MERCURY

SINGLE-SIDED STABLE SWAP FOR DEFI 2.0

Version 2.0

EXECUTIVE SUMMARY

MERCURY is an optimized liability-centric single-sided DeFi 2.0 protocol designed to serve as a capital-efficient Automated Market Maker for stablecoins on the Aptos blockchain. Unlike DeFi 1.0 decentralized exchanges, MERCURY introduces several new dynamics to the Stable AMM technology to reduce impermanent loss risks to a bare minimum, thus increasing capital efficiency.

VISION

Despite the uniqueness and vibrancy of Aptos Blockchain, the ecosystem lacks a reliable, Stable Swap with the necessary features to serve the future of finance. Exchanges in the current Aptos ecosystem are susceptible to various weaknesses that hinder the delivery of excellent user experiences. For example, businesses that leverage automated market-making are prone to liquidity fragmentation due to a closed liquidity pool structure. DeFi 1.0 exchange models are susceptible to slippages, capital inefficiency, and lower scalability due to the invariant curve mechanism and deficiency of multi-assets integration. MERCURY intends to address the deficits of the Aptos ecosystem by designing a StableSwap with deep liquidity, including lower slippage, higher scalability, and better user experience. These features will mitigate top challenges in the crypto industry, creating a pathway to the transformation of DeFi 2.0. Successful deployment of MERCURY StableSwap will cater to the long-term progression of growth in the Aptos ecosystem as a more compelling and capital-efficient decentralized exchange for stablecoins than its competitors.

CONTENTS

LIMITATIONS OF DEFI 1.0
STABLESWAP PROTOCOLS

Even though DeFi 1.0 StableSwap protocols have significantly impacted the crypto industry, the technology has flaws that have limited various functions and conveniences. For instance, these protocols are vulnerable to high slippage and poor user experience, hindering efficiency and scalability. This section discusses some of the top DeFi 1.0 protocol weaknesses and elaborates how MERCURY addresses these issues from both the user and liquidity providers' standpoint.

A) IMPERMANENT LOSS

Decentralized exchanges that use automated market maker models rely on liquidity providers to provide market liquidity. While this model has been effective for a long time, it subjects liquidity providers to the risk of impermanent loss. Impermanent loss is when a user injects liquidity into a liquidity pool, and the price of the acquired assets changes negatively. This result in users getting a reduced value at the withdrawal time compared to when they deposited. In StableSwap protocols, the impermanent loss can result in liquidity providers getting their assets back as a combination of crypto assets different from what they initially provided. Even though stablecoins are designed to remain resistant to value shifts, they are vulnerable to impermanent loss, especially when a coin loses its peg. MERCURY is carefully designed to eliminate/ shield liquidity providers from impermanent loss problems.

B) LIQUIDITY FRAGMENTATION

Most automated market maker protocols have a closed liquidity pool structure. Closed liquidity is a model where liquidity is not shared between separate pools. One of the repercussions of fragmented liquidity is susceptibility to high price slippages. Another common practice in most exchanges is locking a portion of capital in smart contracts leading to capital inefficiencies, where the locked capital is not fully maximized. Capital inefficiencies challenge is most evident in how exchanges handle liquidity in closed pools. For example, USDT liquidity in Curve is spread in five fragmented pools, making the capital requirement for USDT five times higher than what is required. The same scenario replicates Uniswap, over 100 fragmented pools containing USDT. MERCURY does not use a closed liquidity pool model, and the tokenomics are also designed to address the issue of capital inefficiencies.

C) LIMITED SCALABILITY

Most Aptos blockchain exchanges only accept liquidity providers capable of offering liquidity in the form of pairs. In other terms, for users to be liquidity providers, they must have two equal tokens. Some exchanges, such as Curve, have tried to address this challenge by allowing single-sided deposits. However, these exchanges only allow liquidity up to the least productive token in the pool, making unpopular tokens a barrier to the collection's growth. Besides, in these exchanges, adding new tokens to existing pools is impossible, particularly if the new tokens' liquidity does not match existing tokens. This is a significant setback to the scalability of a protocol. MERCURY allows unconditional single-sided liquidity provision. This means users can become liquidity providers even if they only have one token.

