HoldStation: a brokerage-based derivatives Platform for web3 with smart wallets

Tuan Tran, Hoai Nam, Trung Banh

2023/08/23

Executive summary

Holdstation is the first non-custodial derivatives trading flatform that brings the brokerage model from Web2 to Web3. Our products use smart contract wallet technology and are implemented on layer 2 roll-up blockchains such as zkSync Era to optimize the trading experiences and enhance privacy for traders, bring them as close to Web2 trading experiences as possible.

At the current moment and in the short terms, Holdstation delivers five main benefits for users. First, we provide a non-custodial smart wallet. Our smart wallet is currently available on both iOS and Android, and integrates the most innovative technologies such as Account Abstraction and ZkRollups, which offer privacy and modern digital wallet-like customer experience. Second, we provide a non custodial decentralized exchange for perpetual futures trading (DeFutures Exchange). This model is similar to the Forex brokerage model in Web2 and is built in such a way to bring the best parts of both worlds to users. DeFutures also allows traders to use limit , stop-loss and take-profit orders just like a CEX counterpart. Third, our trading platform enables individuals in the financial markets to automatically copy positions opened and managed by other selected individuals (copy trading). This will lead to a decentralized hedge fund /prop trading model in the future. Fourth, Holdstation provide users with a wide-range of data analytic services, where traders can benefit from latest news updates, on-chain data insights and technical indicators to support their trading activities (Holdstation Research). Fifth, Holdstation Launchpad is an upcoming platform that offers a range of services to facilitate successful project launches. We offer the first IDO Launchpad on smart wallet - both apps on iOS and Android.

1 Brokerage trading model

The central idea of Holdstation is to bring the brokerage trading model from Web2 to Web3. We aim to build a universal brokerage solution that connects brokers and traders to trade a wide-range of assets, including real world assets such as currencies, indexes, CFDs and crypto assets, just to name a few. Before doing this, we need to understand what this model is and why is it relevant at all in the crypto world.

Brokerage model is especially popular for Forex traders. A brokerage software allows to connect traders with brokers. More precisely, brokers will use a forex brokerage software to execute customer transactions on other exchanges, they also have an option of taking the other side of each order and transaction that a trader deals through them. In practice, just about all forex brokers will operate under one of the five common broker business models, although some brokers might use a hybrid of two or more of these model. The five common broker business models are:

- Electronic Communication Network (ECN). ECN forex brokers provide their customers with a means for obtaining direct access to the Interbank forex market for pricing and execution that usually consists of an ECN trading platform.
- Straight Through Processing (STP). STP forex brokers generally have a fully automated dealing system for their clients to use.
- Direct Market Access (DMA). Brokers use DMA model to execute transactions for their clients. It matches client orders with dealing prices offered by professional market makers at banks or other major liquidity providers.
- Market Makers. These brokers operate a dealing desk and makes their money by quoting a bid/ask spread to clients.
- Hybrid Forex Broker Model.

Archived copy · cryp2nova.com

There are plenty of forex brokerage softwares. eToro and MetaTrader 4 are two of the most popular forex trading platforms available today. eToro is a social trading platform that allows traders to follow and copy the trades of other traders. It is designed to be user-friendly and is ideal for beginners who are just starting out in forex trading. eToro offers a range of features, including social trading, copy trading, and a wide range of trading tools and indicators.

MetaTrader 4, on the other hand, is a more advanced platform that is used by professional traders and institutions. It offers a wide range of features, including advanced charting tools, automated trading, and the ability to create custom indicators and scripts. MetaTrader 4 is also highly customizable, allowing traders to create their own trading strategies and algorithms.

Unlike a centralized exchange, a broker model is over-the-counter in nature, so it causes traders to be charged more by brokers compared to centralized exchanges. However, the plus side of the brokerage model is to delegate the customer-base building task to brokers, as they are incentivized to do that with add-on fees gain. Besides, brokers have to compete to each other so that they are selected by traders from a list of rivals. And this is why traders will benefit from competitive services and prices. More importantly, just as liquidity is the most critical factor in trading, this brokerage model will be a promising approach to increase trading volume on Holdstation more than a typical DEX could do. The fact is that, many TradFi traders, for example Forex traders and stock index traders are not accessible to the crypto world, and these traders can be led to Holdstation via their own brokers. On Holdstation, they can continue to trade currencies and indexes via tokenized assets, with the same or better fees as well as customer experience than in Web2. This is why we believe that users will gradually immigrate from Web2 to Web3 via dApp as Holdstation, because they will find it more attractive than the tradFi counterparties. Last but not least, a forex broker should also offer value-added services that can increase traders' trading profits. One example is when a broker is offering commission-free trading. Traders can also check for charting tools, technical indicators, and news services that can help them make better decisions when trading.

Trading with forex brokerage softwares in Web2 is not without paint points. First, as brokers make money from traders via commission, traders might find it more expensive to trade with brokers than a centralized exchanges. The fact is that,brokers tend to exploit their unsophisticated clients to charge far higher commissions on trades – this is a direct result of the OTC market structure. Second, as liquidity is fragmented amongst different brokers, it might lead to wide bid-ask spreads for traders, which can be considered as implicit transaction fees. Third, as the nature of trading in Web2 is centralized and custodial, traders can be exposed to price manipulation, losses of funds, account freezing, brokers' lack of liquidity or being defaulted, and even fraudulent.

