Verifiable Scheme for Hedge Fund Investment Strategies Based on ZK Interval Proofs

Conflict Between Confidentiality and Transparency in Hedge Funds

In the highly confidential, lightly regulated, and potentially lucrative investment realm of hedge funds, the core investment strategies are typically not disclosed to the public. This confidentiality stems from the complex trading structures of hedge funds and the need to maintain competitiveness in the market. By keeping strategies confidential, hedge funds can sustain their unique profitability in a fiercely competitive market environment, while granting fund managers greater flexibility to employ innovative approaches to capture market opportunities. Furthermore, the confidentiality of investment strategies prevents competitors from copying them, thereby ensuring the fund's excess returns; it protects innovative techniques from external interference; and it avoids potential negative impacts on fund performance from market herding behavior.

Excessive confidentiality in hedge funds can lead to multiple issues such as information asymmetry, investor trust problems, and compliance concerns, which not only affect fund operations but may also adversely impact the entire market ecosystem.

Both investor trust issues and compliance concerns can be attributed to information asymmetry, although they manifest and impact differently.

1. **Information Asymmetry as the Root Cause**

Information asymmetry refers to the significant difference in the amount of information available to fund managers and investors. In hedge funds, due to the confidentiality of investment strategies, investors often cannot obtain sufficient information to assess

risks and returns. This information asymmetry is not only the starting point of investor trust issues but also provides conditions for potential non-compliance.

2. **Chain of Investor Trust Issues**

Information asymmetry makes it difficult for investors to grasp the true operating situation of the fund, especially when assessing risks. This weakens investors' trust, hinders capital inflows, and adversely affects the long-term development of the fund and the healthy growth of the industry. Therefore, investor trust issues essentially stem from changes in investor psychology and behavior caused by information asymmetry.

3. **Extensions of Compliance Concerns**

Information asymmetry allows fund managers to operate with less external scrutiny, providing cover for non-compliant behaviors such as insider trading and fund misappropriation. This situation not only threatens market transparency and fairness but may also trigger systemic financial risks. Since traditional regulatory approaches rely on information disclosure, information asymmetry exacerbates regulatory difficulties.

To break information asymmetry and seek a balance between confidentiality and transparency in hedge funds, this paper proposes a technical solution based on homomorphic commitment and zero-knowledge interval proofs. This solution achieves information verifiability while protecting the confidentiality of investment strategies.

Cryptographic Construction

Pedersen Commitment with Homomorphic Properties

A commitment scheme serves to convey trustworthy information between participants, akin to an "encrypted envelope." The committer initially generates a commitment value, encapsulating the information without disclosing its contents. Later, when needed, the commitment can be revealed to verify the authenticity of the content.

Pedersen Commitment is defined in a cyclic group based on the hardness of the discrete logarithm problem. For a message m , a secret value r is randomly selected, and the commitment value is calculated as: $C_r(m) = g^m h^r \, mod \, p$. Disclosing the commitment is accomplished by revealing m and r.

p	A large prime number
q	A prime number that satisfies $q \mid p - 1$
$G = Z_p$	A group of integers modulo p
g and h	An element in group G of order q , where the discrete logarithm $log_g(h)$ is unknown
$hash$	A cryptographic hash function with a range of $[0, q - 1]$

Pedersen Commitment boasts the following characteristics:

1. Hiding: The content of the commitment remains completely confidential to observers, even if they know the commitment result and public parameters.
2. Binding: The committer cannot alter the content when revealing it.
3. Homomorphism: Operations can be performed directly on commitment values without revealing the content of the commitment. This means that arithmetic operations on two messages can be directly conducted through their commitment values, enabling computation under encryption.

Here, we focus on the homomorphism of Pedersen Commitment:

The commitment for message m_1 is $C_1 = g^{m_1} h^{r_1} \, mod \, p$.

The commitment for message m_2 is $C_2 = g^{m_2} h^{r_2} \, mod \, p$.

The addition of messages m_1 and m_2 can be achieved through the multiplication of commitments C_1 and C_2:

$$C_1 \cdot C_2 = g^{m_1} h^{r_1} \cdot g^{m_2} h^{r_2} \bmod p = g^{m_1+m_2} h^{r_1+r_2} \bmod p = C_{r_1+r_2}(m_1 + m_2)$$

Thus, even without knowing the specific messages m_1 and m_2 hidden in the two commitments C_1 and C_2, anyone can compute the commitment for any fixed linear combination of them.

Interval Proofs Based on Zero-Knowledge Proofs

Zero-knowledge proof technology allows the prover to prove to the verifier that they know a secret information without revealing the content of the information. For a message m promised by Pedersen, the prover has m and r, such that $C_r(m) = g^m h^r \bmod p$ holds.

