PACT SWAP: Unlocking the full value of a decentralised crypto exchange

The PACT SWAP Contributors

March 25, 2025

Version 0.8

Abstract

Crypto exchanges are lucrative businesses and also major economic driving forces in the blockchain ecosystem, with centralised exchanges dominating the market. In 2024 , it is estimated that the total crypto trading volume will exceed $100 trillion[1]. Decentralised infrastructure has numerous advantages over centralised, but many functions are more difficult to implement as decentralised, and DEXes suffer from multiple shortcomings compared to their centralised counterparts. Despite this, the role of decentralised exchanges (DEX) is expanding, DEXes capturing 14.22%[11] of the spot trading volume as of July 2024.

PACT SWAP is a cross-chain DEX built on innovative infrastructure, addressing inefficiencies and other limitations found in existing DEX applications. Multiple technical innovations and a novel economic model, designed to rival those of CEXs, unlock significant growth potential through extended value capture. PACT SWAP revenue streams extend beyond core DEX functionality, using aggregated data to unlock powerful community roles and functions designed to mitigate severe issues obstructing the current blockchain ecosystem, simultaneously acting as a force to accelerate innovation.

Keywords: DEX, value capture, cross-chain, capital efficiency

1 Introduction

Crypto exchanges are essential components of the blockchain ecosystem and are also extremely lucrative businesses. Centralised exchanges still dominate the market, and in the first 6 months of 2024, the trading volume on the top 10 exchanges exceeded **$33.9** trillion[9]. The exact amount of revenue generated from this is not publicly known, but using published data from exchanges such as Coinbase and Binance as examples reveals that for Q1 2024, Coinbase, having a quarterly trade volume of **$312** billion ($3.4 billion daily volume), earned **$1.0767** billion from transaction fee revenue alone that quarter[2]. Binance, which is the largest exchange, reported **$18** billion in revenue from trading fees from a total trading volume of **$9.580** trillion in 2020[4] ($26.2 billion daily volume). These numbers indicate a fee level of **0.34%** and **0.18%** for Coinbase and Binance,

Archived copy · cryp2nova.com

respectively. Of course, exact fee levels charged by other exchanges will differ, but the average levels are likely to be within a broadly similar range for most centralised exchanges. It is hardly surprising that the largest exchanges are highly profitable, but even considerably more modest and conservative examples will show impressive results. An exchange with a trading volume of **$250** million daily, charging 0.1% trading fee will generate **$91.25** million per annum from trading fees alone.

Although centralised exchanges still dominate the market, the market share captured by decentralised exchanges is expanding and currently (July 2024), it represents 14.22% of the spot trading volume[11]. The demand in the market for specific capabilities enabled by decentralised infrastructure has been strong enough to drive this growth despite current DEXes having significant limitations on key exchange functionality in comparison with centralised exchanges. It is expected that substantial additional DEX growth potential can be unlocked by new innovations in decentralised infrastructure and by improving current DEX economic models, closing the gap to centralised exchanges and enabling capabilities not available in CEXes.

This paper presents PACT SWAP, a cross-chain DEX built on a radically new infrastructure that allows significant optimisations and functionality enhancements. PACT SWAP unlocks massive DEX growth potential by mitigating multiple severe limitations and inefficiencies of existing DEX applications. PACT SWAP also introduces a novel economic model designed to optimise value capture and community incentivisation through targeted activation and utilisation of parallel value streams induced by the main volume drivers.

2 Current landscape

The current cryptocurrency exchange landscape is multidimensional. A large number of exchanges span several categories, differentiated by provided services and functionality, technical and organisational structure, economic model, target audience, and traded assets and asset types.

2.1 Different types of exchanges

Crypto exchanges can be divided into two main categories, centralised exchanges (CEX), and decentralised exchanges (DEX). The main difference between the two is that CEXs are implemented on centralised infrastructure, typically owned and controlled by commercial companies or other centralised entities, whereas DEXs are implemented on decentralised infrastructure, controlled and operated by a community of contributors.

Both categories of exchanges provide a diverse set of functionalities and services, often with some overlap, but specific capabilities typically differ between CEXs and DEXs. As separate entities, CEXs typically have more diverse and developed revenue streams than DEXs.

2.1.1 Different types of DEXs

Most centralised exchanges are built using a similar architecture, using a local digital representation of the real assets, balances and trades. This makes it easy to enable trading between any assets as their local representation is technically identical.

The situation is very different for DEXs. DEXs must be able to convert payment in one asset into settlement in a different asset. Since there is no central authority, these functions have to be

Archived copy · cryp2nova.com

automated using a decentralised infrastructure.

Single-chain DEXs If the assets exist on the same blockchain network, this process is relatively easy to implement using smart contracts since the proof, verification, and execution mechanisms are secured by the validators of that blockchain. We can call these DEXs single-chain DEXes.

Cross-chain DEXs However, if the assets to be exchanged are on independent blockchains, the necessary mechanisms become more difficult to implement. DEXs that exchange assets between independent blockchains are called cross-chain DEXs.

2.2 Range of services and functions

Trading of listed assets This is the core offering for most exchanges and often the main driver of revenue, as well as customer acquisition. Some exchanges support multiple types of markets and asset types, such as derivatives and spot trading, while others are more specialised.

Token sales/fundraising The largest centralised exchanges often include launchpads / IEOs as part of their offered services. These are used as platforms for the sale of digital assets prior to the listing of the asset on an exchange, where a portion of the tokens are allocated to customers on the exchange.

- Individual launchpads are also often decentralised, in principle working in the same way, but are most often decoupled from public listing.
- Launchpads and IEO often offer limited-size allocations at a fixed price.
- Exchanges and individual launchpads typically require that projects be vetted before they are allowed to use the service.
- Other decentralised variants are IDO (Initial DEX Offering) and ILO (Initial Liquidity Offering). IDOs often sell placeholder tokens that are later convertible to the real token, while ILOs sell tokens that have been made available through a liquidity pool.

Incubators/investment funds Many exchanges are active investors in projects through investment funds.

Paid/promoted listing The largest exchanges typically charge projects for listings. Promotion is often part of the paid listing service. Payment is often a mix of project tokens and high-liquid assets.

Service privileges Special privileges and discounts can be purchased directly or received as rewards for the staking of tokens.

Archived copy · cryp2nova.com

3 PACT SWAP contributions

3.1 Technical innovations

The technical architecture of PACT SWAP incorporates a diverse set of significant technical innovations, both as functionality derived from the Coinweb protocol primitives, but also includes novel application-specific solutions, which unlock key capabilities of the PACT SWAP.

3.1.1 Consensus-free cross-chain DEX supporting independent blockchains including Bitcoin

Single-chain DEXs like Uniswap work by executing smart contracts on a single chain, where payment and settlement happen within the same transaction on the same blockchain. The blockchain nodes validate that the payment and settlement of the exchange transactions have been executed correctly using the blockchain rules and the consensus system of that particular blockchain. Cross-chain DEXs[1] must be able to trigger settlement transactions on a destination chain based on payment transactions executed on a source chain. However, nodes in one independent blockchain cannot observe or verify transactions or any other events that happen in other independent blockchains. They can also not execute transactions on other independent blockchains. This means that a cross-chain DEX has to implement mechanisms to observe and verify transactions on multiple chains. It must also provide a mechanism for the creation and execution of transactions on multiple chains. Since the native nodes of the different blockchains are incapable of performing the necessary functions, cross-chain DEXs have been implemented by creating a new network of specialised nodes with its own separate consensus system to both monitor and execute transactions on different networks[2]. While this is a solution that works, it comes with several disadvantages, which will be discussed in further detail in Chapter 4. PACT SWAP is a cross-chain DEX implemented without a separate consensus network. This novel approach contributes significant innovation to the space and unlocks multiple new capabilities and major optimisations.

3.1.2 Optimised collateral allocation

Cross-chain DEX transactions are typically backed by staked collateral as an economic incentive to ensure that settlement transactions are executed correctly to protect any liquidity reserves from illicit transactions without matching incoming DEX payments. Collateral in the form of staking/bonds is also often used by the consensus system of the network, thus multiple different collateral allocations can be used in different parts of a single cross-chain system. When capital is bound as collateral, it increases the capital cost of operating the system. This typically results in higher costs for users and lower returns for community participants and stakeholders. Consensus-based cross-chain systems typically allocate collateral through some sort of auction-based process, sometimes with the stated goal of locking up as much collateral as possible[3] to create a demand for the protocol token, which will then be used to fund resource subsidisation as well as community incentives necessary to secure the application specific consensus system of the cross-chain DEX.

[1] Decentralised exchanges exchanging assets across independent blockchains (Blockchains with independent consensus networks)

[2] Other solutions such as atomic swaps exists, but come with multiple other limitations

Archived copy · cryp2nova.com

Having a goal of maximising the amount of locked-up collateral is in direct conflict with capital efficiency optimisation requirements necessary for cost reductions and market capture. Also, it imposes an artificial lower bound on liquidity provisioning costs.

