Pencils Protocol: Scroll Native Gateway for Yields, Auctions, and Multilayer Rewards

Monday 16th September, 2024

Abstract—Pencils Protocol is a one-stop DeFi aggregation platform that offers auction platform for blockchain native assets , along with unified and leveraged yield aggregation services for users to maximize asset utilization and obtain Multilayer Rewards. Pencils Protocol also serve as Scroll native gateway for liquid staking and restaking assets. Pencils Protocol redefines the Layer-2 sectors by utilizing Scroll's zero-knowledge technology. We focus on scalable and private DeFi services, enhancing yield aggregation and staking. By leveraging the synergy between our launchpad and staking solutions, we aim to become the primary TVL gateway for the Scroll ecosystem. We have also considered the security risks and legal risks that may exist in the Defi ecosystem with high TVL, high yield, and high risk, and designed some technical solutions to ensure the compliance of Pencils Protocol and protect user privacy while complying with KYC and AML laws.

Index Terms—DeFi, Auction, Yield Farming, Permissioned DeFi, Zero Knowledge, Liquidity Pooling, AML

1 Introduction

BLOckchain is a decentralized distributed ledger technology that ensures data security and integrity through cryptographic algorithms and consensus mechanisms. Blockchain emerged during the 2008 financial crisis when traditional finance exposed various issues. An anonymous author, Satoshi Nakamoto, released "Bitcoin: A Peer-to-Peer Electronic Cash System" [1], which proposed a purely peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution. The advent of Bitcoin marked the official introduction of blockchain. The features of blockchain—trustlessness, immutability, decentralization, transparency, traceability, and automation—address the shortcomings of traditional finance, save significant costs, and enhance financial scalability and efficiency.

In recent years, blockchain-based financial applications have seen substantial development, with automated financial systems bringing both risks and rewards to users. The diversity of asset forms on the blockchain leads to various investment return formats. For ordinary users, the entry barrier into the DeFi (Decentralized Finance) field is high, and they may face substantial losses at any time. Most investors seek stable returns amid the current economic instability, while risk-averse customers need more aggressive investment strategies. Users require a systematic DeFi aggregation platform to manage returns comprehensively.

However, the anonymity and high decentralization of blockchain also bring risks. Criminals exploit blockchain for Ponzi schemes, money laundering, fraud, embezzlement, extortion, and tax evasion. These illicit activities leverage Bitcoin's anonymity to obscure audit trails. It is estimated that in 2017, $770 million worth of Bitcoins were used for illegal activities, with a quarter of Bitcoin users deemed malicious and 46% of Bitcoin activities considered illegal. In 2023, the value received by illegal cryptocurrency addresses dropped significantly compared to 2022, totaling

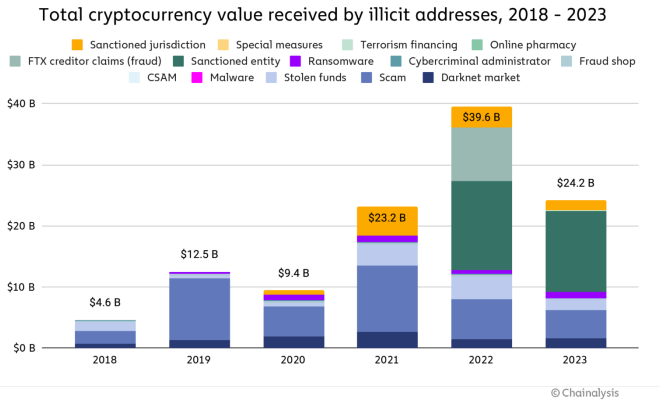

Fig. 1: Total cryptocurrency value received by illicit addresses, 2018 - 2023

$24.2 billion, but it remains a concern. The FTX financial fraud case and the Luna-UST collapse in 2022 had a massive impact, with losses exceeding $200 billion. These losses, due to regulatory negligence and model mechanism failures, surpass ordinary crimes.

In traditional finance, participants must obtain approval from central authorities to access services. This includes identity verification, personal and financial status checks, and more. Decentralized finance (DeFi) does not have these restrictions because they do not align with the characteristics of blockchain. The development of technologies such as Zero Knowledge, permission control, and multi-signatures makes the integration of centralized finance (CeFi) and DeFi increasingly clear. The main advantage of Permissioned DeFi is that it offers the best of both worlds: the efficiency, autonomy, and transparency of decentralized finance, as well as the security and compliance of traditional systems.

We have considered various Permissioned DeFi implementation schemes and integrated them as pluggable components into the system. By leveraging various cryptographic techniques, we aim to meet regulatory and compliance requirements while ensuring user privacy and operational efficiency. The emergence of illegal patterns in complex networks has sparked the need for research and crowdsourced development of intelligent methods. These methods will assist intelligence companies and law enforcement agencies in enhancing the protection of financial systems and promoting the implementation of anti-money laundering (AML) regulations. Both supervised and unsupervised learning methods have been widely applied to Bitcoin blockchain monitoring tasks with promising results [2] [3]. We use Graph Convolutional Networks (GCN) to perform supervised learning on the behavior of system nodes, identifying malicious nodes in a timely manner and preventing criminal activities within the system.

The organization of this paper is as follows: Section 2 introduces related work, Section 3 describes the system architecture of the Pencils Protocol, Sections 4-6 respectively introduce the main business functions of the Pencils Protocol: Vaults, Yield Farming, and Auctions. Section 7 briefly discusses the economy of the Pencils Protocol, including incentive mechanisms and token usage. Section 8 covers the design for system security and regulatory compliance, and the final section provides the conclusion and summary.

1.1 Related Works

1.1.1 Decentralized Finance

Decentralized financial(Defi) applications are a new type of open financial applications deployed on publicly accessible, permissionless blockchains. A rapid surge in the popularity of these applications saw the total value of the assets locked in DeFi applications (TVL) grow from $675 million at the outset of 2020 to an excess of $40b in July 2024.

After the emergence of Ethereum, which can support the deployment of smart contracts, Rune Christensen proposed the concepts of MakerDAO and DAI on the reddit forum, called eDollar. The concept of a decentralized stablecoin first began to emerge on Ethereum. The following year, vbuterin's reddit post introduced the concept of a decentralized exchange (DEX) with an automated market maker (AMM), and DEXs based on AMMs became independent of centralized order books. Bancor and Uniswap were launched in 2017. MakerDAO and Compound then launched the first decentralized stablecoin and decentralized lending protocol, respectively. In 2016, BitMEX launched perpetual swaps, but they were still dependent on intermediaries. Perpetuals are similar to traditional futures contracts, with no fixed expiration date, and can provide derivative markets for illiquid assets. CLOB-based dYdX and MCDEX emerged as non-intermediary perpetual contracts. 2020's Yearn Finance brought Defi Summer to a climax.

The financial services provided by DeFi protocols [4] mainly include decentralized exchanges, lending protocols, asset management, cross-chain interoperability, etc. The benefits that DeFi protocols can provide include a wider range of financial services, lower service costs, and a business model that operates at lower operating costs, as well as ultimately greater privacy. However, it also brings greater risks of crime and lower costs of doing evil. Money laundering, extortion, and attacks on financial accounts are frequent occurrences on the blockchain. Pencils Protocol is committed to becoming a DeFi aggregation platform, and at the same time, it has a well-designed architecture to ensure the security and privacy of users' transaction processes, taking into account regulatory and compliance requirements.

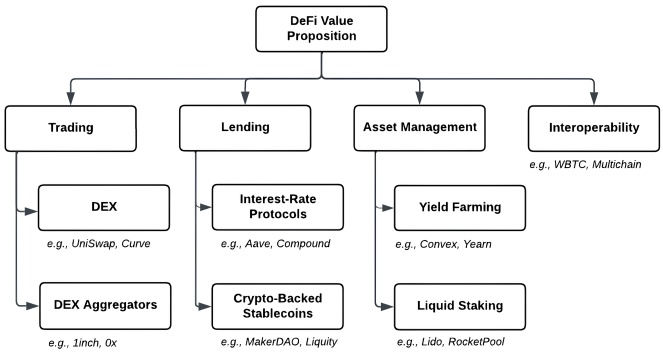

Fig. 2: Value Proposition and Design of DeFi Protocols

1.2 Scroll

Scroll[1] is a zkRollup for scaling Ethereum, which is equivalent to EVM. The basic idea of zk-Rollup is to aggregate multiple transactions into a single Rollup block and generate a compact proof of validity for the block off-chain. Then, the smart contract on Layer 1 only needs to verify the proof and directly apply the updated state without re-executing these transactions. This can help save a lot of gas fees, because proof verification is much cheaper than re-executing the calculation. ZK's compression of blocks also reduces transaction costs. The core of Scroll is ZKEVM, which is used to prove the correctness of EVM execution in layer 2, generate a proof of validity for each transaction, and finally aggregate all block proofs into a single proof and upload it to layer 2 to achieve the purpose of scaling. Scroll's ZKRollup solution and security measures can reduce costs and overhead for Dapps running on it.