In addition, the prover can also prove that the message m satisfies a certain condition $\varphi(m)$ without disclosing m. This can be expressed as:

$$ZKP\left(m, r \mid C = g^m h^r \bmod p, \varphi(m)\right)$$

Schnorr OR Proofs is a zero-knowledge proof technology based on the Schnorr protocol, suitable for proving that a message m satisfies a set condition, such as:

$$ZKP\left(m, r \mid C = g^m h^r \bmod p, m \in \{0, 1\}\right)$$

The prover can prove that m indeed belongs to 0, 1 without revealing the specific value (0 or 1) of message m.

The proof data consists of $\{C, r_1, r_2, c_1, c_1\}$, which satisfy the following conditions:

$$c_1 + c_2 = hash(a_1, a_2) \bmod q$$

$$a_1 = h^{r_1} C^{-c_1}$$

$$a_2 = h^{r_2} (C/g)^{-c_2}$$

Using this, we can see the interval proof:

$$ZKP\left(m,\ r \mid C\ = g^{m}h^{r}\ mod\ p,\ m\ \in \left[0,\ 2^{k}\ -\ 1\right]\right)$$

The following is the construction and verification process of interval proof:

Construction of interval proof

1. Binary expansion

Expand m into binary form $m\ =\ \sum_{i=0}^{k} 2^{i}a_{i}$, and generate a corresponding commitment $C_{i}\ =\ C_{r_{i}}\left(a_{i}\right)$ for each bit a_{i};

2. Adjust the last commitment

Set the last commitment to $C/\prod_{i=1}^{k}\left(C_{i}^{2^{i}}\right)$, ensuring that the relationship $C\ =\ \prod_{i=0}^{k}\left(C_{i}^{2^{i}}\right)$ holds;

3. Proof of each

Compute the Schnorr OR Proofs for each bit a_{i} to prove $a_{i}\in\ \{0,\ 1\}$.

Verification of interval proof

1. Check whether k Schnorr OR Proofs are valid, ensuring that each bit a_{i} is 0 or 1;
2. Verify whether the commitment relationship $C\ =\ \prod_{i=0}^{k}\left(C_{i}^{2^{i}}\right)$ holds.

If we need to prove that m is in any threshold interval $\left[T,\ 2^{k}\ -\ 1\ +\ T\right]$, we can simply replace C with $C\ /\ g^{T}$ and follow the same process to construct an interval proof.

Hereinafter, we will simplify $ZKP\left(m,\ r \mid C\ /\ g^{T}\ = g^{m}h^{r}\ mod\ p,\ m\ \in \left[T,\ 2^{k}\ -\ 1\ +\ T\right]\right)$ to $ZKP_{k}(m\ \geq T\ )$.

Verifiable solutions for investment strategies of hedge funds

In the field of hedge fund financial investment, verifiable investment strategies are a framework that simultaneously considers both return and risk control. Their core principle is to use ZK interval proof technology based on homomorphic commitments to break information asymmetry without disclosing specific investment strategies, providing investors with a certain degree of risk transparency and information verification capabilities.

In our proposed verifiable solution for hedge fund investment strategies, we adopt a hierarchical information disclosure approach to clarify which content is publicly available and which content is hidden but verifiable through ZK interval proof technology based on homomorphic commitment.

Public content:

1. All investment categories or specific investment projects included in the investment strategy, such as stocks and derivatives;
2. The risk factors and their correlations of various types of investments are calculated and disclosed by fund managers through professional models.

Based on the above disclosure, we can verify the following hidden content:

1. Investment weight constraint: Whether the weight of each investment falls within the preset range.
2. Risk limit constraint: whether the overall and local risk levels of the investment portfolio are within the established risk limit.

The verifiability of investment weight based on ZK interval proofs technology

In hedge fund investment strategies, investment weight constraints are a key mechanism used to ensure that funds do not over-bet on a single security. Through this constraint, the fund can diversify investment risks and avoid over-reliance on a single asset or market change.

1. **Portfolio weight allocation**

After collecting investors' funds, fund managers allocate these funds to multiple assets based on different investment strategies and statistical analysis methods. The fund manager will define a collection of assets:

$$A = \{A_1, A_2 \ldots\ldots A_n\}, |A| = n \in N$$

where n represents the total number of assets.

Each investor's funds are allocated to these assets according to a specific ratio, which is represented by the weight W. The fund manager will define an investment portfolio:

$$W = \{W_1, W_2 \ldots\ldots W_n\}, \sum_{i=1}^{n} W_i = 1$$

Where, W_i represents the investment weight in asset A_i, which is the proportion of the asset in the overall investment portfolio.