PACT SWAP uses a collateral allocation mechanism that is detached from conflicting consensus-bound costs but instead directly facilitates the opposite incentives, allowing dynamic and fine-grained collateral allocation, reducing overall capital costs, and improving liquidity provisioning efficiency. PACT SWAP transactions are secured using the PACT implementation pattern leveraging collateralised reactive smart contracts as a replacement for off-chain staked node infrastructure.

3.1.3 Modular Order Settlement

PACT SWAP leverages Coinweb smart contracts to enable flexible and extensible settlement facilities for orders. These settlement facilities are implemented as smart contracts, and new such facilities are expected to emerge over time. Some of the settlement facilities include:

- Settlement to a Coinweb token such as CWEB. This is the simplest settlement facility as these tokens are directly controlled by Coinweb smart contracts.
- Direct p2p settlement through order-bound dust-lock UTXOs (see 4.4). This is an innovative and cost-effective option for direct peer-to-peer order settlement. This settlement facility allows users of Bitcoin-derived blockchains to settle cross-chain swaps directly with each other without an intermediary. A UTXO containing dust (a very small amount) outsources order matching to the blockchain miners.

With modular and extensible settlements, more swap types are possible, such as:

- Multi-sig Bitcoin vault settlement. This is a cost-effective option for market-makers. For p2p trades, vault settlements require two on-chain transactions. Vaults often also require relatively expensive incentive structures if vault turnover is low, but on the flip side, it allows for synthetic L2 asset creation that solves important use cases.
- Lightning network settlement. This settles the Bitcoin payment on the lightning network through payment of a LN invoice specific to the payer. Proof of payment is possible through publishing of the payment preimage.
- DEX settlement. This settles the cross-chain swap by paying into another swap like Uniswap[3], AshSwap[4], or Jupiter[5][6], thus making several orders of magnitude more swaps available by tapping into chain-local liquidity.
- Non-Fungible Token (NFT) settlement. This settles the cross-chain swap by transferring a specific NFT.

[3]See Uniswap: https://uniswap.org
[4]AshSwap: The one-stop DeFi hub on MultiversX: https://ashswap.io/
[5]Jupiter: A leading DEX on Solana: https://jup.ag
[6]Coinweb has indicated upcoming connectivity with Solana

Archived copy · cryp2nova.com

Virtual native vaults Virtual native vaults are sets of native liquidity commitments secured by L2 collateral. Passive L1 liquidity providers can earn yield by making their L1 assets available for settlement transactions. These commitments are registered in a PACT as unconfirmed signed transactions. Market makers use them by extending the unconfirmed transactions with the final settlement address and broadcasting them to the blockchain. The liquidity provider is paid interest and a trading fee commission if and when the liquidity is utilised.

Multi-asset order type PACT SWAP removes substantial capital costs by using the PACT approach, limiting collateral to the duration of a trade. However, there is another inefficiency in both DEXs and CEXs: liquidity fragmentation between markets.

Consider a swap market for 5 tokens: BTC, LTC, ETH, BNB, and MATIC. Makers, represented by $M_{i,j}$, are accepting i in exchange for j (makers are those placing a limit order or in pools, liquidity providers).

An example of liquidity fragmentation is when a maker having BTC needs to decide between providing liquidity into the $M_{LTC,BTC}$ market or the $M_{ETH,BTC}$ market. A type of maker, the *market maker* might not have a strong preference about receiving either LTC or ETH as long as the price is right, but is forced to select one of the markets.

	BTC	LTC	ETH	BNB	MATIC
BTC	–	$M_{BTC,LTC}$	$M_{BTC,ETH}$	$M_{BTC,BNB}$	$M_{BTC,MATIC}$
LTC	$\mathbf{M}_{\text{LTC,BTC}}$	–	$M_{LTC,ETH}$	$M_{LTC,BNB}$	$M_{LTC,MATIC}$
ETH	$\mathbf{M}_{\text{ETH,BTC}}$	$M_{ETH,LTC}$	–	$M_{ETH,BNB}$	$M_{ETH,MATIC}$
BNB	$M_{BNB,BTC}$	$M_{BNB,LTC}$	$M_{BNB,ETH}$	–	$M_{BNB,MATIC}$
MATIC	$M_{MATIC,BTC}$	$M_{MATIC,LTC}$	$M_{MATIC,ETH}$	$M_{MATIC,BNB}$	–

A solution to this is to introduce a common exchange token which is often $USDT$ on centralised exchanges, while it can be a platform token in DEXs. The number of markets is then reduced as one side of the market is always this token, labelled X

	X	BTC	LTC	ETH	BNB	MATIC
X	–	$M_{X,BTC}$	$M_{X,LTC}$	$M_{X,ETH}$	$M_{X,BNB}$	$M_{X,MATIC}$
BTC	$\mathbf{M}_{\text{BTC,X}}$	–	–	–	–	–
LTC	$\mathbf{M}_{\text{LTC,X}}$	–	–	–	–	–
ETH	$M_{ETH,X}$	–	–	–	–	–
BNB	$M_{BNB,X}$	–	–	–	–	–
MATIC	$M_{MATIC,X}$	–	–	–	–	–

However, there are still inefficiencies with this approach. The first being that our market maker which now has the X token, still has a liquidity fragmentation problem in deciding where to allocate capital between $M_{BTC,X}$ or $M_{LTC,X}$.

However, there is another problem related to volatility. The inherent volatility, and thus risk, increases when an intermediate token is introduced.

As an example, LTC might closely follow the price of BTC, but both might have high volatility compared to $USDT$. Thus, $BTC \xrightarrow{swap} USDT \xrightarrow{swap} LTC$ will introduce volatility which market makers must cover through higher spreads.

Archived copy · cryp2nova.com

	X	BTC	LTC	ETH	BNB	MATIC
X	–	**high**	**high**	*high*	*high*	*high*
BTC	–	–	**low**	*low*	*low*	*low*
LTC	–	–	–	*med*	*med*	*med*
ETH	–	–	–	–	*med*	*high*
BNB	–	–	–	–	–	*high*
MATIC	–	–	–	–	–	–

An alternative solution to this is the multi-asset order type, where a single asset allocation is used in multiple markets at the same time, as indicated below.

The maker orders (limit order) inside the red box all utilise the same BTC and thus $3x$ the liquidity is added to the DEX compared to the situation with liquidity fragmentation, but without the volatility penalty of trading through a common token.

In the order, a vector of prices is provided; thus, the lower volatility between BTC and LTC in our example can be expressed in the market without liquidity fragmentation.

Note that the multi-asset order does not have to include all tokens. In this example, the market maker included only three markets in the multi-asset order.

	BTC	LTC	ETH	BNB	MATIC
BTC	–	$M_{BTC,LTC}$	$M_{BTC,ETH}$	$M_{BTC,BNB}$	$M_{BTC,MATIC}$
LTC	$\mathbf{M}_{\mathbf{LTC,BTC}}$	–	$M_{LTC,ETH}$	$M_{LTC,BNB}$	$M_{LTC,MATIC}$
ETH	$\mathbf{M}_{\mathbf{ETH,BTC}}$	$M_{ETH,LTC}$	–	$M_{ETH,BNB}$	$M_{ETH,MATIC}$
BNB	$\mathbf{M}_{\mathbf{BNB,BTC}}$	$M_{BNB,LTC}$	$M_{BNB,ETH}$	–	$M_{BNB,MATIC}$
MATIC	$M_{MATIC,BTC}$	$M_{MATIC,LTC}$	$M_{MATIC,ETH}$	$M_{MATIC,BNB}$	–

3.1.4 Order book

The main order type on PACT SWAP is the limit order similar to what is found in a CEX. Concentrated liquidity pools, well known from Uniswap v3 have the advantage of being able to be quite similar to an order book and also emulate a constant product automatic market maker (CPAMM).

However, order books have a unique advantage in that each limit order can be identified, and this identifier can be tied to transactional behaviour such as the UTXO dust-lock (see 4.4). As an initial focus is on the Bitcoin market, this order type is particularly well suited. Additionally, an order book is most easily integrated into existing tooling for market makers working on CEXs.

3.2 Serverless front end support

PACT SWAP addresses the issue of front end censorship by implementing a fully decentralised, serverless front end that can be loaded directly from any blockchain. This approach ensures that the DEX front end is immune to censorship attempts[10] directed at specific infrastructure providers or web hosting services. By decentralizing the front end, PACT SWAP enhances operational security and ensures that the DEX remains accessible and functional regardless of external

Archived copy · cryp2nova.com

pressures. The serverless front end also enables DAO control of DEX "screen real estate"[5] and front end functionality, allowing additional DAO-controlled revenue streams, such as, for example, paid promotion, to be activated.