D) POOR USER EXPERIENCE

User experience is a fundamental aspect of a crypto platform. Regardless, most Aptos ecosystems exchange struggles to offer users a seamless experience. One reason exchanges cannot provide a satisfactory user experience is the practice of composability. Composability mandates users to navigate protocols to access some features, which complicates the protocols' usability, making it difficult for inexperienced users. Composability is also a security threat; it increases the attack surface for hackers since users' assets are spread across different protocols.

MERCURY addresses all the challenges above by providing a user-friendly, StableSwap by employing a simple user interface that appeals to many users, impermanent loss problems, and offers maximum capital efficiency.

MERCURY – AN OPTIMAL SOLUTION
TO ALL STABLECOIN AMM PROBLEMS

MERCURY is an ultramodern StableSwap exchange protocol based on the Aptos blockchain that transforms the DeFi sector by mitigating the most pertinent issues ailing DeFi 1.0. The protocol leverages a mix of cutting-edge technologies and innovative techniques in the crypto industry to create a trading ecosystem with an unmatched user experience. Some of the defining features of the MERCURY include

A) LOWER SLIPPAGE

MERCURY features various mechanisms designed to address asset price slippages. One of these mechanisms is the single-sided open liquidity pools that encourage higher capital efficiency and, thus, lower slippage.

B) HIGHER SCALABILITY

MERCURY is built with scalability at its core giving liquidity providers the flexibility of adding and removing tokens from the main pool. This flexibility allows pools to scale naturally based on organic demand and supply.

C) ENHANCED USER EXPERIENCE

MERCURY interface accommodates a wide range of users, including novices learning about DeFi. The platform will also feature simple procedures. For example, users can deposit and withdraw tokens with just a few clicks. The platform will also have a support feature where users can seek help and have their inquiries addressed.

MERCURY
VS DEFI 1.0 STABLESWAPS

MERCURY is quite different from typical exchanges in the Aptos ecosystem, assuming a unique design and employing novel technologies with a different mindset from DeFi 1.0 exchanges in the crypto economy. This section discusses some significant differences between MERCURY StableSwap and existing Stable Automated Market Makers.

A) SHARED LIQUIDITY

As mentioned in the previous paragraphs, decentralized exchanges in DeFi 1.0 are designed to use closed liquidity pools. Such a model creates fragmented liquidity since liquidity is not shared between separate pools. For example, in Fig 1, when a user exchanges USDT for DAI, the slippage is determined using the invariant Curve between the liquidity in the USDT-DAI pool. In this case, assuming A=100, the slippage is 0.05 percent.

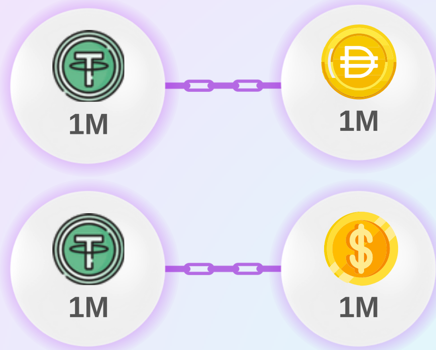


Fig 1: *Liquidity in separated pools is not shared; hence higher slippage*

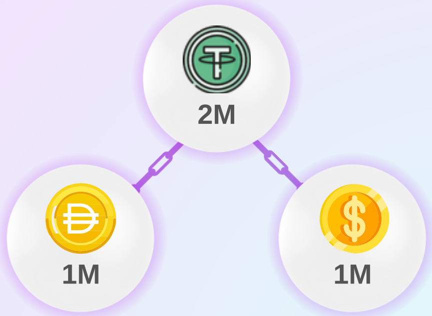


Fig 2: *Liquidity between tokens is shared hence reduced slippage.*

MERCURY protocol addresses this issue by sharing liquidity across all pools. Fig 2 demonstrates how liquidity is shared across pools in the MERCURY protocol. From the illustration, USDT's liquidity between the two closed pools is now shared. Consequently, the slippage is just 0.01 percent.