1.3 ERC 4626

A Vault is a smart contract address used for accounting, depositing, and withdrawing. Users can deposit tokens into it and then run predetermined strategies to invest these deposits. Different DeFi protocols set different data structures and functions for their Vaults, leading to a small amount of liquidity being dispersed across many different DeFi applications, which are not interoperable. Pencils Protocol is dedicated to helping users find the best returns for their crypto tokens by executing different strategies. The way these strategies are completed may vary slightly, which can be prone to errors or waste development resources. The key

1. https://scroll.io/

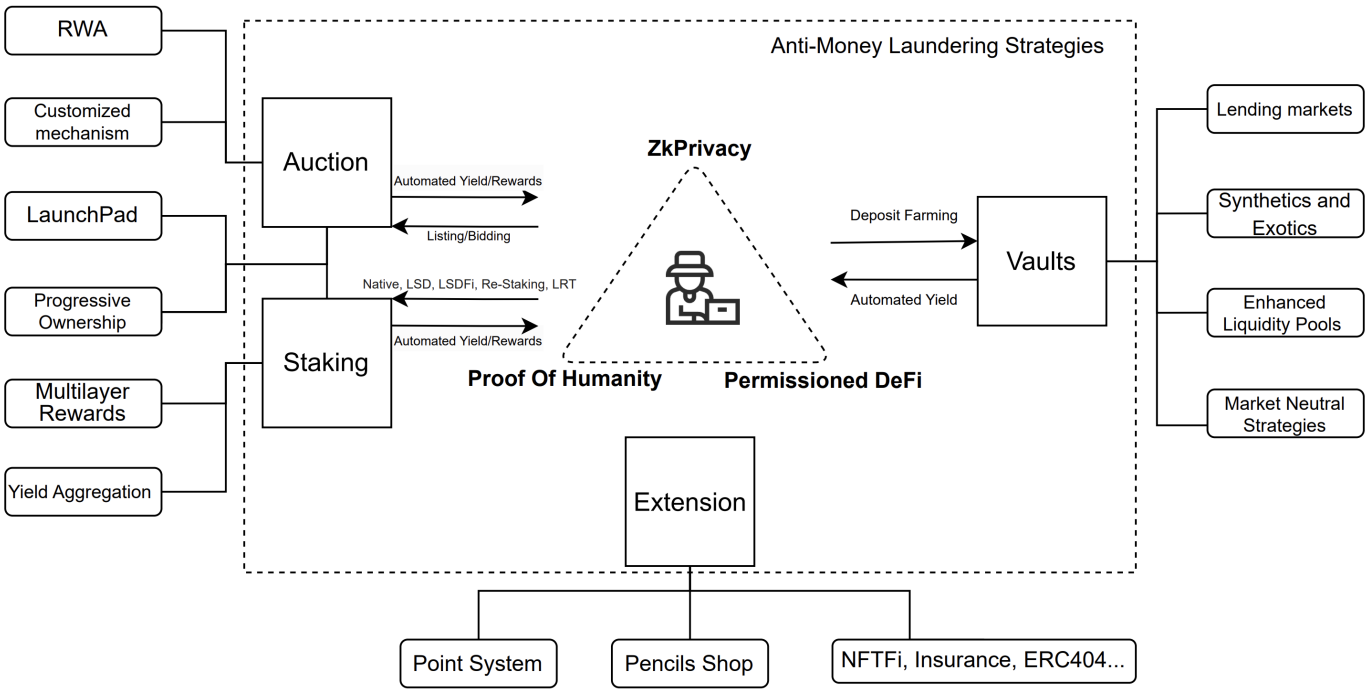

Fig. 3: Pencils Protocol architecture

issue lies in the potential compatibility problems during the development process of different strategies.

ERC-4626[2] is a standard that optimizes and unifies the technical parameters of yield Vaults. It provides a standard application interface for tokenized yield Vaults that represent shares of a single underlying ERC-20 token. By creating a more consistent and robust implementation pattern, ERC-4626 reduces the integration workload and unlocks pathways for earning returns across various applications without requiring developers to provide specialized work.

ERC-4626 inherits from ERC-20, and the vault shares are represented as ERC-20 tokens: Users deposit a specific ERC-20 underlying asset (such as WETH) into the vault, and the contract mints a corresponding amount of vault share tokens (such as pWETH). When users withdraw the underlying asset from the vault, the equivalent amount of vault share tokens is burned. The 'asset()' function returns the token address of the underlying asset of the vault.

2 Architecture

Pencils Protocol provides auction platforms and yield aggregation financial services in the Scroll ecosystem, specifically Vaults, Staking and Auction. Vaults are used to implement yield optimization strategies, mainly Yield Farming (liquidity mining). The Pencils Protocol Vaults offer more innovative products, including Yield Stripping, Market Neutral Strategies, etc., and are designed to enhance liquidity pools. Staking provides unified and leveraged yield aggregation services, further developing various liquid staking methods such as Liquid Staking and Restaking, Liquid Staking Derivatives, LSDFi, Liquid Restaked Tokens, etc. Users can earn multiple benefits in Pencils Protocol. Pencils Protocol provides multiple auction mechanisms, mainly serving auctions of Real World Assets, native tokens and NFT assets. The LaunchPad Alliance and Progressive Ownership features initially provided by Pencils Protocol contribute innovative solutions for token issuance and user loyalty, and can provide scalable infrastructure for auctions and staking.

Considering the risks, privacy and security of decentralized finance, Pencils Protocol has designed ZkPravicy, Proof of Humanity and Permissioned DeFi based on the native functions of Scroll to provide a secure underlying guarantee for the Pencils ecosystem. On top of the existing Defi protocol stack, we have designed many extensions, including a points system (to ensure that active contributors are recognized and rewarded), the Pencils Protocol Shop (supporting multi-chain point transactions, pre-market trading, custom unlocking tools, Web3 equity cards, celebrity tickets, fan benefits, RWA, ERC721, ERC404, etc.), NFTFi, decentralized insurance services, ERC404 Dex, etc.

3 Vaults

In DeFi, vaults are smart contract systems for secure asset storage and automated management. They allow users to deposit cryptocurrencies, which are then used to generate returns through predefined strategies by investing and reinvesting these funds across various DeFi protocols and blockchains. Vaults can serve multiple purposes such as yield farming, lending, and liquidity provision. By pooling funds from numerous individual users, vaults can achieve economies of scale and create diversified investment strategies that are difficult for individual investors to attain.

2. https://github.com/ethereum/ERCs/blob/master/ERCS/erc-4626.md

Vaults automatically handle all transactions, staking, and portfolio rebalancing according to their built-in strategies.

The Pencils Protocol Vaults 1.0 will first integrate with Scroll's leading DEX, and the Vaults Pool will connect to the DEX liquidity pool. Users can participate by selecting their preferred LP tokens in the Pencils Protocol Vaults Pool, and flexibly set different leverage multiples. The Vaults contract will automatically allocate the required leverage funds from the Staking deposit pool, satisfying high-risk appetite investors' pursuit of higher returns and providing a convenient and efficient fund appreciation experience. It also provides market neutral strategies for lower risk-profile investors.

Early active participants in Vaults will not only receive the base rewards from deposit staking and LP staking, but can also earn additional high multiples of Pencils Protocol, Pencils, DEX, and Scroll token rewards.

Vault 2.0 will add collaboration with the leading Liquid Restaking protocol, allowing participating users to enjoy both the native restaking yield and multiple token rewards (including EigenLayer, LRT, Pencils Protocol, DEX, and Scroll). This upgraded comprehensive rewards matrix aims to attract more users and assets.