Holdstation, which is a non-custodial and decentralized brokerage-based trading model on blockchain, can offer solutions to remedy the pain points of the brokerage trading in Web2, such as lower fees, more accurate market prices thanks to decentralized price oracles such as Chainlink and Pyth, no loss of funds nor account freezing etc. In the same time, Holdstation can leverage the best part of the brokerage trading model in Web2, which is to aim at boosting trading volume and enhance the trading experience for traders with supporting tools, community and the likes.

CRYP2NOVA

2 Holdstation's Visions

In short, our visions are.

- zkSync and the likes will be the most competitive Layer 2 solutions.
- Smart wallets (ERC-4337) and mobile apps will be the norm in near future.
- Multichain support is necessary to enhance the customer experience.
- Crypto derivatives market still has a lot of room for the DEXs.
- The oracle based pricing model will last for long due to its price slippage competitiveness.
- A CEX-like perp DEX with all types of orders supported and trading services will be future.

2.1 On technology

Vitalik Buterin, the co-founder of Ethereum, has posted a new roadmap [] entitled "The Three Transitions," which lays out the development he expects to occur on the world's top smart contract platform over the next few years. The transitions identified include the layer-two (L2) scaling transition, where everyone

Archived copy · cryp2nova.com

moves to rollups, the wallet security transition, where everyone moves to smart contract wallets, and the privacy transition, where developers ensure that "privacy-preserving funds transfers are available," and that other services being developed, such as social recovery, are also privacy-preserving. According to Vitalik, firstly, without the L2 scalability transition, Ethereum fails because each transaction costs $3.75 ($82.48 if we have another bull run), and every product aiming for the mass market inevitably forgets about the chain and adopts centralized workarounds for everything. Secondly, Ethereum will fail without wallet security "because users are uncomfortable storing their funds (and non-financial assets)," noting that this would push users to hold funds on centralized exchanges, an increasingly dangerous proposition given the current regulatory landscape in the U.S. Without privacy, Ethereum fails because having all transactions available publicly for literally anyone to see is far too high a privacy sacrifice for many users, and everyone moves onto centralized solutions that at least somewhat hide your data.

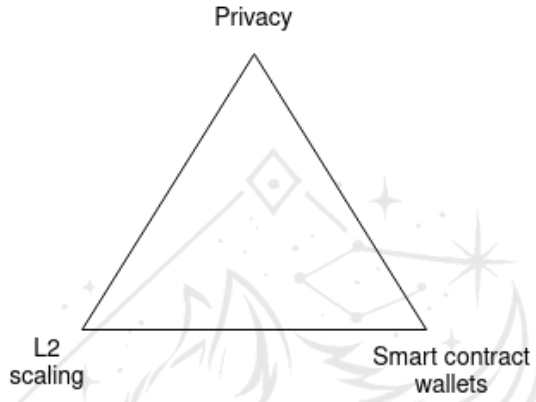


Figure 1: The ecosystem transition triangle [Vitalik Buterin]

Our visions on technology are inline with those of Vitalik Buterin. We aim at building a trading flatform that is scalable, supports smart contract wallets, and guarantees privacy for users. For these reasons, we bet on the success of smart wallets as well as zkSync technologies, a game-changing Layer 2 scaling solution. We believe the next few months zkSync and smart wallets will be part of mass adoption.

Holdstation wallet is taking a giant leap towards the future of decentralized finance with its integration of zkSync. This integration will allow for a smoother, faster, and more secure user experience while also opening up new possibilities for account abstraction and token trading.

2.1.1 Primers on ZkRollups

In this subsection, we argue why do we choose zkSync as a way to go.

Layer 2. zkSync is one of the most popular Layer 2 solutions for scaling Layer 1 blockchains such as Ethereum. Concretely, a Layer 2 network is a secondary protocol built on top of an existing blockchain (Layer 1). This additional layer aims to increase the transaction speed and cost-efficiency of the network by taking transactions off the Layer 1 and processing them separately in the Layer 2. More importantly, Layer 2 solutions also enjoy the security and consensus of the underlying blockchain. Layer 2 networks offer a way to scale blockchain networks without compromising their core principles of security, decentralization, and trustlessness. There are many Layer 2 solutions, including Side chains, States channels, Plasma and Rollups.

Rollups. Let us dive deeper into Rollups. first of all, they're called Rollups because they roll up transactions and fit them into a single batch. There is an on-chain smart contract that maintains a state root with things like the account balances and contract code inside the Rollup. A batch is a compressed collection of transactions. When a user publishes a batch with the previous state root and the new state root with processed transactions, the smart contract makes sure it all matches up. Then it will switch the old state root to the new state root. Why other Layer 2 solutions as Side chain, Plasma and State Channels try to move both the data and its computation off-chain, Rollups move state storage and computation off-chain but keep some of the data on-chain. This requires some compression tricks to improve efficiency, and while the main chain's bandwidth still limits scalability for Rollups, it still retains a favorable ratio. Next, to prevent a fraudster from submitting a post-state root that conveniently transfers the assets

Archived copy · cryp2nova.com

inside the Rollup to themselves, there are two solutions that lead to the split of Rollups into two different camps: Optimistic Rollups and zk Rollups. Optimistic Rollups allow participants to submit transactions to a Layer 2 chain without immediate verification. Instead, they rely on a fraud-proof mechanism that ensures the correctness of transactions. This mechanism assumes that most participants are honest and will not attempt to submit fraudulent transactions. If an invalid transaction is detected, a 'challenge period' allows other participants to present evidence and prove the fraud. On the other hand, zk Rollups use cryptographic proof (SNARK) that proves the post-state root is correct after it executes the batch, without needing to process each transaction in the batch individually. zkProofing also gives users greater privacy by letting them validate information without needing to share sensitive data. This approach thus significantly reduces the computational overhead and storage requirements on the mainnet while maintaining high security and privacy. In a world of privacy breaches and hacks, protecting data transmission is vital for internet protocols.

