The Hybrid Exchange Model

December 5th 2024
Aries.com

Based on the work of Philipp Zimmerer, Reda Falih, and team.

Abstract

The financial landscape is currently defined by fragmentation.

Investors and consumers must navigate a maze of apps: one for brokerage accounts managing stocks and options, another for banking, and yet another for crypto assets. The ultimate aspiration is a global unified, full-service financial platform.

Years of regulatory warfare, particularly the government's assault on crypto, have hindered progress toward this vision. However, as of this writing in December of 2024, there are clear signs of a cessation of government hostilities. A new era of peace and prosperity is around the corner

This brings us to an essential question: what seeds are necessary plants for the future? Our North Star is the creation of an integrated ecosystem where individuals can seamlessly manage all financial assets on a single platform.

We begin with three foundational principles:

Openness: The platform must be open and inclusive. No single entity, regardless of its size or resources, can fully meet the demands of a global market. By prioritizing APIs, widgets, toolkits, and diverse data sources, the platform should function more like a software language—akin to UNIX—rather than a proprietary application.

Collaboration Over Competition: The outdated dichotomy between centralized and decentralized exchanges must be resolved. By synthesizing the strengths of both models, we can forge a revolutionary hybrid exchange that transcends the limitations of either approach. This harmony will lay the groundwork for sustainable innovation and enhanced user trust.

User-Centric Design: Simplifying financial management for users remains paramount. The platform should emphasize open source intuitive design, seamless functionality, and a user-first philosophy. By ensuring accessibility for everyone—from seasoned investors to newcomers—we can build a system that empowers rather than overwhelms.

This vision is not merely an ambition—it is a blueprint for the future of financial innovation.

We are well on our way to building the first piece - an open brokerage platform. Last month, we launched Aries.com. We unveiled a complete developer toolkit, called Aries Engine, to allow people to build on our platform. We also launched Aries Infinite, an open source infinite canvas environment that allows people to design their own custom trading interface. We go to market with both products in Q1 of next year.

This paper outlines a novel strategy for solving the traditional problems of centralized/decentralized exchanges and how we can integrate that solution into our FINRA/SIPC open brokerage platform.

Introduction

Ever since the Mt. Gox incident, a pattern has repeated like clockwork. While digital asset exchanges have proven to be the most robust and profitable business use case in crypto, the dominance of exchanges has fluctuated considerably.

Hundreds of exchanges have been founded over the years, most of them failing to overcome the liquidity “chicken and egg” problem any exchange faces: Traders are attracted by the liquidity they are supposed to bring - but which one comes first?

Many of those that did manage to attract significant liquidity have later fallen off, either by becoming complacent rent-seekers and being overtaken by innovators (Poloniex, Bittrex) or by falling victim to controversy or straight up implosions like FTX.

Aries is designed to overcome the liquidity problem via three unique pillars that are based on technological, architectural, and economic innovation respectively.
It will retain liquidity by being and remaining the most advanced, secure, transparent, and user friendly digital asset exchange on the market.

Due to the recent events surrounding many centralised exchanges, the time is ripe for a novel approach to digital asset exchanges.

Aries does not enter the debate surrounding transparency, custody, and proof of reserves. Instead, we avoid this debate entirely by committing to a Hybrid Architecture that ensures full transparency by design.

Aries keeps all funds and proofs on chain, with traceable ownership and history, while delivering a best-in-class user experience through the utilization of an off-chain matching engine and user experience in line with Tier 1 centralised exchanges.

Hybrid Architecture

Hybrid Architecture means on-chain security and transparency and off-chain user experience, execution, and APIs. Aries users will feel right at home if they have used Binance, Coinbase, or FTX before, thanks to an off-chain matching engine and all other UX advantages of centralised exchanges.