In the future, Vaults will continuously integrate more high-quality asset offerings, striving to become users' preferred fund yield management tool by providing diversified, efficient, and secure asset appreciation channels. These will include on-chain delta-neutral strategies, on-chain synthetic yield, and on-chain exotic options.

Considering Scroll as an ETH Layer 2, which cannot achieve as high TVL as Layer 1, Pencils Protocol has explored various ways to improve the utilization and efficiency of liquidity provision. One implemented method is the Pencils Points System, which provides multi-layered rewards to incentivize investors to provide more liquidity. Additionally, automated strategies and portfolio rebalancing are used to optimize liquidity allocation and enhance capital efficiency.

Pencils Protocol uses ERC-4626 to standardize the implementation of Vaults, facilitating unified asset management and enhancing the interoperability of strategies. Users call the `deposit(uint assets, address receiver)` function to deposit `assets` units of an asset, and then call `mint(uint shares, address receiver)` to mint the corresponding amount of vault shares to the `receiver` address. Share tokens are generally named with a `pToken` prefix, such as staking ETH to receive `pETH`. During the withdrawal process, users need to call `redeem()` to burn the vault shares before they can call `withdraw()` to extract the corresponding amount of assets from the vault.

Furthermore, Pencils Protocol employs additional mechanisms to boost capital efficiency, primarily enhanced liquidity pools, cross-chain interoperability, and yield stripping. The protocol builds on Uniswap V3's concentrated liquidity market maker (CLMM) to implement the logic for enhanced liquidity.

3.1 Enhanced Liquidity Pools

Concentrated liquidity allows liquidity providers (LPs) to concentrate their liquidity within any chosen price range. This enhances the capital efficiency of the pool and permits LPs to estimate their preferred price curve (a process that will be automated within the Pencils Protocol) while simultaneously providing highly efficient aggregated liquidity with the remaining funds in the pool.

Concentrated liquidity addresses the issue that within certain ranges on the AMM curve, which are close to the coordinate axes, the value transformation is drastic. In these ranges, the trading pairs on the DEX deviate significantly from their actual value. Due to the presence of arbitrage mechanisms, value transformations do not occur within these ranges, resulting in low capital efficiency. Over 99% of the remaining funds are almost never utilized.

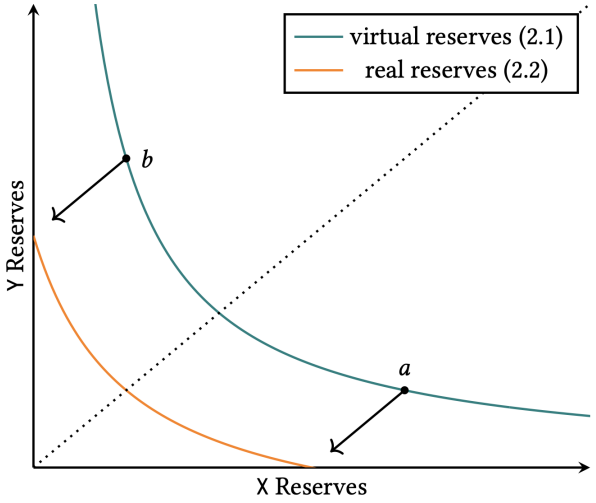

Fig. 4: Centralizing Liquidity Reserves

We refer to liquidity concentrated within a specific range as a "position." A position only needs to maintain sufficient token balances to support trading within that range [5].

Taking the price range $[p_a, p_b]$ as a position, and shifting the original curve $x \cdot y = k$ to $(x + x_b)(y + y_a) = k$, where $p_a = \frac{y_a}{x_a}, p_b = \frac{y_b}{x_b}$

we ultimately obtain:

$$(x + \frac{L}{\sqrt{p_b}})(y + L\sqrt{p_a}) = k = L^2 \tag{1}$$

To implement custom liquidity provision, the potential price space is divided into discrete points known as ticks. Liquidity providers can supply liquidity within any range defined by two ticks (which need not be adjacent).

Each range can be defined by a pair of tick indices: a lower tick (i_l) and an upper tick (i_u). Ticks represent prices that can be adjusted by the contract's virtual liquidity. We assume that the price is always expressed as the amount of $token_1$ per $token_0$. The assignment of $token_0$ and $token_1$ is arbitrary and does not affect the contract logic (apart from potential rounding errors).

Conceptually, a tick exists whenever the price p is an integer power of 1.0001. We use an integer i to represent the tick index, such that the price at this point can be expressed as:

$$p(i) = 1.0001^i \tag{2}$$

By definition, the price movement precision between two adjacent ticks is 0.01

In practice, trading pair pools use the square root of the price $\sqrt{price}$ to track ticks, which corresponds to the integer power of $\sqrt{1.0001}$. This can be converted to the equivalent square root price form:

$$\sqrt{p}(i) = \sqrt{1.0001}^i = 1.0001^{\frac{i}{2}} \tag{3}$$

When liquidity is added to a range, if one or both ticks are not already used as boundary points by existing positions, the tick will be initialized. Pencils Protocol handles liquidity mining for vaults by providing concentrated liquidity according to positions defined by different tick indices.

In cases of low TVL or low trading volume token pairs, liquidity can be shallow. By allowing multiple trading pair liquidity providers to share liquidity for a common token, the average liquidity can be enhanced, leveraging smaller pools for greater liquidity impact. Consider N token pairs $T_0, T_1, \ldots, T_i, \ldots, T_{N-1}$ against a highly liquid currency T_c (e.g., ETH). We analyze the liquidity and prices of these pairs on an AMM over a constant time interval I. The price of a token at time t is denoted as $p(t)$.

A cryptocurrency will have liquidity within certain price ranges over different intervals. By setting numerous positions within I, liquidity providers (LPs) in different positions aggregate and share their currency reserves [6]. Pencils Protocol uses smart contracts to automatically allocate funds to shared reserve pools based on the TWAP [7] (time-weighted average price) oracle from Uniswap, managing LP mints and withdrawals.The main operational process [8] is as follows:

The total available shared reserves of T_c, represented by R, are split between busy reserves R^b and *available* reserves R^a, such that $R = R^a + R^b$. $L[k]$ and $r'_{i,c}[k]$ represent the liquidity and corresponding T_c reserves at a particular tick k.

When the price of T_i decreases, causing the tick to transition from K_i to $K_i - 1$, with the new interval having $r'_{i,c}[K_i - 1]$ skeleton T_c reserves, the following events occur:

- The new active interval secures $r'_{i,c}[K_i - 1]$ units of T_c from the available reserve pool such that:

$$r'_{i,c}[K_i - 1] = R^a \left(\frac{r'_{i,c}[K_i - 1]}{\sum_{j=0}^{K_i - 1} r'_{i,c}[j]} \right) \tag{4}$$

- This is achieved by reducing the available reserves pool and increasing the busy reserves pool. Since $r'_{i,c}[K_i - 1]$ is always a fraction of the available reserves R^a, it never goes negative after the operation. The actual liquidity can be derived from real reserves using the relations:

$$\begin{cases} r'_a(p) = L\left(\frac{1}{\sqrt{p}} - \frac{1}{\sqrt{p_1}}\right) \\ r'_b(p) = L\left(\sqrt{p} - \sqrt{p_0}\right) \end{cases} \tag{5}$$

- The token T_i in tick K_i becomes inactive, with its amount stored in memory. It reactivates in the future when the tick transitions from $K_i - 1$ to K_i.

When the price of T_i increases, causing the tick to cross from K_i to $K_i + 1$, the accumulated T_c in the newly inactive tick K_i is transferred from busy reserves to available reserves, and any T_i reserves stored in memory are released for tick $K_i + 1$.

Pencils Protocol primarily enhances liquidity by utilizing concentrated liquidity, transforming liquidity price ranges into individual ticks, and enabling shared liquidity between ticks of the same token.

3.2 Yield Stripping

Yield stripping loosely refers to the process of splitting a yield-generating asset into two components: its principal and yield components. Principal Token (pToken) represents the original value of the depositor's savings asset, excluding future yield. Yield Token (yToken) is the interest yield that the depositor earns in the Pencils Protocol. The contract of Pencils Protocol calculates the maturity yield based on the depositor's set savings duration. Upon locking the deposit, the contract automatically issues pTokens equivalent to the savings amount and yTokens equivalent to the yield amount. Depositors can use pTokens and yTokens within the Pencils Protocol for investment profits.