2.1.2 Primers on smart contract wallets

Why do we choose smart contracts as a way to go?

For short, smart contract wallets are a type of wallet, mainly on Ethereum, that is made possible by account abstraction (AA). This AA standard allows wallets to rely on contract accounts (CA) instead of externally-owned accounts (EOA). It offers enhanced security, usability and interoperability for Ethereum users. Instead of controlling a wallet with a private key, the user controls a smart contract holding the funds. Smart contract wallets offer recovery without seed phrases, transfer limits, account freezing and multi-signature (multisig) transactions. These features make smart contract wallets more secure, user-friendly and interoperable than regular wallets.

It is no exaggeration to say that smart wallets will become a game changer for Web3. But before seeing why it is so, let us dive deeper into the technology aspect of smart wallets.

Externally-owned accounts (EOA): an EOA is generated using an external wallet software (like MetaMask) and managed by a cryptographic pair of public and private keys. Thus account owners in EOAs are responsible for storing the seed phrase offline and protecting it against potential hacks. Meanwhile, they have to ensure that they do not lose private keys. EOA is limited to executing basic operations—like initiate an transaction (send and receive crypto currencies), and pay for gas fees for EVM execution.

Contract account (CA): CA is deployed as a smart contract and controlled by logic written in code instead of a private key.Therefore, it is programmable and can execute arbitrary logic depending on code stored at the address. However, CA cannot exist independent from EOA and cannot initiate transactions like EOA. Wallet users must maintain their EOAs with sufficient fund balance so that the underlying smart contract can execute transactions.

Account Abstraction (AA), or ERC-4337. Unlike CA which depends on EOA, AA enables creation of independent, custom smart contracts that can seamlessly initiate and execute transactions without needing EOAs. Contract accounts, when implemented, will abstract away some details about interacting with the blockchain. From a user-level perspective, "account abstraction" means certain technical details about interacting with Ethereum accounts are concealed behind higher-level interfaces. This improves wallet designs and significantly reduces the complexity of using web3 applications.

Smart wallets, viewed as a combination of contract account (on-chain wallet) and EOA (off-chain wallet) via account abstraction, offers many utilities for users, including the followings.

- Multi-signature authentication. This is similar to EOAs in which multiple parties are accountable for controlling a single account. However it is better as it simplifies the account recovery process in case any party loses account access.
- Transaction bundling. ERC-4337 allows various transactions to be bundled into a single UserOperation so that it can quickly be verified and executed on the network level. Imagine you want to use your wallet account to interact with multiple dApps. With the AA feature, you do not need to initiate separate transactions for each interaction, instead you can bundle all the transactions into single operations and get instant approval.
- Two-factor Authentication Security Model. AA allows to add an extra layer of security, which can be a code, or OTP sent to the smartphone, ensuring that the funds and users' digital assets are always safe.
- Seedless accounts & wallet recovery. AA does not require seed phrase recovery. Users can program and enable a suitable account recovery method into their smart wallet itself, e.g., two-factor authentication or social recovery.

Archived copy · cryp2nova.com

- Automated payments & operations. AA allows wallet users to schedule and complete payments automatically, exactly what happens with the traditional banking system.

Account abstraction is no doubt becoming an inevitable trend in Web3. Many new L2 chains have surfaced as viable alternatives for developers to experiment with AA. These include the following:

- zkSync was the first EVM-compatible chain to implement native AA at the protocol level. This means that all accounts are required to implement the IAccount interface, which is fully programmable and allows for various customizations.
- Similarly, the zk-rollup solution, StarkNet, has also implemented AA. Examples include Argent, which is used by 80% of StarkNet users. Visa's delegable accounts and auto-payment experiments were also done on the chain.
- Optimistic rollups such as Optimism and Coinbase's Base have also implemented forms of AA. They provide APIs for developers to create new solutions with supported features such as Social Onboarding and gasless transactions. Most recently, the Base, Safe, and Gelato teams have provided bounties at ETHDenver to encourage projects that incorporate AA in their projects.

2.2 On derivatives market

	dYdX	GMX	Gains Network	Kwenta	MUX	Level Finance	Perpetual Protocol	Holdstation
Protocol Details								
Launch	Apr 2020	Sept 2021	Apr 2021	Jul 2021	Aug 2022	Dec 2022	Dec 2020	June 2023
Model	**Order Book** powered by an off-chain matching engine	**Oracle-based** liquidity supplied by GLP holders	**Oracle-based** liquidity supplied by gDAI vault	**Oracle-based** liquidity supplied by Synthetix debt pools	**Oracle-based** liquidity supplied by MUXLP holders	**Oracle-based** powered by three low-high-risk tranches	**vAMM** with trades processed through Uniswap V3	**Oracle-based** liquidity supplied by hsUSDC vault
Blockchain	Ethereum (StarkEx), dYdX Chain*	Arbitrum, Avalanche	Arbitrum, Polygon	Optimism	Arbitrum, BNB Chain, Optimism, Avalanche, Fantom	BNB Chain, Arbitrum	Optimism	zkSync
Token	DYDX	GMX, GLP	GNS, gDAI	KWENTA	MCB, MUX, MUXLP	LGO, LVL	PERP	HOLD, hsUSDC
Key Metrics								
30D Trading Volume (US$B)	22.1	2.8	2.3	4.5	1.2	1.9	0.6	0.1
TVL (US$M)	345.4	576.0	50.3	-	60.1	25.0	18.1	1
Market Cap (US$M)	350.4	497.7	139.0	22.9	43.1	16.6	34.7	N/A
Daily Users	85	771	304	448	186	49	235	200
Daily Fees (US$K)	129.1	144.7	45.5	54.5	23.5	35.7	13.0	2.0