3.2.1 Permissionless listing of native assets from different chains

A fundamental property and repeating pattern of the most successful blockchains and dApps, with Bitcoin as the prime example, is their permissionless design. The permissionless property allows the largest number of participants and the most diverse innovation space. This is also evident for DEXs, where the introduction of single-chain DEXs with permissionless listing has seen explosive expansion and also fueled immense innovation in the DeFi space. As a unique feature of PACT SWAP, anyone can list cross-chain DEX pairs simply by executing a transaction deploying the smart contract code for the new trading pair. Permissionless listing encourages innovation within the DeFi space and establishes DEXs as central points for early access to innovative projects for investors and community participants.

PACT SWAP can optionally charge a listing fee for the deployment of new trading pairs. The fee amount can be set by the PACT SWAP governance and is paid in the $PACT token, which will be burnt. Multiple models can be applied, such as higher initial trading fees as an alternative to initial listing fees. Premium listing options can be made available, where newly listed pairs will get extra exposure in the PACT SWAP front end.

3.2.2 Cross-chain DeFi composability

Consistent cross-chain operations combined with full L1 data availability in a deterministic computation framework enables DeFi abstractions previously found only within the boundaries of single blockchain networks to be expanded across a large number of independent blockchains. This composability includes consensusless DEXs such as PACT SWAP, which enable cross-chain permissionless listings and programmatic swapping, but do not stop there. With PACT SWAP as a powerful liquidity hub, cross-chain DeFi abstractions have a powerful engine to further extend with complex cross-chain DeFi abstractions with access to capital and liquidity far beyond what exists on single blockchains. PACT SWAP itself will benefit from an open, modular architecture, taking full advantage of its first-mover advantage.

3.3 Economic model

Two of the main factors that determine the competitiveness and profit potential of a DEX are competitive advantages derived from superior:

- Technical characteristics
- Economic model

PACT SWAP's economic model is designed to fully leverage decentralisation's unique and valuable properties while enabling diversified revenue streams and value appropriation strategies similar to those commonly used by centralised exchanges.

A novel concept is to establish PACT SWAP as an entity with financial leverage within the blockchain ecosystem, complementing and rivalling that of centralised exchanges. This financial

Archived copy · cryp2nova.com

leverage will be used to gain privileged access to financial opportunities and mechanisms currently only available to a limited group of centralised actors, such as large centralised exchanges.

PACT SWAP governance and self-optimising vetting mechanisms are key functions behind this strategy, all of which are directly driven and controlled by the $PACT token.

The $PACT token

The $PACT token is unique in many ways, and its functions are essential for PACT SWAP's success and stakeholder value appropriation. The $PACT token is deflationary by design; only a fixed number of $PACT tokens will ever be issued, and most token utility requires burning $PACT tokens. Each $PACT token represents proportional ownership of the PACT SWAP fee accumulation pool, where $PACT token holders are free to release and redeem their portion of the pool at any time by burning $PACT tokens. However, the $PACT token has far more utility than a right to release funds from the fee accumulation pool. $PACT token holders are also the governors of PACT SWAP and direct stakeholders and beneficiaries of the PACT SWAP DEX revenue streams, financial activities and returns.

4 PACT SWAP technical architecture

PACT SWAP is implemented on the Coinweb platform using collateralised reactive smart contracts following the PACT implementation pattern[7].

4.1 Coinweb capabilities

Coinweb is a unique dApp platform that provides a deterministic computation framework on top of a consensusless interoperability layer; Coinweb smart contracts run in WebAssembly VM instances in a batch sequential execution model on top of each connected blockchain, enabling high-capacity parallel processing on top of each chain. Smart contracts can emit new transactions as output, which can be passed between the execution environment on top of each blockchain. The Coinweb interoperability layer ensures consistency for cross-chain operations. Coinweb smart contracts can hold gas balances and self-activate, allowing them to run continuously in a manner similar to background processes on regular computers. They can also monitor any events in the underlying L1 blockchains, giving Coinweb dApps full data availability across all connected chains[8]. PACT SWAP utilises several of Coinweb's enhanced dApp capabilities to enable multiple, significant advantages over current similar dApps.

4.2 The PACT implementation pattern

PACT (Penalty Adjudication for Cross-chain Transactions) is a novel and versatile blockchain interoperability primitive and implementation pattern, allowing expensive and insecure off-chain infrastructure to be replaced with easily deployable smart contracts. PACTs are essentially Coinweb reactive smart contracts that control collateral and distribute this collateral based on a set of programmable rules and observed events from underlying blockchains.

[7] See https://docs.coinweb.io/learn/usecases/pact

[8] See https://explorer.coinweb.io for connected blockchains

Archived copy · cryp2nova.com

A typical use case for PACT for a cross-chain asset swap would allow a maker to create an offer for selling a native asset on a specific chain (for example, BTC on Bitcoin) in exchange for an asset on a different chain (for example, USDT on Ethereum). The offer would contain the makers' deposit address, a rate and time of expiry, and a collateral deposit locked by the PACT smart contract. A taker can accept the offer by depositing USDT to the deposit address specified in the PACT. This deposit is observed on the Ethereum blockchain by the PACT. The PACT also monitors the Bitcoin blockchain to verify that the maker deposits BTC to the taker's address according to the offer specified in the PACT. If the maker settles the trade according to the offer, the collateral held by the PACT is then released back to the maker. If the maker fails to settle the trade according to the order, collateral is then released to the taker, compensating for the missing BTC settlement. (Additional mechanisms can be implemented on top of this such that the collateral will be converted to the asset specified in the PACT (in this case, BTC) so that the taker will receive the compensation in the asset they requested.

4.2.1 Advantages of PACTs

In addition to significant efficiency and security gains, PACT allows permissionless listing of cross-chain trading pairs, open access to liquidity provisioning and dApp composability in the same manner as DEXes like Uniswap residing on single chains. We expect this to be a catalyst for a significant increase in cross-chain DEX traffic and cross-chain DeFi innovation.

PACTs enable many significant advantages over current blockchain interoperability approaches:

Technical complexity and overhead

- Problems with current implementations:
  - Current interoperability infrastructure is built using off-chain infrastructure such as staked validator nodes, interoperability blockchains, relayers, oracle networks or completely centralised services. Deployment of such custom systems comes with a high level of complexity and introduces multiple levels of potential security vulnerabilities and high costs. Operating custom off-chain infrastructure is expensive and requires significant resource subsidisation. This is typically done by bootstrapping separate project communities for each custom implementation, incentivised by the validator and stake rewards necessary to maintain interchain consensus mechanisms.
- Reduced technical complexity and overhead with PACTs:
  - PACTs can be implemented entirely as smart contracts and require no additional off-chain infrastructure such as validator nodes, oracle networks, in-between blockchains or centralised services. This removes a large number of potential security risks and makes deployment easy, low cost and largely uniform across any blockchain system. PACTs do not require any additional consensus mechanism, which removes the need for expensive resource subsidisation schemes such as validator/mining rewards and bootstrapping specific communities to support these mechanisms.

Archived copy · cryp2nova.com

Capital efficiency

- Problems with current implementations:
  - The widespread use of constant-product liquidity pools typically leads to slippage costs in the 0.1%-0.3% range for even the most liquid assets.
  - Resource subsidisation and protocol security typically depend on staked assets locked as slashable collateral. Collateral used to back transaction flow is typically not optimised to match transaction size and execution time but instead tied to general protocol parameters, leading to unnecessary over-collateralisation, potential security vulnerabilities, and unutilised capital resources.
  - Security mechanisms implemented as L1 smart contracts lead to high transaction costs.
  - Liquidity reserves are bound to the resource subsidisation and protocol security mechanisms, making capital optimisation more difficult.
  - Non-deterministic cross-chain operations increase the risk of inter-chain inconsistencies and interoperability failures, making cross-chain operations more risky and expensive
- Increased capital efficiency with PACTs:
  - No resource subsidisation cost for custom off-chain infrastructure, community bootstrapping and incentives for protocol operation.
  - No additional capital lock-up for consensus-driven security
  - Fine-grained adjustment of backing collateral for transaction flow both for execution time and transaction size, reducing capital cost per transaction significantly while also providing optimal transparency and security.
  - Just-in-time liquidity provisioning for each transaction, maximising capital velocity and minimising volatility risk for liquidity providers even with rapidly changing transaction volumes
  - Coinweb's deterministic computation layer guarantees the consistency of cross-chain operations and provides a protocol-level settlement layer that always reflects the consensus of the underlying L1 blockchains, reducing the risk and, hence, the cost of cross-chain operations.

Value capture

- Problems with current solutions
  - Isolated revenue streams, locked inside rigid custom infrastructure
    * Rigid, application-specific off-chain infrastructure isolating revenue streams. Current cross-chain solutions are largely implemented as custom, incompatible systems. They are also adding separate consensus systems, eliminating the deterministic properties from L1. These deterministic properties are essential

Archived copy · cryp2nova.com

for building blocks in complex DeFi abstractions, and eliminating their consistency excludes cross-chain revenue streams from accumulating extended value from innovative, profit-generating DeFi ecosystems.

- Increased composability and value generation with PACTs
  - PACTs are deterministically executed smart contracts with guaranteed consistency over all blockchains. Additional abstraction layers can easily be applied on top of PACTs, allowing innovative liquidity provisioning mechanisms, market mechanisms for capital volatility protection, etc., to be implemented on top of the PACT smart contracts.