A) FLEXIBLE POOL COMPOSITION

In current decentralized exchanges, the invariant's equilibrium state is predefined when all tokens in a pool have the same liquidity. When the organic supply of one token is diminished, the entire pool's liquidity equilibrium is adversely impacted. As a result, it is impossible to introduce new assets in DeFi 1.0 Stable Swaps, as seen in Fig 3

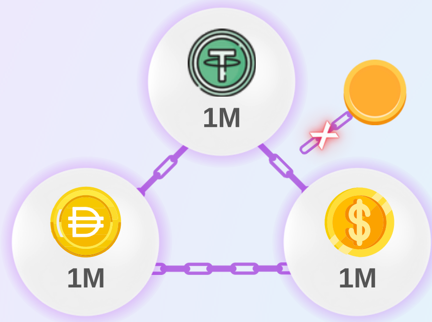


Fig 3: *It is almost impossible to add new tokens to a pool in traditional DEx.*

For example, Curve has a complex pool composition that involves pairing up the 3CRV LP token with the new token. MERCURY makes it easier to introduce new tokens in a liquidity pool. The protocol's equilibrium state is determined by the same coverage ratio instead of the same liquidity. This model enables pool assets to scale naturally by their organic supply and demand.

C) SINGLE-SIDED TOKEN

One of the distinct features of the MERCURY is allowing users to deposit and withdraw the same type of tokens without worrying about the size, composition, and difference between their tokens and LP tokens. This quality makes the liquidity provision process much more convenient. Also, the convenience allows more users to become liquidity providers since LP must not provide liquidity in pairs, thus categorizing the entire exchange as an open liquidity pool, as seen in Fig 4 below.

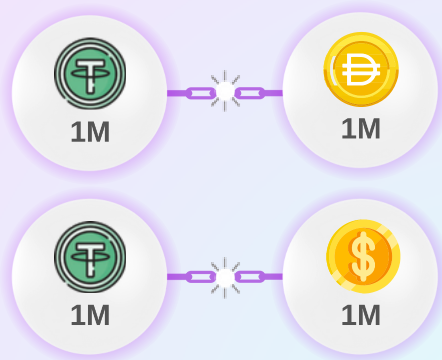


Fig 4: *MERCURY supports single-sided tokens. Paired LP token is not necessary.*

DEFI 2.0: ASSET-CENTRIC vs.
LIABILITY-CENTRIC SYSTEM

In DeFi 1.0 StableSwap platforms, liquidity providers are awarded LP tokens when they deposit to represent their partial ownership of the pool (Asset centric). Such token models do not specify the exact type of tokens awarded. Pools are composed of multiple assets, and if the token ratios are altered, the liquidity provider's asset amounts may change at withdrawal. Consider the example below.

System State (Before Mary's action)

ASSET	LIABILITY
Token A: 100	Peter: 100

System State (After Mary's action)

ASSET	LIABILITY
Token A: 200 Token B: 300	Peter: 100 Mary: 400

Table 1*: Asset-centric system design*

Fig 5: *A protocol built on the DeFi 1.0 asset-centric Model*

In Table 1, Peter owns 100 units of token A before Mary's action. After Mary deposits 100 units of Token A and 300 units of Token B into the pool, Peter owns 40 units of token A and 60 units of token B, totaling 100 units.

MERCURY introduces a new dimension to the Automated Market Maker concept called Liability (Liability Centric - Asset Liability Management). Liability is a new concept not available in existing StableSwaps that handles the deposit ratio differently. Liquidity provider deposits are converted into LP tokens, but MERCURY specifies the exact number of tokens and precise token type deposited. This information ensures that liquidity providers receive the same token type and amount at the withdrawal time. See the illustration below.

Before Mary's action:

System State (Token A)

ASSET	LIABILITY
Token A: 100	Peter: 100

System State (Token B)

ASSET	LIABILITY

After Mary's action:

System State (Token A)

ASSET	LIABILITY
Token A: 200	Peter: 100 Mary: 100

System State (Token B)

ASSET	LIABILITY
Token B: 300	Mary: 300

Table 2: *Liability-centric system design*
Fig 6: *Liability-centric system*

In the diagram above, tokens A and B have independent balance sheets, implying that the tokens cannot be mixed up regardless of the activities in the liquidity pools. Unlike in the previous scenario, Peter is guaranteed to withdraw the exact number of tokens irrespective of Mary's actions.