Figure 2: Comparative snapshot highlighting key details and metrics of perpetual futures protocols [Binance Research, data by July 31 2023]

Archived copy · cryp2nova.com

Crypto derivatives are financial instruments whose value depends on underlying assets, much like traditional derivatives. Perpetual futures and options contracts are among the most commonly traded derivatives in DeFi. Unlike dated futures where each contract has a maturity, perpetual futures or perps, for short, have no maturity or execution date. Traders can enter and exit the long/short contract at any time they want. In the long run, the profit and loss (PnL) from trades will be expected to be equal to the price return of the traded asset during the holding period, multiplied by the leverage ratio. This means that perps PnL are similar to spot trading, except a leverage coefficient applies. In practice however, that PnL excludes any effect of funding rates that either long/short position has to pay to the other. Funding rates play an important role in maintaining price stability by aligning the contract price with the spot price of the underlying asset. When there are more long volume than short volume, long side has to pay funding rates to short side and vice versa. The funding rate is proportional to the price discrepancy between the perps rate and the spot rate to incentivize traders to buy perpetual contracts when the price is low and sell when the price is high relative to the index.

Why do we choose derivatives DEX in general, and perps DEX particularly, as our core products? As a matter of fact, crypto market is dominated by derivatives. Crypto derivatives currently constitute 74.2% of the market share in trading volume. In fact, the two most widely traded crypto assets, Bitcoin and Ethereum, have a spot-to-futures volume ratio of 0.23 and 0.13 (Binance research, derivatives data from Coingecko by July 31, 2023). However, derivatives trading on DEXes is yet to take off in comparison to their centralized counterparts, with DEX-to-CEX futures trade volume at 1.4%. Why this huge difference? It is well known that CEXes had a favorable advantage due to their first-mover advantage, having productized crypto derivatives as early as 2012. More interestingly, the DEX-to-CEX spot trade volume ratio has grown from 0.23% to 16.9% in just over three years 2019-2023. Considering all facts above, we can translate them into simple words as follows. 1-Derivatives market is huge. 2-DEXs still underperform compared to CEXes but is growing faster. It's reasonable to predict significant potential for decentralized protocols to capture more of the total crypto derivatives market share.

There are many protocols that has built theirs own design for modeling perpetual contracts. The most popular models include central limit order book (dYdX), virtual automated market maker (Perpetual Protocol), or oracle-based model (led by GMX, then followed by Gains Network, Kwenta, MUX, and Level Finance, etc. just to name a few). Amongst these protocols, dYdX dominates daily trading volumes, averaging over US$1B in 2023, significantly ahead of the second-largest protocol, GMX. In fact, throughout this year, dYdX has consistently demonstrated impressive monthly volumes, even surpassing some leading CEXes like Derbit and Kraken. There are several factors for this success of dYdX. First, it is amongst first player in the league. Second, its LOB model provide institutional-grade, familiar trading experiences for individuals and traditional market makers. Third, the protocol invested heavily in incentives and has attractive fee structure.

However, Despite boasting high trading volumes, dYdX still generates less fees than GMX. The dYdX protocol realizes their disadvantages of the centralized model, they are therefore implementing a decentralized version of the LOB model, which will no doubt cause high gas fees for traders. This means that the centralized LOB model of dYdX would be almost unprofitable given their current model, both centralized and decentralized versions, and therefore we predict that dYdX will be not able to compete against the GMX V1 model. We then choose the Gains Network model, a variant of the GMX model as the way to build our own perp DEX. Similar to GMX, Gains Network utilizes a liquidity pool and relies on oracle-fed prices. It has emerged as a strong competitor in the market, with a relatively high daily trading volume at US$65.1M. We believe that oracle-based will continue to thrive in the future because of its attractive zero-slippage feature.

GMX and GNS have two most important following features.

- Transaction prices are determined by price oracles rather than relying on an arbitraging mechanism.
- No price impact (or price slippage).

In our DeFutures Exchange, the first feature will be kept, and the second one will be modified to help LPs reduce the impermanent loss.

3 Holdstation's products and technologies

- Core products: Holdstation provides a non-custodial derivatives trading flatform, including perpetual futures and options. We support copy-trading with the aim at developing a decentralized hedge fund model.

Archived copy · cryp2nova.com

- Smart contract wallets. With these, Holdstation aims at bringing user experience closer to that with digital wallet, facilitating trades, and enhance security.

- zkRollups technology. We build our dApps on zkSync Era. Following aforementioned reasoning, ZK technology allows faster transactions, account abstraction, increased scalability, and enhanced security.

- Supported chains. In fact, multiple L2 solutions causes the lack of composability and interoperability. This will require users to create multiple accounts for different blockchains, which is an unnecessary abundance. We solve this problem by supporting all layer 2 EVM blockchains so that users do not need to worry about what blockchain they are using and can therefore focus on what matters most to them: trading.