Improved users journeys

- Compatibility with existing signature schemes and address formats.
  - Coinweb enables PACTs to be compatible with any underlying blockchains' signature scheme and address formats. This can be used to simplify user journeys by, for example, allowing wallets with compatible signature schemes to be used across different blockchains.

4.3 How capital-efficient are PACTs for cross-chain DEXs?

A significant contributing factor to the capital efficiency of PACT-based cross-chain state machines is the ability to record when the state machine has finished. When it is finished, any collateral associated with the PACT is released, reducing the overall bound capital to earn yield. As Figure 1 shows, the held collateral is dynamically adjusted to the amount and execution time

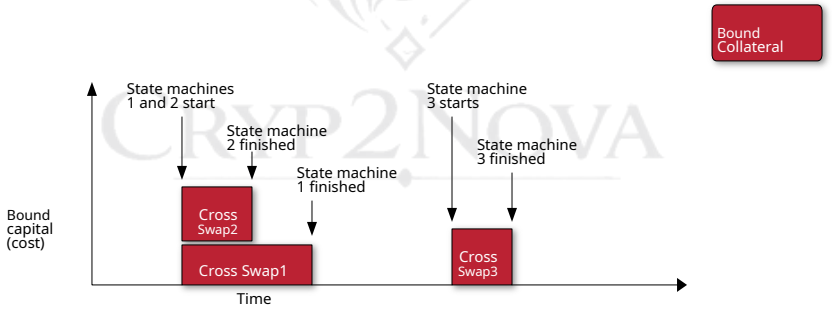


Figure 1: Cross-chain DEX transactions based on PACTs. Held collateral is marked in red

of each transaction. The diagram below shows a typical setup using staked validator nodes competing in staking amounts to become part of the validator set.

Archived copy · cryp2nova.com

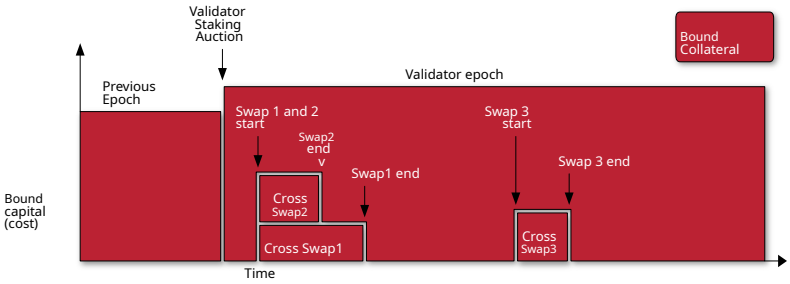


Figure 2: Fig 2. In validator/oracle-based systems, the amount of bound collateral is not directly adjusted to the transaction volume or execution time. Instead, the collateral bound is tied to the consensus mechanism of the specific interoperability protocol, where participants typically compete in binding up the most capital for staking.

4.4 Direct p2p settlement through order-bound dust-lock UTXOs

For users who directly use the Bitcoin payment network, swapping through a centralized or decentralised exchange using a vault or pool structure always involves indirection.

For example, if Alice wants Bitcoin and has token X, while Bob wants Bitcoin and wants token X, then for a centralized exchange, Alice needs to send Bitcoin to it, while Bob needs to execute a withdrawal. Two transactions are required. The same is true for a decentralized exchange where the Bitcoin is held in vaults or pools on behalf of the exchange.

A more efficient swap between Alice and Bob would involve Bob directly sending Bitcoin to Alice, as then only a single transaction would be needed, and the savings in fees could support lower prices and spreads.

The problem here is a coordination problem. Both the centralized exchange and the decentralized exchange's vaults are trusted through reputation or collateral; thus, deposits to this custodial structure can be separated from swapping.

If Alice or Bob puts up enough collateral compared to the orders they engage in, trading with them can be safe, but this can be impractical (and expensive!) for p2p trading. Instead, we need a technique to uniquely tie a single payment to a single order, and for that, we can use a "dust-lock", sometimes also referred to as "TX pinning". A "dust-lock" is a specific UTXO that is required to be included in a payment for it to match an order. The UTXO has the flag ANYONECANPAY, meaning anyone can include it in their transaction.

Since UTXOs can only be spent once, a miner will only select a single transaction among all transactions that include a given dust-lock. An order in PACT SWAP that accepts this type of settlement chooses a required dust-lock UTXO that must be present in payments in addition to other requirements, and thus, only a single transaction can match the order at any given time. This avoids any double payment issues in the p2p scenario.

Bitcoin supports the construction of dust-lock transactions using the Partially Signed Bitcoin Transaction (PSBT) standard. These transactions can be presented as QR codes in Bitcoin wallets that support PSBT.

Dust locks are provided by a separate service. The order pays for the use of the dust lock. Dust lock providers earn money when orders are matched.

Archived copy · cryp2nova.com

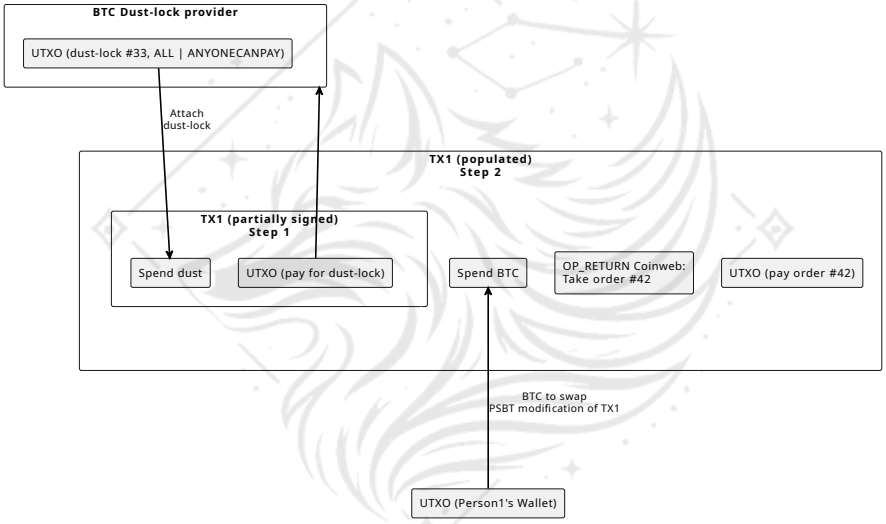


Figure 3: The dust lock mechanism prevents duplicate settlements on UTXO-chains

Archived copy · cryp2nova.com

5 PACT SWAP economic model and the $PACT token

$PACT token utility and function
The $PACT token is the utility and governance token of PACT SWAP. It is used to activate almost all of the PACT SWAP functionality, either through staking, burning, or both. the $PACT token is, however, not used to collect fees from DEX transactions; all DEX fees are accumulated in a fee accumulation pool, fully locked in by the $PACT token.

5.1 $PACT token incentives

PACT SWAP's participant incentives are designed to align the interests of all stakeholders and promote active participation in the ecosystem. Key incentives include:

- **Trading Fee Discounts**: Staking $PACT tokens allows traders to benefit from reduced trading fees, encouraging long-term commitment to the platform.
- **Affiliate Program**: Resellers can direct traffic to PACT SWAP and receive affiliate commissions. Registration requires a fee paid in $PACT tokens, which are then burned, reducing the total supply of $PACT tokens.
- **Governance Participation**: $PACT token holders can participate in the governance of the platform, influencing key decisions such as fee structures, new listings, and promotional campaigns. This ensures that the community has a direct say in the platform's development and strategic direction.
- **Burn Mechanism**: All fees collected in $PACT tokens are burned, preventing spam and other undesirable usage.

Narrowing the gaps between DEX and CEX
The ability to identify, unlock and optimise any beneficial sources of value is essential for sustained competitiveness and capture of market share. A holistic approach during the analysis and design of the economic model can make alternative profit models and synergies more easily identifiable. An example could be a model based on minimising/subsidising the cost of sensitive services such as exchange transactions on certain trading pairs as a strategy to maximize growth in transaction volume and user base, for then to capitalise on high-margin, more profitable revenue streams derived from the large transaction volume and number of user interactions. A comparison between DEXs and CEXs will quickly show how CEXs typically combine a more diverse set of revenue streams than DEXs, for example, token launches, listing fees, promotion, advertising, incubation services/investments, etc. In the coming sections, we will go through PACT SWAP's competitive advantages from efficiency gains and other optimisations; we will then look at combining these advantages with additional value streams unlocked from PACT SWAP usage.

5.2 Core ideas

The goal of the economic model is to enable PACT SWAP to gain a stronger position in the blockchain ecosystem, which is more comparable to that of large CEXs than to other DEXs.