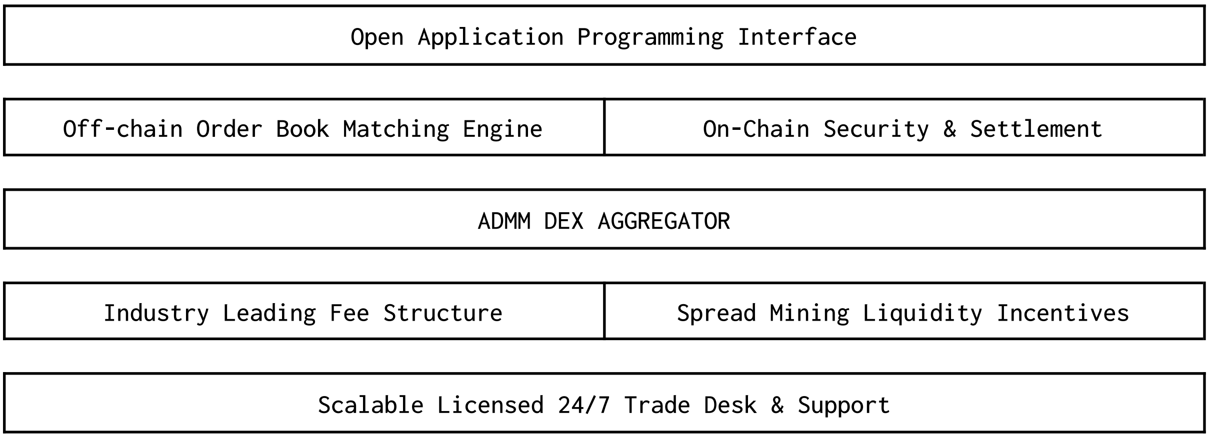


Figure 1: *Aries Hybrid Architecture*

We believe that Aries's hybrid architecture is a necessary evolution in the realm of trading platforms. FTX's fate is just another repeated cycle of a rising and falling exchange. Aries is built to mirror the rise by creating an environment that attracts liquidity immediately, but to withstand the fall due to an architecture that turns ethics and transparency from a mere promise into an immutable fact.

The lack of transparency, or rather the abundance of complete opacity, is an unfortunate compromise everyone accepts when using a centralised exchange. No-one should be forced to make this compromise.

Aries will implement a Proof of Reserves (PoR) mechanism, as proposed by Ethereum founder Vitalik Buterin, which relies on blockchain technology to create transparency regarding an exchange's reserves, assuring users that the assets they deposited indeed exist and are not being misrepresented.

This mechanism revolves around two key technologies: Merkle Trees and zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge).

Incentivize Relevant Liquidity: Spread Mining

Token-based liquidity incentives are not a new invention. In fact, the concept has already gone through multiple iterations, improving every time. Let’s review:

Volume Mining

Fcoin/BitMAX style “volume mining”, where users were rewarded in tokens for trading, based on the fees they generated for the exchange. In a way, it was treated like a veiled token sale; participants would wash trade to mine tokens in exchange for trading fees. The exchange fees were then (partially) routed to the tokens being staked, effectively closing the loop minus any fees that were going to the exchange itself.

To summarise, volume mining uses token incentives to onboard trading volume, however the volume is not genuine as it relies largely on wash trading.

Ultimately these concepts have faltered because they are negative sum games - once external factors such as retail hype begins to waver, there is no system in place to prevent a downward spiral in token value and trading volume, as these two factors go hand in hand with wash trading. And although we have seen these concepts reappear (e.g LOOKS), they have all ultimately proven the model to be unsustainable over time.

Governance Incentivisation

Then came Curve, using its governance token veCRV to direct incentives to liquidity pools, thus ensuring liquidity by paying depositors in these pools via newly issued CRV tokens. This system has proven relatively sustainable so far. Projects secure veCRV emissions by purchasing and locking CRV directly, via proxies like Convex, or via what is colloquially called “bribes” (in reality, incentives) to veCRV or vlCVX holders. This process allows them to periodically ensure liquidity for their token of choice on the Curve exchange.

Despite the undeniable success of the Curve model, there are still some inefficiencies present:

A lot of incentivised liquidity is mostly useless because it's in pairs that barely get traded, causing utilization to be very low. Economically, this means that capital is only incentivised by CRV inflation without actually being productive and generating real value. This is unsustainable in the long term, as liquidity providers are getting paid by inflation without their liquidity generating meaningful trading fees for Curve.

Liquidity Mining

Adjacent to Curve, there are various AMM based DEXes like Sushiswap that use or have used a practice called “liquidity mining” to incentivise liquidity:

Liquidity Mining incentives give out reward tokens to incentivise liquidity, but it's again mostly dead liquidity because Uniswap-Style AMMs favour remaining liquid over tight spreads. As a result, liquidity mining incentivises liquidity that barely gets used on one hand, because most of it sits far from the spread (to ensure the AMM stays liquid), and very vulnerable to impermanent loss on the other hand, because price changes immediately affect the value of your shares in the pool. This results in attracting mostly mercenary capital that expects to be paid very well for their liquidity to offset their potential impermanent loss.

