spam from other traders. Validators would not accept totally nonsensical transactions, but attackers can still spam low-stakes transactions—e.g., calling a no-op function, or moving funds between wallets they own. Attackers would have the goal of getting the validators to fill blocks with these useless (but valid) transactions plus their profit-taking transaction, before an honest user's other transactions such as order cancellations or order updates can get through.

Sifchain levels the playing field here by requiring that validators reorder all transactions in a block so that those with the highest transaction fees are processed first. This way, traders can post transactions for cancellations and order updates with substantially higher gas fees than the average transaction so that they are prioritized ahead of others (and so that the costs of spamming the mempool is prohibitively expensive for attackers).

# Cross-Chain Communication

Sifchain uses a two-way peg protocol which results in the swap of pegged tokens. For example, a trade of LTC for TRX would be executed as transactions of pegged tokens (cLTC and cTRX) on a Cosmos SDK blockchain.

The technical architecture of each pegged token will differ depending on the blockchain but each will have some common infrastructure. Each source chain (for example, Stellar or Cardano) will have a specified peg chain (also known as a peg zone) in the Cosmos Network with its own validators separate from Sifchain. Sifchain can verify peg zone validators' transactions through Cosmos Network's IBC.

Peg zone validators must run a full node only for their peg zone blockchain and the blockchain to which they are pegged. For example, a Tezos peg zone validator only needs to run a full node for the Tezos peg zone and the Tezos blockchain. Peg zone validators can choose to validate multiple peg zones (the Cosmos Hub will likely be the peg zone for multiple blockchains) but this is not required.

---

[4] What is Tendermint?
[5] Inter-Blockchain Communication (IBC)

# Perennial Permissionless Asset Listing

Anyone can create a new CLP by pooling Rowan and a new token into a pool initialization transaction.  The price of the new token will be set based on the amount of Rowan pooled. Sifchain will enforce a minimum CLP size, but multiple depositors can contribute to the creation of a single CLP.