Archived copy · cryp2nova.com

The economic model should no longer be designed with a single-utility focus but instead combine the inherent unique advantages of DEXs with proven strategies from CEXs to establish a decentralised economic powerhouse, complementing and rivalling the current CEXs. Two main strategies are devised to enable this transition:

1. Activate and leverage a diversified set of revenue streams and induced synergies.
2. Use competitive advantages and increased revenue streams to accumulate and gain financial leverage through an allocation in a fee accumulation pool.

Successful execution of these strategies unlocks the following additional advantages:

- Diversified revenue streams increase overall revenue and can generate more profit directly, but they can also be used in combination, where price-sensitive, high volume, low-margin services can be subsidised to gain increased exposure for separate services where margins and profits are higher.
- Accumulated cash reserves unlock strategic financial opportunities that would otherwise not be accessible. PACT SWAP will enable and incentivize powerful analyst and vetting community roles. Through these roles and associated mechanisms, $PACT token holders will be well-positioned to identify and benefit from attractive opportunities that arise in the ecosystem.

5.3 PACT SWAP Competitive advantages

In addition to the multiple competitive advantages derived from unique technical solutions and optimisations, PACT SWAP also introduces novel liquidity optimisation mechanisms and innovative business strategies. The utilisation of these powerful capabilities is coupled with specifically tailored stakeholder incentive mechanisms throughout the different stages of the project lifecycle.

5.3.1 Technical optimisations

Some of PACT SWAP's multiple technical optimisations have been described in detail in chapter 3 and 4. Key advantages such as removing the need for subsidisation of application-specific infrastructure, including consensus incentives and reverse collateral allocation incentives encouraging optimised allocation instead of overallocation, both provide PACT SWAP with unique competitive advantages by reducing operational and capital costs.

5.3.2 Unique features

PACT SWAPs unique smart-contract implemented cross-chain architecture provides it with a unique set of features and functionality compared to fixed-function cross-chain DEXs. This architecture gives PACT SWAP many of the same useful properties as single-chain DEXs but extends to work across a large number of blockchains. Importantly, PACT SWAP is composable in the same manner as DEXs like Uniswap, and powerful cross-chain DeFi abstractions can be implemented using PACT SWAP as their core engine and liquidity hub.

Archived copy · cryp2nova.com

5.3.3 Censorship resistant, serverless front ends

A commonly ignored issue with the current Web3 infrastructure is that most of the dApp front ends are not decentralised. Centralised front ends are more difficult to control through decentralised governance mechanisms, making it possible to bypass dApp stakeholders when dApp-generated value is distributed. Centralised front ends are also less resistant to censorship than their decentralised dApp back-end cores. There are multiple examples of how centralised front ends reduce the utility of the dApp and direct revenue flows away from DAO stakeholders.

PACT SWAP will implement a server-less front end interface, where front end code and UI elements are loaded from data embedded into blockchains. The front end is displayed by utilising customised loaders, which can be embedded in regular web pages or loaded from wallet apps or plugins. PACT SWAP affiliates can add their affiliate IDs to receive affiliate rewards from the traffic they generate through their loader interfaces.

The serverless front ends mitigate many constraints and limitations currently resulting from centralised dApp front ends. Since no centralised entity is required to pay for server costs, any centralised control of the dApp front end is no longer necessary. This will prevent cases such as Uniswap Labs' front end fee and censorship of the front end, which also happened to Uniswap[10]. With a fully decentralised front end, dApp governance can also be fully decentralised, gaining full control over the dApp. This is a huge advantage for capturing additional revenue streams from the dApp, as protections against shutdown, circumvention and altering of the front end are built in and controlled by on-chain governance mechanisms. Any updates to the dApp parameters or front end elements will require the burning of the $PACT token. .

5.3.4 Trading fees - a key to market dominance

While definitely not the only factor, competitive exchange fees are one of the most important factors determining the uptake and volume of both centralised and decentralised exchanges. This is especially true when competing for volume from resellers such as DEX aggregators and wallets. The DEX with the lowest fees will always be attractive for large segments of the market. If a DEX can maintain the lowest fees in the market over time, it is likely to significantly strengthen its market position and increase both its user base and trading volume during that time. This last point is important, as it would be naive to assume that optimal fee levels and overall value capture can be achieved indefinitely without performing continuous adjustments and improvements. A DEX must be able to provide the appropriate incentives and mechanisms for such ongoing market adjustments. From the above discussion, we can conclude that significant consideration should be given to the design and implementation of the fee structure so that the DEX is always in a position to underbid competitors while at the same time being able to provide the necessary incentives to remain competitive and maximise value capture potential.

The balance between fee levels and prolonged competitiveness

Following the reasoning above, we can deduce that an ideal balance must exist between facilitating the necessary incentives and mechanisms for staying competitive over time and the actual level of value to extract from the usage of the DEX to pay for these. If more is charged in exchange fees than the DEX can cover from cost optimisations, other unique advantages, or subsidies taken from other revenue streams, the DEX will no longer be able to provide the lowest exchange

Archived copy · cryp2nova.com

costs, and competitors can increase their relative market share by offering lower costs. However, without incentives and mechanisms to adjust to changing market conditions, the DEX will not be able to remain competitive over time.

The history of Uniswap fees

An interesting case study for the setting of DEX fees is Uniswap. The lack of underlying technical competitive advantages combined with weak or misaligned community incentives have so far prevented the activation of Uniswap protocol fees. This is despite the fact that the mechanisms for activating fees have been implemented in the protocol, and multiple reports and analyses partially supported by evidence[6] suggest that properly applied protocol fees can contribute to the long-term competitiveness and growth of the project. Realising that Uniswap would require improvements and adjustments to retain its position as the market leader, Uniswap Labs devised an ad hoc fee solution to fund necessary development work. An exchange fee was added to selected pairs for swaps initiated using the Uniswap Labs front end interface. Initially, a 0.15% fee was imposed, subsequently increased to 0.25%. This strategy has shown good monetary results. Uniswap Labs currently collects between $200 k and $800 k daily in front-end fees[5]. However, there are some suboptimal aspects of this strategy. Protocol-generated revenue now bypasses the already established DAO governance mechanism introduced with the UNI token. Instead, the revenue is directly transferred to the same centralized entity that effectively controls most of the core protocol.[] Since this entity (Uniswap Labs) is centralised, it is less transparent and vulnerable to a much larger array of potential attacks and other risk factors (This has already become evident by the fact that Uniswap Labs have been forced to remove several trading pairs from their front end, reducing the utility and competitiveness of the Uniswap)[10].[9]

Current DEX fee strategies

DEXs have implemented multiple fee strategies. Single-chain DEXs on the same chain are, in principle, bound to the same infrastructure constraints determined by the properties of the L1 blockchain, thus the fee strategy directly impacts the obtainable price optimisation of the DEX. Current Cross-chain DEXs are largely implemented using application-specific custom off-chain hardware configurations and community incentive mechanisms for resource subsidisation, securing asset vaults, L1 settlements, liquidity provision and core consensus mechanism. Due to the differences and independence between the different cross-chain DEX solutions, the competitive impact from the different fee strategies of these systems is not directly comparable to the same degree as on single-chain DEXs.

Single chain DEXs

Starting with single-chain DEXs, again using Uniswap as an example, we observe that Uniswap has yet to activate protocol trading fees. There are likely multiple reasons for this:

[9] ***Improvements to the Uniswap labs solution:*** *By applying a few adjustments and improvements, the monetary success achieved by the Uniswap Labs interface can be significantly expanded and secured. By adding more features for value capture and extending the DEX dApp decentralisation, the DEX front end can also be implemented as fully decentralised and serverless, loaded directly from blockchain-embedded data. More functionality and improved operational security would increase the total value capture and allow increased competitiveness for price-sensitive functionality, accelerating exchange volume and user base growth.*

Archived copy · cryp2nova.com

- Being isolated to single L1 blockchains, Uniswap has no technical platform-specific competitive advantages over other DEXs on the same blockchain. Adding additional fees to the existing gas and liquidity fees would allow competitors to implement equivalent DEXs without protocol fees and provide the same service at a lower cost.

- The initial funders and founders of Uniswap might be able to indirectly profit from increased traction in the Ethereum ecosystem created by Uniswap, for example, if they are invested in ETH or yield-generating dApps using Uniswap.

- Uniswap successfully capitalised on its popularity by launching the UNI token, which immediately accrued value, likely from speculation that a protocol fee could be distributed in the future. The speculative value of the UNI token can be used to fund protocol improvements as long as there is a belief that the tokens will stay valuable.

- After implementing the functionality to add protocol fees, the proposal to enable protocol fees was voted down by the UNI token holders. This might be because the incentives to secure the long-term success of the project might not be fully aligned with the majority of UNI holders, who are users of the DEX. It can also be because the majority of participants in the vote wanted the collected fees to be distributed independently of the UNI token holders.

Multiple examples exist of Uniswap equivalents that have activated protocol fees. Pancake Swap, for example, deducts a part of the swap fee to the Pancake swap treasury, CAKE token buybacks, and burns; the remaining is rewarded to the liquidity providers. Despite the added fee, Pancake Swap remains the dominant DEX on the Binance chain measured in exchange volume.