COVERAGE
RATIO

Through the concept of liabilities, MERCURY is the first StableSwap to use coverage ratio in its dynamics to delineate equilibrium states. The coverage ratio is a crucial aspect of the MERCURY protocol that must be maintained above a certain threshold to avoid defaults. For example, the coverage ratio prevents instances where users' withdrawal requests exceed the number of assets in a token account.

Coverage Ratio = Asset/Liability

Account (USDT)

ASSET	LIABILITY
Cash: 1,000	Deposit: 1,100

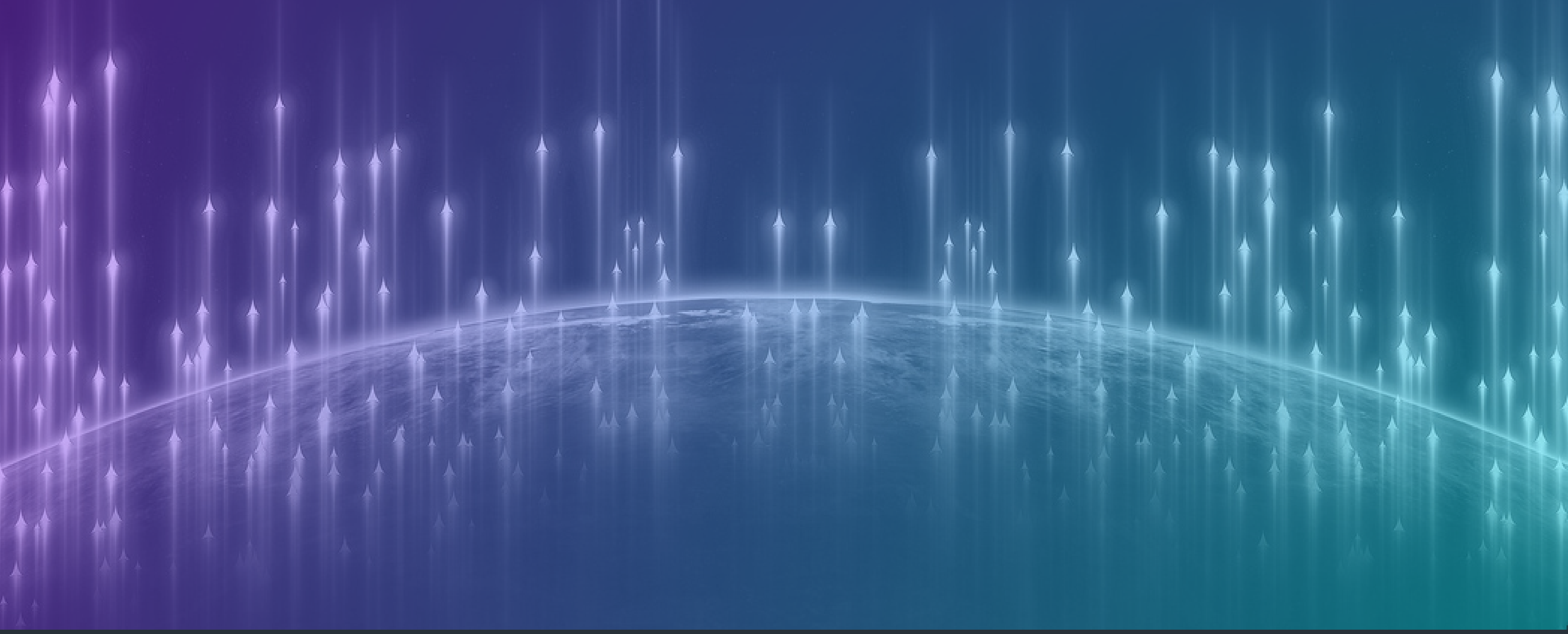
Account (ETH)

ASSET	LIABILITY
Cash: 31	Deposit: 30

Table 3: *Coverage Ratios*

Fig 7: *the coverage ratio for USDT is 0.909 (1,000/1,100), ETH 1.033 (31/30)*

In MERCURY, when a transaction happens, liquidity for the swap-from token increases while liquidity for the swap-to token decreases. MERCURY also penalizes transactions that diverge from equilibrium to encourage transactions that move the system towards equilibrium through price slippage, a function of the coverage ratio.