If the depositor redeems the funds according to the set savings duration, the redeemed funds are $D_p + D_y + P$, where D_p and D_y are the principal and yield values, and P is the additional profit during the depositor's savings period, which can be less than 0. Redemption can only be completed if $D_p + \frac{t}{T} \cdot D_y + P \geq 0$; otherwise, liquidation will be triggered. Here, t is the current savings duration, and T is the set savings duration.

If a staker redeems before maturity, the redeemed amount is $D_p + \kappa(t, T) \cdot \frac{t}{T} \cdot D_y + P$. The parameter function $\kappa(t, T)$ is time-related and satisfies $\kappa(0, T) = 0$ and $\kappa(T, T) = 1$, used to adjust the interest yield rate for early redemption. Typically, $\kappa(t, T)$ is a concave function of t. Similarly, liquidation will be triggered if the total amount of principal and interest is less than the loss.

In general, considering the principal risk of savers in the Pencils Protocol, we offer a stable return method for the principal, while savers can use yTokens for additional investment. In this case, we assume that no liquidation mechanism is required during the savings process. If a saver incurs a principal loss during the savings process, meeting the condition $D_p + \rho \cdot D_y + P < 0$ (where $0 < \rho < 1$ is a constant decided by community vote), the liquidation mechanism will be triggered, and the funds redeemed by the saver will be less than the original deposit.

In the current savings protocol of Pencils Protocol, only pTokens is used as the staking credentials for savers. Similar to

yield stripping, pTokens are 1:1 value-bound to the staking funds. For example, if a user stakes ETH, they can obtain wrapped tokens (pETH) in the Pencils Protocol that are value-bound to ETH. Users can directly use pTokens for additional investment to gain more profits. Currently, the savings in Pencils Protocol are on-demand, meaning that savers can deposit and withdraw assets at any time. To mitigate the impact of market fluctuations causing savers to withdraw funds intensively, we have designed a floating interest rate function:

$$Fr = \epsilon \cdot \phi \cdot \frac{Bf}{Sf} + r_0 \tag{6}$$

where r_0 is the base yield rate, ϕ is an adjustment function related to the user's credit, behavior, and fund amount, ϵ is an interest rate adjustment parameter decided by community vote, which will be adjusted according to the development stage and market conditions of Pencils Protocol. Bf and Sf are the value of funds used for borrowing and the total amount of staking funds, respectively. A higher borrowing activity or intense fund withdrawal by staking users causes the interest rate in the system to rise, which in turn stimulates users to stake for profits.

3.3 Cross-Chain Interoperability

Pencils Protocol leverages Scroll's validity-proof capabilities and scalability, along with various cross-chain bridges, to securely map assets to other Layer1 networks for yield farming. In the future, more complex mechanisms like re-staking and LRT (Liquid Restaking) can be employed to achieve greater returns.

Re-staking allows for the shared staking value to enhance security sharing, which helps further maintain the security of the Ethereum network while providing investors with higher returns. Liquid Restaking can be combined with yield stripping, where depositors receive pTokens and yTokens that can be used for leveraged point farming on Layer 1 or within the ecosystem.

4 Staking and Yield Farming

Yield farming involves depositing tokens into DeFi protocol liquidity pools to earn rewards. The yield from yield farming primarily comprises liquidity providing fees or dividends, interest income from lending, liquidity mining, token rewards, options and derivatives, and insurance pools. Pencils Protocol offers automated yield aggregation services for vault stakers. Pencils Protocol will start with a loan feature.

When users deposit tokens into a Pencils Protocol Vault, their funds enter a pool that borrowers can access to leverage their positions. As a depositor, they'll earn a yield generated from the interest paid by these borrowers. Pencils Protocol Vaults prioritizes the safety of their deposited funds by carefully evaluating each borrower's principal and imposing strict limits on their leverage. This approach ensures that your assets remain secure. The depositors will enjoy a diverse range of rewards. In addition to the yield from dynamic interest rates, depositors also earn Pencils (Pencils Protocol points) and Scroll points, and many other enhanced yields from our partners. These rewards provide additional opportunities for depositors to benefit from their participation in the platform.

Pencils Protocol Farming will initially support five types of assets:

- ETH (Native ETH, WETH, LSDs, LRTs)
- WBTC (EVM-compatible BTC collateral tokens)
- Stablecoins
- Scroll Token (when Scroll launches)
- Pencils Protocol Token

The APR earned by depositors in Pencils Protocol Vaults is determined by a floating interest rate model, similar to those used in mainstream lending protocols. This model adjusts the interest rate based on the availability of funds in the deposit pool, ensuring that depositors are rewarded fairly for their contributions.

When the utilization rate of the deposit pool is high, meaning that a larger portion of the funds is being borrowed, the interest rate (APR) will increase. This higher APR rewards depositors for providing liquidity when it is in high demand and encourages more users to deposit their tokens.

Conversely, when the utilization rate is low, indicating that there is an abundance of available funds in the deposit pool, the interest rate will decrease accordingly. This dynamic adjustment helps maintain a balanced ecosystem and prevents overly high interest rates during periods of low borrowing activity.

By employing this floating interest rate model, Pencils Protocol Vaults ensures that depositors receive competitive returns on their tokens while also promoting a stable and efficient lending environment.

In Pencils Protocol, we currently treat the process of depositing tokens into Vaults as Liquid Staking. Users can earn Pencils points by staking tokens and participating in ecosystem activities. These points will serve as proof of stake within the Pencils ecosystem, and we will introduce the Pencils points system in later chapters. In the future, we plan to expand the Liquid Staking protocol of Pencils Protocol based on the points system, and staking tokens in Vaults will also extend to Restaking to enhance investor returns.

5 Auction Platform

Pencils Protocol offers an Auction Platform to assist users in selling their digital assets while helping investors achieve higher and more stable returns in the secondary market. The Auction Platform supports various auction types, including English auctions, Dutch auctions, fixed-price auctions, batch auctions, Liquidity Bootstrapping Pools (LBP), Gradual Dutch Auctions and so on.

English Auction: This auction type increases the asset price from low to high. The seller sets a starting price and a minimum increment. Investors place bids within a given

time period, and the highest bidder at the end of the auction wins the asset.

Dutch Auction: The seller sets a starting price and a decrement rate, then gradually lowers the token price according to a set rule until all investors accept the price, or the asset is sold out.

Fixed-Price Auction: The seller sets a fixed price for the asset, and tokens are sold to investors at this price until sold out or the deadline is reached.

Batch Auction [9]: This auction type balances prices by allowing investors to submit their desired asset quantities and prices within a time frame. The Pencils Protocol's system contract automatically determines the optimal price and allocates assets to investors who bid at or above this price.

Liquidity Bootstrapping Pools (LBP) [10]: LBP is a variant of the Dutch auction, originating from Balancer's auction model. The seller creates a pool of tokens and stablecoins, setting an initial weight ratio and a change rate. Investors acquire tokens through swaps, and the token's weight in the pool decreases over time, lowering its price. Each token pair in a pool has a spot price defined by their weights and balances:

$$SP_i^o = \frac{\frac{B_i}{W_i}}{\frac{B_o}{W_o}} \tag{7}$$

- B_i is the balance of token i, which is being sold.
- B_o is the balance of token o, which is being bought.
- W_i is the weight of token i.
- W_o is the weight of token o.

Gradual Dutch Auctions (GDA): GDA divides asset sales into a series of Dutch auctions, including discrete GDA (for selling NFTs and other integer-quantity assets) and continuous GDA (for selling fungible tokens).

In a discrete GDA, every auction starts simultaneously, with each successive auction having a higher starting price. The price of each auction is given by a price function, $p_n(t)$, where n is the auction index and t is the time since the auction started.