Cross-chain DEXs

Cross-chain DEXs are typically built around separate blockchain or consensus-based systems where individual validator nodes participate in the consensus mechanism, and DEX operations usually put up stakes and bonds to be allowed to participate. To achieve a reasonable level of security, a distributed consensus system requires a relatively large number of participating nodes, and for stake-based systems, each participating node must also lock up a significant amount of staked capital. Operating a node requires significant skill and effort since the staked collateral can be slashed, both if the node is offline or, in other ways, if misbehaving due to hacking or errors occurring from other causes. Operational costs are included in addition to the cost of hiring or buying the necessary hardware, as well as the costs of node hosting and connection costs[**?**]. Due to the large number of nodes necessary, the total cost of operating such an application-specific network is significant. In addition to this comes capital costs for available liquidity reserves and collateral. These costs must be covered by the value extracted from the exchange volume in the network, the potential speculation value extracted from the project token, or the loss of value from the available liquidity pools.

For sustainable operation[8], the operational costs must eventually be covered by exchange fees or other revenue-generating services that the network can provide. Typically, cross-chain DEXs operate with a multitude of different fees and costs, some of which are derived from the protocol definitions. In contrast, others are implicit, often varying in size depending on non-deterministic processes within the system. For example, protocol-determined slippage vs. actual

Archived copy · cryp2nova.com

slippage can differ greatly. Often, this is caused by front-running and arbitrage costs that occur internally within the system. Also, external costs such as L1 settlements can be subject to additional protocol fees added to the actual transaction costs.

PACT SWAP trading fees and costs
PACT SWAP has fewer and lower fixed costs than other cross-chain DEXs to incentivise market adjustment mechanisms and secure stakeholder value appropriation just from trading fees alone. The incentives necessary for market adjustments are nearly insignificant compared to the huge overhead of consensus-driven systems, where whole communities and expensive infrastructure must be subsidised and incentivised for continued operation. PACT SWAP can typically underbid competitors with cost reductions from at least 50% to several orders of magnitude. While certainly beneficial on its own, when used strategically, this advantage can be used to enable other compoundable sources of value.

5.4 Unresolved problems = Market opportunities

The blockchain ecosystem and technology have gone through rapid development and growth since its inception. There are, however, many unresolved problems that must be solved for the technology to reach even a fraction of its full potential. Although these problems are constraining the pace of development and growth, they also represent huge opportunities for those who are able to solve them. PACT SWAP provides novel solutions to several of these problems, not only by improving DEX primitives for better cross-chain DEXing but also by taking advantage of indirect value streams that are unlocked through the core functionality. In this section, we will go through some of these existing problems and show how PACT SWAP solutions transform these problems into accessible value streams.

5.4.1 Collateral allocation inefficiency

Current cross-chain DEX implementations often suffer from ineffective collateral allocation. This inefficiency arises from the need to lock up significant amounts of collateral to secure transactions, which is not optimised to match transaction size and execution time. This leads to unnecessary over-collateralization, potential security vulnerabilities, and unutilized capital resources.

PACT SWAP market opportunity:
PACT SWAP's PACT framework addresses these issues by allowing fine-grained adjustment of backing collateral for transaction flow, both for execution time and transaction size. This significantly reduces the capital cost per transaction while also providing optimal transparency and security. Just-in-time liquidity provisioning for each transaction maximises capital velocity and minimises volatility risk for liquidity providers, even with rapidly changing transaction volumes.

5.4.2 Underutilised liquidity

Liquidity is underutilised for various reasons. Improved liquidity efficiency and utilisation correlate closely to increased market capture and growth. PACT SWAP enables more effective use of

Archived copy · cryp2nova.com

liquidity through increased blockchain connectivity, cost savings and reduced complexity, programmatic cross-chain exchange, novel order types that reduce slippage, and improved liquidity utilisation (modular order settlement, multi-asset order type).

Limited number and connectivity of cross-chain solutions

Cross-chain DEXs are much more complex to implement and currently suffer from multiple disadvantages compared to single-chain DEXs. The availability of cross-chain DEX solutions is thus far inferior to that of single-chain DEXes. Cross-chain DEXs are generally less flexible, and available pairs are typically relatively limited. A listing of new pairs often comes with multiple levels of overhead, both technically and governance-related, or is subject to high capital costs due to a limited number of available slots. Cross-chain DEXs are also typically limited to chains within the same ecosystem, such as EVM chains. This further reduces the number of solutions available and the overall liquidity in the market. Currently, there are 3 cross-chain DEXes that support native BTC, Thorchain, Maya Protocol and Chainflip. They support 30,26 and 7 native assets, respectively, with several overlapping assets between them. Compared to single-chain DEXes, the difference is staggering. Uniswap on Ethereum alone has over 3000 different assets listed. PancakeSwap has more than 2800 different assets, and Raydium on Solana has more than 1200. Most pairs are listed against the most liquid asset on each chain.

Lack of native Bitcoin connectivity

The most evident example of such under-utilisation of liquidity is the low connectivity between native Bitcoin and other crypto assets. While being the far most liquid cryptocurrency in existence and involving almost 40% of the spot volume on centralised exchanges, the native BTC portion of DEX volume is almost non-existent, accounting for less than 1% of the total DEX volume. Compared to smart contract-based DEXs like Uniswap, it is difficult to set up new trading pairs with native Bitcoin, as these are currently implemented in custom off-chain infrastructure that is not accessible to external projects. PACT SWAP is the first cross-chain DEX that enables permissionless listing of cross-chain trading pairs with native Bitcoin in the same way as, for example, ERC20 tokens on Uniswap. PACT SWAPs permissionless pairing of native BTC to any asset on other chains and activation of native Bitcoin cross-chain DeFi composability is likely to unlock a large amount of dormant capital and generate significant cross-chain liquidity flows.

PACT SWAP market opportunity:

As the first DEX that enables the most liquid and price-correlating native crypto asset, BTC, available for permissionless listing and programmatic exchange against any assets between a large number of independent blockchains, PACT SWAP will significantly increase the liquidity flow between the Bitcoin chain and other blockchains. Swapping through BTC will often lower slippage costs compared to swaps going through stable tokens due to a generally stronger correlation between BTC and other crypto assets than with fiat-pegged stable tokens. PACT SWAP's modular order settlement architecture and novel order types further increase the efficiency of cross-chain liquidity flow.

Archived copy · cryp2nova.com

5.4.3 Other isolated chains

Other isolated chains face issues similar to Bitcoin's in terms of integration with DEXs. These chains often require custom solutions that are not compatible with existing DeFi infrastructure, causing reduced community activity and stagnation. PACT SWAP allows these chains' assets to be seamlessly integrated through permissionless listing, enabling trading and DeFi composability across multiple blockchains.

PACT SWAP market opportunity:
The Coinweb platform can relatively easily add technically diverse blockchains to its network. Coinweb also allows the addition of a large number of different blockchains. Many isolated blockchains or blockchain networks with significant communities and TVL exist, where a DEX allowing permissionless listing against the most liquid assets in larger networks would be a welcome addition to their ecosystem. Community support for PACT SWAP could be anticipated.

5.4.4 Expensive Resource subsidisation

Current cross-chain DEX implementations often rely on custom off-chain infrastructure such as staked validator nodes, interoperability blockchains, relayers, and oracle networks. These systems require significant resource subsidisation to maintain their operations. This subsidisation typically involves bootstrapping separate project communities for each custom implementation, incentivized by the validator and staking rewards necessary to maintain interchain consensus mechanisms.

The operation of such a custom off-chain infrastructure is expensive and introduces multiple levels of potential security vulnerabilities. The high costs and complexity associated with these systems are passed on to the end-users, making cross-chain transactions more costly and less efficient. The typical cost of running a cross-chain DEX node is between $2000 and $3500 per month, not accounting for the necessary maintenance effort required from highly skilled node operators. A typical network consists of 100 to 150 active nodes, resulting in a monthly net cost of maintaining the custom infrastructure at around 150*($3500+$2000)/2=$2750 per node* 150= $412500 [7]in server fees alone, not accounting for the monetary compensation of highly skilled node operators. The high operational costs can also impact the sustainability of the network, currently the largest consensus based cross-chain DEX is running at a deficit, with the network expenses more than doubling that of the revenue.

Inflated settlement costs
One common strategy used by current cross-chain DEX implementations to subsidise operational and infrastructure costs is to inflate the price of transaction settlements. In addition, the actual execution cost of L1 transactions can be more expensive than normal due to different control mechanisms implemented as L1 smart contracts.

PACT SWAP market opportunity:
In contrast, PACT SWAP's PACT framework eliminates the need for custom off-chain infrastructure and the number of fees. Expensive L1 settlements (Bitcoin and Ethereum) can often

Archived copy · cryp2nova.com

be made directly between users, potentially cutting the network transaction costs in half for common assets.