4 Holdstation's smart contract wallets

4.1 Account abstraction features

Holdstation is committed to providing a seamless and user-friendly experience for all our users. That's why we have integrated account abstraction features into our platform. This innovative technology simplifies multiple process

- Paymaster model (no gas fees paid up-front).

- Simplifies token swaps with no need for token approvals.

- Users can pay gas fees with any token, not just ETH

- Option to sponsor gas fees for other users.

- User can pay gas for other chain without bridging the token

- Ability to log in with web2 authentication methods like Twitter or Discord.

- Provides a seamless and user-friendly experience for interacting with the blockchain.

- Saves users time and money by streamlining the token swap process and reducing gas fees.

By implementing these account abstraction features, Holdstation is taking a significant step towards creating a more inclusive and accessible platform for all users.

4.2 Cross-chain wallet

Holdstation Wallet supports multiple EVM-based chains, allowing users to access a wide range of assets and services. For popular blockchains as Ethereum (ETH), Binance Smart Chain (BSC), Polygon (MATIC), Fantom (FTM), Avalanche (AVAX), Arbitrum (ARB), Optimism (OPT), we offer the lowest transaction fee rate of 0.2%. For new chains such as zkEVM, zkSync Era, Linea, Base, users can now enjoy lightning-fast transactions with a 0% transaction fees.

To create cross-chain wallet, in the near term we will follow Chainlink's Cross-Chain Interoperability Protocol (CCIP). This is a new generalized cross-chain communication protocol that provides smart contract developers with the ability to transfer data and tokens across blockchain networks in a trust-minimized manner. Currently, applications deployed across multiple blockchains suffer from the fragmentation of assets, liquidity, and users. With CCIP, developers can utilize token transfers and arbitrary messaging to enable the creation of decentralized applications that are composed of multiple different smart contracts deployed across multiple different blockchain networks that interoperate to create a single unified application. This Web3 design pattern is known as the cross-chain smart contract.

Archived copy · cryp2nova.com

4.3 Crypto on ramp, off ramp services

Holdstation utilizes the crypto on-ramps and off-ramps services. These are the processes of transferring money between crypto and fiat. On-ramping is the process of using your regular, fiat money (probably your debit card) to buy some crypto. Conversely, off-ramping is when you "cash out" of crypto, converting your coins or tokens back into fiat money, or sometimes goods and services. There are a number of different options for both on and off-ramping – these options are not symmetrical. The process of transferring money between crypto and fiat is essentially moving value between two totally separate monetary systems, with different rules and dynamics, and entry requirements1. Crypto ramps are key components in achieving Web3's true potential. An on-ramp is any platform that facilitates users to acquire crypto assets or enter their markets. On the other hand, an off-ramp is a platform that facilitates a user to dispose of crypto assets or exit their markets. Some platforms perform both of these two functions.

5 Brokerage module: HyperLiquid flatform

Beside the perp DEX, Holdstation also provides front-end software development kits (SDKs) to help traders connect to brokers or to the DeFutures Exchange (see the next section). This means that DeFutures also acts as an independent broker. These SDKs include pre-built functions and classes that allow developers to easily connect to the API or the smart contracts to retrieve data and execute trades. Thus Holdstation is only responsible for the trades between traders and DeFutures, and on-chain settlements. Holdstation is not responsible for the trades between traders and other brokers that utilize Hyperliquid flatform. Beside, Holdstation also provides built-in whitelabelling process to adhere new brokers to the Hyperliquid flatform.

With Brokerage module, brokers can create their own exchanges based on Holdstation technology. The goal of Brokerage module is to help Holdstation to gain more users from the brokers network. Brokers compete to each other by lowering fees or provide can set up their own bid-ask spread or trading fees and it is up to traders to decide who will be their counterparty. As for brokers, their goal is to build their own set of customers (traders) so that they can either trade directly with them to benefit from market making spreads, or to connect their traders to DeFutures and gain the commissions.

6 DeFutures Exchange

DeFutures Exchange is the go-to platform for trading all assets, including cryptocurrencies, forex, commodities, and indices, with up to 500x leverage. DeFutures Exchange supports EVM blockchains and integrate smart wallets.

6.1 DeFutures Exchange architecture

DeFutures Exchange has three layers to : pricing layer, position opening and position closing. To fully understand these layers, we need to understand perpetuals. Mathematically, a perpetual futures written on an underlying price process $(S_t)_0^\infty$ is an agreement between the long and the short side. There is zero cost to enter the agreement. After entering, both the long side and the short side can terminate the contract at any time t. There are two important rules to remember:

- Payoff at the termination of contract: At time t, if one of the two sides decide to terminate the contract, then the short needs to pay the long $F_t - F_0$ for each unit shorted, where $(F_t)_0^\infty$ denotes the price process of the perpetuals.
- To keep the futures price F_t close to spot price S_t, there is a mechanism called Funding Rate, where the long has to pay the short a rate that is proportional to $F_t - S_t$. This rate is revised periodically, usually 8 hours.

From an arbitrageur point of view, if $F_t >> S_t$, he will take the short position with the hope that the price will later on reverse to S_t to realize a profit. There will be two sources of profit for him: the funding rate $F_t - S_t$, and the terminal payment $F_t - F_T$ paid by the long side. Despite such economical soundness, unlike fixed-maturity futures, perpetuals are not guaranteed to converge to the spot price of their underlying asset at any time. The reason is clear: there is no hard no-arbitrage argument available for perpetuals like fixed-maturity futures.