Various price functions can be used, such as:

$$p_n(t) = k \cdot \alpha^n e^{-\lambda t} \tag{8}$$

Here, the price decays exponentially with a decay constant λ, the starting price increases by a scale factor α, and the initial price of the first auction is k. The total cost for purchasing a set of NFTs M during the time T is:

$$P(T) = \sum_{n}^{M} p_n(T) \tag{9}$$

Continuous GDAs incrementally make more of an asset available for sale at a constant emission rate, r. The price function is independent of the index:

$$p(t) = k \cdot e^{-\lambda t} \tag{10}$$

The cost after T seconds of the auction is:

$$P(T) = \int_{T}^{T+q/r} p(t)\, dt = \frac{k(e^{\lambda q/r} - 1)}{\lambda e^{\lambda T}} \tag{11}$$

In Pencils Protocol's Auction Platform, both assets and sellers participating in auctions must undergo verification, while buyers do not. The AML system of the Auction Platform continuously monitors transactions and triggers alerts if any anomalies are detected.

6 Pencils Protocol Economy

The native cryptographically-secure fungible protocol token of Pencils Protocol (ticker symbol $DAPP) is a transferable representation of attributed utility functions specified in the protocol/code of Pencils Protocol, and which is designed to be used solely as an interoperable utility token thereon.

$DAPP is a functional multi-utility token which will be utilised for governance, Auction Platform collateral, medium of exchange between participants on Pencils Protocol in a decentralised manner, and the economic incentives which will be distributed to encourage users to exert efforts towards contribution and participation in the ecosystem on Pencils Protocol.

The goal of introducing $DAPP is to provide a convenient and secure mode of payment and settlement between participants who interact within the ecosystem on Pencils Protocol without any intermediaries such as centralised third party entity/institution/credit. It is not, and not intended to be, a medium of exchange accepted by the public (or a section of the public) as payment for goods or services or for the discharge of a debt; nor is it designed or intended to be used by any person as payment for any goods or services whatsoever that are not exclusively provided by the issuer. $DAPP does not in any way represent any shareholding, ownership, participation, right, title, or interest in the Company, the Distributor, their respective affiliates, or any other company, enterprise or undertaking, nor will $DAPP entitle token holders to any promise of fees, dividends, revenue, profits or investment returns, and are not intended to constitute securities in the British Virgin Islands, Singapore or any relevant jurisdiction. $DAPP may only be utilised on Pencils Protocol, and ownership of the same carries no rights, express or implied, other than the right to use $DAPP as a means to enable usage of and interaction within Pencils Protocol. The secondary market pricing of $DAPP is not dependent on the effort of the Pencils team, and there is no token functionality or scheme designed to control or manipulate such secondary pricing.

$DAPP creates a mutually beneficial system where every participant is fairly compensated for its efforts. $DAPP is an integral and indispensable part of Pencils Protocol, because

without $DAPP, there would be no incentive for users to expend resources to participate in activities or provide services for the benefit of the ecosystem. Given that additional $DAPP will be awarded to a user based only on its actual usage, activity and efforts made on Pencils Protocol and/or proportionate to the frequency and volume of transactions, users of Pencils Protocol and/or holders of $DAPP which did not actively participate will not receive any $DAPP incentives.

Governance: $DAPP enables holders to actively participate in community voting, influencing decisions on development directions, interest rate impacts, protocol policies, and emergency measures, ensuring a democratic governance structure. The right to vote is restricted solely to voting on features of Pencils Protocol; it does not entitle $DAPP holders to vote on the operation and management of the Company, its affiliates, or their assets or the disposition of such assets to token holders, or select the board of directors or similar bodies of these entities, or determine the development direction of these entities, nor does $DAPP constitute any equity interest in any of these entities or any collective investment scheme; the arrangement is not intended to be any form of joint venture or partnership.

Token Farming: To encourage long-term community engagement, the $DAPP token staking program will launch after TGE. Token holders can stake $DAPP in Pencils Protocol Farms to receive $pDAPP, which may then be further staked or provided as liquidity for DEX for users to participate in the ecosystem. By active participation and engaging with the protocol, users would be able to earn $DAPP rewards from their activities.

Auction Platform Collateral: To list assets on the Auction Platform, sellers are required to stake $DAPP. This staking mechanism serves as a safeguard against malicious activities, with the community overseeing the auction process. In instances of misconduct, the staked $DAPP is redistributed among community members.

Access token: $DAPP functions as an access token, so users staking $DAPP in Vaults will accumulate multiple points from Pencils Protocol and its partners, providing access to various benefits. These privileges include higher leverage multiples and priority access to exclusive, limited strategy products.

Expansion of Financial Services: Pencils Protocol is committed to integrating the$DAPP token into a variety of DeFi products offered on Pencils Protocol or through integrations with various third party protocols. Planned financial solutions include liquidity protocols and lending services, allowing users to optimize their asset allocation by providing liquidity, borrowing, or participating in staking, and earning additional rewards from these activities.

Point System Rights Mapping: Early participants in Pencils Protocol will receive Pencils points, which correspond to rights in $DAPP. In the future, $DAPP will replace some of Pencils' functions. $DAPP holders will also enjoy priority access to new farming methods and preferential policies.

Virtual Shop: In the Virtual Shop, users can leverage $DAPP (the platform currency) for trading margin in NFTs, Real-World Assets (RWAs), points, and derivatives, expanding the utility and application of their holdings within the Pencils Protocol ecosystem.

6.1 Point System

Pencils is the community points system of Pencils Protocol, designed to reward community members who contribute to Pencils Protocol. Community members can earn Pencils points by participating in staking, promoting Pencils Protocol's marketing activities, becoming influencers, ambassadors, volunteers, partners, etc. Pencils points are non-transferable and represent a member's contribution and support for the Pencils Protocol community. As a measure of contribution, Pencils points can be redeemed for exclusive items from the Pencils Protocol store, used to participate in Pencils Protocol launch projects at discounted rates and gain exclusive access, or utilized in Pencils Protocol's vaults to access higher leverage.

6.2 Progressive Ownership

Decentralization is a necessary condition for web3 to achieve security, openness, and community ownership. In more traditional businesses, decentralization helps stakeholders participate and make more informed decisions. However, achieving full decentralization from the start can be challenging, or even impractical. The trade-offs of decentralization include inefficiency, difficulty in regulation, and reduced cost of malicious behavior. Almost all web3 costs have some degree of centralization, which is reasonable. This is where Progressive Decentralization comes in, breaking down product business into independent "Minimum Decentralized Units" (MDUs) and decentralizing each dimension separately. Progressive Ownership builds upon progressive decentralization. This approach uses economic incentives to gradually increase user loyalty and retention, ultimately achieving ownership. In this model, users are incentivized through revenue sharing (e.g., ETH or stablecoins) but can choose to convert personal income into tokens representing a share of community income. The functionality of the $DAPP token is a form of Progressive Ownership distribution, where community members, promoters, ecosystem developers, and high-quality users all have the opportunity to participate in the system's revenue sharing.

6.3 Profit

Pencils Protocol's main business includes asset management, vault lending, Pencils Shop, digital asset auctions, and more. Pencils Protocol will extract management fees from each of these businesses, including management fees and commissions for asset management, lending fees, and management fees and commissions from the digital asset auction process. We will sell exclusive products or items in collaboration with partners in the Pencils Shop and may also offer additional services on the platform. Pencils Protocol will develop a plug-and-play Permissioned DeFi system based on Scroll and anti-money laundering strategies based on GCN. In the future, this system will be leased out in the form of an SDK.

7 Compliance, Privacy and Security

7.1 Permissioned DeFi

Permissioned DeFi is an emerging DeFi model that offers a new approach to DeFi, meeting compliance framework requirements while preserving the core principles of DeFi. As governments around the world strengthen their responsibilities to prevent money laundering and terrorist financing through new financial tools on the blockchain, DeFi will face regulatory scrutiny. The decentralized architecture of DeFi makes government regulation extremely challenging, at least in the way it regulates traditional finance (TradFi). The way PDeFi operates is by integrating regulatory compliance controls at critical points within the blockchain framework to achieve compliance while not eliminating the permissionless nature of the underlying decentralized processes.

Pencils Protocol constructs Permissioned DeFi through mechanisms such as identity verification services (Proof Of Humanity), KYC/AML, in-transaction permission controls, zero-knowledge proofs, and more. Pencils Protocol implements strict screening policies at every funding entry and exit point of DeFi transactions, ensuring regulatory compliance while maintaining transaction efficiency. Pencils Protocol integrates "deposit administrators" and "screeners" to detect and prevent illegal fund transfers. As long as users complete identity verification and do not engage in misconduct, their privacy during transactions will be safeguarded. Scroll's ZK infrastructure will generate validity proofs for transactions. If funds are attacked or money laundering is detected during transactions, we will challenge and roll back the transactions to ensure the security of the funds.