5.4.5 Other infrastructure shortcomings

Current cross-chain DEX implementations suffer from several technical shortcomings that reduce their performance and scalability. Again, these inefficiencies stem from the reliance on custom off-chain infrastructure, which introduces multiple layers of complexity and potential points of failure. Common issues include:

- **High Latency and Low Throughput**: The use of off-chain validators, relayers, and oracles introduces significant latency in transaction processing. This results in slower transaction times and lower throughput, making the DEX less efficient and less competitive compared to centralized exchanges.
- **Security Vulnerabilities**: Off-chain infrastructure components are not tied to L1 consensus and are often less secure than on-chain smart contracts. They are susceptible to various attacks, including Sybil attacks, collusion, double-spending, and outages. These vulnerabilities increase the risk for users and reduce trust in the DEX. They also increase the risk for cross-chain liquidity providers, which will make expedited transaction services more expensive.

PACT SWAP market opportunity:
PACT SWAP's PACT framework addresses these issues by implementing cross-chain operations entirely as smart contracts. This approach eliminates the need for off-chain infrastructure, reducing latency, improving security, and lowering operational costs. By leveraging the inherent properties of smart contracts and Coinweb's cross-chain consistent settlement layer, PACT SWAP ensures a more efficient, secure, faster and scalable DEX solution.

5.5 Diversified revenue streams - Synergetic growth

As discussed earlier in this and previous chapters, the revenue streams of DEXs are often less diverse than those of CEXs. This is despite the fact that DEXs, in many ways, are better suited to support many of the services that generate many of the additional revenue streams for the CEXs. Where CEXs have to rely upon reputation and regulatory verification as a foundation for their service offerings, DEXs can, to a much larger degree, enable equivalent service offerings on a fully trustless foundation backed by immutable blockchain data driven by transparent smart contract functions. PACT SWAP, as a composable cross-chain DEX is particularly suited for several complementary and synergic service offerings, as data from multiple blockchains and dApps can be aggregated and processed in a fully deterministic and verifiable manner. Following are some of the most interesting additional service offerings that PACT SWAP will enable and the problems they will address.

Archived copy · cryp2nova.com

5.5.1 Preventing rug pulls and scams

Currently, rug pulls and scams might be the biggest problem in the blockchain ecosystem. Technological innovations with great expected transformative potential often cause premature financial hype and misplaced investments. Malicious actors take advantage of the financial hype and use various degrees of inflated and inaccurate claims to deceive uninformed investors. The hype around blockchain technology is certainly not an exception, as the technology itself has opened access to large groups of retail investors with varying degrees of adequate knowledge. Scattered information sources and limited tools to assess information accuracy increase the severity of this problem. It is estimated that investors are deceived of several billion dollars each year, which, for many investors, has severe financial consequences and very damaging effects on the blockchain ecosystem.

PACT SWAP market opportunity - "PACT SWAP LAUNCHPAD" - Blockchain vetted token launches:
Decentralised applications inherit some very valuable properties and capabilities from the blockchains upon which they are built. One of those fundamental properties is the capability of producing and providing immutable and verifiable data, which is highly underutilised for purposes outside of asset transfer. By using these properties, PACT SWAP will, by adding a few simple functions, extend its utility as a very effective cross-chain DEX and also become a unique and powerful tool for avoiding and preventing rug pulls and scams.

Combining and improving current solutions
Many tools already exist that address the problem of misplaced investments in low-quality or fraudulent crypto projects. Centralised exchanges play a role here, where a vetting process is normally required prior to listing of an asset, but there are a huge number of companies, institutions, community projects, investment funds, dApps, publications, influencers and other individuals that in various ways contribute to limit the effect or stop crypto scams. The effectiveness of the various efforts will, to a large degree, depend on one common factor:

- **The ability to access, verify and assess the quality of relevant information.**

Currently, crypto project research involves gathering information scattered among many different sources. The accuracy and quality of the information vary greatly between different sources, but the most accurate information is typically the information that can be found on blockchains, such as transaction data. Unfortunately, most data are not as verifiable as blockchain data, and a lesser degree of certainty can be applied to it. With specific regards to researching blockchain projects prior to investment, certain platforms provide "hybrid" data, where some data can be at least partially verified on-chain.

Decentralised launchpads are such platforms, where prelaunch data, such as launch price, etc., are sometimes available, and metrics such as current ROI can be **verified with on-chain data from DEXs.** The trade data from DEXs are very valuable here, and a lot of useful information can be extracted with a high degree of verifiability. Curated launchpads add another metric, as the launchpad itself can be measured against the performance of the projects they have launched. A common limitation with these is that there is often no specific link to specific analysts or curators. This gives less visibility and also limits incentives for each individual analyst. Launchpads that

Archived copy · cryp2nova.com

link projects with specific curators or analysts typically attract more investors to projects linked to known, well-performing curators/analysts.

While these platforms provide useful tools, it is easy to see how they could be made much more powerful and unlock significant additional value for investors, stakeholders, and participants.

Using PACT SWAP data and community roles to unlock accumulated value

PACT SWAP's many competitive advantages as a DEX will drive both trading volume and user acquisition. Many DEX users trading listed tokens are also likely interested in participating in token launches. PACT SWAP will leverage the user base from DEX trading by providing a novel token launch platform. This token launch platform will implement multiple self-improving quality assessment mechanisms through defined ecosystem roles, automatically and continuously graded, primarily from PACT SWAP historical transaction data but also from other verifiable sources. The set of roles is controlled by the $PACT token holder DAO, but an initial set could be limited to the following roles, where some could be optional.

- **Curator** The role of a curator would likely not be optional, and curators would be linked to each project they are curators for. The curator would be assigned a soul-bound NFT, and association with the project would be achieved through a signed transaction linking the NFT with the project. The curator would continuously be assigned a reputation score based on the current performance (ROI, etc) of his associated projects, using trading data from PACT SWAP.

- **Analyst** The analyst role could be optional, and Analysts could link their project analysis and assessment score to projects prior to launching using their sole bound tokens and potentially also embedding their project analysis as immutable data. Analysts' reputation score would be calculated relative to the performance of the project and their committed project assessment score.

- **Promoter** The promoter role could also be optional. The role is sometimes connected with the curator role. Linking promoters with projects would use the same soul-bound NFT mechanism as the other roles.

Quantified Performance

PACT SWAP introduces a quantified performance system to enhance transparency and trust within the ecosystem. This system tracks and evaluates the performance of various participants and projects based on predefined metrics. By providing a clear and objective performance assessment, PACT SWAP ensures that users can make informed decisions and mitigate the risks associated with rug pulls and scams.

Self-improving mechanism

Each part-taker in the PACT SWAP Launchpad role system is rated by a continuously updating reputation score. Projects that want to launch on the PACT SWAP Launchpad must be linked to a curator. Investor confidence will likely be influenced by the curator's reputation score as well as that of other connected launch participant roles such as Analyst or Promoter. The rated launch

Archived copy · cryp2nova.com

participants with the highest reputation score will likely be most sought after by projects wanting to use the PACT SWAP Launchpad. The highest-rated launch participants would typically also demand the highest compensation. A drop in accuracy and linking to poorly performing projects would reduce the launch participants' reputation score, likely leading to lower compensation from launching projects.

5.5.2 Opening access to early investment opportunities

A very lucrative part of the Centralised Exchange's business model is incubators or investment vehicles (Labs). While playing an important role in funding and promoting new projects, the financial backing of crypto projects from dominant centralised actors can lead to market bias and stifle innovation. Often, early access to investment opportunities and participation is, in practice, closed to others than centralised investment funds or exchanges.

PACT SWAP Market Opportunity - PACT SWAP Incubator:
PACT SWAP, as a DEX, is in an ideal position to establish a decentralised alternative, which would likely lead to more diversification within the ecosystem and also provide an additional source of financial return for PACT SWAP stakeholders.

$PACT token and the Fee accumulation pool - Building financial leverage
With the right strategy, PACT SWAPs' many competitive advantages, including significant cost savings, can provide PACT SWAP privileged access to several of the largest and most profitable financial opportunities within the crypto economy. These opportunities are currently accessible only to a limited number of centralised actors, such as the largest centralised exchanges.

A key to enabling PACT SWAP and $PACT token holders to access these exclusive financial opportunities is to gain sufficient financial leverage for DAO holders of $PACT. Fortunately, PACT SWAP provides the right set of features and functions to do just that since fee revenue and multiple other revenue streams can be activated while still underbidding other market participants on cost and also providing a broader set of functionality and capabilities.

All DEX (exchange fees) fees are charged in CWEB and are then locked in a fee accumulation pool. **Burning $PACT tokens is the only mechanism to release funds from the fee accumulation pool!** The fee accumulation pool is owned by the $PACT token holders, and all $PACT holders can release their portion of CWEB from the fee accumulation pool at any time by burning their $PACT tokens. All $PACT tokens represent the same proportion of the accumulated fees in the pool. Upon burning $PACT tokens, the fee pool contract instantly releases a proportional amount of CWEB to the address where the burnt $PACT tokens were held. For example, burning 10% of the total supply of $PACT tokens, releases 10% of the fee accumulation pool.