All these three concepts face their own design problems, but at the same time, they are (or were) successful in their own way, creating billions in value each while paving the way for future iterations and improvements.

Spread Mining

Aries’s Spread Mining iterates on liquidity incentivisation by taking the best of the aforementioned approaches while resolving all inefficiencies.

In spread mining, rewards for liquidity providers get paid out when the order is actually taken, based on:

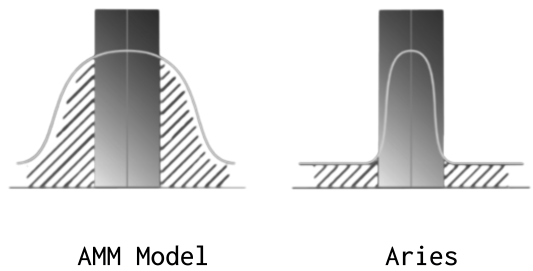
- Share of relevant liquidity
- Time in the OB within 2% of mid price (1% for major coins, 0.05% for stables)
- Proximity to spot price

Aligning Incentives for healthy order books

	Factors that influence rewards
Bob places an order 0.1% away from Spread	Proximity to spread
Bob’s order is for 0.1 BTC	Size of Order
Bob’s order is live for 4 seconds	Length of Order

Bob’s trading PNL is supplemented by rewards from his activity.

We provide incentives only in relevant zones.



Dynamic Targeted Incentives ensure depth where it matters.

Figure 2: *Using Spread Mining To Incentivize Relevant Liquidity*

Aries rewards your relative share of liquidity for the relative amount of time it was within a certain percentage of spread before the order was taken.

Aries only incentivises liquidity where it matters. None of the liquidity incentivised is dead, because it is a) close to spread, and b) needs to be taken to be eligible for rewards.

Wash trading is eliminated via a time factor in rewards calculation.

Spoofing is useless because orders need to be taken to be rewarded.

When you incentivise liquidity using Aries, all orders need to be matched with a taker to generate revenue in the form of trading fees for the exchange. Every incentive payout is revenue-generating for Aries, by design.

With Aries's market-making rewards, anyone can become a market maker and earn profits, even those who cannot extract direct value from market-making. This incentivises traders to participate in market-making and increases profitability through ARS rewards.

Attribute	Spread Mining	Volume Mining	Governance Inventivization	Liquidity Mining
Trade Execution Required for Payout	+	+		
Maintains Tight Spread	+			
Wash Trading Protected	+		+	+
Impermanent Loss Protection	+	+		
Capital Efficiency	+			

Figure 3: *Comparison Against Traditional Mining Mechanisms*

Aries Grid Pool (AGP) Liquidity Providers

Where previous concepts can be considered negative sum games as described above, Spread Mining is a highly interactive positive sum game encouraging active, intraday liquidity provisioning. Spread Mining is designed to evolve into a meta-game attracting professional market makers and (self-selected) higher skill traders. While the emission of ARS tokens to all participants introduces a positive sum element that allows bad trades to turn profitable in sum, the active, high-frequency nature of Spread Mining will turn off some participants.

To allow for more easy access to Spread Mining incentives, Aries will be offering Grid Pools to users who prefer passive liquidity provisioning. AGPs operate similarly to traditional liquidity mining schemes, with users providing one of the two paired assets as liquidity, which will be employed by a Grid Spot Trading Algorithm to provide liquidity within relevance criteria to participate in Spread Mining rewards.

Users are fully exposed to profits, drawdowns, maker rebates, and Spread Mining incentives generated by the AGP, net a 10% performance fee. AGPs will receive additional esARS incentives early on to encourage users to become familiar with the product.

AGP introduces a simple and familiar-feeling product to become a liquidity provider on Aries while ensuring activity on all Spread Mining incentivised trading pairs.

ARS Token

The ARS token is the native utility token of the Aries exchange.A limit of 100,000,000 ARS ERC-20 will be issued on the Ethereum network. The pool of tokens will never increase.

Repurchase & Burn Protocol

Each quarter, 50% of our profits will be allocated to repurchasing and burning ARS tokens. This process will continue until half of the total ARS supply (50,000,000 tokens) has been repurchased. All buy-back activities will be publicly disclosed and fully verifiable.