7.2 Proof Of Humanity and ZkPrivacy

Scroll, as a ZK Layer2 solution, can provide security verification and validity proofs for all transactions occurring on it. Pencils Protocol utilizes W3C's Verifiable Credentials Data Model [11], zero-knowledge proofs, and potentially third-party KYC or biometric verification institutions to implement the Proof Of Humanity functionality.

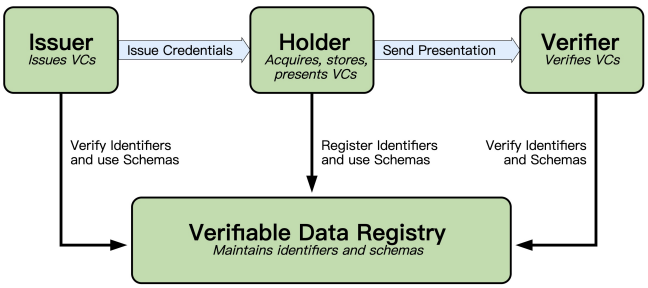

Fig. 5: The roles and information flow for verifiable credentials

During the user registration process, we issue verifiable credentials to users based on the identity verification information they submit, either through designated KYC institutions or smart contracts. This identity verification process involves using KYC or other biometric verification agencies. Once users receive their credentials, they automatically send the proof and information to the verifier. Simultaneously, validity proofs are generated on Scroll to re-authenticate the user's identity and ensure the legality and validity of the transaction process.

The information from the user registration is encrypted and stored in the distributed, verifiable data registry of Pencils Protocol. The user registration data is managed through multi-signature by the user, registration institutions, Pencils Protocol, and other organizations. Typically, without the user's signed consent, registration information cannot be accessed by anyone. If a user engages in malicious activity, other parties, excluding the user, will complete the multi-signature process and cooperate with regulatory agencies to extract the user's information. Scroll's ZK feature gives Pencils Protocol protection against witch attacks and sandwich attacks.

7.3 Anti-Money Laundering Strategies

Pencils Protocol aims to effectively prevent money laundering activities and ensure platform compliance by combining user identity verification, transaction monitoring, smart contract auditing, compliance collaboration, data security, multi-signatures, and decentralized governance. Within the Proof of Humanity (POH) implementation, user identity verification and multi-signatures are achieved, while smart contract auditing and compliance collaboration are completed during the product development process. Data security is ensured through access control and zero-knowledge proofs.

Next, we discuss how to mitigate money laundering, attacks, and other criminal activities within the system through transaction monitoring. Graph networks are widely used as an important framework to analyze the relationships between transactions in the Bitcoin blockchain and capture illegal activities [12]. Graph Convolutional Networks (GCNs) are a type of convolutional neural network that operates directly on graphs and utilizes structural information. Node features are convolved with a kernel to induce new node features, which are considered as real-valued embeddings. GCN aims to filter graph signals using trainable kernels, with local kernels approximated using Chebyshev polynomials. We can use GCN as an efficient node classification algorithm to monitor and classify node behaviors in Pencils Protocol, filtering out nodes potentially involved in attacks or money laundering.

Considering the transaction network graph $G = (V, E)$ in Pencils Protocol, where V and E represent the set of nodes (participants in Pencils Protocol) and edges (payment flows) respectively, $|V| = n$ represents the number of transactions. A is the adjacency matrix of the transaction graph, and $H^{(l)}$ is the node embedding matrix at layer l. $W^{(l)}$ is the trainable weight matrix used to update the embedding matrix to the output $H^{(l+1)}$. The multi-layer GCN can be described by the following layer-wise propagation rule:

$$H^{(l+1)} = \sigma(\hat{A}H^{(l)}W^{(l)}), \tag{12}$$

where $\hat{A}$ is the normalization of A, defined as:

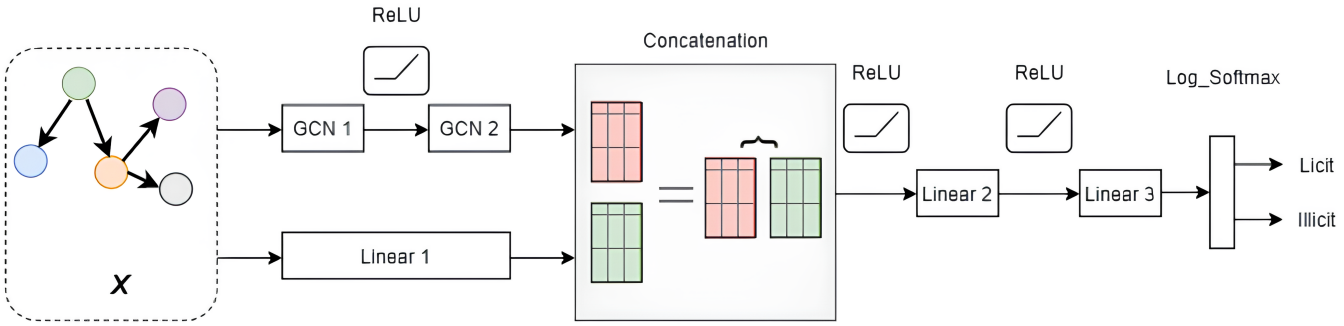

Fig. 6: nti-Money Laundering Strategy Architecture Based on GCN

$$\begin{cases} \hat{A} = \tilde{D}^{-1/2}\tilde{A}\tilde{D}^{-1/2} \\ \tilde{A} = A + I \\ \tilde{D} = \text{diag}(\sum_j \tilde{A}_{ij}) \end{cases} \tag{13}$$

Here, $\hat{A}$ is the adjacency matrix of the graph G with self-loops added. σ denotes the activation function, such as $\text{ReLU}(x) = \max(0, x)$. $H^{(0)}$ is the activation matrix, referred to as the node embedding matrix. The initial embedding matrix is derived from node features and is represented as $\chi = H^{(0)}$.

For 2-hop neighborhood feature aggregation, a 2-layer GCN is used, typically represented as:

$$H^{(2)} = \text{softmax}(\hat{A} \cdot \text{ReLU}(\hat{A} \cdot \chi \cdot W^{(0)})W^{(1)}), \tag{14}$$

where $W^{(0)}$ and $W^{(1)}$ contain trainable weights learned through gradient descent. The softmax function is defined as:

$$\text{softmax}(x) = \frac{\exp(x_i)}{\sum_j \exp(x_j)}, \tag{15}$$

where $x = \sum_i x_i$.

The model includes a 2layer GCN. The first model is based on a spectral method, and the second model is based on a Euclidean domain linear transformation feature matrix method [13]. The output of the last layer is concatenated with the output of a linear layer that takes the original node features as input. The overall output is then compressed by the ReLU activation function and passed to two consecutive linear layers. Subsequently, the second linear layer is compressed by the ReLU function, and the final layer is stepped through the log_softmax function, outputting the logarithms of the predicted probabilities for different categories. χ is the node feature matrix derived from the graph network of Pencils Protocol, and the output is a prediction of legal/illegal transactions. The input to the GCN is provided by the transaction graph of Pencils Network, with the node feature matrix χ, while the input to the linear layers is provided solely by χ.

8 Future

In addition to basic asset management, Pencils Protocol will explore extended protocols including NFTFi, decentralized insurance, and ERC404.

NFTFi: Pencils Protocol's current farming setup is based on fungible tokens (FTs). In the future, the protocol will support lending, virtual automated market makers (vAMMs), and other derivative trading of NFT assets.

Decentralized Insurance: To mitigate the inevitable risks brought about by market volatility, stakers might incur losses when using pTokens for trading, and vault users could face losses after setting up leveraged returns. Pencils Protocol will consider using the Takaful insurance model to design decentralized insurance services for users. $DAPP holders can participate in mutual insurance within the system and share insurance proceeds. Takaful [14] is a form of decentralized insurance that describes a risk-sharing mechanism where participants mutually trade risks among themselves, rather than primarily transferring risks to an insurance company as in traditional centralized insurance.