SLIPPAGE
OPTIMIZATION

Crypto trading typically involves dealing with volatility and unpredictability. Prices of crypto assets on exchanges are constantly changing, and sometimes, users are forced to endure failed transactions due to slippages. The bid-ask spread determines slippage, and relatively large transactions attract higher slippages. One of the strengths of the MERCURY protocol is lower slippage levels. The sections below describe how the internal dynamics of the protocol function to de-risk capital risk and increase security.

A) WITHDRAWAL ARBITRAGE RISKS AND SECURITY

Withdrawal arbitrage is a risk that manifests as an input in the slippage function that translates into the coverage ratio. MERCURY has a security mechanism to mitigate this risk, as described below.
Let us assume a liquidity pool contains deposits of assets and liabilities of 100, as shown in fig 8. And there is a whale who owns 20 percent of the pool and can generate risk-free profit by making a series of transactions as described in step 1.

USDT

ASSET	LIABILITY	COV RATIO
100	100	1

Fig 8: *Liquidity pool contains deposits of assets and liabilities of 100*

Step 1:

The whale acquires 20 percent of the pool tokens by trading with another token, causing the coverage ratio to fall to 0.8 since assets in the pool have reduced to 80. The pool still has 100 tokens for liquidity providers, but users undertaking transactions in the new situation will suffer a certain degree of slippage.

USDT

ASSET	LIABILITY	COV RATIO
80	100	0.8

Fig 9: *Whale withdraws 20 percent of the pool tokens*

Step 2:

The whale withdraws all the liquidity (20 tokens), causing the coverage ratio to reduce to 0.75.

USDT

ASSET	LIABILITY	COV RATIO
60	80	0.75

Fig 10: *The whale withdraws all liquidity*

Step 3:

The whale reverses the transaction in step 1, swapping back 20 percent of the tokens he acquired. The coverage ratio is reverted to 1 from 0.75. Since the protocol rewards transactions that pull the coverage ratio to the equilibrium, the whale is awarded a favorable exchange in the form of positive slippage.

USDT

ASSET	LIABILITY	COV RATIO
80	80	1

Fig 11: *liquidity pool after step 3*

Note

Swap slippage charged in step 1 is for a coverage ratio from 1 to 0.8, while the slippage fee in step 3 is for a coverage ratio from 0.75 to 1. Due to the slippage curve convexity, the reward for step 3 is more significant than the penalty for step 1, thus generating a risk-free profit. The exact process can be continuously executed multiple times until the pool is drained. This type of attack on the system is called withdrawal arbitrage. MERCURY protocol seals this attack by introducing a withdrawal fee. Even though withdrawal fees can be punitive for liquidity providers, they are harmless to users and still effective at curbing withdrawal arbitrage when kept minimal. For example, when the coverage ratio in MERCURY is 0.8, the withdrawal fee will be 0.01 percent. The MERCURY operating dynamics are designed to make the marginal slippage more significant at any coverage ratio than the withdrawal fee.

Let us assume the withdrawal amount equals 1 percent of the pool.

COV RATIO	MARGINAL SLIPPAGE	WITHDRAWAL FEES
1	-0.01%	-0.0000%
0.9	-0.03%	-0.0011%
0.8	-0.08%	-0.0093%
0.7	-0.24%	-0.0518%
0.7	-0.83%	-0.2731%

Fig 12: *Coverage ratio and withdrawal fee*

Figure 12 shows that users whose transactions restore the systems coverage ratio to a healthy position will always have a more significant financial incentive than those who withdraw. It is important to note that MERCURY can support withdrawal transactions even when the coverage ratio is below one because of banking's fractional reserve assumption – it is rare for all liquidity providers to withdraw their assets at once. This assumption is anchored on trust among users remaining intact and withdrawals from a few individuals unable to drain a significant portion of the pool. Lastly, it is essential to note that MERCURY has deposit arbitrage/deposit fees to prevent unnecessary flash loans.

B) SLIPPAGE FEE DYNAMICS

Conventionally when transacting two tokens, the coverage ratio for one token increases while for the other decreases. The balance for the from-token increases, and that of the to-token drops. Consider the case below without slippage.