Allocation of strategic cash reserves
Most of the Fee Appropriation pool will be controlled individually by the $PACT token holders. The proportion set aside for financial leverage is expected to be relatively small; the idea is that the value it represents will grow larger with the return from strategic placements. It is up to the PACT SWAP community to decide when and how the proceeds from these funds will be distributed. They can be accumulated to gain additional leverage or distributed directly to $PACT

Archived copy · cryp2nova.com

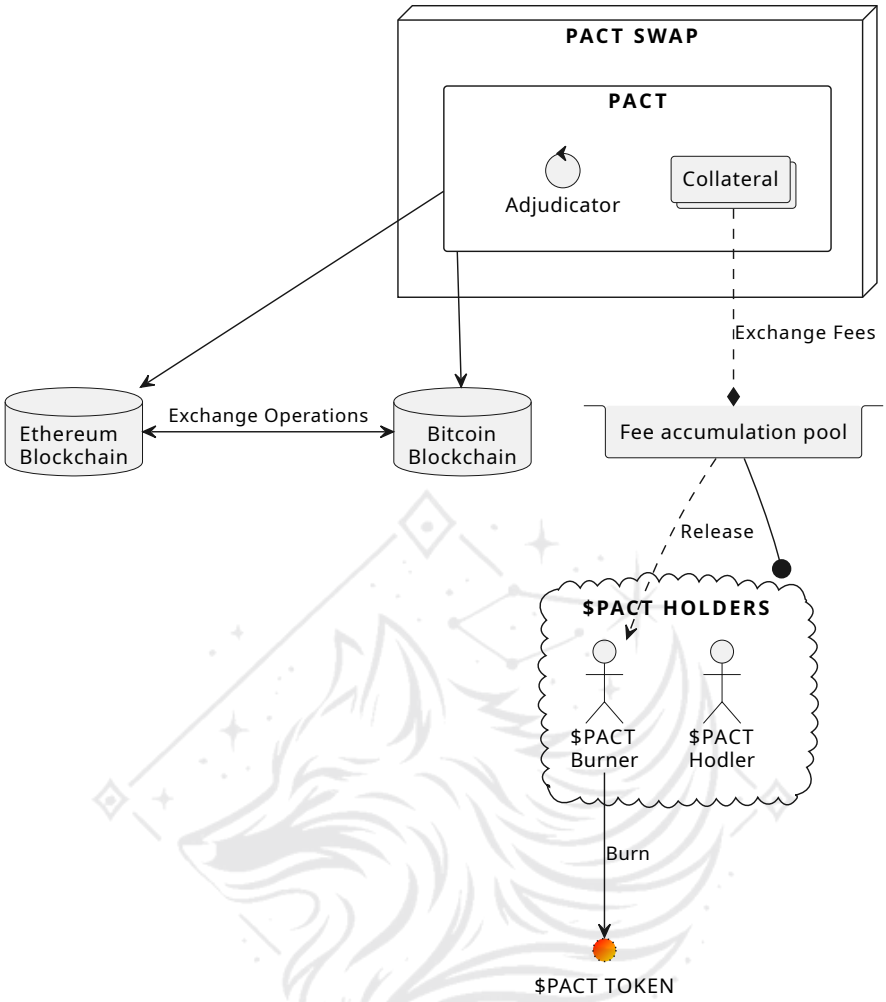


Figure 4: Fees accumulate in the fee accumulation pool and can only be released by burning $PACT tokens

token holders or any combination of the two. It is important to note that the funds represented by the strategic financial allocation can only be accessed when the allocated $PACT tokens are burnt. Any renewed strategic allocations would have to consist of $PACT tokens bought in the market but then potentially from the proceeds of the previous funds.

5.6 PACT SWAP governance

The PACT SWAP DAO governs PACT SWAP. Each $PACT token holder has the same proportional voting rights as all other $PACT holders.

Voting

Voting is done by burning $PACT tokens. This allows strong opinions to be expressed accurately and prevents large token holders from dominating the governance process forever. Burning as part of voting releases the proportional funds from the fee accumulation pool as normal.

Archived copy · cryp2nova.com

Proposals
Any $PACT holder can make proposals to the DAO by burning $PACT tokens. A minimum limit might be imposed to prevent spam.

Protocol parameters
Protocol parameters are voted on in the same manner as other votes by burning $PACT tokens.

Market fee adjustment
PACT SWAP employs a dynamic market fee adjustment mechanism to ensure competitive trading fees across different trading pairs. The fee structure is designed to be flexible, allowing adjustments based on factors such as trading volume, volatility, and market conditions. This approach ensures that PACT SWAP can offer the lowest possible fees while maintaining the necessary incentives for sustained market optimisation and stakeholder value appropriation.

5.6.1 Participants Performance Score

The PACT SWAP DAO can assign a Participant Performance Score for certain community roles. This score is not the same as the reputation score from the PACT SWAP Launchpad launch participants, but it could be assigned for roles such as fund managers, etc. The Participants Performance Score is a metric that evaluates the behaviour and reliability of individual participants within the PACT SWAP ecosystem. This score is calculated based on factors such as transaction history, adherence to protocol rules, and overall contribution to the network. High-performing participants are rewarded with incentives, while those with low scores may face restrictions or penalties. This system encourages responsible behaviour and fosters a trustworthy environment for all users.

5.6.2 Project Performance Score

The Project Performance Score assesses the credibility and success of the projects listed in the PACT SWAP. This score is determined by analysing various aspects such as project milestones, community participation and financial performance. Projects with high scores gain greater visibility and access to additional resources, while those with low scores may be subject to delisting or other corrective actions. By maintaining a rigorous evaluation process, PACT SWAP ensures that only high-quality projects thrive within its ecosystem.

5.6.3 Verified information

PACT SWAP addresses this issue by implementing a robust system for verifying information. All data related to transactions, liquidity, and trading pairs is verified through smart contracts and consensus mechanisms. This ensures that users have access to accurate and reliable information, reducing the risk of misinformation and fraud. Information from Analysts and partner community research portals could also be verified and assessed using the PACT SWAP information quality assessment system, controlled by the PACT SWAP DAO or authorised delegates.

Archived copy · cryp2nova.com

5.6.4 Quality assessed information

In addition to verification, PACT SWAP introduces a quality assessment system for information. This system categorises data according to its reliability and relevance, providing users with a clear understanding of the quality of the information they are accessing. By giving information quality scores, PACT SWAP improves transparency and trust within the ecosystem, enabling users to make better informed decisions.

6 Conclusions

Building on a novel consensus-less platform architecture, PACT SWAP enables significant efficiency improvements and extended functionality compared to existing cross-chain DEXs in the market. Important capabilities such as the permissionless listing of native assets between different blockchains and extended DeFi cross-chain composability from deterministic cross-chain computation open the possibility of successful DEX extensions and other DeFi abstractions found on single-chain systems being expanded to cross-chain implementations. Furthermore, a strategy to accelerate the closing of the gap between CEXs and DEXs through additional service offerings and value streams is proposed.

References

[1] Binance. Global crypto trading volume heads for $108 trillion in 2024, driven by europe and asia. https://www.binance.com/en/square/post/10788650680217, 2024.

[2] Coinbase. Shareholder letter q1 2024. https://s27.q4cdn.com/397450999/files/doc_financials/2024/05/Shareholder-Letter-Q1-2024.pdf, 2024.

[3] Coindesk. Auctiontheory. https://docs.chainflip.io/concepts/token-economics/auction-theory-ssod#the-auction-system-allocating-validator-slots, 2023.

[4] Coindesk.com. Binance generates 90% of revenue from transaction fees, changpeng zhao says. https://www.coindesk.com/business/2022/12/07/binance-generates-90-of-revenue-from-transaction-fees-changpeng-zhao-says/, 2022.

[5] dlnews.com. Uniswap labs raises front end fee. https://www.dlnews.com/articles/defi/uniswap-raises-its-user-interest-fee-to-025-from-01/, 2024.

[6] Gauntlet Team. Uniswap protocol fee report. https://www.gauntlet.xyz/resources/uniswap-protocol-fee-report, 2024.

[7] thorchain.org. Costs of running a node. https://docs.thorchain.org/thornodes/overview#costs, 2023.

[8] Thorcharts.org. Thorchain revenue vs expenses. https://thorcharts.org/thorchain_revenue_vs_expenses, 2023.

Archived copy · cryp2nova.com

[9] Tokeninsight.com. Crypto exchange report q2 2024. https://tokeninsight.com/en/research/reports/crypto-exchange-report-q2-2024, 2024.

[10] Uniswap.org. Unsupported token list. "https://support.uniswap.org/hc/en-us/articles/18783818770701-Unsupported-Token-List, 2024.

[11] www.theblock.co. Dex market share surges to record high, outpacing centralized exchanges. https://www.theblock.co/post/308132/dex-market-share-surges-to-record-high-outpacing-centralized-exchanges, 2024.

Archived copy · cryp2nova.com