Utility

1. Exchange Fee Discounts: ARS can be used to pay for all Aries exchanges fees including but not limited to: Trading Fees, Withdraw Fees, Listing fees, and margin fees. Holding ARS tokens grants discounts on trading fees within the Aries platform. The discount increases with the amount of ARS held, reaching a maximum of 50% for those holding ARS tokens worth more than what is equivalent to $3 million USD.

When ARS is used to pay for fees, the fees will be discounted early on to spike ARS adoption:

	Year 1	Year 2	Year 3	Year 4	Year 5
Discount Rate	50%	25%	12.5%	6.75%	0%

Figure 4: *ARS Exchange Fee Discount Rate Over Time*

2. Spread Mining Prioritization: Order book priority, which is especially important for large traders who keep our books tight, will be scaled based on the traders ARS holdings with higher book priority given to larger ARS holders.

3. Collateral: Aries may allow for ARS to be used as collateral against leveraged positions. This will come only after market stability, and will be scaled based on NET ARS DAILY TOTAL VOLUME.

Allocation

Label	Amount	Percentage
Aries Financial Inc.	50,000,000 ARS	50%
Airdrop Beta Users	40,000,000 ARS	40%
Angel Investors	10,000,000 ARS	10%

Vesting: Initially 20% of Aries Financial Inc. tokens will vest, followed by 20% per year for four years.

Figure 5: *ARS Token Allocations & Vesting*

Velocity Implications of Different Utilities

Liquidity Utilization

For projects: Projects and DAOs with their own native token or stablecoin, especially those that own their own liquidity, can incentivise utilization of liquidity by directing spread mining rewards to their token. They are incentivised to lock large portions of ARS for extended periods to ensure constant liquidity for their markets.

What differentiates vlARS to veCRV is that vlARS spread mining rewards will never incentivise dead liquidity, because spread mining incentives only pay out as orders get taken. Therefore, if CRV emissions are a strategy employed by projects to incentivise liquidity of their token, then ARS spread mining rewards are the strategy to incentivise liquidity utilization of their token.

For market makers: vlARS allows projects to incentivise professional liquidity providers to prioritise their pairs via ARS incentives. Liquidity gained this way is entirely productive liquidity due to the spread mining mechanics.

For users: Locks represent a temporary removal of ARS from circulation. From a game theory perspective, if the sentiment is a future increase of fundamental performance of Aries, every staker should become a locker to ensure their relative fee shares keep up via boosted Multiplier Point accumulation.

Velocity Implications

General utility is key to ensuring a reason to hold some tokens is always present. Specifically, trading fee discounts invite every platform user to hold ARS, because doing so will make any trade slightly more efficient. Building from there, any other features implemented in the platform will be tied to ARS, making it the tokenised centrepiece of the Aries platform.

Flywheel

A primer on flywheels: Flywheels are reflexive by nature. This means that the process outlined in the graphic above can reverse at some point and lead to collapse, unless the underlying business can develop a robustness to reflexivity. As described earlier, see volume mining exchanges. See Olympus DAO/OHM and its forks. See LUNA. Fragility to reflexivity killed them.