2. **Calculate the ZK interval proofs**

The fund manager makes a commitment C_i for the investment weight W_i of each asset A_i. After confirming that the investment weight satisfies the constraint condition T_i, the fund manager calculates the corresponding ZK interval proofs based on the ZK-based interval proofs construction process, denoted as I:

$$I = ZKP_k\left(W_i \geq T_i\right),\ i = 1,\ 2 \ldots\ldots\ n$$

$I = \{I_1,\ I_2 \ldots\ldots\ I_n\}$ represents the set of ZK interval proofs calculated by the fund manager for each investment. These ZK proofs are sent to investors.

3. **Verify the investment weight**

Investors verify each ZK interval proof in the set I based on the ZK-based interval proof verification process. In this way, investors can confirm whether each investment weight W_i promised by the fund manager falls within the specified interval $\left[T_i,\ 2^k - 1 + T_i\right]$, ensuring that the investment weight meets the set constraints without revealing specific investment weights.

In this case, the core function of ZK-based interval proof is that it allows investors (verifier) to verify whether the investment weight W_i of the fund managers (prover) meets the agreed investment weight constraint T_i, based on only knowing the commitment set $\{C_i\}$ and the corresponding constraint set $\{T_i\}$.

The verifiability of risk limits based on ZK interval proofs technology

In investment, investors usually hope to control the investment risk while pursuing high returns. However, if too much capital is invested in high-risk assets, it may conflict with the interests of investors, leading to dissatisfaction with the fund manager's decisions.

1. **Calculate risk factors**

To estimate the risk of each asset in the portfolio, the fund manager calculates the corresponding risk factor R_i for each asset A_i to measure its potential risk. The set of risk factors can be represented as $R = \{R_1,\ R_2 \ldots\ldots\ R_n\}$.

2. Calculate the ZK interval proofs

The fund manager assesses the overall risk level of the portfolio based on the risk factor set R and the investment weight set W. In order to ensure that the investment risk meets the requirements of investors, the fund manager will set a risk limit T_R and calculate the corresponding ZK interval proofs:

$$I_R = ZKP_k\left(\sum_{i=1}^{n} W_i R_i \geq T_R \right)$$

Where, $\sum_{i=1}^{n} W_i R_i$ represents the weighted total risk value of the portfolio. The fund manager makes a commitment C_{WR} for the weighted total risk value.

Next, the fund manager uses its private key sk to digitally sign the I_R:

$$\sigma_{I_R} = Sign_{sk}\left(I_R, ts\right)$$

It should be noted that a timestamp ts needs to be added here. Time stamps are a key factor, and their main purpose is to address potential data aging issues caused by dynamic market changes.

σ_{I_R} is sent to investors by fund managers.

3. Verify risk limits

The investor first verifies the σ_{I_R} using the fund manager's public key pk, decrypts it to obtain the I_R, and records its corresponding timestamp ts.

Investors verify the I_R to confirm whether the weighted total risk value of the portfolio promised by the fund manager falls within the specified interval $\left[T_R, 2^k - 1 + T_R\right]$,

thereby ensuring that the weighted total risk value meets the set constraints without revealing specific risk values.

In this case, the core function of ZK-based interval proofs is that it allows investors to verify whether the weighted total risk value I_R of the investment strategy designed by the fund managers meets the agreed constraint T_R, based on only knowing the commitment C_{WR} and corresponding constraint T_R.

Risk correlation

In hedge fund strategies, the correlation of risk factors is the key to the assessment and control of overall risk. By relating the risk factor $R_{i,j}$, the mutual influence between any two assets A_i and A_j can be effectively described. The ZK interval proofs can be expressed as:

$$ZKP_k\left(W_i W_j R_{i,j} \geq T_{R_{i,j}}\right)$$

Risk correlation has a great impact on hedging strategies. For example:

1. **Opposite positions in the spot and derivatives markets**

Buying or selling a certain cryptocurrency in the spot market, while selling or buying futures contracts of the same amount of the cryptocurrency in the derivatives market such as the futures market. The setting of such opposite positions is the core manifestation of the hedging strategy. The price difference between the spot and derivative markets is worth noting here. By holding positions in both markets simultaneously, we can lock in this price difference and achieve profitability when the derivative contract expires.

The purpose of holding opposite positions is to hedge risks. When the spot market price rises, short positions in the derivatives market may incur losses, but long positions in the spot market will be profitable, thereby offsetting the losses in the derivatives market.

Similarly, when the spot market price falls, long positions in the derivatives market will be profitable, offsetting the losses in the spot market.

2. **Simultaneously open long and short positions for paired trading**

By opening both long and short positions simultaneously, traders can reduce risk and earn profits without relying on the overall trend of the market. Investors will engage in paired trading, which involves establishing long positions in one asset and short positions in another. This strategy is actually using the relative price changes between two assets for hedging and arbitrage.