Archived copy · cryp2nova.com

6.1.1 Pricing layer

Dynamic price feed (DPF). This is a key component in ensuring accurate pricing for all assets traded on the platform. The DPF algorithm is designed to calculate an accurate average price for all assets on the platform. This is achieved by collecting data from multiple sources, including external oracles and centralise trading data. By incorporating multiple data sources, the DPF helps to minimize the impact of incorrect oracle values or trading anomalies. This helps to ensure that the pricing data is as accurate and reliable as possible. Note that we do not use any on-chain service such as Chainlink, but rather create our own centralized price oracles.

Plexible market making. Holdstation DeFutures Flexible Market Making (FMM) model is inspired by the DoDo Proactive Market Making model. The essential idea is to use oracle price as the reference price (or mark price), and linear price slippage, i.e. price impact is proportional to the trading volume. More precisely, assume that we have a buy order of size Δx_0,

$$P_1 = P_0(1+R), R = a\frac{\Delta x}{x_0},$$

where P_0 denotes the initial mark price, given by an oracle price, and P_1 denotes the updated mark price, R denotes the price return of the transaction. R is a linear function of the relative trading size $\frac{\Delta x}{x_0}$. The constant a denotes the liquidity concentration ratio. For example, if $a = 0.1$ and the mark price is $\$100$ then the entire liquidity will be approximately concentrated in the price interval $[\$95, \$105]$ with flat density.

The slippage will be equal to

$$S = \frac{R}{2} = \frac{a\Delta x}{2x_0}.$$

The FMM model is different from the PMM model in that, it does not have an absolute inventory control by adjusting the reference price based on the reserves inventory $x - x_{initial}$. However, by allowing the slippage to be a function of the relative position size, the model can somewhat controls the relative inventory ratio, i.e. the value proportion of one token in the pool, which is good enough in practice.

6.1.2 Position opening layer

When a long/short position is created, the mark price is given by the oracle (Dynamic Price Feed). Depending on the asset class and the collateral asset value, a position size will be determined. A price slippage will be calculated based on the relative position size. Finally, the average transaction price can be calculated based on slippage and mark price.

6.1.3 Position closing layer

When a long/short position is closed, there will be two cases, either the position is liquidated or not. If there is no liquidation, then the calculation will be similar to the position closing case, except that a PnL settlement has to be calculated. If liquidation takes place, an amount of collateral will be liquidated and liquidator can request liquidation fee from the trading storage.

An exciting feature of DeFutures Exchange is to allow traders use limit, profit-taking and stop-loss orders. Regarding automated execution, whenever the taking-profit or stop-loss thresholds and market prices are met, the trading service will take a portion of the collateral asset to cover for the PnL of the trades, and send the leftover to users.

6.2 DeFutures Vaults

One of the defining feature of GMX is that, the protocol utilizes a unique multi-asset liquidity pool that deviates from the traditional models of multiple single-asset pools. This feature is no longer retained in our model.

Just like Gains Network, in Holdstation, not only crypto currencies are traded, but also **tokenized real world assets** such as currencies, and commodities (OIL and GOLD) are also traded. Each asset class (such as crypto, forex and commodities) has a different price volatility, or different risk contribution to the total portfolio. Therefore, they should be treated differently in terms of trading fees and leverage (or margin requirement or liquidation requirement). For instant, crypto assets are much volatile than forex currencies,

Archived copy · cryp2nova.com

hence forex leverage should be much larger than crypto leverage, and forex trading fees should be smaller than crypto trading fees. This is the main reason why DeFutures assets are split into three different vaults.

DeFutures Vault is a core function in our architecture, with the main functions of split the trading fees and allow traders to earn great yields on them. Additionally, Defuture Vault has the potential for future token drops.

Asset class	Open-close fee %	Leverage	Vol
Crypto	0.08	150X	75
Forex	0.008	500X	15
Commodity	0.05	250X	20

6.3 Copy trading

Holdstation's Copytrade Bot feature will allow users to easily follow and copy the trades of experienced traders on our DeFutures Exchange. By monitoring the performance of a wide range of traders on our platform, users can choose to automatically replicate the trades of top-performing traders with just a few clicks. This feature not only makes it easier for novice traders to enter the market and potentially make profitable trades, but also allows experienced traders to increase their earnings by sharing their trading strategies and insights with others.

The most interesting feature is Smart Vault Trading: Copy Trades using ERC-4337 Smart Contract Wallet.

Copy trading is just a middle step in the phase of building a decentralized hedge fund [Nam to discuss]. By combining the zkSync technology and AI, fund managers can create their own trading bots with high out-of-sample trading performance without revealing their strategies to the outside world. As trading bots can be ranked and compared, traders can allocate capital to the bots they prefer, and this open new possibilities for passive income on blockchain.

6.4 LP insurance

The most crucial question that any perpetual futures exchange has to answer is whether or not they should hedge the LPs' position. Apparently, there are two extremes.

First, no hedging at all. This sounds counter intuitive, but the fact is that most of the time traders loose and the exchange win as they take the opposite position. Therefore, no hedging will be the best solution most of the time. However, this solution is really risky if traders have private information.

Second, hedging all the time to ensure delta neutral. This solution is impossible because the cost of hedging will very quickly outweigh the gain from trading fees.