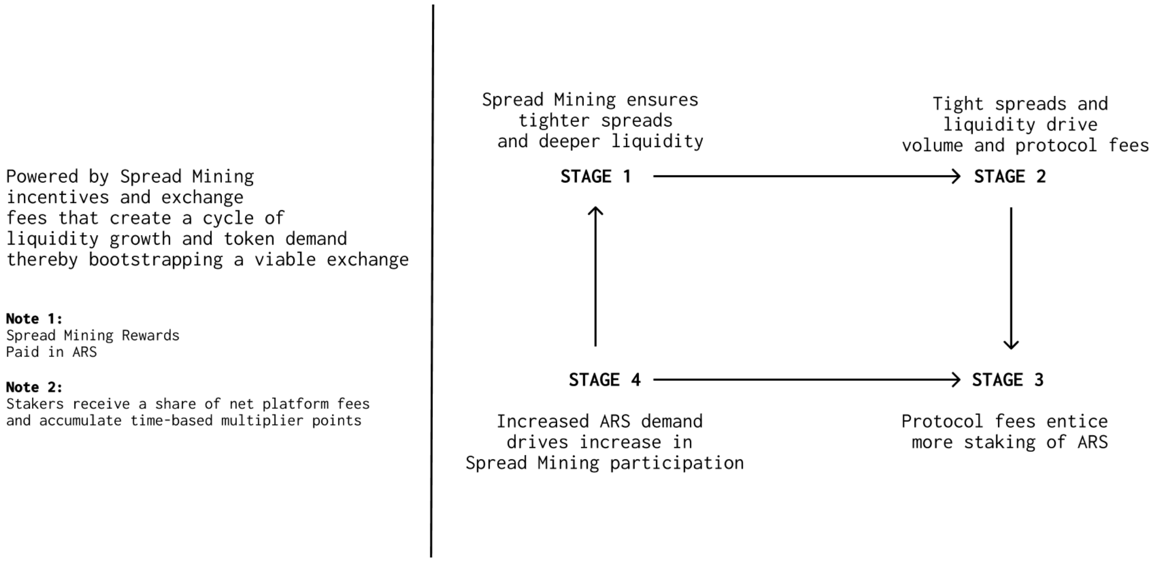


Figure 6: *Spread Mining <> Exchange Liquidity Flywheel*

Aries's flywheel, unlike these other examples, has a clear purpose that allows it to develop robustness by bootstrapping an intrinsically viable business. In the graphic depiction, between Stage 4 and Stage 1, an increase in ARS demand "drives an increase in Spread Mining participation". This means that competition for the now more valuable token pool released to spread miners increases. Unlike traditional liquidity mining, Spread Mining is not based on an AMM pool that scales linearly with liquidity, but actually a concept that allows for competition between participants.

Increased competition for increased reward value means competing for maintaining more liquidity (a core driver of the organic viability of Aries) within the spread bounds of eligibility for Spread Mining incentives.

In clear terms: The Spread Mining Flywheel promotes an increase in relevant liquidity (defined as liquidity that is maintained close to spread and relevant for immediate trade execution) every time it turns.

Exchanges attract (retail) users primarily via the ample availability of relevant liquidity. This means that the Aries flywheel scales liquidity and attracts users, which eventually becomes a self-powering virtuous cycle.

New users will go where the liquidity already is, because they want to trade on a liquid exchange, bringing their own liquidity with them. Once organic trading from retail users occurs, professional liquidity providers can monetize even without the flywheel.

The flywheel is a tool to bootstrap liquidity and organic volume, solving the chicken and egg problem all exchanges face. As it turns, it becomes increasingly robust to reflexivity, instead of increasingly fragile like the aforementioned examples.

An important effect of building up robustness via an underlying use case (ensuring tight spreads and relevant liquidity) is that users are onboarded outside of the flywheel. Eventually, traders will start using Aries because of the liquidity the flywheel bootstraps, not to profit off the flywheel directly. These traders generate fees that are paid out to stakers in Step 2, so they help keep the momentum going without actually participating in the profit share.

In summary: The Aries flywheel attracts organic, long-term customers to a liquid exchange.

Aries Ecosystem Integration

The Aries ecosystem is designed as a cohesive environment where every component seamlessly interconnects to deliver a unified financial experience. Integration with the ecosystem ensures that users benefit from a holistic platform that combines multi asset class brokerage and crypto asset management.

The integration of crypto functionality into the Aries ecosystem represents the next evolution of financial management. By leveraging the security and reliability of our FINRA/SIPC-compliant platform, we aim to address the longstanding challenges of centralized and decentralized exchanges while enhancing user trust and operational efficiency.

Through these interconnected components, the Aries ecosystem empowers users to manage all their financial assets seamlessly, paving the way for a truly integrated and innovative financial future.

Aries Mobile: Open source mobile trading app that provides users with unmatched speed, simplicity, and the ability to trade across devices with synchronized charting.

Aries Infinite: Open source professional trading software to offer an infinite canvas interface, allowing users to design their own custom trading environment with limitless possibilities.

Aries Engine: A comprehensive suite of APIs, tools, and foundational elements that provides developers all the possible necessary components to build a wide range of fintech applications.

Licenses & Regulation

Aries Financial Inc. “Aries” is a Delaware corporation. Through its subsidiaries it holds multiple licenses: (1) Ram Financial LLC, a wholly owned Aries subsidiary, is a FINRA/SIPC member broker dealer; (2) Aries Futures LLC, a wholly owned Aries subsidiary, is a CFTC & NFA registered Introducing Independent Broker; (3) Aries Crypto LLC, a wholly owned Aries subsidiary, will be the sole owner of all Aries Exchange related licenses.

END