For example, token A has increased in price by more than 200%, while token b has lost more than 50% during the same period. A market neutral trader can open a long token A position to profit from a price increase and a short token B position to profit from a significant decline in the asset's value.

This practice of opening multiple long and short positions simultaneously is actually a hedging mechanism. Even if the overall market trend is uncertain or volatile, traders can still reduce risks and obtain profits through this type of paired trading.

If the market as a whole falls, although the price of token A may be affected and fall, the price of token B may fall more, partially or completely offsetting the loss of token A position. Similarly, if the market as a whole rises, although the price of token B may rebound, the price of token A may rise more, resulting in greater profits.

3. **Statistical arbitrage by buying and shorting two stocks with strong correlation**

By simultaneously buying and shorting two stocks with strong correlation, usually based on factors such as historical price trends, industry background, and market position, to earn price differences.

Investors seek out stock pairs where the short-term price deviates from the long-term average relationship, then buy one stock at a relatively low price and sell the other stock

at a relatively high price. When the prices of these two stocks return to their historical average levels, investors will close their positions and make profits.

When the price difference between two stocks reaches a certain level, investors can start to establish opposite positions. Investors need to execute trading operations in accordance with trading rules and close positions in time to profit when price differences shrink.

Verifiable Factor Extension

In portfolio management, in order to effectively control risks and meet strategic needs, assets can be grouped according to specific criteria, and constraints can be set for each subgroup to limit investment amounts, weights, and risks.

The following introduces G_i as the basis for grouping, which is used to classify and constrain different asset categories or characteristics. The construction method of ZK interval proof is:

$$ZKP_k\left(\sum_{i=1}^{s} G_i W_i \geq T_{G_i}\right)$$

where s represents the number of groups, which can be any value. T_{G_i} represents the weight limit allowed for investment in each group.

1. Limit on short or long positions

G_i represents the short or long asset group in the portfolio, which is used to build constraints related to specific positions.

In this grouping method, s is usually 2, that is, all short assets are grouped together, and all long assets are grouped together.

Limiting the combination of short and long positions can reduce the potential risk of excessive leverage, especially in the following areas:

Liquidity risk: Excessive short or leveraged positions may lead to difficulties in liquidating assets or forced liquidation during market fluctuations.

Risk hedging: Balancing long and short positions can mitigate the impact of sharp price changes on the investment portfolio.

2. Distribution restrictions on industries and asset categories

G_i represents a grouping of specific industries or asset classes, used to reflect the investment weight of each industry asset in the portfolio.

In this grouping method, s can be any value. $\sum_{i=1}^{s} G_i W_i$ represents the weight of total investment in a specific industry.

Limiting the distribution of industries and asset classes in the investment portfolio has the following advantages:

Risk diversification: Avoid investment concentration in a single industry or asset class, effectively reducing systemic risk.

Stability of income: Through distribution equalization, reduce income fluctuations and enhance the robustness of the investment portfolio.

Summary and Prospect

In summary, this article carefully explores the challenges faced by hedge fund investment strategies in seeking a balance between confidentiality and transparency, especially information asymmetry, investor trust deficit, and compliance issues. To address these complex issues, we have designed a verifiable scheme for hedge fund investment strategies through zk interval proof technology based on homomorphic commitment. This solution not only ensures the confidentiality of hedge fund investment

strategies is effectively maintained, but also provides investors with a verifiable transparency tool, significantly enhancing trust and reducing compliance risks.

The program is fully supported by ZEROBASE, which provides high-quality, customized circuit development and efficient, decentralized proof generation services. If you have sensitive information such as fund investment strategies that need to be processed in accordance with compliance standards, ZEROBASE will use TEE technology to generate ZK proofs in a secure isolated area to ensure that your computing and data privacy are strictly protected.

Looking ahead, ZEROBASE's technical solutions undoubtedly provide valuable reference and lessons for the robust development of the hedge fund industry in the emerging regulatory environment. With the increasing maturity of privacy protection technology, innovative means such as ZK and TEE are expected to be widely used in more financial fields, finding a more perfect balance between privacy protection and compliance requirements. Furthermore, we anticipate that, with the collective efforts of various parties, we can foster in-depth dialogue and collaboration among policy makers, investors, and fund managers to jointly construct a more transparent, secure, and efficient financial ecosystem. ZEROBASE's composable compliance framework will undoubtedly provide robust support and assistance in this regard, allowing organizations to seamlessly interact with Web3 applications, leveraging TEE to generate ZK proofs in secure enclaves, and comprehensively safeguarding the privacy of computations and data.

We sincerely invite you to walk alongside ZEROBASE and jointly paint the blueprint for a more stable financial market in the future.