A middle way solution is to do partial hedging. There are many delta-netral hedging strategies to protect LPs in GMX with infrequent hedges but still guarantee low impermanent loss. These strategies are implemented by third parties, so it is up to LPs to choose hedging strategies for themselves. This will be the solution for the current moment for DeFutures.

In this whitepaper, we propose an LP insurance solution via selling put options in a periodic manner. This solution will be implemented in the near future. The brief idea is as follows. We create an Insurance pool so that policy sellers can mint put options and deposit collaterals for those options. Put options expire monthly, it has as many strikes as policy sellers wish to mint. An LP can send a buying request at any time to the insurance pool, and insurance pool can mint the option of interest to the LP.

So how can an option be priced? We apply the Black-Scholes model to have

$$p_t = P(K, T - t, r, \sigma).$$

The most important parameter that needs to be priced is the implied volatility. We assume σ to be constant across different strikes and maturities. If we denote U_t as the utilization ratio of options nominal, or the total option demand devided by total option supply, and g_t as the gain rate of a representative option seller, then the implied volatility can be expressed as follows

$$\sigma = e^{-Ag_t} F(U_t).$$

Where F is an increasing function. The equation means that if U increases, i.e. there is more demand of put options, then the implied vol will increase to make it more expensive and vice version. More interestingly, when $g_t > 0$, i.e. options seller gains more than looses by selling options, the exponential decay will

Archived copy · cryp2nova.com

make implied volatility cheaper, thus put options become cheaper and gain rate of option sellers will be lower.

6.5 Real Yield calculation

Crypto real yield as a metric compares a project's offered yield against its revenue. If the returns for staking are greater in real terms than the provided interest, the emissions are dilutionary. This means that their yield isn't sustainable or, in lay terms, "real." Real yield isn't necessarily better than dilutionary emissions, which are often used for marketing purposes. However, this indicator can serve as a useful tool for gauging a project's long-term yield-bearing prospects. Real yield is generated from revenue sources instead of token emissions.

As for Holdstation, users stake HOLD can receive yields in terms of USDC from the protocol revenue. Moreover, HOLD stakers benefit from allocation in launchpad projects, reducing trading fees in the protocol. They can also pay HOLD token cross-chain as fees.

7 Other products

7.1 Holdstation Club (NFT)

Our exclusive 8888 Holdstation NFT collection represents the Holdstation Social Club - an elite community of crypto enthusiasts. Users join the club to become part of an exclusive community of like-minded individuals who are passionate about trading, blockchain, and all things crypto.

Here's what you can expect as a member of the Holdstation Club:

- Unique and rare NFTs that represent your membership in the club.
- Exclusive access to events, meetups, and other activities organized by Holdstation.
- Bragging rights as part of an elite group of Holdstation enthusiasts.
- Opportunities to earn special rewards and bonuses based on your level of involvement in the club.

7.2 Holdstation Foundation

Holdstation Foundation will operate as a decentralized autonomous organization (DAO), where token holders will have the power to propose and vote on changes to the network. This includes proposing new features, changes to the network parameters, and allocation of resources for community development and ecosystem growth, and most importantly, the decision on future token drops.

The community development and ecosystem growth will be a key priority for the DAO, and resources will be allocated towards supporting initiatives and projects that benefit the network as a whole. Token holders will be able to vote on proposals to allocate resources towards community development, ecosystem growth, and other initiatives that support the DAO's mission.

In summary, the Holdstation Foundation's DAO governance mechanics will prioritize community engagement and empowerment, incentivizing active participation from delegates and allocating resources towards community development and ecosystem growth.

7.3 Holdstation Analytics

Get the latest insights, analysis, and news on the crypto market with our research hub. We provide in-depth knowledge on current trends, giving our community a strong foundation to build their investment strategies. Our **Holdstation Research** team conducts extensive research to offer users with deep analytics and high-quality contents. **Holdstation's Market News** provides up-to-date information from the market and delivers key insights for the crypto world. While **Trends and Hidden Gems** focuses on identifying early investment opportunities with high profit potential. Our experienced Research Team analyzes data provided by reputable partners to evaluate quality investment projects and make informed investment decisions.

Archived copy · cryp2nova.com

7.4 Holdstation Launchpad

Holdstation launchpad is an upcoming platform aiming to become a central launchpad within the zk Ecosystem. Focused on supporting early-stage projects within the zero-knowledge space, Holdstation offers a range of services to facilitate successful project launches. Our Launchpad aims to help promising projects gain traction and funding from a community of dedicated investors.

8 Holdstation tokenomics

This section aims to explain the functionalities of Holdstation tokens, revenue structures, token allocation and incentive programs introduced by the Holdstation protocol.

8.1 Utility & Governance tokens

Holdstation has two tokens.

- Native token: HOLD: This serves as the backbone of the Holdstation protocol, offering core functions such as fee payments, protocol governance, incentivization (in-apps benefits), protocol insurance. The token holders are incentivized to hold a minimum balance to maximize their future earnings under the protocol. Holding more HOLD will increase the chances of receiving future token rewards.

- Utility token: uGold. An exchange token that facilitates the conversion of GOLD Reward Points to uGOLD, which can then be used to trade and transact on the platform or to pay fees.

HOLD token distribution follows a fixed supply, decaying emission model as a general principle. This means that as time passes, the token emission decreases according to a fixed schedule. This distribution model is designed to reward users who stake or hold tokens for longer periods.

uGOLD tokens are mintable and can only be minted through a redeemable process using onchain GOLD Reward Points.