USDT

ASSET	LIABILITY
100	100

r=1

USDC

ASSET	LIABILITY
100	100

r=1

Fig 13: *Before swap*

USDT

ASSET	LIABILITY
110	100

r=1.1

USDC

ASSET	LIABILITY
90	100

r=0.9

Fig 14: *After swapping 10 USDT for USDC*

The figures above describe a mechanism similar to the constant sum market maker (CSMM) that does not penalize large volume transactions, thus encouraging users to drain the pool. For example, a swap of 100 USDT for USDC would drain the USDC pool.

MERCURY protocol penalizes all transactions that increase the coverage ratio irrespective of their volume. The protocol defines the swapping slippage using the formula in figure 15.

$$S_{i \to j} = S_i + (-S_j) = S_i - S_j$$

Fig 15: *swapping slippage formula*

Si and Sj must be negatives, implying Si is the reward for the swap, Sj is the penalty, and $Si \to j$ is the fee. Because of the convexity of the slippage function, transactions that diminish the coverage ratio between the two tokens are rewarded since $Si \to j$ is negative. In contrast, transactions that widen the coverage ratio of the two tokens are penalized since $Si \to j$ is positive.

From the previous example, we can deduce that.

$$S_{USDT} = -\frac{g(1.1) - g(1)}{1.1 - 1} = 0.0097\,\%$$

$$S_{USDC} = -\frac{g(0.9) - g(1)}{0.9 - 1} = -\,0.0218\,\%$$

Consequently,

$$S_{USDT \to USDC} = -\,0.0097\% - (-0.0218\%) = 0.0121\,\%$$

Since swap slippage is 0.0121 percent, the user who swaps 10 USDT will get

$$S_{USDT \to USDC} = -\,0.0097\% - (-0.0218\%) = 0.0121\,\%$$

When users swap 10 USDT for USDC, they are given 9.9988 USDC. The protocol charges 0.0121 USDC as slippage. It is important to note that the protocol keeps the slippage as a transient reserve until the reverse action is done to revert the system to equilibrium. This approach is referred to as a "Path-independent" property. The new liquidity pools will look as shown in figure 16 below.

USDT		USDC	
ASSET	LIABILITY	ASSET	LIABILITY
110	100	90.0121	100
r=1.1		r= 0.9001	

Fig 16: *pools after a swap*

C) POOL REBALANCE AND DYNAMIC INTEREST RATE

The interest rate model is the only model that auto balances pools based on variable interest rates that allow automated market maker users to earn handsomely from their staked assets. This model can be described as 'the higher the coverage ratio, the greater the reward to the stablecoin account.' One of the model's key strengths is protecting against coverage ration manipulation. DeFi 1.0 protocols that use this model use arbitrage activities to rebalance their pools.

MERCURY leverages a new approach that is based on ELE emission to rebalance its pools. This model is designed to bar unscrupulous users from tricking the system into claiming disproportionately huge rewards with abundant capital. This new model incentivizes balance across pools; all users are guaranteed stable yields on their investments. Users can earn more from their deposits by taking advantage of natural market movements. The protocol rewards existing liquidity providers who shift their liquidities to restore stable coin accounts' coverage ratios to healthy positions.

RISK
MANAGEMENT

A) WITHDRAWAL

There is a possibility of instances when some tokens suffer shortages while large liquidity providers want to withdraw their shares. In such cases, MERCURY may not be able to satisfy the transaction needs of the user. MERCURY will deal with this risk by informing users that they can only withdraw what the system can offer at the time. However, they can return and withdraw their balance when equilibrium is restored. Alternatively, the system will allow users to remove other assets well covered in the protocol, even if they are not the ones they provided when depositing.

B) PRICE ORACLE

Most protocols usually assume assets inside the pool are always pegged. While the understanding is true most of the time, sometimes, it is not the case. MERCURY will use price oracles to monitor the price difference between tokens and reverse transactions where the price deviation between the tokens is more significant than a certain percentage.

CONCLUSION

In this whitepaper, we explained how MERCURY helps create a capital efficient decentralized Stablecoin exchange to minimize price fluctuations, increase capital power, and efficiently respond to market conditions in the ecosystem. The economics and technical approaches to implementing the fundamentals and mass adoption will play a critical role in embracing the high likelihood and success of the platform. Blockchain economics is multiplying, and more use cases are emerging with a need for reliable collateral to pioneer the decentralized financial sector. We strongly believe MERCURY will provide tremendous opportunities to innovate new experiments to shape the crypto space of the future.