ERC404: ERC404 is defined as Fractionally Represented Non-Fungible Tokens, allowing fractional management and ownership of NFTs within a single contract. This approach enables ERC-721 NFTs to coexist seamlessly with ERC-20 tokens, thereby enhancing liquidity and accessibility without the need to split the NFT itself or require explicit conversion steps. The standard includes mechanisms for partial and complete token transfers, approvals, and event emissions. ERC404's optimization of NFT liquidity and scalability can be applied to numerous real-world scenarios, including the reuse of rights in DeSci articles, patents, and copyrights. Using ERC-404, each element within an article (graphics, theories, algorithms) can have its copyright license represented as part of the entire article's copyright license, enabling readers to efficiently obtain licenses and allowing everyone to bypass publishers to share results and earn revenue. In the combination of RWA (Real World Assets) and DeFi, ERC404 can fractionalize ownership of high-value assets, lowering the barrier for retail participation. Additionally, these assets can be turned into collateral for lending and liquidity mining through ERC404, allowing participants to earn higher returns from real-world assets in DeFi. Furthermore, in the intersection of blockchain and AI, ERC404 can play a significant role in data monetization,

model ownership, and revenue distribution. Inscriptions have a similar data structure to ERC404. We can use Scroll's validity proof and cross-chain bridges to map inscriptions to ERC404 in Pencils Protocol for DeFi trading. We can design a unified ERC404 DEX within Pencils Protocol, leveraging AMM to incorporate the rarity settings of the NFT portion of ERC404 and develop an automated farming system.

9 Conclusion

Pencils Protocol is a complete, secure, and pluggable regulatory DeFi aggregation platform.

Pencils Protocol is a robust, secure DeFi aggregation platform offering pluggable regulatory features. As the native gateway for Scroll, it provides services such as yields, auctions, and multilayer rewards.

Users can stake assets to earn stable returns or initiate vaults to gain leveraged returns. Pencils Protocol has designed various methods to increase capital utilization effectively, enhancing user returns, while users can obtain multilayer rewards based on cross-chain interoperability. The Auctions Platform supports various common and innovative auction types to meet diverse user needs, with auction sellers and the auction process being subject to regulation and user oversight.

Pencils Protocol offers pluggable permissioned DeFi services, primarily using identity verification services (Proof of Humanity), KYC/AML, permission control within transactions, zero-knowledge proofs, and other mechanisms. Additionally, we use GCN (Graph Convolutional Network) to construct AML strategies within the system to prevent potential criminal activities.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] M. Harlev, H. Yin, K. Langenheldt, R. R. Mukkamala, and R. Vatrapu, "Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning," 01 2018.

[3] P. Monamo, V. Marivate, and B. Twala, "Unsupervised learning for robust bitcoin fraud detection," in *2016 Information Security for South Africa (ISSA)*, 2016, pp. 129–134.

[4] K. Gogol, C. Killer, M. Schlosser, T. Bocek, B. Stiller, and C. Tessone, "Sok: Decentralized finance (defi) – fundamentals, taxonomy and risks," 2024. [Online]. Available: https://arxiv.org/abs/2404.11281

[5] H. Adams, N. Zinsmeister, M. Salem, R. Keefer, and D. Robinson, "Uniswap v3 core," *Tech. rep., Uniswap, Tech. Rep.*, 2021.

[6] S. F. Singh, P. Michalopoulos, and A. Veneris, "Deeper: Enhancing liquidity in concentrated liquidity amm dex via sharing," in *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2023, pp. 1–7.

[7] A. Adams, X. Wan, and N. Zinsmeister, "Uniswap v3 twap oracles in proof of stake," SSRN, October 2022, available at SSRN: https://ssrn.com/abstract=4384409 or http://dx.doi.org/10.2139/ssrn.4384409.

[8] S. Singh, P. Michalopoulos, and A. Veneris, "Deeper: a shared liquidity dex design for low trading volume tokens to enhance average liquidity," 09 2023.

[9] Gnosis Auction, "Gnosis auction," https://gnosis-auction.eth.limo/#/docs#topAnchor, 2020, gnosis Auction enables Batch auctions for everyone.

[10] Balancer, "Liquidity bootstrapping pools (lbps)," Balancer Documentation, 2021. [Online]. Available: https://docs.balancer.fi/concepts/pools/liquidity-bootstrapping.html

[11] World Wide Web Consortium (W3C), "Verifiable credentials data model v1.1," https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations, Mar. 2022, w3C Recommendation.

[12] S. Bistarelli and F. Santini, "Go with the -bitcoin- flow, with visual analytics," *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017. [Online]. Available: https://api.semanticscholar.org/CorpusID:36055862

[13] I. Alarab, S. Prakoonwit, and M. I. Nacer, "Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain," *Proceedings of the 2020 5th International Conference on Machine Learning Technologies*, 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:220846564

[14] R. Feng, M. Liu, and N. Zhang, "A unified theory of decentralized insurance," *SSRN Electronic Journal*, 01 2022.

APPENDIX: LEGAL DISCLAIMER

PLEASE READ THE ENTIRETY OF THIS "LEGAL DISCLAIMER" SECTION CAREFULLY. NOTHING HEREIN CONSTITUTES LEGAL, FINANCIAL, BUSINESS OR TAX ADVICE AND YOU ARE STRONGLY ADVISED TO CONSULT YOUR OWN LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S) BEFORE ENGAGING IN ANY ACTIVITY IN CONNECTION HEREWITH. NEITHER PENCILS PROTOCOL LTD (THE COMPANY), ANY OF THE PROJECT CONTRIBUTORS (THE PENCILS TEAM) WHO HAVE WORKED ON PENCILS PROTOCOL (AS DEFINED HEREIN) OR PROJECT TO DEVELOP PENCILS PROTOCOL IN ANY WAY WHATSOEVER, ANY DISTRIBUTOR AND/OR VENDOR OF $DAPP TOKENS (OR SUCH OTHER RE-NAMED OR SUCCESSOR TICKER CODE OR NAME OF SUCH TOKENS) (THE DISTRIBUTOR), NOR ANY SERVICE PROVIDER SHALL BE LIABLE FOR ANY KIND OF DIRECT OR INDIRECT DAMAGE OR LOSS WHATSOEVER WHICH YOU MAY SUFFER IN CONNECTION WITH ACCESSING THE PAPER, DECK OR MATERIAL RELATING TO $DAPP (THE TOKEN DOCUMENTATION) AVAILABLE ON THE WEBSITE AT HTTPS://PENCILSPROTOCOL.IO/ (THE WEBSITE, INCLUDING ANY SUB-DOMAINS THEREON) OR ANY OTHER WEBSITES OR MATERIALS PUBLISHED OR COMMUNICATED BY THE COMPANY OR ITS REPRESENTATIVES FROM TIME TO TIME.

Project purpose: You agree that you are acquiring $DAPP to participate in Pencils Protocol and to obtain services on the ecosystem thereon. The Company, the Distributor and their respective affiliates would develop and contribute to the underlying source code for Pencils Protocol. The Company is acting solely as an arms' length third party in relation to the $DAPP distribution, and not in the capacity as a financial advisor or fiduciary of any person with regard to the distribution of$DAPP.

Nature of the Token Documentation: The Token Documentation is a conceptual paper that articulates some of the main design principles and ideas for the creation of a digital token to be known as$DAPP. The Token Documentation and the Website are intended for general informational purposes only and do not constitute a prospectus, an offer document, an offer of securities, a solicitation for investment, any offer to sell any product, item, or asset (whether digital or otherwise), or any offer to engage in business with any external individual or entity provided in said documentation. The information herein may not be exhaustive and does not imply any element of, or solicit in any way, a legally-binding or contractual relationship. There is no assurance as to the accuracy or completeness of such information and no representation, warranty or undertaking is or purported to be provided as to the accuracy or completeness of such information. Where the Token Documentation or the Website includes information that has been obtained from third party sources, the Company, the Distributor, their respective affiliates and/or the Pencils team have not independently verified the accuracy or completeness of such information. Further, you acknowledge that the project development roadmap, protocol functionality are subject to change and that the Token Documentation or the Website may become outdated as a result; and neither the Company nor the Distributor is under any obligation to update or correct this document in connection therewith.