8.2 Revenue structure

The Holdstation protocol collects fees from various economic activities within the Holdstation ecosystem. The collected fees contribute to the Holdstation DAO treasury which get then redistributed to stakeholders. The revenue sources include:

- Trading fees.

- Swap fees.

- Lending and funding rates.

- Staking rewards from collateral assets.

- Brokers' fees.

- Liquidation penalty.

8.3 Referral program

Holdstation offers a rewarding referral program that allows you to earn both GOLD and USDC. Users just need to refer their friends to join the Holdstation platform. The more a user's friends trade, the more she earns. The referral program is multi-levels.

As an affiliate agency, user can earn up to 40% in USDC rebase for every direct referral she brings in. The best part is that, user can earn rewards from her referrals' referrals too! With our three-tier referral system, users can earn more when their friends refer more friends.

Archived copy · cryp2nova.com

8.4 Early adopter program

Holdstation's Early Adoption Program is designed to incentivize early adopters, traders, and affiliate agencies to build and grow with us. The program will run for a duration of 3 to 6 months, during which we aim to achieve the highest possible user growth.Early adopters stand to gain significant benefits, as they will be rewarded for their support in the early stages of our ecosystem's growth. By participating in this program, users can help to establish a strong foundation for future growth and development of Holdstation.

9 Roadmap

Q3 & Q4-2022

- Launch Holdstation Research: Insightful crypto news hub.
- Introduce Holdstation Wallet: User-friendly self-custodial wallet.
- Design Holdstation DeFutures architecture.

Q1 & Q2-2023

- Launch Holdstation DeFutures: On-chain future trading on zkSync.
- Holdstation DeFutures In-Apps Trading.
- 3 Tiers Referral Programs: Earn rewards in rebase USDC.
- Expand Asset Classes: Forex & Commodities trading (XAU / OIL / EURUSD,...)
- Monitoring System: Real-time cash flow monitoring & discrepancy alert.
- Reduce Gas Costs: Smart contract optimization.

Q3 - 2023

- ERC-4337 Development: Sponsor gas fees for users.
- Gas Payment by Other Tokens: USDC, USDT gas payments.
- Multi Layer 2 Integration: Linea, Base, Mantle.
- Major UI/UX Update: Revamp for enhanced user experience.
- Cross-chain Swap Integration: Easy token swaps and bridging across chain.
- Smart Contract Wallet & Seedless Recovery
- MPC Integration: Advanced privacy & security.

Q4 - 2023

- Brokerage Trading Module: Built-in Front-end SDKs and Whitelabeling empower anyone to craft exchanges with a certain discount on volume trade & assets class
- Smart Vault Trading: Copy Trades with Fortified Security using ERC-4337 Smart Contract Wallet
- Holdstation Club NFTs: an NFTs that blend fun with real-world utility.
- Holdstation Launchpad: A Gateway to Early Access and Creative Projects.

Archived copy · cryp2nova.com

10 Team

Our team is composed of experienced professionals from diverse backgrounds who share a passion for innovation and creating value for our users.

Hoai Nam, CEO, Founder. Founder Partner of Binance in P2P trading, KOL in the crypto world in Vietnam, with 7 years of experience in developing crypto community in Vietnam, Founder of UB Holding community and former admin at Tradecoin Vietnam since 2017. Nam believes that the future of crypto is self-custodial and Holdstation provides an easy and convenient futures trading platform to help popularize Blockchain to everyone.

Trung Banh, PM. "A cool and dynamic product manager who co-founded Film Viet Tai Uc & VeOnline Ticketing System. With an insatiable curiosity for all things tech, Trung took on the role of Project Manager, crafting the cutting-edge stock & commodities trading platform, EQUIX, for Australian, Vietnam & US markets. Trung works along with tech Team at Rabobank & ING before he triumphantly returned to build Holdstation DeFuture Wallets, driven by a firm belief in permissionless blockchain on trading & self-custodial world."

Thanh Nguyen, CTO. "With 4 years in fintech as a Senior Engineer at Techcom Securities, and 5 years as a Co-Founder in mobile game development, I'm starting Holdstation Wallet, a blockchain project combines two these domains. The blend of finance and gaming has the potential to reshape our interaction in fintech. Through Holdstation Wallet, I aim to create an intuitive and enjoyable financial experience, introducing an innovative framework for everyone".

Tuan Nguyen, COO. "15 years of experience in IT. Former Director of ViettelPay, Founder of FinX (P2P lending platform). In my point of view, Blockchain will be increasingly improved in the field of technology and applied more deeply in a variety of fields and industries. So, I worked with my team to created Holdstation DeFutures Wallet, the first wallet support on-chain trading. My very first leg of decentralized journey."

Hieu Do, Head of Parnership. Formerly a Relationship Manager at Asia Commercial Bank, kindled his collaboration fervor through interactions with clients and organizations. Advancing to positions at Pioneer Group and Vinfast, he refined partnership navigation and deal-crafting ability. Acknowledging decentralized finance and crypto's potential, Hieu took on the role of Business Development Manager at Holdstation, leading the charge in driving DEX platform growth and adoption.

References

[1] https://vitalik.ca/general/2023/06/09/three_transitions.html

[2] https://vitalik.ca/general/2021/01/26/snarks.html

[3] https://vitalik.ca/general/2023/06/20/deeperdive.html

[4] https://research.binance.com/static/pdf/navigating-defi-derivatives-.pdf

[5] https://research.binance.com/static/pdf/a-primer-on-account-abstraction.pdf

Archived copy · cryp2nova.com