Validity of Token Documentation and Website: Nothing in the Token Documentation or the Website constitutes any offer by the Company, the Distributor, or the Pencils team to sell any$DAPP (as defined herein) nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or investment decision. Nothing contained in the Token Documentation or the Website is or may be relied upon as a promise, representation or undertaking as to the future performance of Pencils Protocol. The agreement between the Distributor (or any third party) and you, in relation to any distribution or transfer of $DAPP, is to be governed only by the separate terms and conditions of such agreement.

The information set out in the Token Documentation and the Website is for community discussion only and is not legally binding. No person is bound to enter into any contract or binding legal commitment in relation to the acquisition of $DAPP, and no digital asset or other form of payment is to be accepted on the basis of the Token Documentation or the Website. The agreement for distribution of$DAPP and/or continued holding of$DAPP shall be governed by a separate set of Terms and Conditions or Token Distribution Agreement (as the case may be) setting out the terms of such distribution and/or continued holding of$DAPP (the Terms and Conditions), which shall be separately provided to you or made available on the Website. The Terms and Conditions must be read together with the Token Documentation. In the event of any inconsistencies between the Terms and Conditions and the Token Documentation or the Website, the Terms and Conditions shall prevail.

Deemed Representations and Warranties: By accessing the Token Documentation or the Website (or any part thereof), you shall be deemed to represent and warrant to the Company, the Distributor, their respective affiliates, and the Pencils team as follows:

(a) in any decision to acquire any $DAPP, you have not relied and shall not rely on any statement set out in the Token Documentation or the Website;

(b) you shall at your own expense ensure compliance with all laws, regulatory requirements and restrictions applicable to you (as the case may be);

(c) you acknowledge, understand and agree that $DAPP may have no value, there is no guarantee or representation of value or liquidity for $DAPP, and $DAPP is not an investment product nor is it intended for any speculative investment whatsoever;

(d) none of the Company, the Distributor, their respective affiliates, and/or the Pencils team shall be responsible for or liable for the value of $DAPP, the transferability and/or liquidity of $DAPP and/or the availability of any market for $DAPP through third parties or otherwise; and

(e) you acknowledge, understand and agree that you are not eligible to participate in the distribution of $DAPP if you are a citizen, national, resident (tax or otherwise), domiciliary, and/or green card or permanent visa holder of a geographic area or country: (i) where it is likely that the distribution of $DAPP would be construed as the sale of a security (howsoever named), financial service or investment product; and/or (ii) where participation in token distributions is prohibited by applicable law, decree, regulation, treaty, or administrative act (including without limitation the United States of America, Canada, and the People's Republic of China); and to this effect you agree to provide all such identity verification documents when requested in order for the relevant checks to be carried out.

The Company, the Distributor and the Pencils team do not and do not purport to make, and hereby disclaims, all representations, warranties or undertaking to any entity or person (including without limitation warranties as to the accuracy, completeness, timeliness, or reliability of the contents of the Token Documentation or the Website, or any other materials published by the Company or the Distributor). To the maximum extent permitted by law, the Company, the Distributor, their respective affiliates and service providers shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including, without limitation, any liability arising from default or negligence on the part of any of them, or any loss of revenue, income or profits, and loss of use or data) arising from the use of the Token Documentation or the Website, or any other materials published, or its contents (including without limitation any errors or omissions) or otherwise arising in connection with the same. Prospective acquirors of $DAPP should carefully consider and evaluate all risks and uncertainties (including financial and legal risks and uncertainties) associated with the distribution of $DAPP, the Company, the Distributor and the Pencils team.

$DAPP Token: $DAPP are designed to be utilised, and that is the goal of the $DAPP distribution. In particular, it is highlighted that $DAPP:

(a) does not have any tangible or physical manifestation, and does not have any intrinsic value/pricing (nor does any person make any representation or give any commitment as to its value);

(b) is non-refundable, not redeemable for any assets of any entity or organisation, and cannot be exchanged for cash (or its equivalent value in any other digital asset) or any payment obligation by the Company, the Distributor or any of their respective affiliates;

(c) does not represent or confer on the token holder any right of any form with respect to the Company, the Distributor (or any of their respective affiliates), or their revenues or assets, including without limitation any right to receive future dividends, revenue, shares, ownership right or stake, share or security, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property or licence rights), right to receive accounts, financial statements or other financial data, the right to requisition or participate in shareholder meetings, the right to nominate a director, or other financial or legal rights or equivalent rights, or intellectual property rights or any other form of participation in or relating to Pencils Protocol, the Company, the Distributor and/or their service providers;

(d) is not intended to represent any rights under a contract for differences or under any other contract the purpose or intended purpose of which is to secure a profit or avoid a loss;

(e) is not intended to be a representation of money (including electronic money), payment instrument, security, commodity, bond, debt instrument, unit in a collective investment or managed investment scheme or any other kind of financial instrument or investment;

(f) is not a loan to the Company, the Distributor or any of their respective affiliates, is not intended to represent a debt owed by the Company, the Distributor or any of their respective affiliates, and there is no expectation of profit nor interest payment; and

(g) does not provide the token holder with any ownership or other interest in the Company, the Distributor or any of their respective affiliates.

Notwithstanding the $DAPP distribution, users have no economic or legal right over or beneficial interest in the assets of the Company, the Distributor, or any of their affiliates after the token distribution. For the avoidance of doubt, neither the Company nor the Distributor deals in, or is in the business of buying or selling any virtual asset or digital payment

token (including $DAPP). Any sale or distribution of tokens would be performed during a restricted initial period solely for the purpose of obtaining project development funds, raising market/brand awareness, as well as community building and social engagement; this is not conducted with any element of repetitiveness or regularity which would constitute a business.

To the extent a secondary market or exchange for trading $DAPP does develop, it would be run and operated wholly independently of the Company, the Distributor, the distribution of $DAPP and Pencils Protocol. Neither the Company nor the Distributor will create such secondary markets nor will either entity act as an exchange for $DAPP.

Informational purposes only: The information set out herein is only conceptual, and describes the future development goals for Pencils Protocol to be developed. In particular, the project roadmap in the Token Documentation is being shared in order to outline some of the plans of the Pencils team, and is provided solely for INFORMATIONAL PURPOSES and does not constitute any binding commitment. Please do not rely on this information in deciding whether to participate in the token distribution because ultimately, the development, release, and timing of any products, features or functionality remains at the sole discretion of the Company, the Distributor or their respective affiliates, and is subject to change. Further, the Token Documentation or the Website may be amended or replaced from time to time. There are no obligations to update the Token Documentation or the Website, or to provide recipients with access to any information beyond what is provided herein.

Regulatory approval: No regulatory authority has examined or approved, whether formally or informally, any of the information set out in the Token Documentation or the Website. No such action or assurance has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of the Token Documentation or the Website does not imply that the applicable laws, regulatory requirements or rules have been complied with.

Cautionary Note on forward-looking statements: All statements contained herein, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Company, the Distributor and/or the Pencils team, may constitute forward-looking statements (including statements regarding the intent, belief or current expectations with respect to market conditions, business strategy and plans, financial condition, specific provisions and risk management practices). You are cautioned not to place undue reliance on these forward-looking statements given that these statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results to be materially different from that described by such forward-looking statements, and no independent third party has reviewed the reasonableness of any such statements or assumptions. These forward-looking statements are applicable only as of the date indicated in the Token Documentation, and the Company, the Distributor as well as the Pencils team expressly disclaim any responsibility (whether express or implied) to release any revisions to these forward-looking statements to reflect events after such date.

References to companies and platforms: The use of any company and/or platform names or trademarks herein (save for those which relate to the Company, the Distributor or their respective affiliates) does not imply any affiliation with, or endorsement by, any third party. References in the Token Documentation or the Website to specific companies and platforms are for illustrative purposes only.

English language: The Token Documentation and the Website may be translated into a language other than English for reference purpose only and in the event of conflict or ambiguity between the English language version and translated versions of the Token Documentation or the Website, the English language versions shall prevail. You acknowledge that you have read and understood the English language version of the Token Documentation and the Website.

No Distribution: No part of the Token Documentation or the Website is to be copied, reproduced, distributed or disseminated in any way without the prior written consent of the Company or the Distributor. By attending any presentation on this Token Documentation or by accepting any hard or soft copy of the Token Documentation, you agree to be bound by the foregoing limitations.


Pencils Protocol